# Genian Documentation

GENIANS, INC.

Jan 16, 2026

# DEPLOYMENT GUIDE

DOWNLOAD PDF

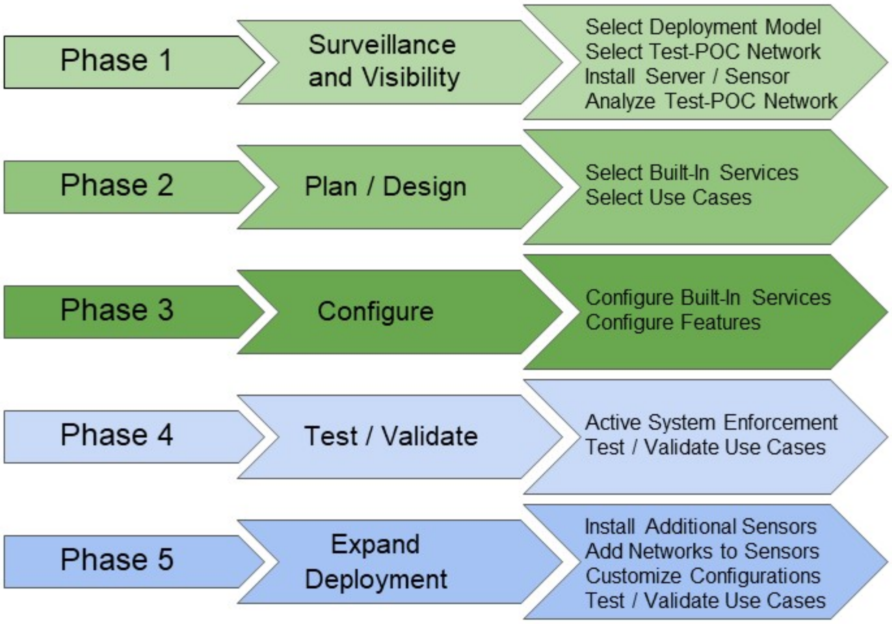
CHAPTER

ONE

# DEPLOYMENT OVERVIEW

There are 5 recommended phases for Zero Trust Network Access (ZTNA) deployment.

- **Phase 1** - Network Surveillance / Visibility
- **Phase 2** - Plan / Design
- **Phase 3** - Configure
- **Phase 4** - Test / Validate
- **Phase 5** - Expand Deployment



Following the steps documented in the various phases will allow Administrators with any level of experience with ZTNA to successfully deploy the Genian ZTNA Solution. While not every specific use case or edge condition is addressed, the steps outlined in each phase cover the most common deployment scenarios and use cases for ZTNA.

CHAPTER

TWO

# PHASE 1 - NETWORK SURVEILLANCE / VISIBILITY

Gaining visibility into the network will allow Administrators to understand what nodes are active on the network by various information including IP, MAC, Platform Type, Location, Ownership and Status. This information will be used during Phase 2 when designing Grouping and Enforcement Policies.

## 2.1 Step 1 - Select Deployment Model

The first step when deploying the system is to choose a deployment model. Initially, the following decisions need to be made:

- Will the Policy Server be On-Prem or Cloud?
- Will the Policy Server and Sensor be Physical or Virtual?

The information below provides details that will assist Administrators in choosing the Deployment Model that is best for their environment:

- *Understanding Components*
- *Deployment Considerations*

## 2.2 Step 2 - Select Test/POC Network

It is a recommended Best Practice to select a test/POC network when initially deploying the system. Typically, the test network is easily accessible to IT staff and includes one or more IT staff member. Information that will be needed when identifying the test network include, VLAN ID, subnet/mask, and gateway. This information will be required when configuring the system to monitor the test/POC network.

**Example:** VLAN 10, 192.168.10.0/24 , 192.168.1.1(gateway)

## 2.3 Step 3 - Install Policy Server / Sensor

Instructions for installing the Policy Server / Sensor are listed below which include steps on downloading the ISO image and installing the image in a virtual environment or on hardware.

- *Installing Ubuntu OS*
- *Installing Policy Server*
- *Installing Network Sensor*
- *Installing ZTNA Gateway*

## 2.4 Step 4 - Deploy Sensor on Test/POC Network in Monitoring Mode

Once the Policy Server / Sensor have been installed, follow the steps below to add the test/POC network to the Sensor for Visibility. The Sensor will start to collect information for all nodes in the designated network in the form of Device Platform Intelligence.

- *Administration Console*
- *Adding and Deleting Network Sensors*
- *Genian Device Platform Intelligence (GDPI)*

The information gathered in this Phase will be used in Phase 2 when planning and designing how the system will be implemented.

CHAPTER

THREE

# PHASE 2 - PLAN / DESIGN

After Visibility has been enabled and Device Platform Intelligence has been analyzed for the test/POC network, the next step is to decide what features of the system will be enabled and what use cases are relevant for the deployment. There are no configuration tasks in this Phase, just decisions that will determine which steps will be executed in the following Phase when configuring the system.

## 3.1 Step 1 - Select from Optional Built-In Services

**Note:** None of these services are required for Visibility or Enforcement and are all optional.

Genian ZTNA has several built-in services which are available by default. These services include a DHCP Server, RADIUS Server, Switch Management via SNMP and Syslog Server. Part of the Planning and Design Phase is to determine if any of these services will be utilized.

- DHCP Server? - Y/N
- RADIUS Server? - Y/N
- Switch Management? - Y/N
- Syslog Server? - Y/N

## 3.2 Step 2 - Select Applicable Use Cases

- Block all unknown devices? - Y/N
- Captive Portal for browser capable devices? - Y/N
- Guest registration? - Y/N
  - Internet only access for Guests? - Y/N
  - Role Based Access (RBAC) for Guests? - Y/N
- Categorize networking devices? - Y/N
- Add tag (Trusted for example) to networking devices? - Y/N
- Authenticate Managed Devices? - Y/N
- AD/Domain SSO? - Y/N
- RADIUS SSO? - Y/N

- Role Based Access (RBAC) for Managed Devices? - Y/N
- Authenticate BYOD Devices?
- Internet only access for BYOD? - Y/N
- Role Based Access (RBAC) for BYOD? - Y/N
- Agent Enforcement for Managed Devices? - Y/N
- Agent Enforcement for BYOD? - Y/N
- Agent Enforcement for Guests? - Y/N
- IoT Use Cases? - Y/N
- Add tags to IoT devices? - Y/N
- Specific/restricted access for IoT devices? - Y/N
- Other tag use cases? - Y/N
- Other/Specific Use Cases? - Y/N
- Regulatory Compliance
- Business Specific, Other, etc.
- Network Security Automation? - Y/N
- Publish to External System? - Y/N
- Receive Alerts from External System? - Y/N

CHAPTER

FOUR

# PHASE 3 - CONFIGURE

## 4.1 Step 1 - Configuration Optional Built-In Services

If selected in Phase 2, configure the desired built-in service. As a reminder, these are optional and not required for Visibility or Enforcement.

- *Configuring DHCP Server*
- *Configuring RADIUS Enforcement*
- *Monitoring Switch*
- *Receiving Events*

## 4.2 Step 2 - Configure Features for Grouping, Enforcement and Reporting

If selected in Phase 2, configure the desired features to meet the specific use cases of the deployment. Any feature not selected in Phase 2 may be skipped.

Once all of the desired configurations are completed, they will be used in Phase 4 to Test and Validate use cases.

### 4.2.1 Create Node Groups to categorize Devices/Users

- *Managing Node Groups*

### 4.2.2 Create Tags

- *Tagging Nodes*

### 4.2.3 Create Network Objects/Services/Permissions

- *Creating Permissions*

### 4.2.4 Create Enforcement Policies

- *Creating and Viewing Enforcement Policy for Nodes*

### 4.2.5 Configure AD Integration

- *Integrating User Directories*

### 4.2.6 Configure Single-Sign-On (SSO)

- *Single Sign-On*

### 4.2.7 Configure Captive Portal

- *Authentication using Captive Web Portal*

### 4.2.8 Configure Network Security Automation

- *Sending Events*
- *Integrating Palo Alto Networks Firewall*
- *Integrating FireEye*

### 4.2.9 Configure Alerting / Reporting

- *Managing Reports*

CHAPTER

FIVE

# PHASE 4 - TEST / VALIDATE

## 5.1 Step 1 - Switch Sensor on Test/POC Network to Enforcement Mode

Sensors are deployed in Monitoring mode by default. This means all nodes are allowed on the network and even enabled Enforcement Policies will not be executed. In order to test any use cases which involvement Enforcement, the Sensor will need to be set to Enforcement Mode. The instructions below outline the steps required to activate a Sensor.

An additional consideration is whether or not to Allow or Block new nodes joining the network after the Sensor has been activated. This will essentially enable a Zero Trust model where any node not explicitly permitted by any of the previously configured policies will be blocked until an Administrator specifically grants the node access. When following the steps below, to enable this option, set the New Node Policy under IPAM to “Deny MAC”. If this option is not enabled, the default mode is “Allow” and nodes not machining any particular policy will be granted network access.

*Configuring ARP Enforcement*

## 5.2 Step 2 - Test / Validate Use Cases

With the Sensor now activated, all applicable use cases can be tested and validated. Any use cases not selected in Phase 2 can be skipped.

- Verify Unknown devices are blocked
- Verify Captive Portal
- Verify Guest Registration
- Verify tags for network devices
- Verify Managed Device Authentication
- AD/Domain SSO
- RADIUS SSO
- Captive Portal (non-domain environments)
- Verify Role Based Access (RBAC)
- For Managed Devices
- For BYOD
- For Guests
- Verify Agent Enforcement Actions

- For Managed Devices
- For BYOD
- For Guests
- Verify IoT Use Cases
- Verify tags/access as applicable
- Verify other tag Use Cases
- Verify tags/access as applicable
- Verify other specific Use Cases
- Verify Network Security Automation
- Verify Publish to External System
- Verify Receiving from External System
- Verify Alerting and Reporting

CHAPTER

SIX

# PHASE 5 - EXPAND DEPLOYMENT

## 6.1 Step 1 - Install Additional Sensors / Networks

Follow the steps outlined in Phase 1, Steps 3 and 4 to install additional Sensors or add more networks to an existing Sensor.

## 6.2 Step 2 - Modify / Customize Configurations

If applicable, modify or customize configurations fro the newly added networks, or Sensors. Skip this step if not applicable.

## 6.3 Step 3 - Test / Validate Use Cases

Follow the steps outlined in Phase 4 as a Best Practice when deploying new Sensors or managing new networks to ensure that everything is operating properly based on the configurations. Repeat as necessary.

CHAPTER

SEVEN

# UNDERSTANDING NETWORK ACCESS CONTROL

## 7.1 What is ZTNA?

Zero Trust Network Access (ZTNA) starts by checking whether a device is permitted to connect to a network. Based on this, a device may be allowed or denied access. Such access control is typically provided through a technology known as 802.1X, which provides three important functions called Authentication, Authorization, and Accounting (AAA).

**Authentication**

Authentication is the process of verifying the identity of a user or device connecting to the network. This is usually done through the end user entering a username/password. In some cases the MAC address and digital certificates may be used for authentication.

**Authorization**

Authorization is the process of determining what network resources an authenticated device can access. Depending on the type of authenticated device or group of identified users, network, service and time zone may be restricted.

**Accounting**

Accounting is a process that allows a device to keep records of network access and use it for future billing or security purposes. This allows you to see who technology of network access control. Recently, due to security vulnerabilities of network endpoints, it has become desireable to determine eligibility for used what device, when, where, and how. AAA has long been used as a basic network access by security compliance status of the endpoints. ZTNA solutions function to allow administrators to set security compliance criteria other than usernames and passwords, and to control access based on these varied criteria.

These different aspects of ZTNA can be divided conceptually into functions that occur before the point of network connection, and after network connection.

**Pre-Connect**

Pre-Connect refers to operations performed before the endpoint is connected to the network and normal communication is established. When an endpoint attempts to connect to a network, the endpoint is identified and authenticated using identity information such as a username / password / certificate / MAC address provided by that endpoint. If this process does not confirm that the device is authorized, the network connection will be denied. This process can be provided via 802.1X through a device such as a switch or a wireless LAN access point, or through ARP control.

**Post-Connect**

If the endpoint meets the requirements of the Pre-Connect phase, it will be given access to the network with a certain level of authorization. At the time of connection, the ZTNA begins continuously monitoring the endpoint for compliance to policies set by the administrator. If and when the policy is violated, the network privileges of the endpoint may be reduced or revoked to isolate the endpoint. An agent can be used to monitor the state of the endpoint. The agent monitors the status of the endpoints hardware and software for compliance. Upon change, the ZTNA policy server is notified and network access can be controlled if a violation has occurred.

## 7.2 The Evolution of ZTNA:

**First Generation**

The earliest generation of ZTNA is user and device authentication based on 802.1X protocols. If a device tried to connect to switch ports or wireless access points, it was required to provide a username/password or certificate, to be approved by a RADIUS server. This approach allowed or denied access at the level of the switch port or the wireless access point. This method, while effective can be difficult to implement and is not compatible with all devices.

**Second Generation**

The second generation of ZTNA expanded to information gathering capability through SNMP with network devices or using independent network sensor devices. This generation also introduced access control methods in addition to 802.1X, such as VLAN quarantining, ARP based control, and port mirroring. This era also coincided with an increasing shift to wireless networking. To manage the emerging vulnerabilities of WLANs like rogue access points, solutions like network sensors, wireless controllers and endpoint agents were increasingly utilized for visibility and control.

**Third Generation**

The third generation of ZTNA expanded into automation. Agents became able to automatically configure endpoint devices to comply with security policy, and enabled the creation of a cooperative security model through integration with various systems. For example, a security system operating in the perimeter of the network such as an IDS or firewall may be able to identify threats, but at best, it can only block traffic that flows through it. Integrating with a ZTNA provides the ability to quarantine malicious devices from the rest of the LAN. A ZTNA can also share detailed endpoint and user information to other security systems to enhance their functioning. These integration commonly use standardized protocols such as REST, Webhook, and Syslog.

**Fourth Generation**

The current generation of ZTNA aims to address the issues of reduced endpoint visibility that have come along with the increasing prevalence of IoT and BYOD. A main feature of this generation is an increasing move towards advanced device fingerprinting for managing business concerns such as end-of-life or end-of-support for assets, as well as automated management responses to known and emerging vulnerabilities. Lastly there an increasing reliance on and integrations with cloud technologies, mirroring the increasing use of cloud computing in fast changing networking environments.

## 7.3 Problems Addressed By ZTNA

**Entry By Unauthorized Devices**

Networks that do not implement ZTNA may be accessed by any device that is plugged into a switch port, or connects to a wireless acces point. Even if password protection is enabled, a user may still log into the network with an unapproved devices. This carries a substantial risk of introducing malware into the network. ZTNA can safeguard against these threats by denying access by unapproved devices.

**Lack of Detailed IP Tracking**

Most security systems leave an IP address in the audit trail but may not associate that IP with a user, or a device. This means that in environments with changing IP addresses, it is difficult to determine which device or user may be responsible for a security violation tied to an IP. ZTNA can keep track of all the connected endpoints through continuous network monitoring, and can provide various information about the endpoint that used the IP at a certain point of time in the past.

**Disorganized Asset Management**

properly manage assets and ensure compliance to regulatory standards. However, it is difficult for administrators to accurately identify IT assets Today's IT environment is much more complex than in the past due to BYOD, IoT, and so on. These conditions require thorough assessment in order to and check their status at all times. To reduce administrative burden, ZTNA can provide endpoint details such as the manufacturer, product name, name, location (switch port or physical location), user name, network connection / disconnection time, etc.

**Poor WLAN Security**

As mobile devices such as smart phones spread into business environments, they expand the usage of wireless LAN. In many networks, a shared password is used. Shared passwords can be easily exposed and it is difficult to trace because they can not be linked to a specific user. The company's shared password should, in principle, be changed if an employee who knows the password leaves the company. However, this is not an easy change to manage. To solve this problem, an 802.1X system is required to allow authentication using a personal password when accessing a wireless LAN. By default, ZTNA supports 802.1X, allowing for better wireless security.

**Unauthorized Access Points**

As the network technology develops, the user endpoints can access various types of external networks in addition to the network provided by the company to which the user belongs. Problems such as leakage of internal data may be caused by if a user connected to the internal network creates an access point to the network on their device that is available to outside entities. Data leaks may also occur if a device with sensitive data connects to a public network. ZTNA monitors WiFi that can be accessed from inside the company, and manages and controls which users are connected. Therefore both rogue access points and the use of non corporate networks can be identified and blocked.

**Non-Compliant Endpoints**

To solve security problems, administrators require employees to set up essential software or operating system settings, or may prohibit use of certain programs. However, security incidents are constantly occurring because not all users' endpoints meet their requirements. ZTNA continuously monitors the essential settings, such as antivirus software and screen savers, to ensure that theys are properly complied with, allowing non compliant devices to be blocked/quarantined, and fixed in case of violation.

**Insecure Operating Systems**

The most important thing for security of endpoint is application of latest security patch. ZTNA continuously monitors the endpoint and isolates unpatched endpoints from the network. This is different from typical endpoint management software, in that the control operates at the network level that the endpoint has reached. Through network control, administrators can make strong regulations that users can not bypass.

## 7.4 The Difference Between ZTNA and Firewall

Users who are not familiar with ZTNA technology often confuse their roles with firewalls. Because of the generality of the term Network Access Control, it is easy to think of a firewall as a product of the same function. However, the two products have the following major differences.

**Endpoint vs. Network focused**

A firewall is generally located between two or more networks in its configuration location to provide access control for communication between the networks, while ZTNA controls communiniation between endpoints within a network. For example, ZTNA can control a file share between two PCs on the same subnet, while the firewall generally does not.

**Dynamic vs. Static policies**

Firewall policies are usually made through objects such as addresses and ports of the source / destination called 5 Tuples. Recently, next-generation firewalls have begun to provide control through additional objects, such as users. In ZTNA, devices are organized into groups by multiple criteria. As the devices behavior and attributes change, the group the device is place into changes. Each of the groups can be linked to a security policy with a certain level of network privilege. For example, an endpoint that is not running an antivirus can be identified in real time and quarantined on the network.

**Internal vs. External networking**

A firewall generally controls traffic by blocking non compliant traffic coming into and out of a network, and generally works off simple rule sets. ZTNA acts on the endpoints themselves to control traffic between devices within the network in a more flexible fashion.

ZTNA and firewall solutions play complementary roles by addressing different aspects of network control.

## 7.5 Steps to Implement ZTNA

**Gain Visibility**

The ultimate goal of ZTNA is to control and manage the use of non-compliant end-user devices that connect to the network. For this purpose, however, it is very difficult to immediately apply control functions to the network. For example, when setting up 802.1X, it is often unclear if all networking devices and enpoint are compatible. Additionally, it is not obvious how to collect information for non compliant devices to bypass 802.1X. A proper setup for 802.1X requires visibility. However, 802.1X does not provide visibility until it is full implemented and controlling connections.

Additional strategies must be used to gain endpoint visibility such as IP, MAC, platform type / name / manufacturer, host name, connection switch / port, connection SSID, service port, and operation status. Agents and other means can help establish this visibility.

**Classify Endpoints**

Once the visibility is secured, a security policy should be established. The first step is to classify the endpoints based on the collected data to determine which groups require control. The classification of endpoints ideally groups endpoints in a way relevant to the IT manager's daily tasks or that indicates compliance status with organizational security rules.

**Control Access**

The methods of control should be applicable in a variety of ways, depending on the network environment or the status of the device. Technologies such as: 802.1X, ARP, SNMP switch control, SPAN, and agents may be used, as well as integrations with other security systems. The first consideration in the access control phase is the user's authentication. With identification being an important task, it is generally recommended that the user database be aligned with the existing authentication system in use at the deployment site. LDAP interlocks, such as Microsoft Active Directory, or enterprise services such as Google G-Suite, Office 365, email, and even RDBMS, are common options. The next step is to provide role-based access control on the nature of the device or the user authenticated. The next step is to attributes may be used to allocate VLANs or block connections so that organization provide role-based access control on the nature of the device or the user athenticated. User departments have different access rights for authenticating from devices, or using network resources.

If a user tries to access resources that have ben restricted, they can be redirected to a captive web portal. This portal may be customized so that the user can know which policy they are in violation of, and in turn how to become compliant.

**IT Security Automation**

Automation is the automatic application of security standards set by the administrator, such as operating system/software updates and settings, installation and operation of essential software, etc. This allows for devices that may violate a policy to be brought to a compliant status before network privileges are revoked. For example, a non-compliant device may be identified by the agent, and automatically corrected, without the intervention, of an administrator.

For more detailed deployment practices and considerations, see *Deployment Considerations*.

## 7.6 Features of Genian ZTNA

- **1th Generation ZTNA**

  Genian ZTNA is the flagship product of 1th Generation ZTNA, providing advanced visibility through network sensors, without the need for infrastructure changes. The information discovered can be used to dynamically group endpoints by over 500 criteria in real time. Flexible configuration options make it quick and easy to deploy.

- **Advanced Sensor Based Visibility**

  Genian ZTNA uses network sensors that connect directly to the broadcast domains of each network, minimizing interworking with existing IT infrastructures, even working well in legacy networks. This approach allows for visibility of Broadcast (ARP, DHCP, uPNP, mDNS) and Multicast traffic on each subnet.

- **Advanced Endpoint Platform Information**

  Device Platform Intelligence makes it easy for IT managers to perform daily management tasks by providing detailed endpoint information such as: End-of-Sale , End-of-Support, Network connection method, Manufacturers bankruptcy, Manufacturers merger, Manufacture country, List of published vulnerabilities, etc.

- **Multiple Access Control Methods**

  Genian ZTNA provides the broadest set of access control methods compared to other ZTNA products. These include: ARP control, DHCP server, switch control, SPAN based control, agent based control, and 802.1x. This makes it easy to establish comprehensive security. (See: *Policy Enforcement Methods*)

- **Diverse Security Automation Functions**

  The Genian ZTNA agent make it easy to manage endpoint operating systems, software, and hardware, in addition to collecting detailed information and other services.

- **Enhanced WLAN Security**

  Genian ZTNA collects wireless information through network sensors and agents to deliver security functions such as rogue AP detection, unauthorized wireless LAN connection monitoring/ control, and blocking of soft APs.

- **Excellent Interoperability**

  *REST API*, Webhook, and Syslog, are supported for interworking with existing IT systems.

- **Flexible Configurations**

  On-Premises or Cloud-managed versions provide the right solution for everyone, whether using an in-house IT department, or an out-sourced management service. In addition, it is a software based product, so users can select the hardware or virtual environment they desire to use.

- **Function Based Editions**

  Genian ZTNA is available in 3 Editions based on the implementation steps above. See: *Compare Editions*. The Basic Edition is primarily intended to quickly provide visibility into the early stages of ZTNA deployment without changing the existing network configuration. The Professional Edition provides network access control functions such as 802.1X, ARP control, and SPAN control, and may be upgraded to after the Basic edition is used to assess the network. Finally, the Enterprise Edition can be considered if there is a need to apply automated endpoint control, interwork with other security systems, provide role based administration or high availability deployment.

CHAPTER

EIGHT

# DEPLOYING GENIAN ZTNA

This chapter introduces you to basic information you should know before installing Genian ZTNA.

## 8.1 Understanding Components

To operate Genian ZTNA, various components are required. This chapter describes the role and installation location of each component.

### 8.1.1 Policy Server

The policy server is a central management system that stores all the data and settings of Genian ZTNA. The other components receive the configuration for their operation from the policy server, and then transmit the collected information. Typically, the policy server resides in the organization's data center and is installed on a physical server or virtual machine. The policy server may also be cloud hosted.

Another role of the policy server is to provide the administrator's management console through which all components are managed. You can view the collected information and establish your organization's security policies here.

### 8.1.2 Network Sensor

The network sensor is located in each network segment, monitors the network, detects nodes, collects information about them, and transmits it to the policy server.

The network sensor is connected to a regular network access port and does not require special settings such as port mirroring. However, when collecting information from several VLANs with one physical sensor, it should be configured as a trunk port through 802.1Q. In this case, a separate sensor node will be shown in the web console for each VLAN.

The network sensor monitors broadcast packets such as ARP or DHCP to detect that a new device is connected to the network. And it detects platform or acquires device information through various broadcast packets such as UPNP and NetBIOS.

Therefore, **network sensors must be connected to every broadcast domain**. If there are remote sites connected to the WAN, a separate network sensor is needed for each location. Other sensor deployments (Port Mirror (SPAN) , in-line) are supported, but do not provide all features. For more information see: *Deployment Considerations*

The network sensor functions mainly over a physical or emulated wired ethernet interface. The network sensor may be operated on the same system as the policy server or may be constituted by an independent system. Only one policy server is needed for all network sensors.

### Wireless Sensor

The Wireless Sensor is a sub component of the network sensor. It monitors the radio signal through the wireless LAN network interface to detect the SSID and wireless clients around the sensor. This data is collected in real time around the clock, and logged on our policy server where it is cross referenced with node and user data. This allows for you to identify threats like rogue access points, connection issues like channel conflicts, and to keep detailed accounting of when and by whom your networks are being accessed.

The Wireless Sensor can be configured on the same system as the Network Sensor if a WLAN interface is present. The Wireless Sensor may also be configured on a separate device to better detect signals in different areas of the deployment site.

Wireless sensors may not be used depending on whether wireless related functions are used or not.

**Note:** Network Sensors installed onto a virtual machine typically will not have direct access to the wireless interface on the host hardware. As a result, a wireless sensor will not operate, even if the host machine uses a wireless network interface. Genian ZTNA will detect the hosts wireless interface as a wired sensor interface. In this case, an endpoint agent installed to a device with a wireless NIC can perform the functions of a wireless sensor. See: *Controlling WLAN*

### Network Enforcer

The Network Enforcer is a sub-component of the network sensor that provides independent network access control for devices that violate an organization's policies. This makes it possible to isolate devices themselves without the help of existing network infrastructure. Like the network sensor itself, the Network Enforcer functions over a physical or emulated wired ethernet interface.

By enabling the Enforcer on the network sensor installed in each network segment, ARP-based Layer 2 Enforcement can be provided, which is the easiest way to provide network access control with network sensors without additional hardware.

Another Enforcer can be connected to the core switch with a SPAN Port (Mirroring) to terminate the session upon detection of unauthorized network access. This requires separate independent hardware capable of processing according to the amount of network traffic.

An Enforcer may be deployed as a ZTNA Gateway. With this option, the Enforcer is in-line with network traffic and only authorized traffic will be permitted. Both Cloud ZTNA Gateway and On-Prem ZTNA Gateway options are available.

See: *Installing ZTNA Gateway*

## 8.1.3 Agent

Agent is software installed in the user's desktop system. It periodically collects operating system, hardware, software and network related information and sends it to the policy server when a change is detected. It also provides desktop configuration management capabilities, making it easy to manage the required settings for your organization's security policies.

This is an optional component.

The agent provides its own security functions such as termination prevention and deletion prevention according to the administrator's setting.

Table 1: **Supported operating systems**

| Windows | macOS |
|---|---|
| Windows XP (SP2) | Apple OS X Mavericks |
| Windows Vista | Apple OS X Yosemite |
| Windows 7 | Apple OS X El Capitan |
| Windows 8 | Apple macOS Sierra |
| Windows 8.1 | Apple macOS High Sierra |
| Windows 10 | Apple macOS Mojave |

### 8.1.4 Updating Components

#### Genian Data

The **Policy Server** routinely updates **CVE Information**, **Node Information**, **OS Update Information** and **Platform Information** from the Genians Cloud.

#### Genian Software

Software Updates for the **Policy Server**, **Network Sensor**, and **Agent** can be downloaded and applied from the Genians Cloud in the System software section of the Web UI.

For Genians Cloud-managed subscribers, the Policy Server Software Updates are automatically installed.

For more configuration and update information, See: *Deployment Considerations* and *Managing System Software*

## 8.2 Deployment Considerations

### 8.2.1 Successful ZTNA deployment with Genian ZTNA

Establishing network access control can lead to changes in the network environment. To avoid distruption to end-users, Genian ZTNA uses a phased approach to deployment. Based on the experience gained by deploying ZTNA to many customers over 10 years, Genians highly recommends the following deployment steps:

#### Step 1: Gain visibility into your network assets

Understanding your network and user environment is the most important factor in establishing security policies and successfully applying network access control.

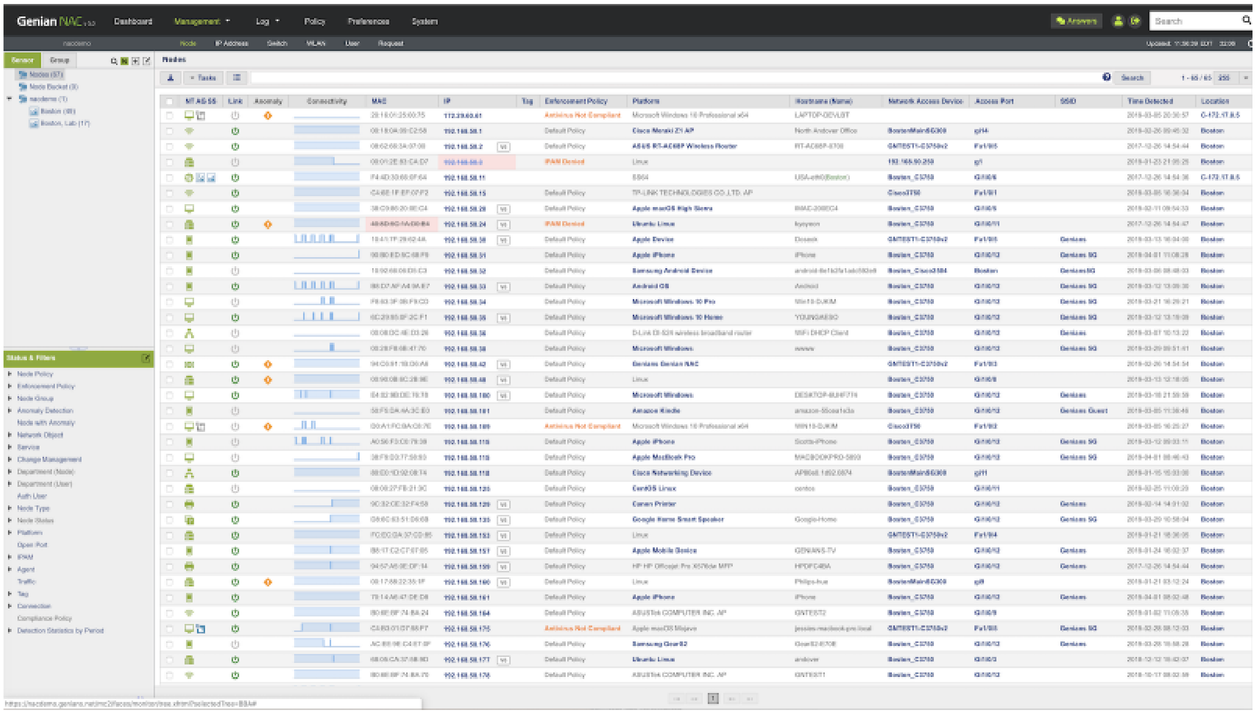
Having visibility into the network and the user device means that the following information can be monitored in real time:

- Exact type and quantity of devices in the network, including switches / routers and their configuration
- Operating system / hardware / software information of the user's device
- Wireless LAN environment

There are many ways to achieve this visibility. We hear from many customers that they have failed to achieve visibility through the 802.1x access control method, which has a high degree of implementation complexity. It is very difficult to establish gradual network access control through 802.1x, because 802.1x is a technology designed for control rather than visibility. This means that network control must be established before visibility is obtained.

Another method is switch device integration via SNMP / CLI. This makes it easier to obtain visibility without control. However, considering compatibility with switch manufacturers and models, as well as un-managed switch devices, there are still considerable limitations.

To address these complexity and compatibility issues, Genians offers a method of securing visibility through an independent **Network Sensor**. The network sensor is connected to each subnet (broadcast domain) and can be deployed without changing the existing network environment. Usually, installation and full visibility can be acheived in under three days.

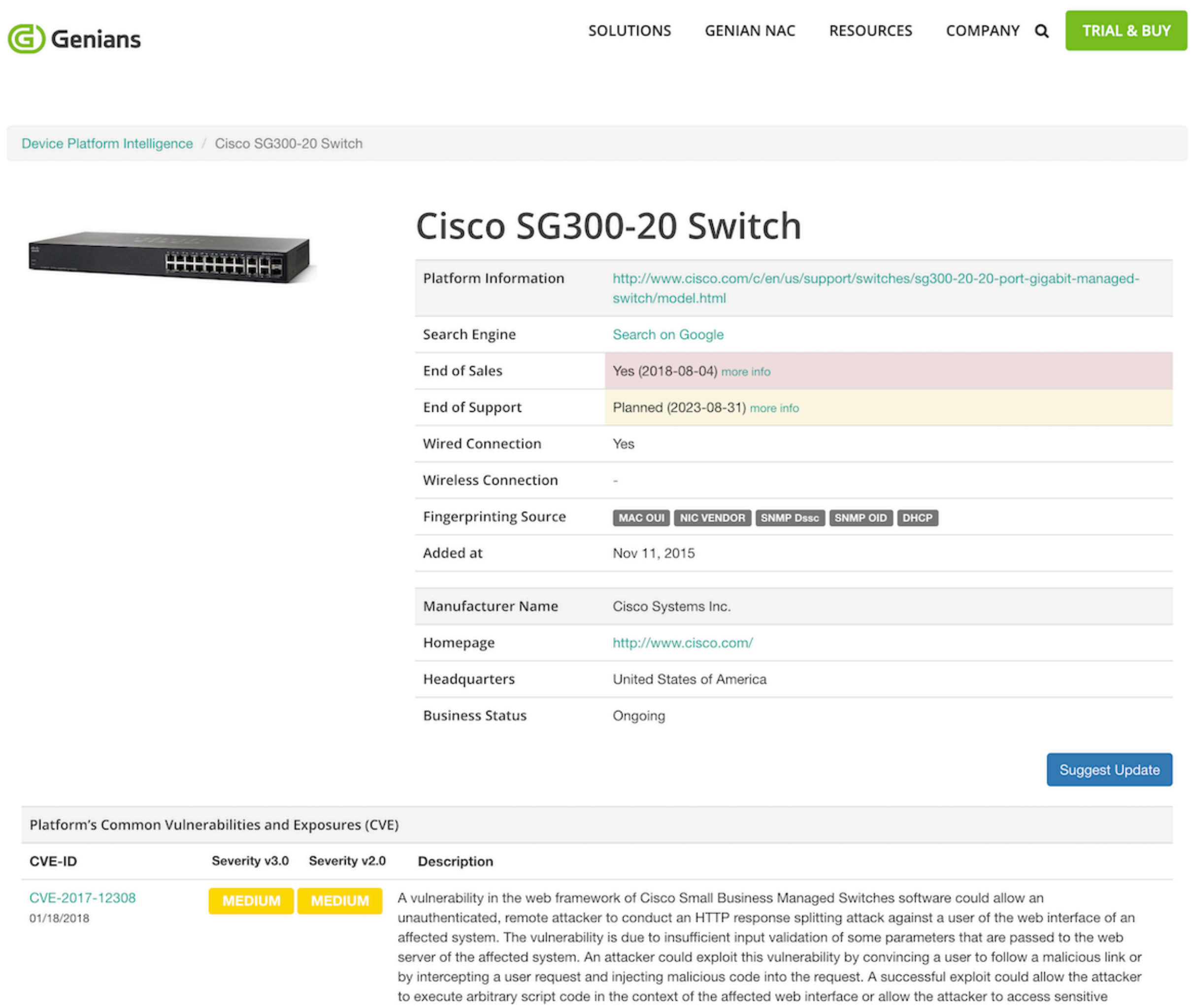


Genian ZTNA also provides **Agent** software for greater visibility into Windows and MacOS operating systems. It can be installed on the user's system to collect information (operating system / hardware / software / update, etc.) desired by the administrator.

## Step 2: Classify assets and check compliance

Once the visibility of the IT assets is established, the next step is to classify known assets. Genian ZTNA offers more than 500 different conditions for grouping assets. Node group membership updates in real time as the status of the node changes.

Ideally, groups are defined by multiple perspectives, such as who the intended user is, what kind of device the node is,or what subnet the nodes are part of. To this end, various additional information such as manufacturer / product name / model information, connection method, and more are provided by Genian ZTNA's Device Platform Intelligence.



Device Platform Intelligence / Cisco SG300-20 Switch

Cisco SG300-20 Switch

| | |
|---|---|
| Platform Information | http://www.cisco.com/c/en/us/support/switches/sg300-20-20-port-gigabit-managed-switch/model.html |
| Search Engine | Search on Google |
| End of Sales | Yes (2018-08-04) more info |
| End of Support | Planned (2023-08-31) more info |
| Wired Connection | Yes |
| Wireless Connection | - |
| Fingerprinting Source | MAC OUI NIC VENDOR SNMP Dssc SNMP OID DHCP |
| Added at | Nov 11, 2015 |

| | |
|---|---|
| Manufacturer Name | Cisco Systems Inc. |
| Homepage | http://www.cisco.com/ |
| Headquarters | United States of America |
| Business Status | Ongoing |

Platform's Common Vulnerabilities and Exposures (CVE)

| CVE-ID | Severity v3.0 | Severity v2.0 | Description |
|---|---|---|---|
| CVE-2017-12308<br>01/18/2018 | MEDIUM | MEDIUM | A vulnerability in the web framework of Cisco Small Business Managed Switches software could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack against a user of the web interface of an affected system. The vulnerability is due to insufficient input validation of some parameters that are passed to the web server of the affected system. An attacker could exploit this vulnerability by convincing a user to follow a malicious link or by intercepting a user request and injecting malicious code into the request. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web interface or allow the attacker to access sensitive |

In addition to administrative classification, classification of devices that violate security regulations is also very important.

In general, groups may be configured for:

- Devices that are not assets of the company are connected to the network (personal devices)
- PC's without antivirus software
- Non-Authenticated devices

### Step 3: Establish IT security policy and remediation

Once an IT security policy is established, control of the device that violates it is required. Becasue it is not easy to control all identified violation devices at once Genian ZTNA provides a step-by-step, automated approach.

The Agent is equipped with a variety of control action plug-ins to automatically process various security settings and configurations without user intervention. The Captive Web Portal (CWP) can also guide you through the tasks you need to perform, such as guest user on-boarding.

For more information on control actions, see *Controlling Endpoints with Agent*

### Step 4: Enforce network access control and Quarantine non-compliance devices

After removing the known unauthorized device through the above steps and completing the necessary security measures for the user's device, the remaining task is to continuously monitor whether the security regulations are complied with, and to control network access by the devices that violate the regulations. At this stage, various control methods can be selected according to the network environment and required security level. Genian ZTNA provides a variety of controls for this.

- 802.1x
- Layer 2 (ARP, DHCP)
- SNMP/CLI (Port Shutdiown)
- Port Mirror (SPAN)
- Inline
- Integration with 3rd party device (Firewall, VPN, etc)
- Agent

For details about each control method, see *Policy Enforcement Methods*

### 8.2.2 Technical Considerations

| Topic | Layer 2 Sensor/Enforcer | SNMP/CLI | Port Mirror (SPAN) | Inline | 802.1x | Agent |
|---|---|---|---|---|---|---|
| **Access Control at Layer 2** | Yes | Yes | No | No | Yes | No |
| **Access Control at Layer 3** | RBAC | Switch Port ACL | RBAC | No | Switch Port ACL | OS Firewall |
| **Post-admission Control** | ARP, DHCP | VLAN/ACL/Shutdown | TCP RST, ICMP unreach. | Filtering | CoA* | OS Firewall |
| **Additional Hardware** | Network Sensor | Managed Switches | Full traffic capable Device,<br>Tap Device,<br>SSL Decryption Device | Full traffic capable Device | 802.1x Switch/AP | No |
| **Endpoint Dependency** | No | No | No | No | 802.1x Supplicant | Agent required |
| **WLAN Security** | Monitoring<br>(WNIC on Sensor) | Monitoring<br>(SNMP with Controller) | No | No | Monitoring / Control<br>(WPA2-Enterprise) | Monitoring / Control<br>(SSID Whitelist) |
| **Layer 2 Security** | Detect MAC Spoofing,<br>Detect Rogue DHCP,<br>Managing IP Conflict | No | No | No | No | No |

*CoA*: Change of Authorization, RFC 5176 - Dynamic Authorization Extensions to RADIUS*

### 8.2.3 Management Considerations

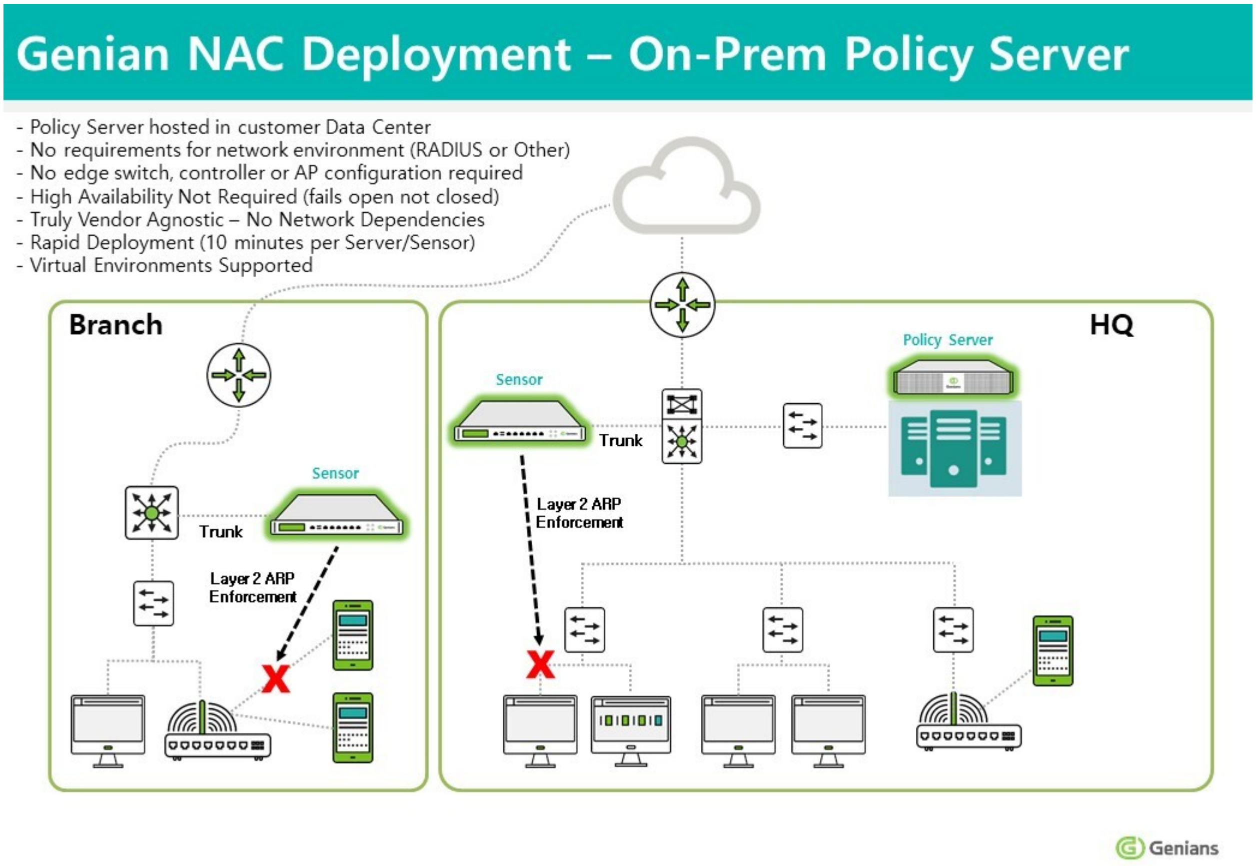
| Topic | Layer 2 Sensor/Enforcer | SNMP/CLI | Port Mirror (SPAN) | Inline | 802.1x | Agent |
|---|---|---|---|---|---|---|
| **Network Config Change** | Trunk port (optional) | Switch Config,<br>VLAN/ACL | Tap Device,<br>SPAN Port | Gateway Change | Switch Config,<br>VLAN/ACL,<br>Endpoint Config | No |
| **Compatibility Issue** | No | Vendor-dependent<br>SNMP MIB/CLI | No | No | RADIUS Vendor Attribute,<br>non-802.1x capable Device<br>(*Poor wired device support*) | OS Type/Version |
| **Easy of Deployment** | Easy | Difficult | Intermediate | Easy | Very Difficult | Intermediate |
| **Phased Deployment**<br>(Discover First, Control Later) | Yes | Yes | Yes | No | Must be controlled from<br>the start of deployment | Yes |
| **Single point of Failure** | No | Yes | Yes | Yes | Yes | No |
| **Vendor Lock-in** | No | Intermediate | No | No | High | Intermediate |
| **Recommended for** | Essential Discovery<br>and Control | Extended information<br>and port control | | | Wireless network | Extended information<br>and enforce compliance |

### 8.2.4 Deployment Models

#### On-Premises

**Policy Server** and **Network Sensor** can be deployed flexibly.

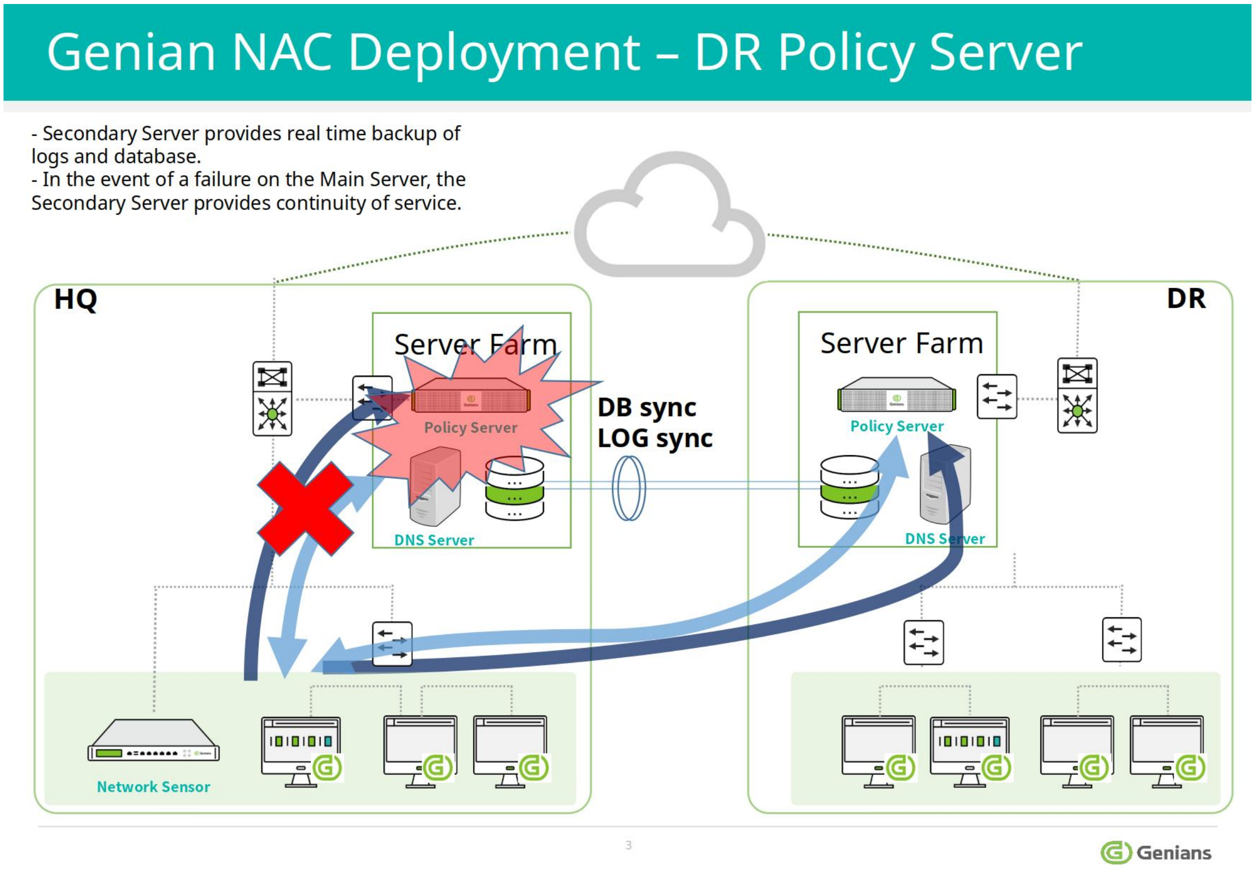
- Policy Server/Network Sensor combined may be hosted on a single appliance or separately
- Sensor(s) may be deployed centrally (802.1Q trunk or mirror port) or distributed between networks.
  - Trunked Sensors support up to 128 Vlans(recommended 64 Vlans)
  - For more info on sensor modes , see: *Controlling Network Access*



Genian NAC Deployment – On-Prem Policy Server

- Policy Server hosted in customer Data Center
- No requirements for network environment (RADIUS or Other)
- No edge switch, controller or AP configuration required
- High Availability Not Required (fails open not closed)
- Truly Vendor Agnostic – No Network Dependencies
- Rapid Deployment (10 minutes per Server/Sensor)
- Virtual Environments Supported

*Configuring High Availability*



Genian NAC Deployment – DR Policy Server

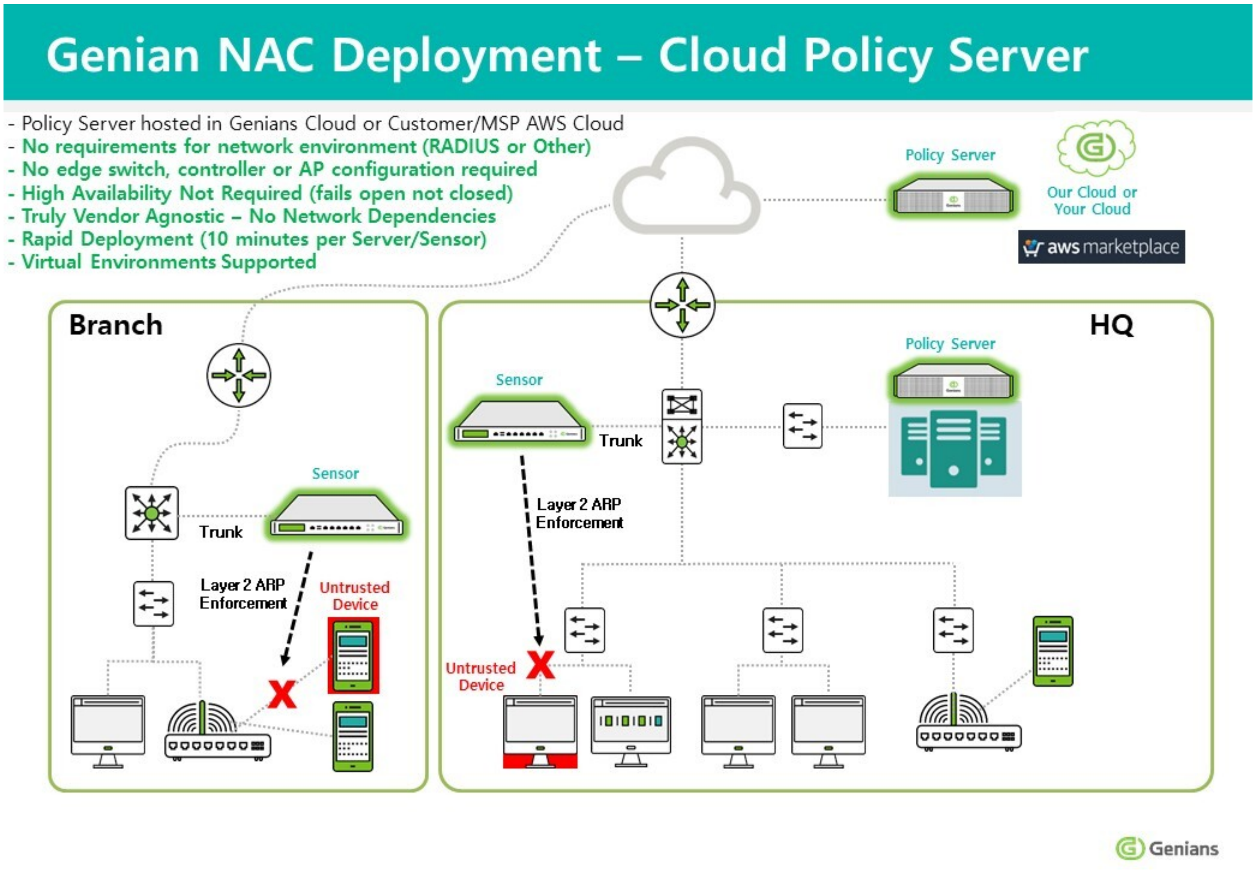
- Secondary Server provides real time backup of logs and database.
- In the event of a failure on the Main Server, the Secondary Server provides continuity of service.

### Your Cloud

The Policy Server may be hosted in an existing Private Cloud by utilizing the publicly available AWS AMI. Deployment instructions are posted in the AWS Market Place product listing for Genian ZTNA Policy Server.

### Genians Cloud

The Policy Server may be hosted in a Private site in the Genians Cloud which can be launched from Genians.com.



Genian NAC Deployment – Cloud Policy Server

- Policy Server hosted in Genians Cloud or Customer/MSP AWS Cloud
- No requirements for network environment (RADIUS or Other)
- No edge switch, controller or AP configuration required
- High Availability Not Required (fails open not closed)
- Truly Vendor Agnostic – No Network Dependencies
- Rapid Deployment (10 minutes per Server/Sensor)
- Virtual Environments Supported

## ZTNA AS A SERVICE (MSP READY)

**Essential Features For CyberSecurity-As-A-Service**

Enhance the way of monitoring your customer network:

- Security infused IT Asset Management empowered by *Device Platform Intelligence*
- Ongoing Compliance-As-A-Service for Networks and Endpoints
- *Network anomaly detection*
- Customizable *dashboards* and *reports*

Secure network connections made by any type of IP enabled devices at the edge:

- *Control unauthorized/rogue/misconfigured devices*
- Support a productive *onboarding process*
- *Quarantine/Remediation*
- *Desktop configuration management*

Plus, the built-in services:

- *RADIUS Server* for AAA (802.1x)
- *DHCP Server* for IP management
- *Syslog Server* for Log and Event Management

**Cloud Ready**

Supports various Cloud environments:

- Public Cloud (AWS, Azure, Google)
- Private Cloud (VMWare, OpenStack)
- Nutanix Hyperconverged Infrastructure (HCI)

*Genian ZTNA Components*:

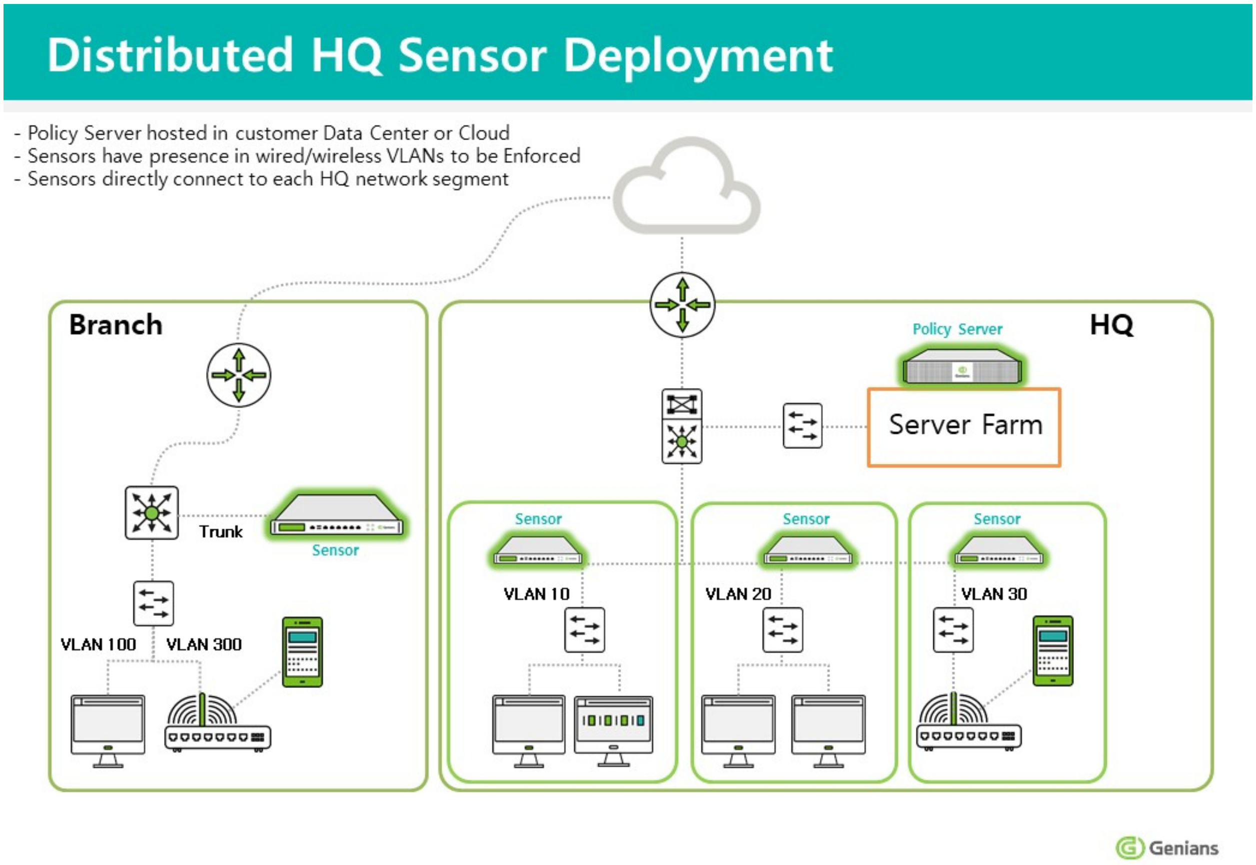
- Policy Server: Supports multi-tenancy (Docker container)
- Network Sensor: Support Universal customer premises equipment (uCPE)
- Agent: Multi functional features and customization

Management:

- One-stop service (sites, users, licenses, subscriptions, billing)
- Virtual domain support
- Centralized dashboard/reports
- Zero Config Provisioning
- White label service

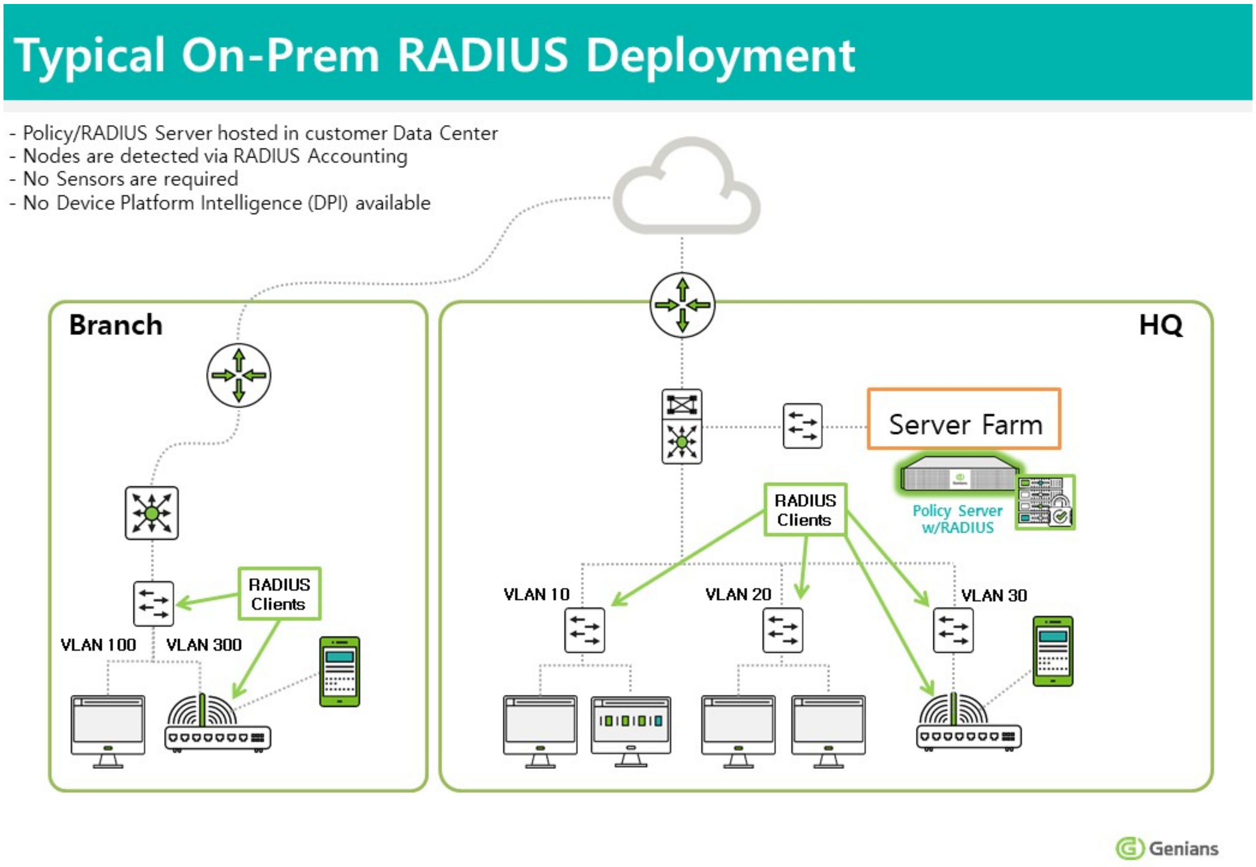
## Additional Deployment Models

### On-Premise



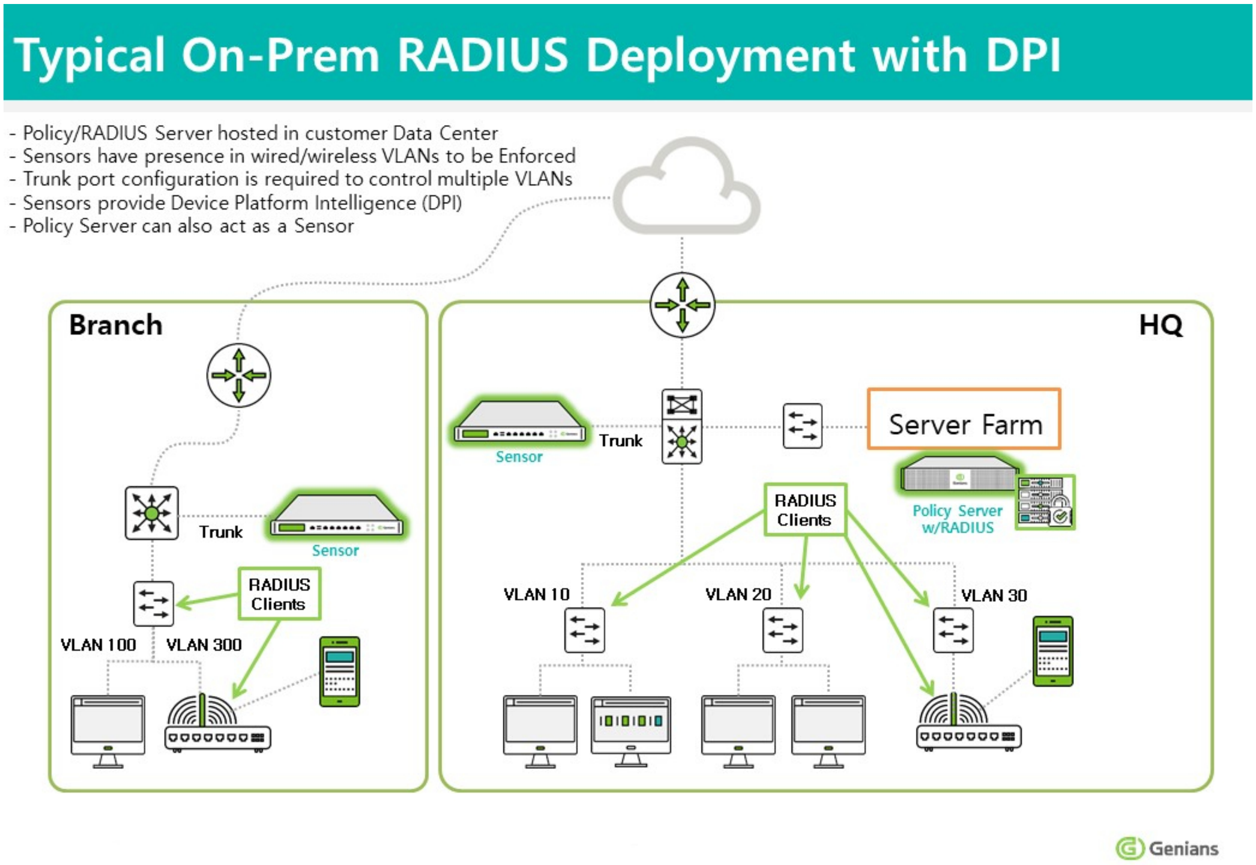
## Distributed HQ Sensor Deployment

- Policy Server hosted in customer Data Center or Cloud
- Sensors have presence in wired/wireless VLANs to be Enforced
- Sensors directly connect to each HQ network segment



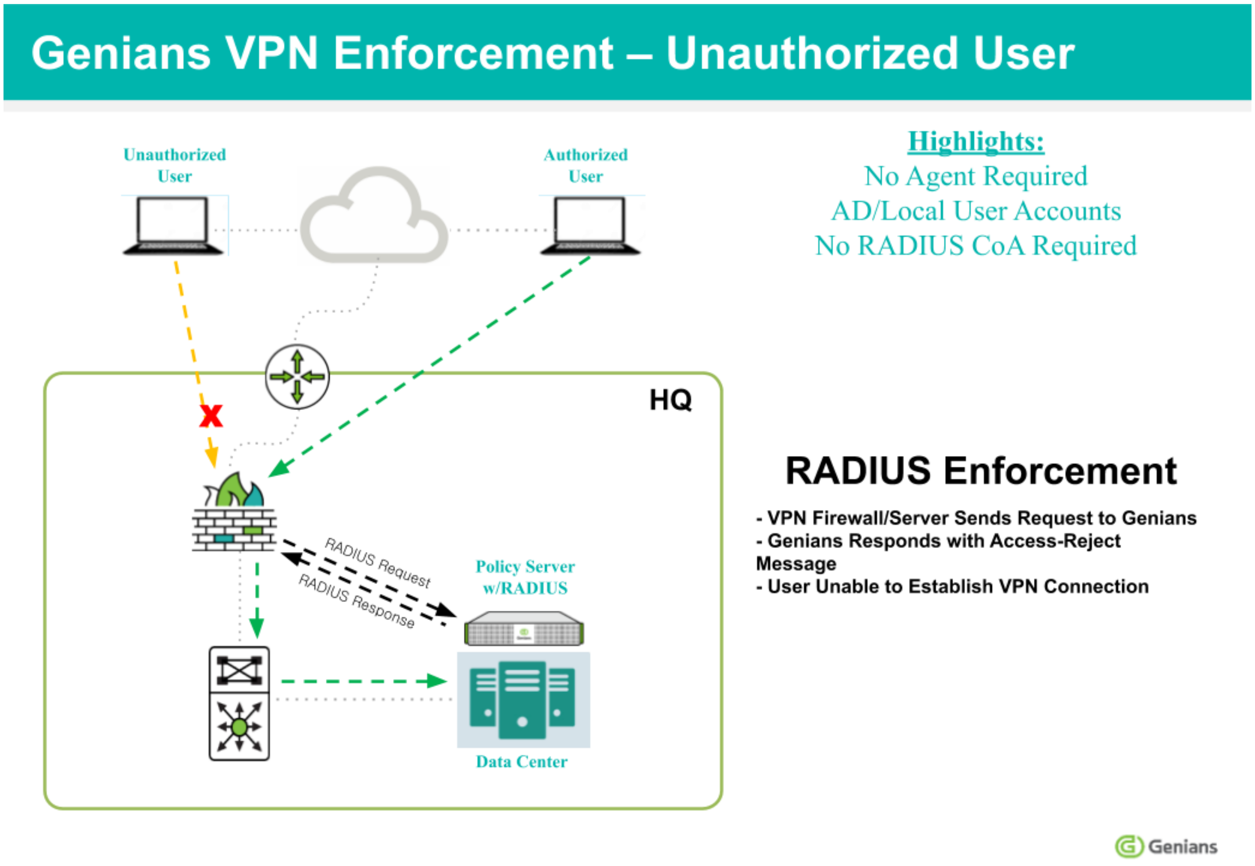
## Typical On-Prem RADIUS Deployment

- Policy/RADIUS Server hosted in customer Data Center
- Nodes are detected via RADIUS Accounting
- No Sensors are required
- No Device Platform Intelligence (DPI) available



# Typical On-Prem RADIUS Deployment with DPI

- Policy/RADIUS Server hosted in customer Data Center
- Sensors have presence in wired/wireless VLANs to be Enforced
- Trunk port configuration is required to control multiple VLANs
- Sensors provide Device Platform Intelligence (DPI)
- Policy Server can also act as a Sensor



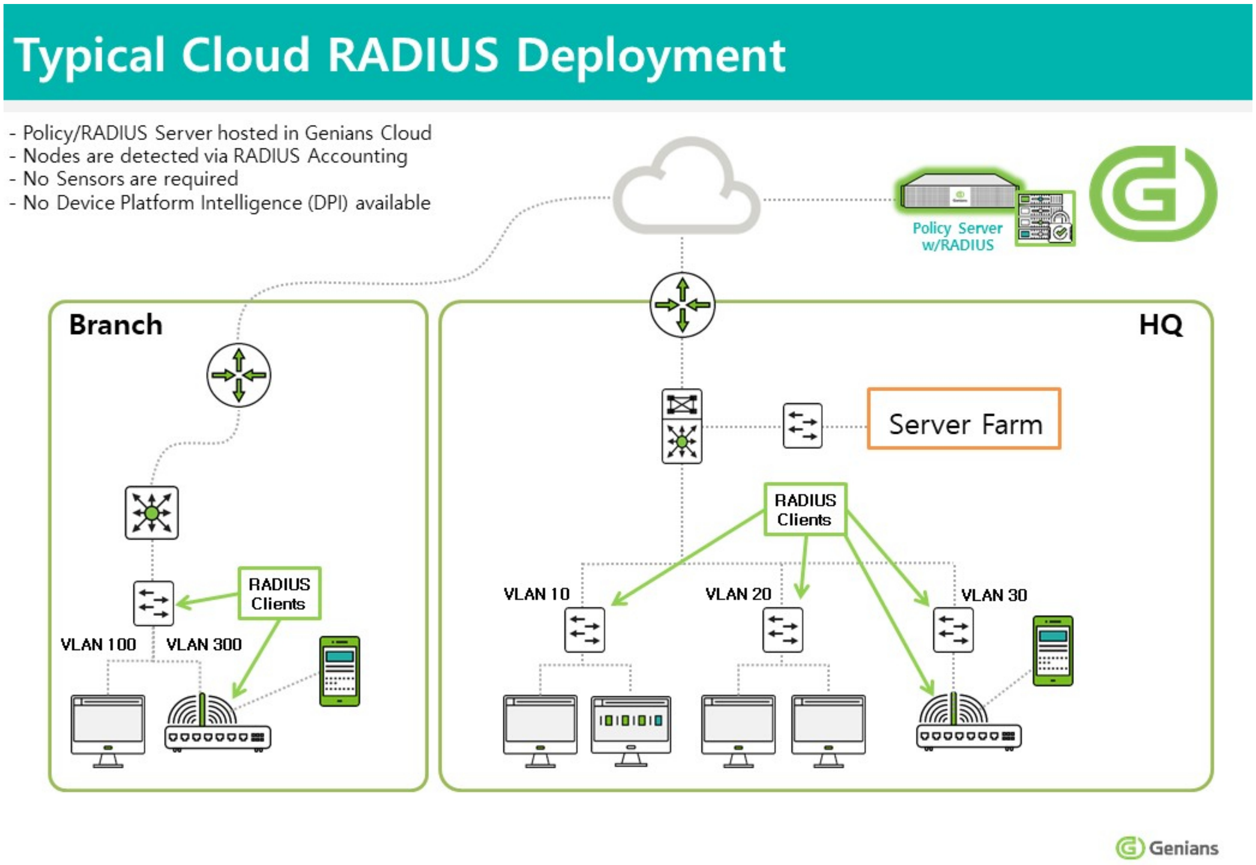
## Genians VPN Enforcement – Unauthorized User

**Highlights:**
No Agent Required
AD/Local User Accounts
No RADIUS CoA Required

### RADIUS Enforcement

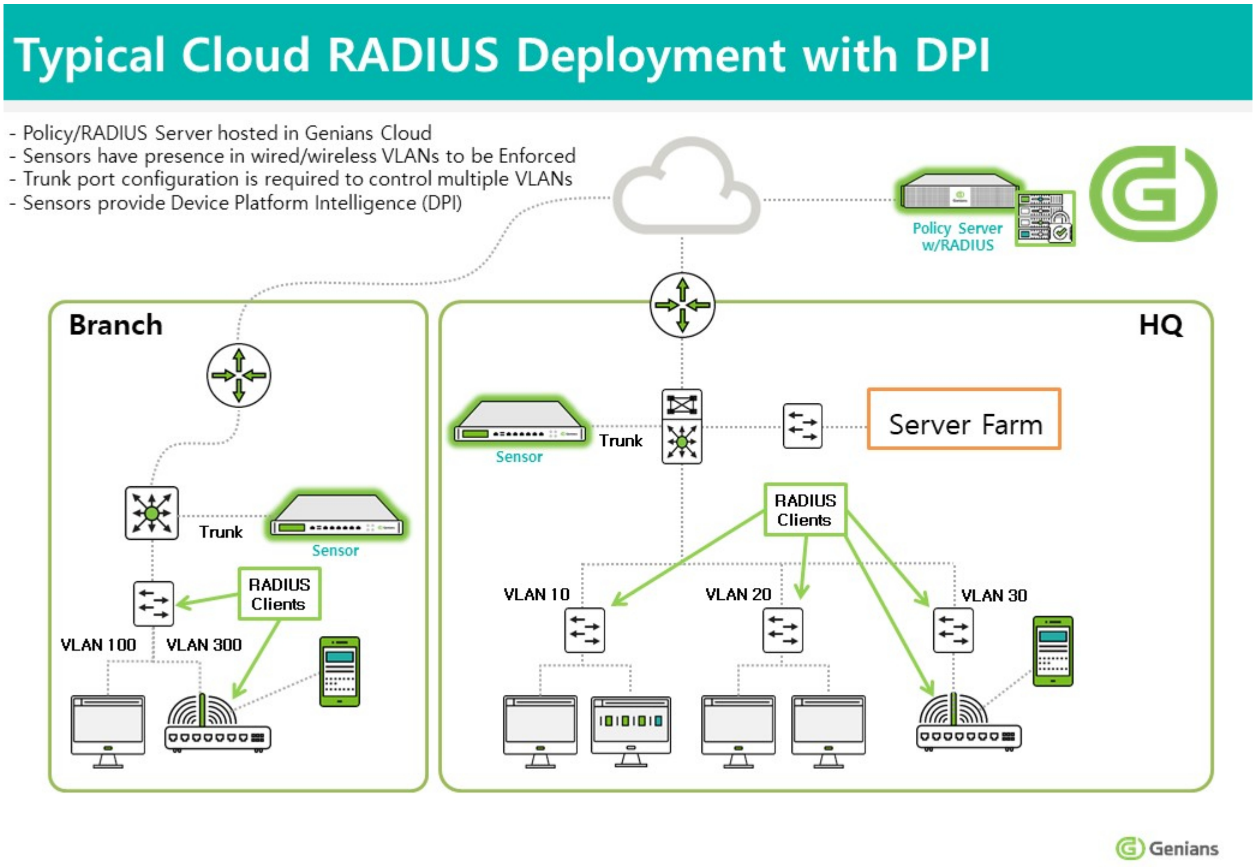
- VPN Firewall/Server Sends Request to Genians
- Genians Responds with Access-Reject Message
- User Unable to Establish VPN Connection

### Cloud



Typical Cloud RADIUS Deployment

- Policy/RADIUS Server hosted in Genians Cloud
- Nodes are detected via RADIUS Accounting
- No Sensors are required
- No Device Platform Intelligence (DPI) available



Typical Cloud RADIUS Deployment with DPI

- Policy/RADIUS Server hosted in Genians Cloud
- Sensors have presence in wired/wireless VLANs to be Enforced
- Trunk port configuration is required to control multiple VLANs
- Sensors provide Device Platform Intelligence (DPI)

## 8.3 Compare Editions

ZTNA is available Enterprise edition.

**Enterprise**

Provides visibility into network and IT assets.
Provides network access control according to IT security policy.
Provides advanced and automated IT security.

| Category | Feature | Enterprise |
|---|---|---|
| Visibility | Detect/Monitor IP-enabled Device | Yes |
| | Device Platform Intelligence (Name, Type, Picture, EOL, Connection, CVE) | Yes |
| | Switch Port Information | Yes |
| | WLAN Monitoring / Security (Rogue/Misconfigured AP) | Yes |
| | Basic Endpoint Information (OS, HW, Software) by Windows/macOS Agent | Yes |
| | Condition based Dynamic Node Group | Yes |
| | Customizable Dashboards (Over 100 Widgets) | Yes |
| | Track Changes / Audit Logs | Yes |
| | Network Anomaly Detection (MAC Spoofing, Rogue Gateway, Ad-hoc) | Yes |

continues on next page

Table 2 – continued from previous page

| Category | Feature | Enterprise |
|---|---|---|
| | Basic Reports (Node, WLAN, Log) | Yes |
| | Notification (Email/Text Message) | Yes |
| | Custom Reports | Yes |
| | Detect OSS usage and provide SBOM details for better software transparency | Yes |
| | Classify endpoints based on threat scores | Yes |
| User Authentication | Captive Portal Login (Web login) | Yes |
| | Google Authenticator Support for Captive Web Portal | Yes |
| | Active Directory SSO | Yes |
| | External User Directory Integration (LDAP/RADIUS/SMTP/POP3/IMAP/SAML2) | Yes |
| | FIDO (Biometric) authentication for administrator, Captive Web Portal and Agent | Yes |
| | Multifactor Authentication (Text Message/Email/Google OTP) | Yes |
| | Hardware security chip TPM EK-based device authentication | Yes |
| Network Access Control | 802.1X based Control (RADIUS Server, EAP, MAB, VLAN Assign, CoA) | Yes |
| | ARP based Layer 2 Enforcement | Yes |
| | Port Mirroring (SPAN) based Enforcement | Yes |
| | In-line Enforcement (Dual-homed Gateway) | Yes |
| | Switch integration (SNMP) based Enforcement | Yes |
| | DHCP based Enforcement (DHCP Server) | Yes |
| | Role based Access Control | Yes |
| | IP Address Management(IPAM) | Yes |
| | Tag-Based Control of Users, Wlans and Devices/Nodes (E.g., Guest devices, temporary privileges, policy exemptions) | Yes |
| Cloud Security | Cloud Workload Visibility | Yes |
| | Policy server operation in the cloud | Yes |
| | Automated Cloud Control using CLI Interface | Yes |
| | Cloud Security Group Management | Yes |
| Remote Work | ZTNA Client (SSL-VPN) | Yes |
| | Always on ZTNA | Yes |
| Zero Trust Network Access (ZTNA) | Role-base Access Control Permission Policy | Yes |
| | Dynamic destination (Node Group) support in Permission object | Yes |
| | ZTNA Cloud Gateway for Security Service Edge (SSE) - AWS, Azure, GCP | Yes |
| | Secure Branch Tunneling (IPSec/GRE) | Yes |
| | Traffic Visibility (netflow) | Yes |
| | URL and Application Filtering | Yes |
| | IP Mobility (VxLAN, Always on ZTNA) | Yes |
| Desktop Management | Compliance Check (Antivirus, OS Update, Required SW, OS Settings) | Yes |
| | OS Configuration (Screenlock, Internet Options, DNS) | Yes |
| | Windows Update Management (Offline Update, Update Cache, Approval) | Yes |
| | External Device Control (USB and etc.) | Yes |
| | 802.1X Connection Profile Provisioning (Wireless/Wired) | Yes |
| | EAP-GTC Plugin for Windows (Support Regacy Password Authentication) | Yes |
| | WLAN Control (SSID Whitelist, SoftAP block) | Yes |

continues on next page

Table 2 – continued from previous page

| Category | Feature | Enterprise |
|---|---|---|
| Integration | User Directory Sync (RDBMS, Active Directory, LDAP, Google) | Yes |
| | Webhook / Syslog / SNMP trap (Outbound) | Yes |
| | REST API (Inbound) | Yes |
| | Syslog Server (Inbound) | Yes |
| Business Process | User Consent Pages | Yes |
| | Request/Approval via CWP (IP, Device, User, Guest User, External Device) | Yes |
| | Role based Administrator | Yes |
| | Custom Fields (Node, Device, User) | Yes |
| | Custom Captive Portal Pages | Yes |
| | Multilingual Support | Yes |
| | Streamline repetitive tasks using workflow templates | Yes |
| Scalability and Availability | High Availability (Policy Server / Network Sensor) | Yes |
| | Interface Channel Bonding | Yes |
| | Disaster Recovery (DB Replication, Redundant Policy Server) | Yes |

## 8.4 Sizing Software and Hardware

### 8.4.1 Five steps to specifying the right software and hardware

This chapter provides a guideline for choosing the right Genian ZTNA software and hardware. Specifying the right software and hardware is dependent on a number of factors and involves developing a usage profile for the users and the network environment.

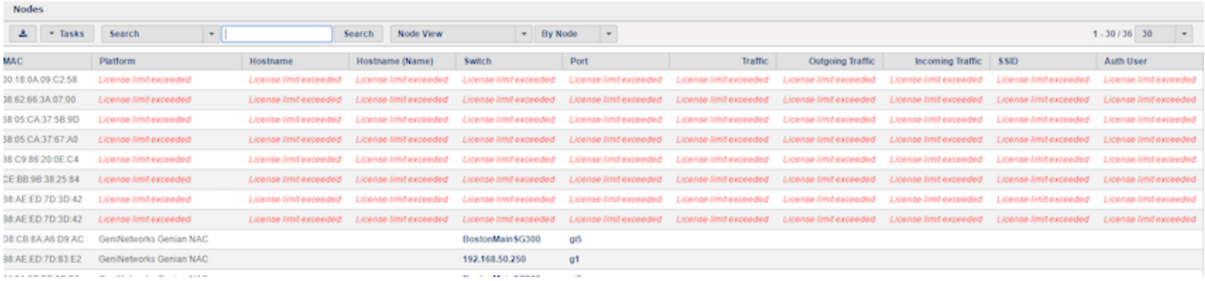
### 8.4.2 Step 1. Identify the Total Active Devices Number for Software License

The license of Genian ZTNA Software is based on the number of devices connected to the network and running. The number of devices is measured by the number of unique MAC addresses connected to the network. In order to purchase Genian ZTNA in the right size, it is necessary to know the number of devices in operation. This value can usually be found in the following ways:

- The number recognized by the IT / Network Administrator
- The existing IT management system (Asset Mgmt, Network Monitoring)
- Verifying actual numbers through Genian ZTNA Trial Version (Download and Identify Devices)

**All devices that use TCP/IP communication, such as IP phones, surveillance cameras, as well as PCs should be considered as devices.**

As your network grows, and the number of devices exceed your License limit, some information of new devices will be hide. But all policies work normally. (Product feature limitations due to license overrun may change without notice.)



| MAC | Platform | Hostname | Hostname (Name) | Switch | Port | Traffic | Outgoing Traffic | Incoming Traffic | SSID | Auth User |
|---|---|---|---|---|---|---|---|---|---|---|
| 00:18:0A:09:C2:58 | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded |
| 08:62:66:3A:07:00 | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded |
| 58:05:CA:37:5B:9D | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded |
| 58:05:CA:37:67:A0 | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded |
| 38:C9:86:20:0E:C4 | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded |
| CE:BB:9B:38:25:84 | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded |
| B8:AE:ED:7D:3D:42 | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded |
| B8:AE:ED:7D:3D:42 | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded | License limit exceeded |
| D8:CB:8A:A6:D9:AC | GeniNetworks Genian NAC | | | BostonMainSG300 | gi5 | | | | | |
| B8:AE:ED:7D:83:E2 | GeniNetworks Genian NAC | | | 192.168.50.250 | g1 | | | | | |

When devices are no longer seen on the network the License will then be carried over to the next active and running device. If you purchase an on-premise product, there are no licensing deadlines, only maintenance expirations. If maintenance contract expires, then you cannot upgrade to a newer version or update any of the various databases.

### 8.4.3 Step 2. Identify the Total Active Nodes Number for Hardware

You need to know the number of nodes to estimate the capacity of the policy server. A node is an endpoint on the network consisting of a combination of IP and MAC. If a system with a single MAC address is using multiple IPs at the same time, the number of devices is one, but the number of nodes can be several. Because Genian ZTNA manages all information on a per-node basis, it is closely related to the number of nodes in the capacity of the policy server.

Depending on the number of nodes in the network you wish to install, we recommend the following minimum specifications:

**Policy Server:**

| | 2,000 Nodes | 10,000 Nodes | 20,000 Nodes | Over 20,000 Nodes |
|---|---|---|---|---|
| CPU | Intel Dual Core | Intel Quad Core | Intel Hexa Core | Intel Octa Core |
| Memory | 8 GB | 16 GB | 32 GB | 64 GB |
| Storage | SSD 128 GB | SSD 256 GB | SSD 512 GB | SSD 1 TB |

**Network Sensor:**

| | 2,000 Nodes | 5,000 Nodes | 10,000 Nodes | Over 10,000 Nodes |
|---|---|---|---|---|
| CPU | Intel Dual Core | Intel Quad Core | Intel Hexa Core | Intel Octa Core |
| Memory | 2 GB | 4 GB | 8 GB | 16 GB |
| Storage | SSD 128 GB | SSD 128 GB | SSD 128 GB | SSD 128 GB |

### 8.4.4 Step 3. Identify the Total Managed Networks Number

Genian ZTNA requires the installation of a sensor for every single layer 2 broadcast domain. Therefore, the number of managed broadcast domains is an important factor in determining the sizing of the product. The number of network sensors required depends on two factors:

- Number of VLANs
- Number of remote networks with routing

A single network sensor can support up to 128 VLANs. When an 802.1Q VLAN Trunk connection is provided through the Core Switch, sensor services for up to 128 networks are provided over a single physical connection. If the managed network is physically separated and configured as a WAN connection, one Sensor will not be able to configure Layer 2 connections to different regions. If this is the case, you will need to configure a separate sensor for each remote network.

For example, if you have a corporate WAN with 4 branches, 1 sensor per branch is required. If any branch has multiple broadcast domains that you cannot access via a 802.1Q trunk port, you will need an additional sensor interface for each broadcast domain. A single sensor device may still be used.

### 8.4.5 Step 4. Identify the Total Agent Applied Devices Number

The number of systems requiring agent installation is closely related to the capacity of the policy server. Data and various events collected by the agent are sent directly to the policy server. Therefore, when the number of agents is large or the agent performs complicated tasks, the load on the policy server becomes high. We recommend that you follow these minimum requirements:

| | 1,000 Agents | 5,000 Agents | 10,000 Agents |
|---|---|---|---|
| CPU | Intel Dual Core | Intel Quad Core | Intel Quad Core |
| Memory | 8 GB | 16 GB | 32 GB |
| Storage | SSD 128 GB | SSD 256 GB | SSD 512 GB |

Genian ZTNA supports agents for windows and macOS operating systems. The quantity of agents may be less than or equal to the number of systems in which Windows and macOS operating systems are installed.

The Genian ZTNA Policy Server can be divided into two parts: a node server that receives and processes data from network sensors and agents, and a database that stores data. In a small to medium-sized operating environment, it is common for two functions to work together on a single server, but in a large-scale operating environment, the two functions can be operated as separate servers. If your network consists of more than 10,000 nodes, consider configuring the node server and database separately.

### 8.4.6 Step 5. Availability and Reliability Requirements

For availability and reliability, Genian ZTNA supports Active/Standby configuration. By configuring Backup system for policy server and network sensor, service can be provided without interruption in case of master system failure. For this, Genian ZTNA provides its own HA capabilities to automatically detect master system failures.

HA configuration requires an additional backup system for each system, so you need to prepare twice the number of devices required for service configuration.

### 8.4.7 Sizing Questionnaire

Please answer the following questions:

| | |
|---|---|
| Number of Devices (Number of unique MACs on network) | |
| Number of Nodes (Number of MAC+IP conbinations on network) | |
| Number of L2 Networks (Number of broadcast domains) | |
| Number of Network Sensors (One sensor supports up to 128 VLANs, each remote network needs a Sensor) | |
| Number of Agent Applied Devices | |
| Policy Server Functional Serparation (Node Server/Database Server) | YES / NO |
| High Availability for Policy Server | YES / NO |
| High Availability for Network Sensor | YES / NO |

## 8.5 Preparing Network

When planning your Genian ZTNA Deployment onto your network there are several considerations.

- Where should the equipment be placed?
- How will it connect to my switches?
- How many pieces of equipment do I need?
- What ports do I need to open for Genians to communicate?

### 8.5.1 Wired Connectivity

The Policy Server should be directly connected to your Core Switch port as an access port. The Network Sensor should be connected to an Edge Switch port that can be an access port, or trunk port.

#### Switches

Network Sensors must be able to see broadcast packets, so they must be connected to all managed subnets.

**VLANs**

To monitor multiple VLANs (up to 128,recommended 64) through a single port, make sure the switch port is configured with 802.1Q trunking and that all VLANs you wish to monitor are allowed on that port.

Switches differ in how to configure this setup.

Below are examples of how to configure 802.1Q Trunk ports for VLANs on common switches. In these examples, we will show how to add VLANs 100 and 200 to port 48, configured with .1q trunk encapsulation.

Cisco Switch

```
Cisco(config)#interface gi1/0/48
Cisco(config-if)#switchport trunk encapsulation dot1q
Cisco(config-if)#switchport mode trunk
Cisco(config-if)#switchport trunk allowed vlan add 100,200
```

HP Switch

```
Procurve(config)#vlan 100
Procurve(config)#tagged 48
Procurve(config)#vlan 200
Procurve(config)#tagged 48
```

**SNMP**

Genians supports SNMP Versions 1, 2c and 3. The read-only community string is used to check whether the node supports SNMP in the process of collecting information about the Node by the network sensor. If the node responds to an SNMP request, the sensor verifies that the node is a switch by verifying that it supports the BRIDGE-MIB through an SNMP query. The read-write community string is used to make changes to the switches for port descriptions and shutting down switch ports. In addition, it can be used for various additional functions such as collecting information of wireless controller using SNMP, detecting platform information of device.

**Note:** Be sure to add the Network Sensor to the access-lists of all switches in the same network segment, and assign necessary permissions for users/groups to view all OIDs. For more info see: *Switch Ports*

#### WAN

If you have more then one location behind WAN Technologies then a Network Sensor would be required at each of these locations.

### 8.5.2 Wireless Connectivity

Network Sensors with Wireless NIC is used to detect wireless packets and identify SSIDs that are both Internal to your network and External (Neighboring) to your network. Placement of the Network Sensor with Wireless NIC is critical as you do not want to place this in a Data closet where you will only detect Wireless SSIDs near the data closet. You will want to place the Network Sensor with Wireless NIC centrally to where you can detect the majority of the SSIDs around it.

### 8.5.3 ZTNA Gateway - Policy Server Connectivity

Both Policy Servers and ZTNA Gateways may be installed in the Cloud or On-Prem. Depending on which components are deployed where will dictate what connectivity is required through Cloud and On-Prem network firewalls and ACLs.

### 8.5.4 Firewall Requirements

The following connections must be allowed for Genian ZTNA to function properly.

[On-Premises]

| SRC IP | DST IP | Service | Note |
|---|---|---|---|
| Policy Server | Log Server<br>DB Server<br>Network Sensor IP, PC IP (Agent)<br>https://alarm2.genians.com<br>https://geniupdate2.genians.com<br>https://cmupdate2.genians.com<br>https://techlab2.genians.com<br>https://pi-api.genians.com<br>https://dzxsljwmt8reh.cloudfront.net<br>https://tuf-repo-cdn.sigstore.dev<br>https://rekor.sigstore.dev | TCP/9200~9300, TCP/9300~9400<br>TCP/3306<br>UDP/3871<br>TCP/8844<br>TCP/8844<br>TCP/8844<br>TCP/8844<br>TCP/443<br>TCP/443<br>TCP/443<br>TCP/443 | Log Server<br>Database<br>Keep Alive, Event Transmission<br>Alarm Service<br>GenianData Update<br>GenianData Update<br>Platform Miss/False Detection Report<br>Genian DPI<br>Syscollect Update<br>SLSA Verification<br>SLSA Verification |
| Network Sensor IP | Policy Server IP/FQDN | UDP/3870<br>TCP/80, TCP/443<br>UDP/514, TCP/6514 | Keep Alive<br>Policy/Action Information Update<br>Syslog |
| | https://dzxsljwmt8reh.cloudfront.net | TCP/443 | Syscollect Update |
| PC IP (Agent) | Policy Server IP/FQDN | UDP/3870<br>TCP/80, TCP/443<br>TCP/8000 | Keep Alive<br>Policy/Action Information Update<br>Windows Update |
| Admin PC | Policy Server IP, Network Sensor IP<br>Policy Server IP | TCP/3910<br>TCP/8443 | SSH<br>Web Console |

[Cloud managed]

| SRC IP | DST IP | Service | Note |
|---|---|---|---|
| Policy Server IP | 52.78.17.154 (geniupdate.geninetworks.com) | TCP/80, TCP/443 | **GENIAN Data** Update |
| Network Sensor IP | Policy Server IP/FQDN | UDP/Random<br>TCP/80, TCP/443<br>UDP/Random, TCP/Random | Keep Alive<br>Update Information/Policy<br>Syslog |
| PC IP (Agent) | Policy Server IP/FQDN | UDP/Random<br>TCP/80, TCP/443,<br>UDP/Random, TCP/Random | Keep Alive<br>Update Information/Policy<br>Windows Update |

**Note:** **UNIQUE PORT:** Specific Port Info for the Cloud Managed Policy Server can be found in the Web Console by selecting **System** on the top panel, and then selecting **Service > Port** from the left menu bar.

**Note:** **Keep Alive** traffic is sent from all Sensor interfaces, including Vlan interfaces (ethX, and ethx.x)

CHAPTER

NINE

# INSTALLING GENIAN ZTNA

This chapter guides you through installing Genian ZTNA on your system and accessing the administrator Web and CLI Console.

## 9.1 Installing Ubuntu OS

Before installing ZTNA, you must first install **Ubuntu OS 24.04**.

**Note:**

In virtualized environments, it is recommended to set **secure boot** to **disabled** before installing Ubuntu OS.
When secure boot is enabled, some modules may not load properly.
VMware secure boot settings

### 9.1.1 Prepare Hardware

You can install the Policy Server on a physical system or a virtual machine.

#### Minimum Requirements

| Component | CPU | Memory | Disk |
|---|---|---|---|
| ZTNA Policy Server | Intel® Core i3-12100 @ 3.3GHz (4C8T) or higher | DDR4 16GB or higher | SSD 512GB or higher |
| ZTNA Network Sensor | Intel® Processor N95 @ Max 3.4GHz (4C4T) or higher | DDR4 4GB or higher | SSD 128GB or higher |

**Note:**

You can install the Policy Server on a virtual machine.
ZTNA supports various hypervisors such as VMware, VirtualBox, and XenServer.

## 9.1.2 Prerequisites

1. **Prepare the image file**
   - Download Ubuntu 24.04.4 LTS image from the official Ubuntu website.
   - The **Ubuntu Server** version is recommended.
2. **If installing on hardware, create a bootable USB**
   - bootable-usb
3. **If installing on an AWS instance**
   - Prepare the instance according to your cloud provider's documentation (e.g., AWS EC2 Launch Instance guide).

## 9.1.3 Install Ubuntu 24.04.4 LTS

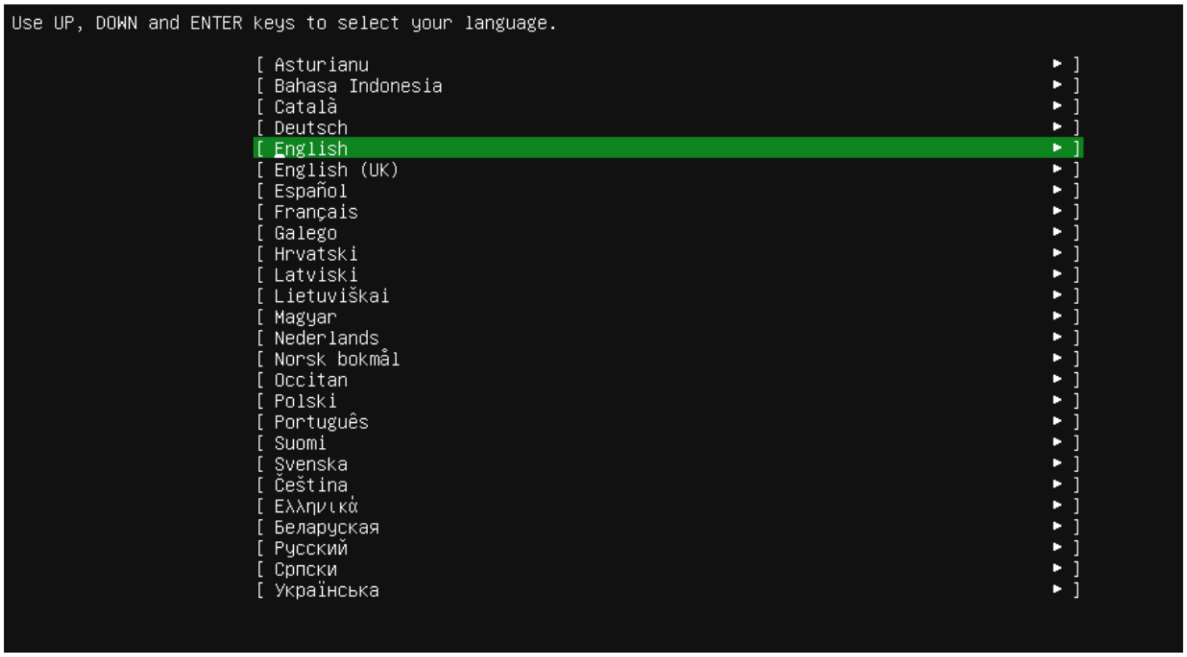
Install **Ubuntu Server** using the image file downloaded from the official Ubuntu website.

### Step 1: Boot the device

- If installing on hardware: Boot the device using the **bootable USB**.
- If installing in a virtual machine: Attach the downloaded **ISO file** to the VM and boot.

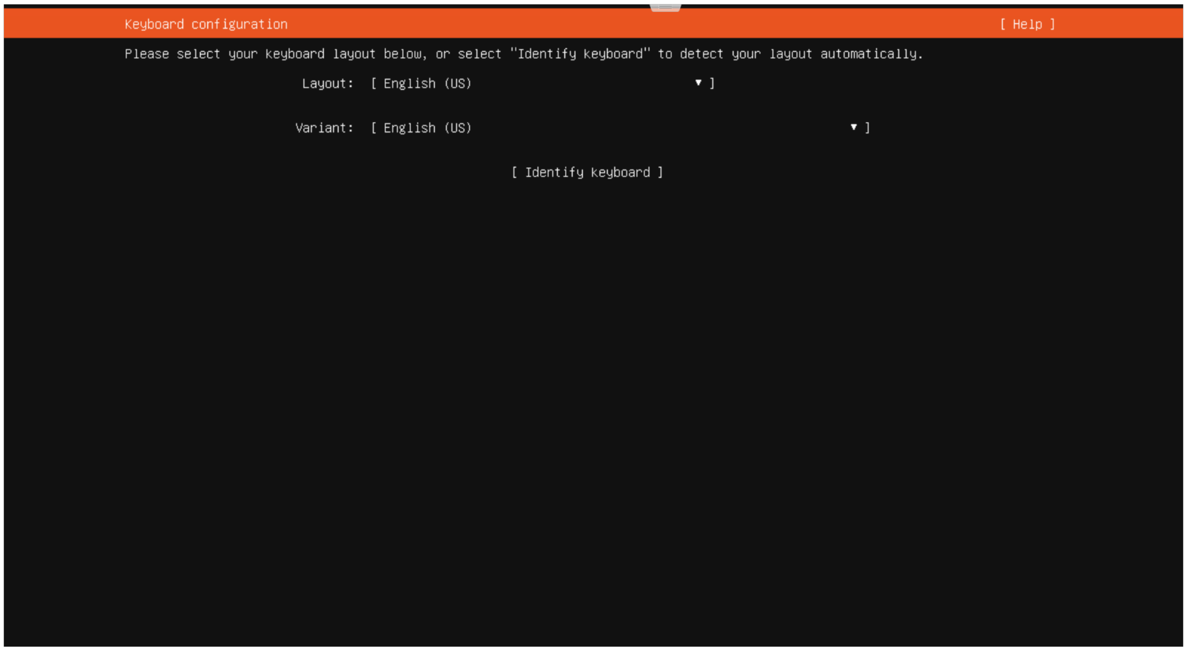
### Step 2: Install Ubuntu

1. Boot from the bootable media that contains the Ubuntu Server installation image.
2. Select the **language** that suits your environment.



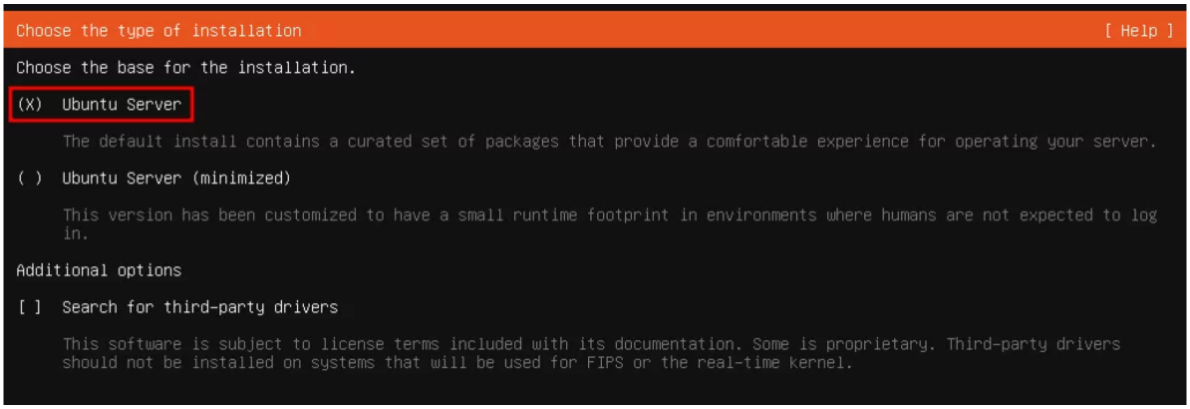
```
Use UP, DOWN and ENTER keys to select your language.

                        [ Asturianu                                                    ▶ ]
                        [ Bahasa Indonesia                                             ▶ ]
                        [ Català                                                       ▶ ]
                        [ Deutsch                                                      ▶ ]
                        [ English                                                      ▶ ]
                        [ English (UK)                                                 ▶ ]
                        [ Español                                                      ▶ ]
                        [ Français                                                     ▶ ]
                        [ Galego                                                       ▶ ]
                        [ Hrvatski                                                     ▶ ]
                        [ Latviski                                                     ▶ ]
                        [ Lietuviškai                                                  ▶ ]
                        [ Magyar                                                       ▶ ]
                        [ Nederlands                                                   ▶ ]
                        [ Norsk bokmål                                                 ▶ ]
                        [ Occitan                                                      ▶ ]
                        [ Polski                                                       ▶ ]
                        [ Português                                                    ▶ ]
                        [ Suomi                                                        ▶ ]
                        [ Svenska                                                      ▶ ]
                        [ Čeština                                                      ▶ ]
                        [ Ελληνικά                                                     ▶ ]
                        [ Беларуская                                                   ▶ ]
                        [ Русский                                                      ▶ ]
                        [ Српски                                                       ▶ ]
                        [ Українська                                                   ▶ ]
```

3. Configure the **keyboard layout**.



```
Keyboard configuration                                                                  [ Help ]
Please select your keyboard layout below, or select "Identify keyboard" to detect your layout automatically.
                          Layout:  [ English (US)                              ▾ ]

                         Variant:  [ English (US)                                                  ▾ ]

                                                [ Identify keyboard ]
```

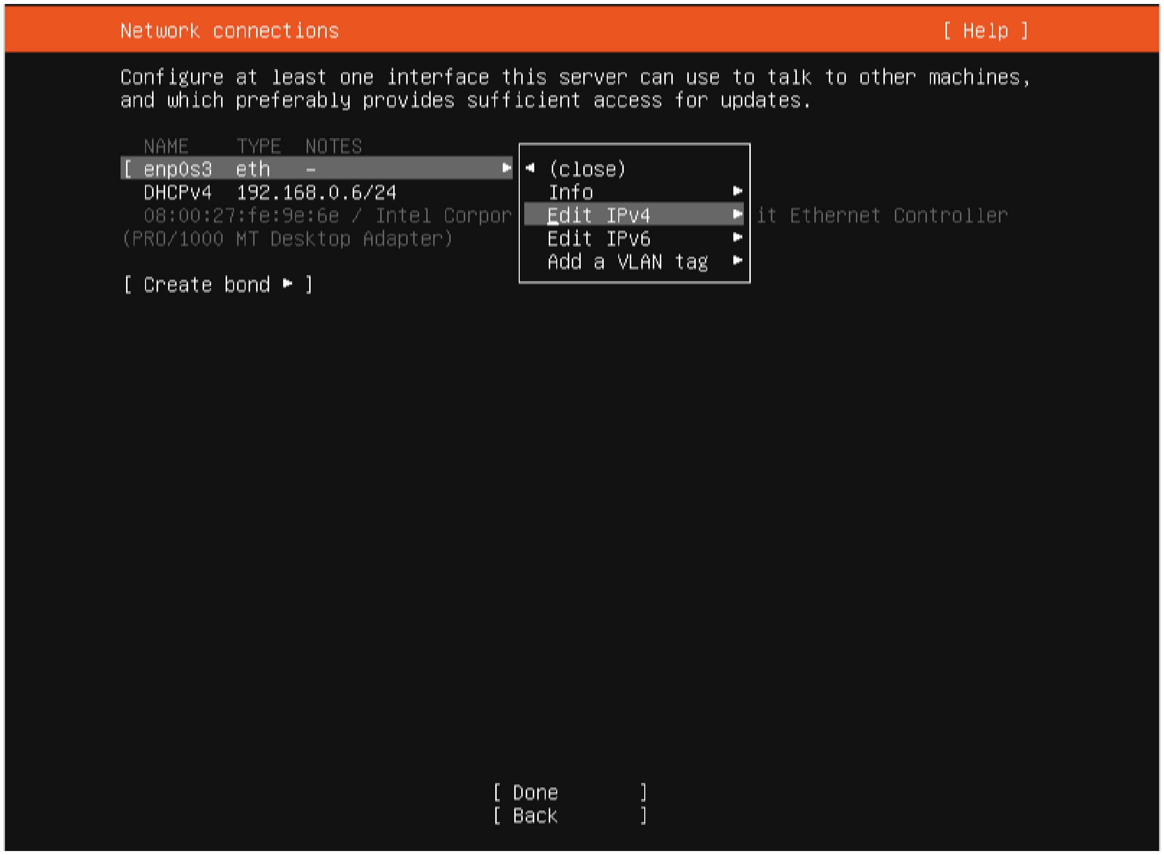
4. Select **Ubuntu Server** as the installation type.



```
Choose the type of installation                                                          [ Help ]
Choose the base for the installation.
(X)  Ubuntu Server
     The default install contains a curated set of packages that provide a comfortable experience for operating your server.
( )  Ubuntu Server (minimized)
     This version has been customized to have a small runtime footprint in environments where humans are not expected to log
     in.
Additional options
[ ]  Search for third-party drivers
     This software is subject to license terms included with its documentation. Some is proprietary. Third-party drivers
     should not be installed on systems that will be used for FIPS or the real-time kernel.
```

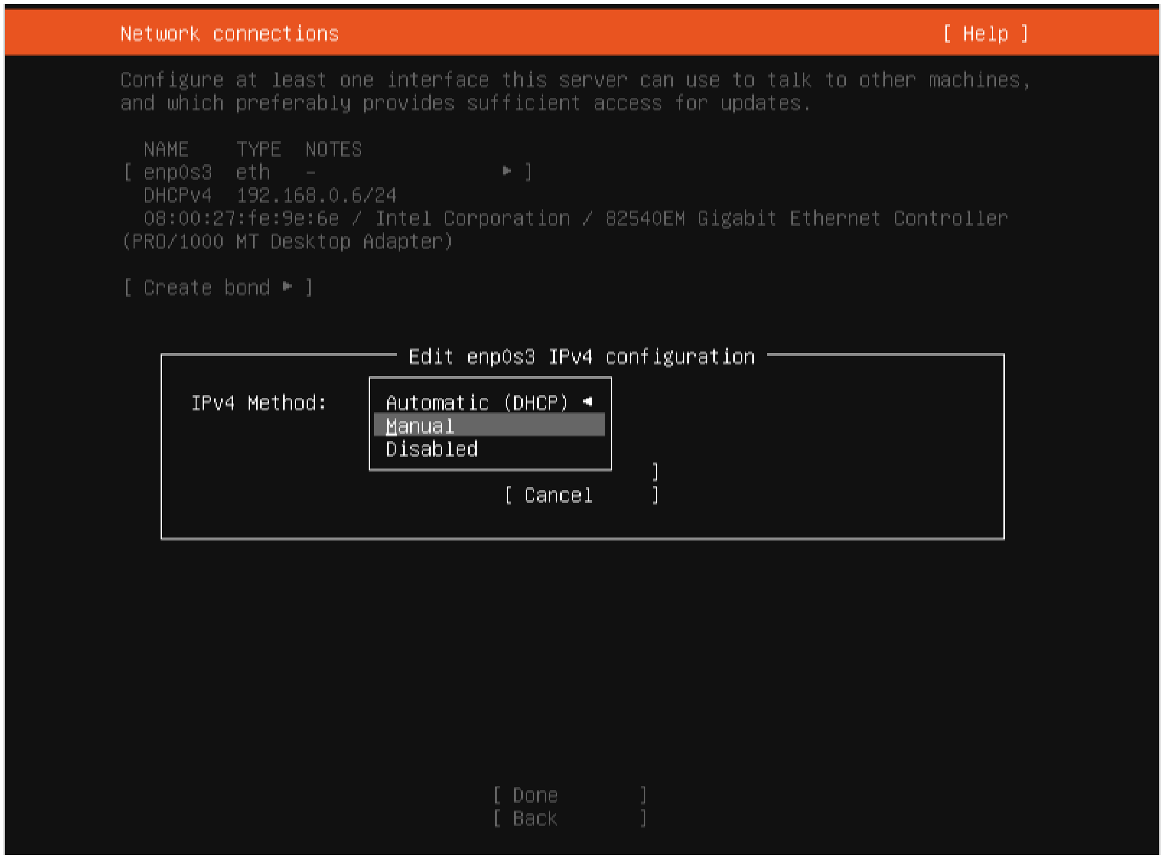
5. For network configuration, select the **network interface** in use.

6. Select **Edit IPv4**.



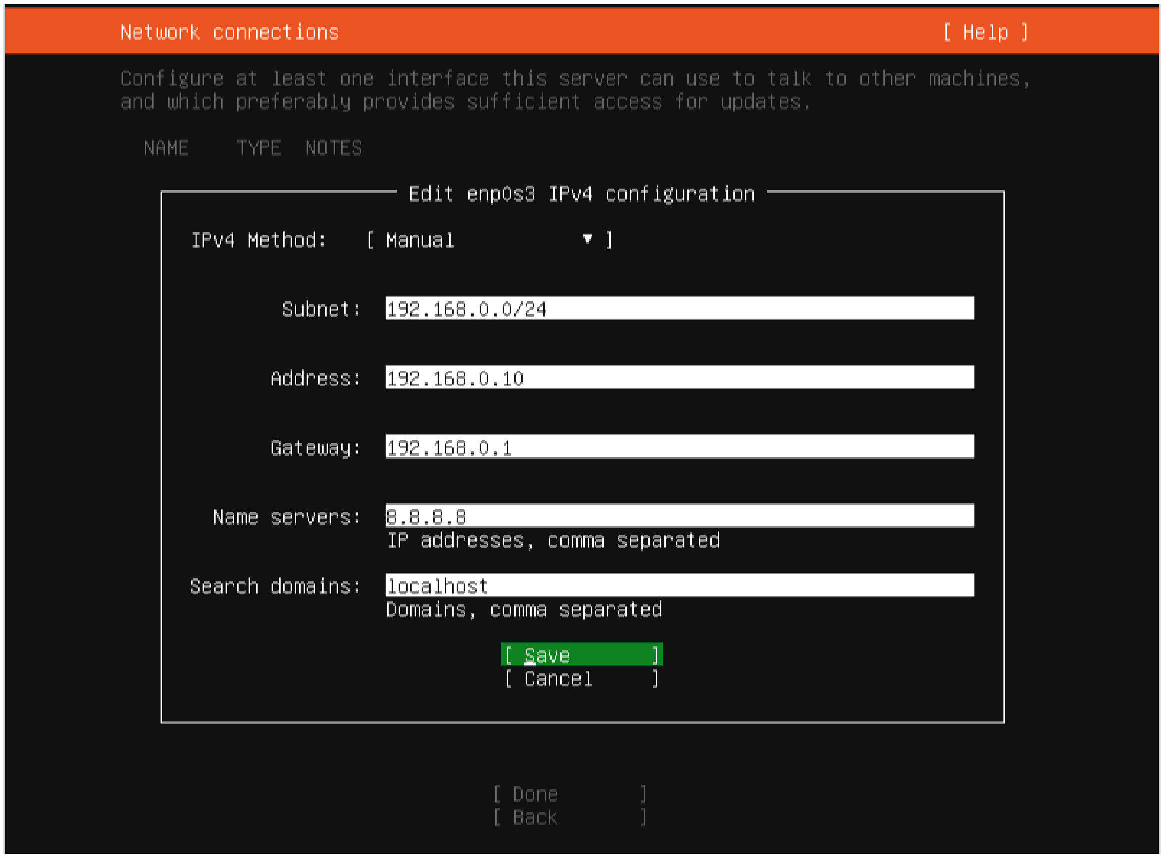
```
Network connections                                                        [ Help ]

Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

  NAME     TYPE   NOTES
[ enp0s3   eth    -                ▸ ◂ (close)
  DHCPv4   192.168.0.6/24              Info          ▸
  08:00:27:fe:9e:6e / Intel Corpor    Edit IPv4     ▸ it Ethernet Controller
(PRO/1000 MT Desktop Adapter)          Edit IPv6     ▸
                                       Add a VLAN tag ▸
[ Create bond ▸ ]

                                [ Done        ]
                                [ Back        ]
```

7. Change **Automatic (DHCP)** to **Manual**.



```
Network connections                                                    [ Help ]

Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

  NAME    TYPE  NOTES
[ enp0s3  eth   -                   ▶ ]
  DHCPv4  192.168.0.6/24
  08:00:27:fe:9e:6e / Intel Corporation / 82540EM Gigabit Ethernet Controller
(PRO/1000 MT Desktop Adapter)

[ Create bond ▶ ]

   ──────────────── Edit enp0s3 IPv4 configuration ──────────────────
   IPv4 Method:   Automatic (DHCP) ◀
                  Manual
                  Disabled
                                       ]
                            [ Cancel   ]

                              [ Done       ]
                              [ Back       ]
```

8. Enter the values according to the table below and select **Save**.

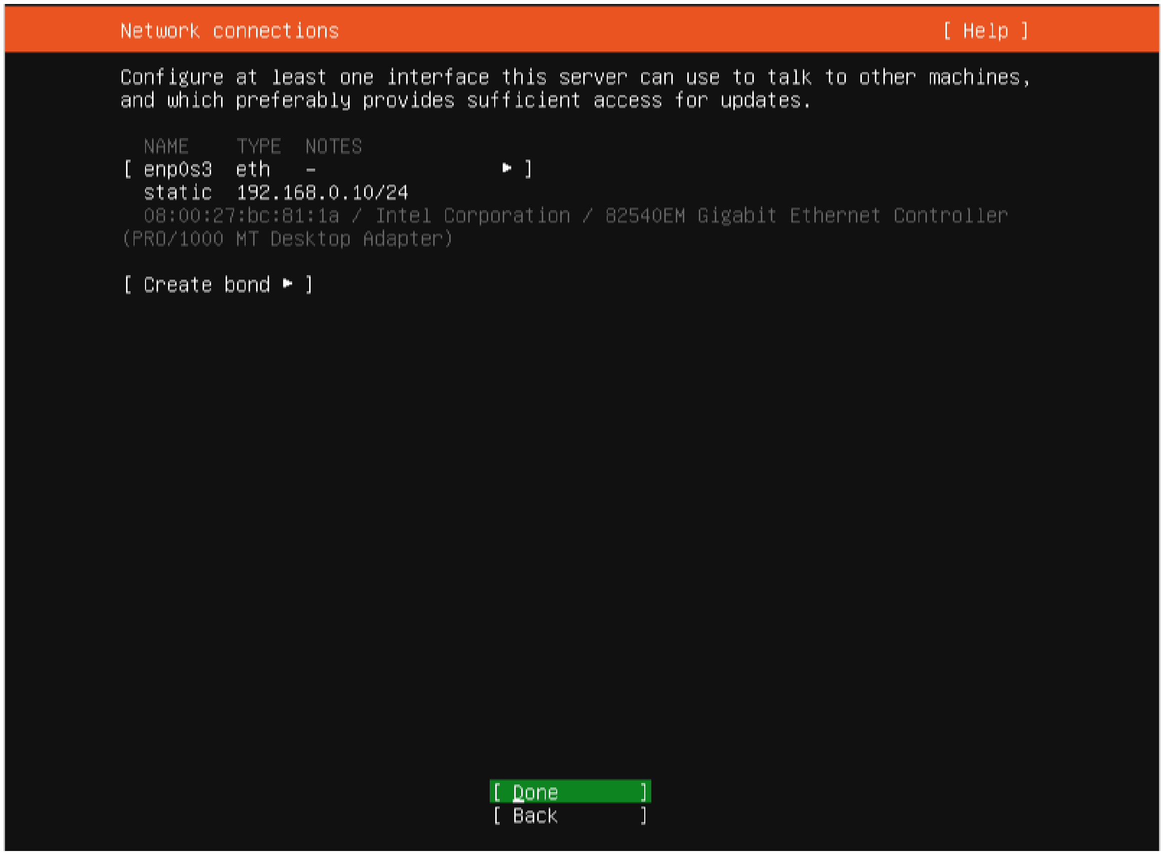


```
Network connections                                              [ Help ]

Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

  NAME    TYPE  NOTES

          ────────────── Edit enp0s3 IPv4 configuration ──────────────

          IPv4 Method:    [ Manual              ▼ ]

                 Subnet:  192.168.0.0/24

                Address:  192.168.0.10

                Gateway:  192.168.0.1

           Name servers:  8.8.8.8
                          IP addresses, comma separated

         Search domains:  localhost
                          Domains, comma separated

                                    [ Save       ]
                                    [ Cancel     ]

                                   [ Done        ]
                                   [ Back        ]
```

**Note:**

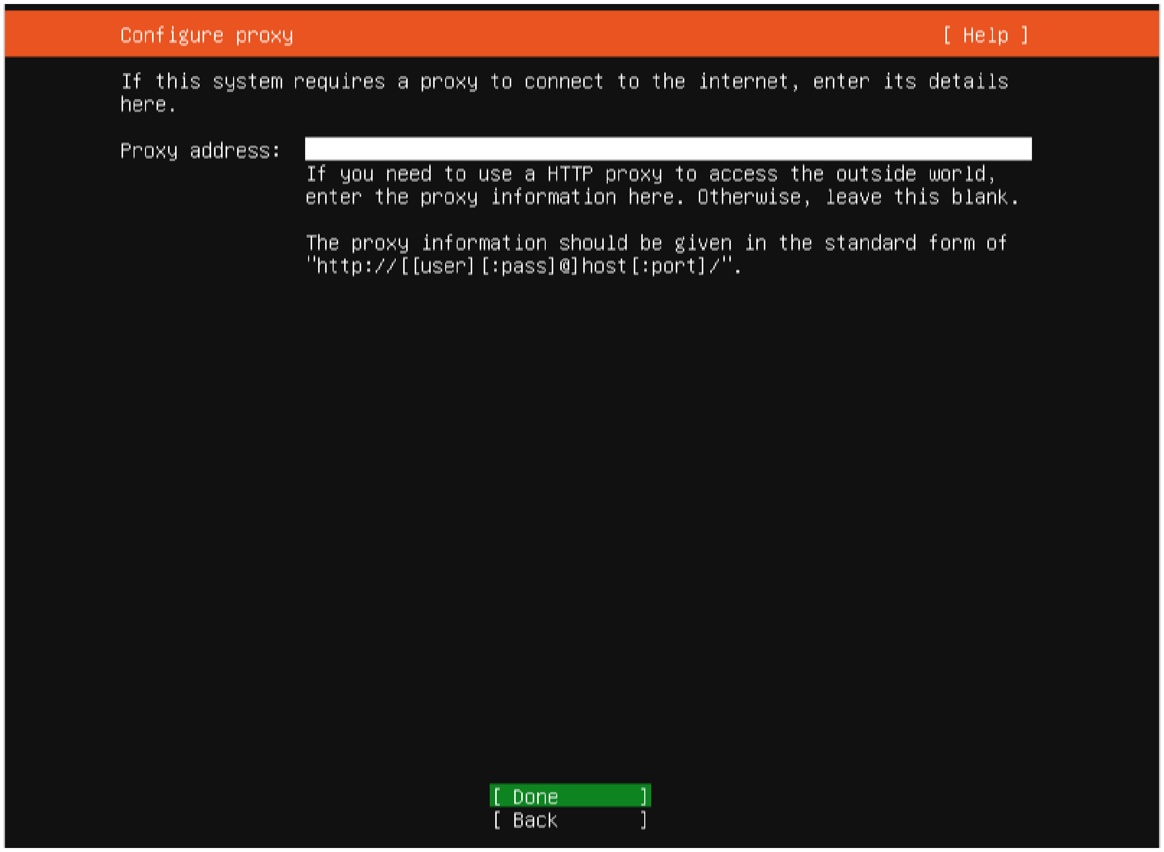
| Field (Required) | Description |
|---|---|
| Subnet | Subnet mask |
| Address | Static IP address assigned to the device |
| Gateway | Gateway address |
| Name Server | DNS server address |
| Search domains | Leave blank |

9. Verify that the configured **static IP** has been applied.



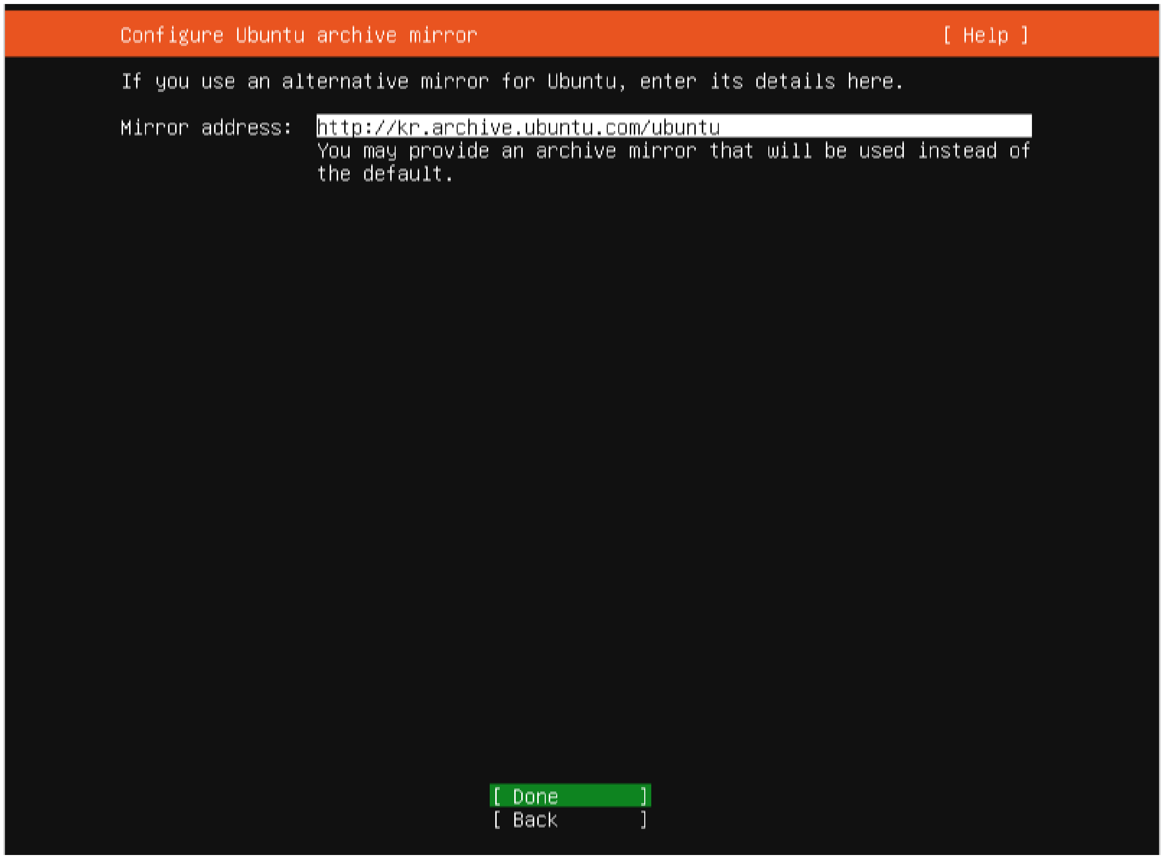
```
Network connections                                                    [ Help ]

Configure at least one interface this server can use to talk to other machines,
and which preferably provides sufficient access for updates.

  NAME    TYPE  NOTES
[ enp0s3  eth   -                ► ]
  static  192.168.0.10/24
  08:00:27:bc:81:1a / Intel Corporation / 82540EM Gigabit Ethernet Controller
(PRO/1000 MT Desktop Adapter)

[ Create bond ► ]
```

10. If using a proxy server, enter the **Address**; otherwise, leave it blank and select **Done**.



```
Configure proxy                                                        [ Help ]

If this system requires a proxy to connect to the internet, enter its details
here.

Proxy address:
                 If you need to use a HTTP proxy to access the outside world,
                 enter the proxy information here. Otherwise, leave this blank.

                 The proxy information should be given in the standard form of
                 "http://[[user][:pass]@]host[:port]/".
```

11. If you have a preferred **Ubuntu Mirror Server**, set it; otherwise, use the automatically populated value and select **Done**.



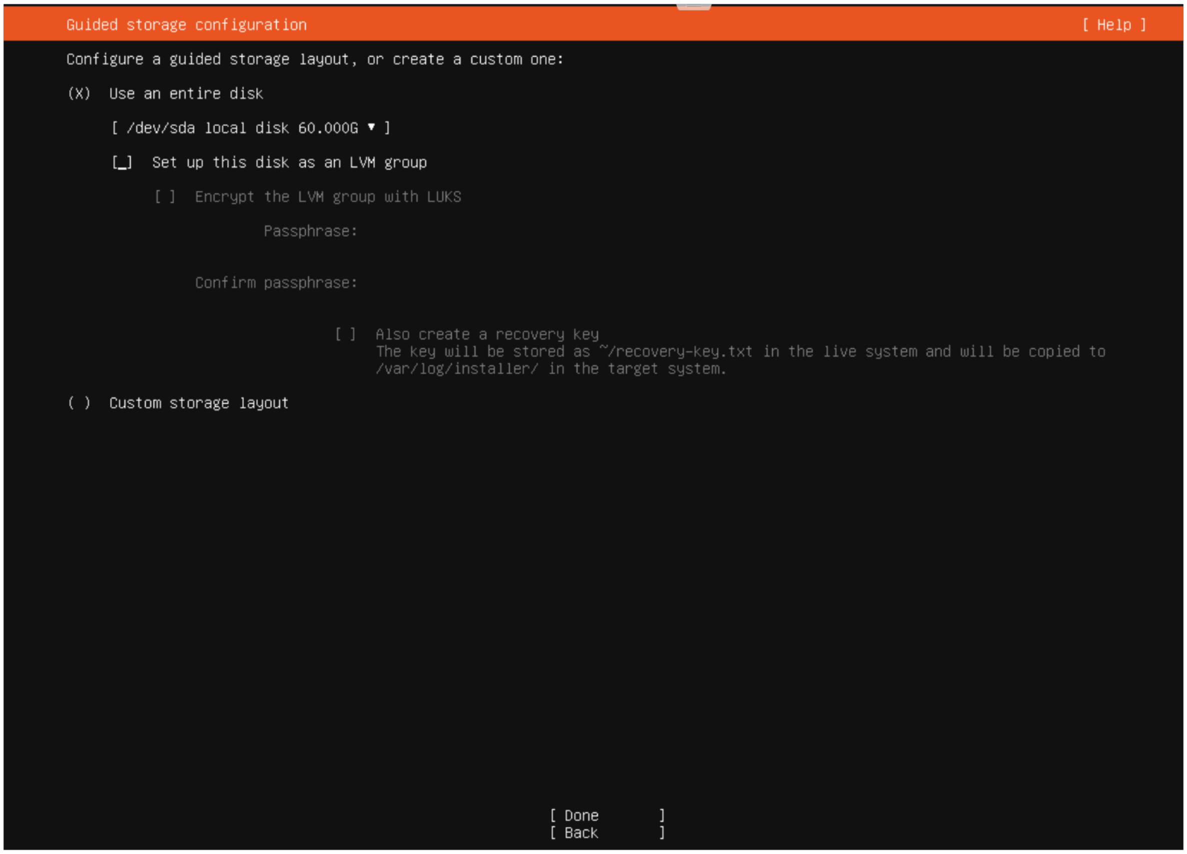
Configure Ubuntu archive mirror

If you use an alternative mirror for Ubuntu, enter its details here.

Mirror address: http://kr.archive.ubuntu.com/ubuntu

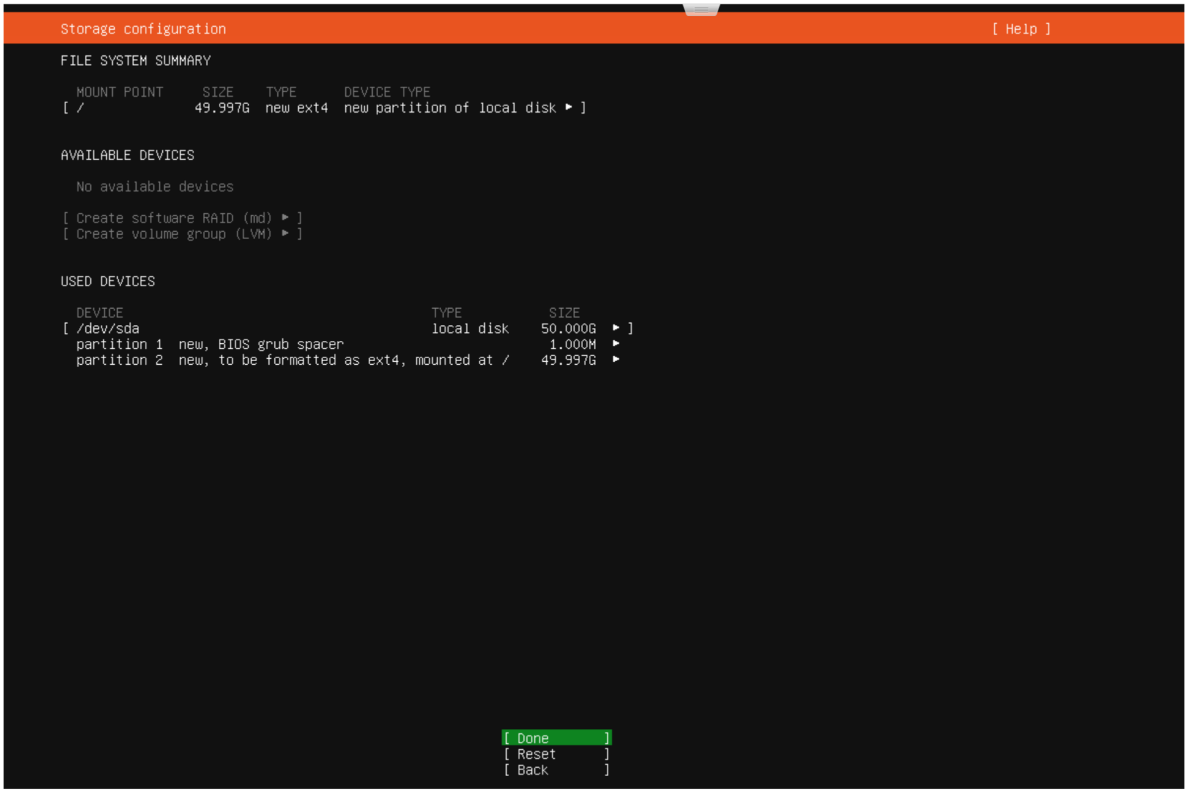
You may provide an archive mirror that will be used instead of the default.

12. Uncheck **Set up this disk as an LVM group** and select **Done**.



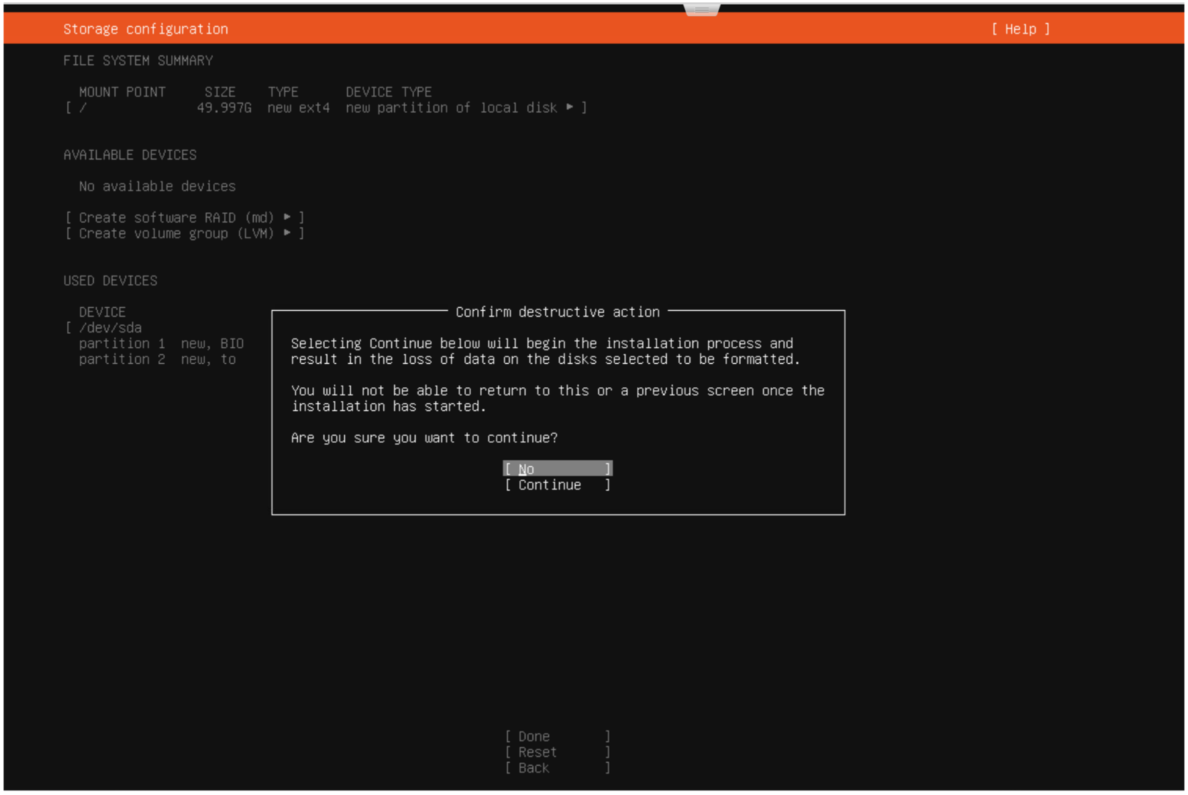
```
Guided storage configuration                                                        [ Help ]
Configure a guided storage layout, or create a custom one:

(X)  Use an entire disk

     [ /dev/sda local disk 60.000G ▾ ]

     [ ]  Set up this disk as an LVM group

          [ ]  Encrypt the LVM group with LUKS

                       Passphrase:


               Confirm passphrase:


                                [ ]  Also create a recovery key
                                     The key will be stored as ~/recovery-key.txt in the live system and will be copied to
                                     /var/log/installer/ in the target system.

( )  Custom storage layout











                                              [ Done       ]
                                              [ Back       ]
```

13. Review the **partition/file system** changes and select **Done**.



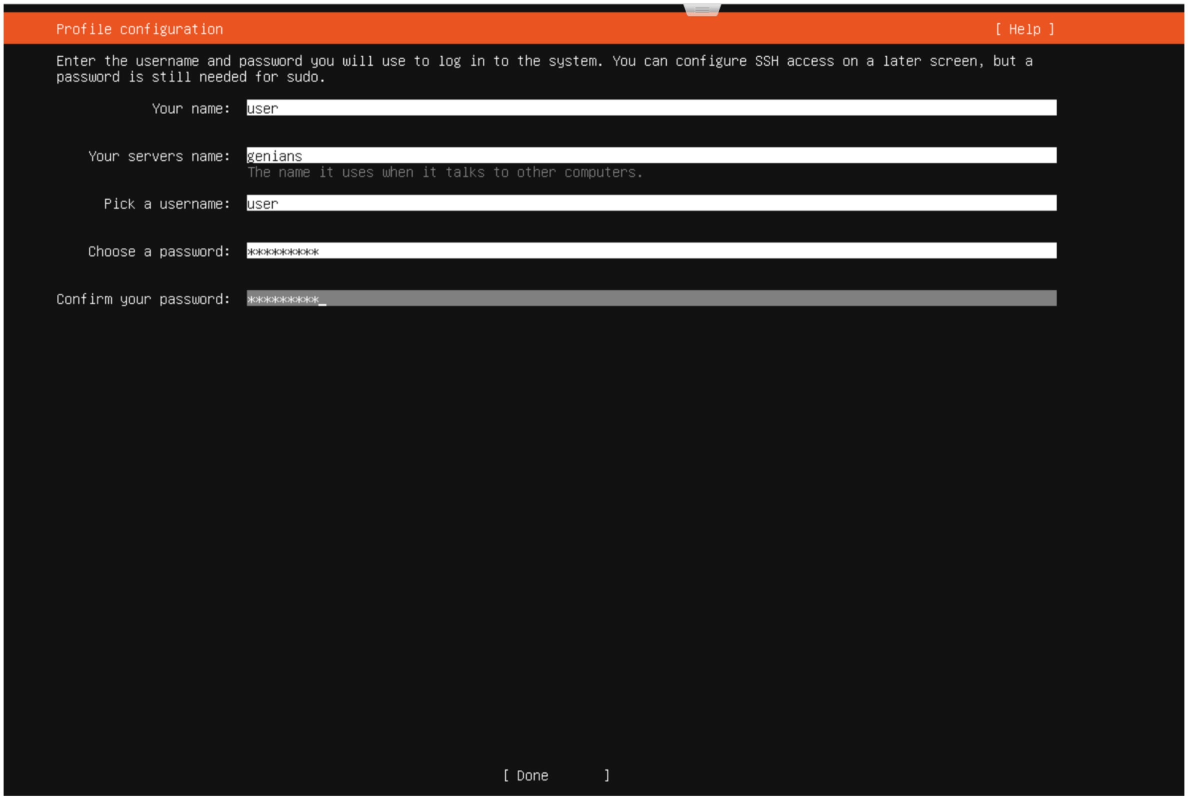
```
Storage configuration                                                  [ Help ]
FILE SYSTEM SUMMARY

  MOUNT POINT     SIZE    TYPE      DEVICE TYPE
[ /              49.997G  new ext4  new partition of local disk ▸ ]


AVAILABLE DEVICES

  No available devices

[ Create software RAID (md) ▸ ]
[ Create volume group (LVM) ▸ ]


USED DEVICES

  DEVICE                                     TYPE          SIZE
[ /dev/sda                                   local disk    50.000G  ▸ ]
  partition 1  new, BIOS grub spacer                        1.000M  ▸
  partition 2  new, to be formatted as ext4, mounted at /  49.997G  ▸













                                             [ Done      ]
                                             [ Reset     ]
                                             [ Back      ]
```

14. If there are **no issues** with the partition changes, select **Continue**.



```
Storage configuration                                                            [ Help ]
FILE SYSTEM SUMMARY

  MOUNT POINT     SIZE    TYPE      DEVICE TYPE
[ /              49.997G  new ext4  new partition of local disk ► ]

AVAILABLE DEVICES

  No available devices

[ Create software RAID (md) ► ]
[ Create volume group (LVM) ► ]

USED DEVICES

  DEVICE                 ┌────────────────────── Confirm destructive action ─────────────────────┐
[ /dev/sda               │                                                                        │
  partition 1  new, BIO  │ Selecting Continue below will begin the installation process and      │
  partition 2  new, to   │ result in the loss of data on the disks selected to be formatted.     │
                         │                                                                        │
                         │ You will not be able to return to this or a previous screen once the  │
                         │ installation has started.                                              │
                         │                                                                        │
                         │ Are you sure you want to continue?                                     │
                         │                                                                        │
                         │                         [ No         ]                                 │
                         │                         [ Continue   ]                                 │
                         │                                                                        │
                         └────────────────────────────────────────────────────────────────────────┘

                                         [ Done       ]
                                         [ Reset      ]
                                         [ Back       ]
```

15. Enter the **Ubuntu OS user information** using the table below and select **Done**.

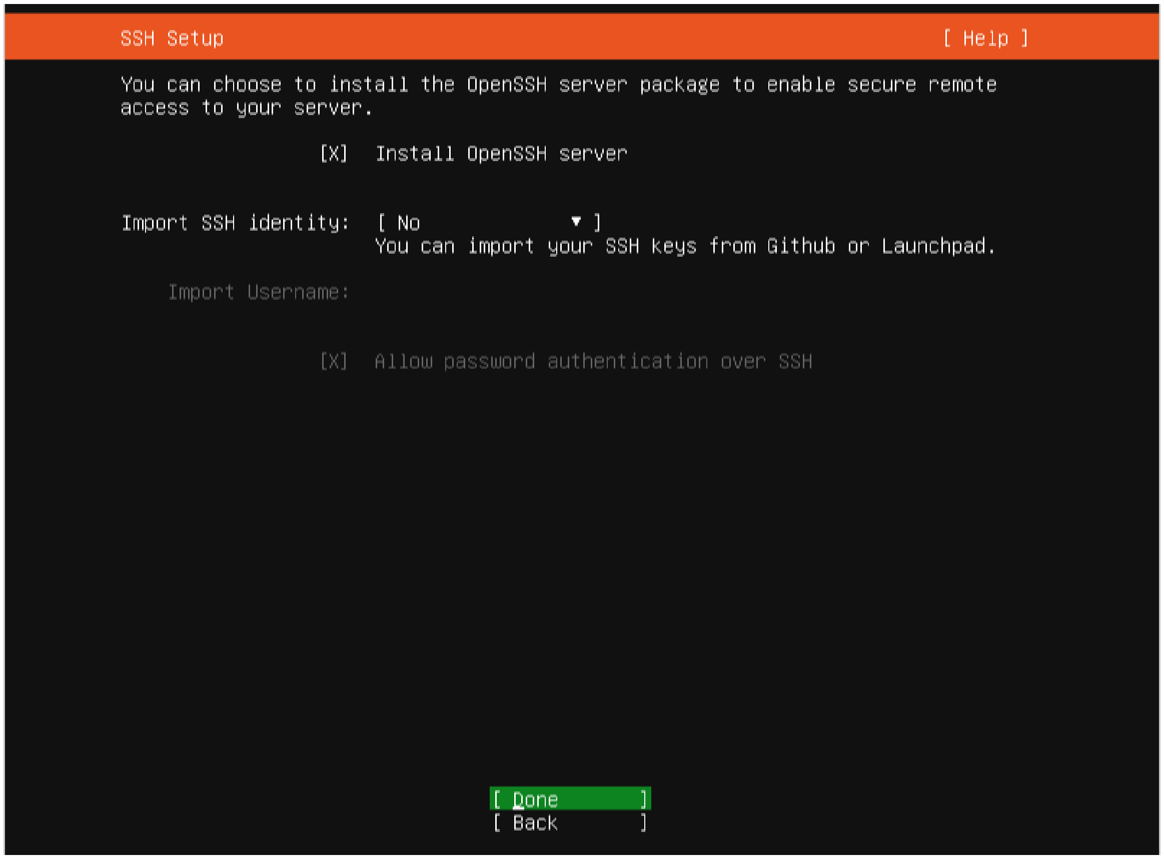


```
Profile configuration                                                              [ Help ]
Enter the username and password you will use to log in to the system. You can configure SSH access on a later screen, but a
password is still needed for sudo.

            Your name: user

    Your servers name: genians
                       The name it uses when it talks to other computers.

      Pick a username: user

    Choose a password: *********

Confirm your password: *********_

                                        [ Done       ]
```

**Note:**

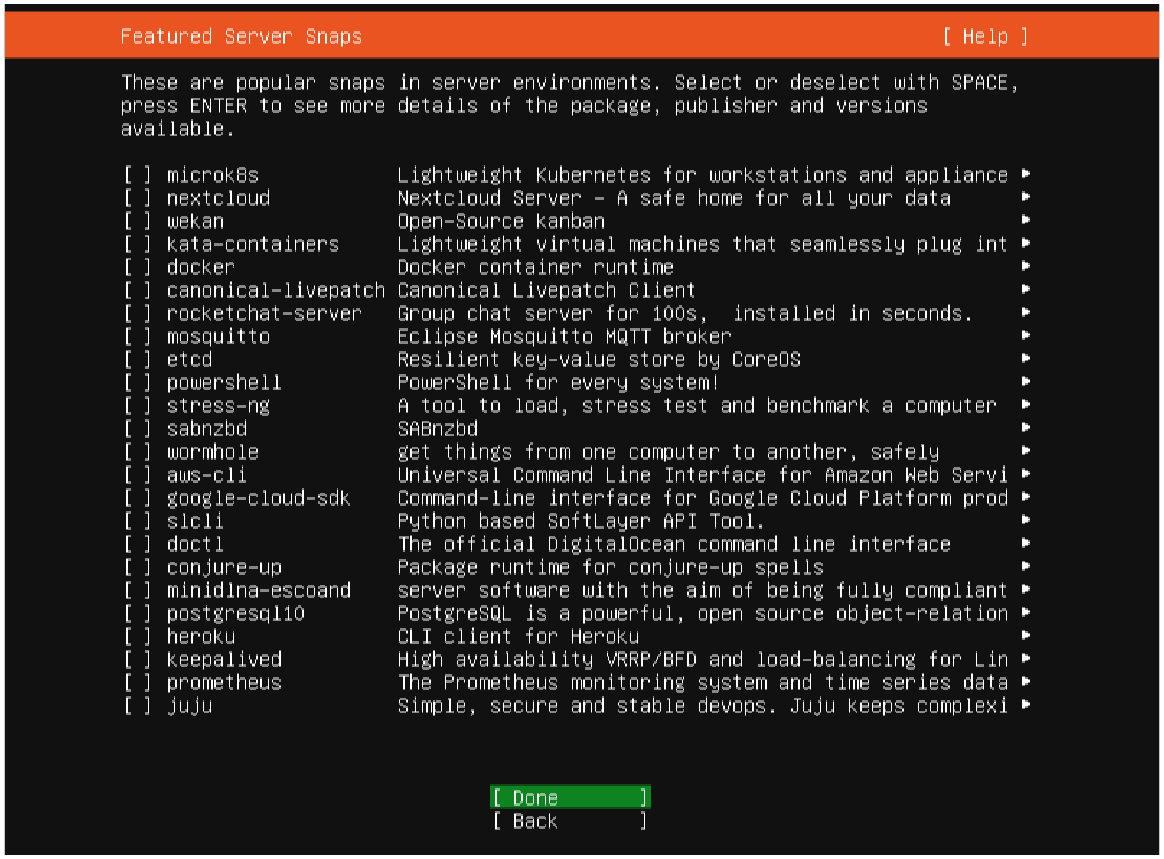
| Field (Required) | Description |
|---|---|
| Your name | User name |
| Your computer's name | Device name |
| Pick a username | Ubuntu login account (ID) |
| Choose a password | Login password |
| Confirm your password | Confirm login password |

16. Check **Install OpenSSH server** for remote access.



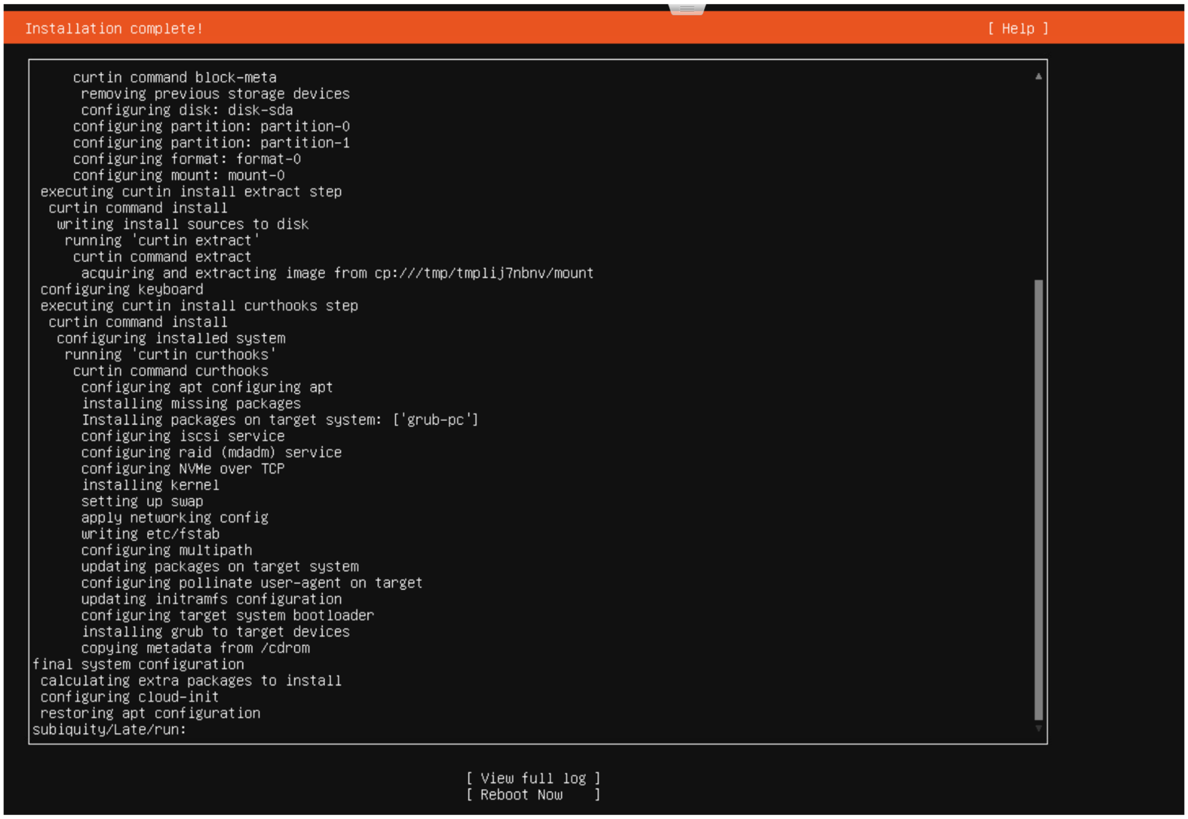
```
SSH Setup                                                        [ Help ]

You can choose to install the OpenSSH server package to enable secure remote
access to your server.

                 [X]  Install OpenSSH server


Import SSH identity:  [ No              ▼ ]
                      You can import your SSH keys from Github or Launchpad.

    Import Username:


                 [X]  Allow password authentication over SSH
```

17. Do **not** install additional features; select **Done**.



```
Featured Server Snaps                                                  [ Help ]

These are popular snaps in server environments. Select or deselect with SPACE,
press ENTER to see more details of the package, publisher and versions
available.

[ ] microk8s            Lightweight Kubernetes for workstations and appliance ►
[ ] nextcloud           Nextcloud Server - A safe home for all your data      ►
[ ] wekan               Open-Source kanban                                    ►
[ ] kata-containers     Lightweight virtual machines that seamlessly plug int ►
[ ] docker              Docker container runtime                              ►
[ ] canonical-livepatch Canonical Livepatch Client                            ►
[ ] rocketchat-server   Group chat server for 100s,  installed in seconds.    ►
[ ] mosquitto           Eclipse Mosquitto MQTT broker                         ►
[ ] etcd                Resilient key-value store by CoreOS                   ►
[ ] powershell          PowerShell for every system!                          ►
[ ] stress-ng           A tool to load, stress test and benchmark a computer  ►
[ ] sabnzbd             SABnzbd                                               ►
[ ] wormhole            get things from one computer to another, safely       ►
[ ] aws-cli             Universal Command Line Interface for Amazon Web Servi ►
[ ] google-cloud-sdk    Command-line interface for Google Cloud Platform prod ►
[ ] slcli               Python based SoftLayer API Tool.                      ►
[ ] doctl               The official DigitalOcean command line interface      ►
[ ] conjure-up          Package runtime for conjure-up spells                 ►
[ ] minidlna-escoand    server software with the aim of being fully compliant ►
[ ] postgresql10        PostgreSQL is a powerful, open source object-relation ►
[ ] heroku              CLI client for Heroku                                 ►
[ ] keepalived          High availability VRRP/BFD and load-balancing for Lin ►
[ ] prometheus          The Prometheus monitoring system and time series data ►
[ ] juju                Simple, secure and stable devops. Juju keeps complexi ►


                                [ Done       ]
                                [ Back       ]
```

18. When **Install complete** appears at the top left, select **Reboot Now**.



```
Installation complete!                                                                     [ Help ]

     curtin command block-meta
      removing previous storage devices
      configuring disk: disk-sda
     configuring partition: partition-0
     configuring partition: partition-1
     configuring format: format-0
     configuring mount: mount-0
 executing curtin install extract step
  curtin command install
   writing install sources to disk
    running 'curtin extract'
     curtin command extract
      acquiring and extracting image from cp:///tmp/tmplij7nbnv/mount
 configuring keyboard
 executing curtin install curthooks step
  curtin command install
   configuring installed system
    running 'curtin curthooks'
     curtin command curthooks
      configuring apt configuring apt
      installing missing packages
      Installing packages on target system: ['grub-pc']
      configuring iscsi service
      configuring raid (mdadm) service
      configuring NVMe over TCP
      installing kernel
      setting up swap
      apply networking config
      writing etc/fstab
      configuring multipath
      updating packages on target system
      configuring pollinate user-agent on target
      updating initramfs configuration
      configuring target system bootloader
      installing grub to target devices
      copying metadata from /cdrom
final system configuration
 calculating extra packages to install
 configuring cloud-init
 restoring apt configuration
subiquity/Late/run:

                                        [ View full log ]
                                        [ Reboot Now    ]
```

19. Log in with the user information you entered earlier.

### 9.1.4 Next Steps After Installation

Ubuntu Server installation is complete. Proceed with the next installation according to your use case.

- *Install Policy Server*
- *Install Network Sensor*
- Install ZTNA Gateway

## 9.2 Installing Policy Server

### 9.2.1 Deployment Models

You can install the Policy Server in two ways depending on scale and management method.

| Type | Description | Note |
|---|---|---|
| **On-premises** | Install the Policy Server inside your network to manage policies and network resources. | |
| **Cloud managed** | Deploy a virtual Policy Server in a cloud environment. Administrators manage policies and networks via the cloud console and Web UI. | Before deploying in the cloud, prepare the cloud environment (VPC, subnets, security groups) per your provider's documentation. |

### 9.2.2 Prepare the Environment

You can install the Policy Server on a physical system or a virtual machine.
Refer to *Install Ubuntu OS* to prepare **Ubuntu OS 24.04.4 LTS**.

**Note:**

You can install the Policy Server on a virtual machine.
ZTNA supports various hypervisors such as VMware, VirtualBox, and XenServer.

### 9.2.3 Prepare Network Connectivity

Genian ZTNA requires at least one static IP address for network connectivity.
For an on-premises deployment, that interface can be used as the management interface.
Genian ZTNA connects to the network broadcast domain to monitor all broadcast packets.
If the target network is reachable only over a WAN, you need a separate, physically placed Network Sensor.

**Note:**

When using a virtual machine, select the network interface type as **Bridge** mode.
If you plan to use VMware ESXi with an 802.1Q trunk port, enable VGT mode. See
https://kb.vmware.com/s/article/1004252

### 9.2.4 Install the Policy Server

**Step 1: Switch to the root account**

```
genian@genian:~$ sudo su
[sudo] password for genian:
root@genian:/home/genian#
```

**Step 2: Update and upgrade packages**

```
root@genian:/home/genian# apt-get update
root@genian:/home/genian# apt-get upgrade
```

**Step 3: Install curl (required for installation)**

```
root@genian:/home/genian# apt install curl
```

**Step 4: Install Genian ZTNA Policy Center**

```
curl -sSLk https://bit.ly/4fX6bQ8 | sudo PROMPT=0 SSHALLALLOW=1 SSHPORT=22 TARGET=GPC␣
↪DEB=ztna LOCALE=en bash -
```

### 9.2.5 Configure the Policy Server

#### Step 1: Access Ubuntu and gnlogin

After installation completes, access Ubuntu and run gnlogin for initial setup.

```
genian@genian:~$ sudo su
[sudo] password for genian:
root@genian:/home/genian#
# Obtain root privileges
root@genian:/home/genian# gnlogin
# Enter Genian Shell
```

**Note:**

You must have root privileges to apply interface settings properly.

#### Step 2: Configure interfaces

Configure the default interface of the device.

1. Enter global configuration mode with the "enable" command.
2. Enter configuration mode with the "configure terminal" command.
3. Set the interface IP address and subnet mask.
4. Set the interface default gateway.
5. Set the device default gateway.
6. Set the device DNS server.
7. Set the device NTP server.

```
genian> enable
Password : (contact Technical Support for the enable password)
genian# configure terminal
genian(config)# interface [interface-name] address [IP] [Subnetmask]
genian(config)# interface [interface-name] gateway [IP]
genian(config)# ip default-gateway [IP]
genian(config)# ip name-server [IP]
genian(config)# ntp server [IP]
// If you configured interfaces during Ubuntu installation, some IP-related settings␣
↪may already be present.
```

#### Step 3: Configure the Database server

Set up the Database server.

1. Set the DB account.
2. Enable the DB server.
3. Set the DB access password.
4. Configure DB access permissions.

```
genian(config)# data-server username [DB-username]
genian(config)# data-server enable
genian(config)# data-server password [DB-password]
```

#### Step 4: Configure the Log Server

Start the Log Server.

```
genian(config)# log-server version 6
genian(config)# log-server enable
genian(config)# log-server publish-port [interface-name]
```

#### Step 5: Configure Web UI and SOAP Server

1. Enable the Web UI.
2. Enable the SOAP server.

```
genian(config)# interface [interface-name] management-server enable
genian(config)# interface [interface-name] node-server enable
```

#### Step 6: Create an administrator account

Create the administrator account for the Genian ZTNA Web UI. This can be set only once.

1. Create the Web UI account.

```
genian(config)# superadmin [admin-id] [admin-password] [admin-email]
```

**Note:**

The administrator password must be at least 9 characters and include letters, numbers, and special characters.

#### Step 7: Access the Web UI

After completing the steps above, log in to the Genian ZTNA Web UI and verify the installation.

**Note:**

For Web UI information, see *Administration Console*.

### 9.2.6 Unsupported hardware

If installation does not proceed normally, contact your partner engineer or Technical Support.

**Note:** If storage devices or network interfaces are not recognized in a virtual environment, change the storage type to SATA or change the network interface driver to an Intel family such as E1000.

### Reporting unsupported hardware

If you have unsupported hardware, such as storage devices, Ethernet adapters, or wireless LAN adapters, during the Genian ZTNA installation process, please collect the information through the following procedure and send it to us at help@genians.com.

1. Install generic Linux distribution like Ubuntu
2. Open Terminal
3. Type following command to create report.txt

   ```
   $ sudo apt install pciutils lshw
   $ dmesg > report.txt
   $ lspci >> report.txt
   $ lshw >> report.txt
   ```

4. Send us a report.txt file

# 9.3 Installing Network Sensor

The Network Sensor is installed in your internal network to collect information and send it to the Policy Server.
Depending on your network design, you may need to install one or more logical/physical Network Sensors.

## 9.3.1 Prepare the Environment

You can install the Network Sensor on a physical or virtual system.
Prepare **Ubuntu OS 24.04** by referring to the guide *Install Ubuntu OS*.

**Note:**

You can install the Network Sensor on a virtual machine.
ZTNA supports various hypervisors such as VMware, VirtualBox, and XenServer.

**Note:** Even if you use the Cloud version, the Network Sensor must be installed inside your internal network.

## 9.3.2 Prepare Network Connectivity

Genian Network Sensor requires network connectivity with one or more static IP addresses.

The sensor must monitor broadcast packets (ARP, DHCP, UPnP, etc.) on the network and be connected to all segments (broadcast domains) you plan to manage.

If you are using VLAN-capable switches, you can set up an 802.1Q trunk port to monitor multiple networks via a single physical interface.

When installing the Network Sensor in a virtual environment, the VM (sensor) must be able to directly communicate with all segments you want to monitor and control.

**Note:** When using a virtual machine, set the network interface type to **Bridge** mode.

To collect wireless LAN information, install a compatible wireless network adapter on the sensor. See the document below.

### Wireless Adapter Compatibility

See all wireless adapter compatible with Genian ZTNA. It can be confirmed by the community (Marked as "CC")

| Vendor | Model Name | Chipset | Band | Type | Status |
|---|---|---|---|---|---|
| AFOUNDRY | AF-PP-ABGN-01 | RT2770 | 2.4G | USB | |
| ALFA Network | AWUS050NH v1 | RT2770 | 2.4G | USB | |
| ALFA Network | AWUS050NH v2 | RT2770 | 2.4G | USB | |
| ALFA Network | AWUS051NH | RT2770 | 2.4G | USB | |
| ALFA Network | AWUS052NH | RT3572 | 2.4G/5G | USB | |
| ASUS | USB-N53 | RT3572 | 2.4G/5G | USB | |
| AVM | FRITZ!WLAN USB Stick N v2 | RT5572 | 2.4G/5G | USB | |
| AirLinkWiFi | UltraSky M27 | RT3572 | 2.4G/5G | USB | |
| Airlink101 | AWLL7025 | RT2870 | 2.4G | USB | |
| Alpha Net | WUS-ND02 | RT2870 | 2.4G | USB | |
| Alpha Net | WUS-ND12B | RT5572 | 2.4G/5G | USB | |
| AmbiCom | WL600N-USB | RT2870 | 2.4G | USB | |
| Askey | WLU5022 | RT3572 | 2.4G/5G | USB | |
| Belkin | F7D4501 Wireless Module | RT3572 | 2.4G/5G | USB | |
| Buffalo | WI-U2-300D | RT5572 | 2.4G/5G | USB | |
| Buffalo | WLI-UC-AG300N | RT2870 | 2.4G | USB | |
| Buffalo | WLP-UC-AG300 | RT2870 | 2.4G | USB | |
| Cameo | WLAN-1501 | RT2870 | 2.4G | USB | |
| Corega | CG-WLUSB300AGN | RT2870 | 2.4G | USB | |
| Cisco | AE1000 | RT3572 | 2.4G/5G | USB | CC |
| D-Link | DHD-131 Wireless Module | RT3572 | 2.4G/5G | USB | |
| D-Link | DWA-160 rev B1 | RT2870 | 2.4G | USB | |
| D-Link | DWA-160 rev B2 | RT5572 | 2.4G/5G | USB | |
| D-Link | DWA-160 rev C1 | RT5572 | 2.4G/5G | USB | |
| D-Link | DWA-160 | RT5592 | 2.4G/5G | USB | CC |
| Edimax | EW-7722UnD | RT3572 | 2.4G/5G | USB | |
| EnGenius | EUB600 v1 | RT3572 | 2.4G/5G | USB | |
| EnGenius | EUB600 v2 | RT5572 | 2.4G/5G | USB | |
| EnGenius | EUB9801 | RT3572 | 2.4G/5G | USB | |
| Gemtek | WUBR-208N | RT2870 | 2.4G | USB | |
| I-O DATA | WHG-AGDN/US | RT3572 | 2.4G/5G | USB | |
| Intel | Dual Band Wireless-AC3160 | | 2.4G/5G | HMC | CC |
| Intel | Dual Band Wireless-AC3160 | | 2.4G/5G | M.2 | CC |
| Intel | Dual Band Wireless-AC8260 | | 2.4G/5G | M.2 | CC |
| JJPlus | ExpandarMax9 (NR25UA5) | RT2770 | 2.4G | USB | |
| LG-Ericsson | USB-1040 | RT3572 | 2.4G/5G | USB | |
| LanReady | WUB2000H10 | RT3572 | 2.4G/5G | USB | |
| Lenovo | 03T8726 | RT5572 | 2.4G/5G | USB | |
| Linksys | AE1000 | RT3572 | 2.4G/5G | USB | |

continues on next page

Table 1 – continued from previous page

| Vendor | Model Name | Chipset | Band | Type | Status |
|---|---|---|---|---|---|
| Linksys | AE3000 | RT3593 | 2.4G/5G | USB | CC |
| Linksys | DMC350 Wireless Module | RT2870 | 2.4G | USB | |
| Linksys | WUSB600N v1 | RT2870 | 2.4G | USB | |
| Linksys | WUSB600N v2 | RT3572 | 2.4G/5G | USB | |
| Loopcomm | LP-7767 | RT3572 | 2.4G/5G | USB | |
| Motorola | TER/NUSB1-N1 | RT2770 | 2.4G | USB | |
| Netis | WF2150 | RT5572 | 2.4G/5G | USB | |
| Netis | WF2151 | RT5572 | 2.4G/5G | USB | |
| Realtek | RTL8821AE | | 2.4G/5G | HMC | CC |
| Rosewill | RNX-N600UB | RT5572 | 2.4G/5G | USB | |
| Rosewill | RNX-N600UBE v1 | RT3572 | 2.4G/5G | USB | |

### Access Port

When monitoring a single network via a switch Access Port, no additional switch configuration is required. If the system has more than one NIC, you can monitor multiple segments through multiple Access Ports.

### Trunk Port

To monitor multiple VLANs from a single interface, configure the switch port as a Trunk Port using the 802.1Q protocol. Below are examples of configuring Trunk Port (802.1Q) on Cisco and HP switches.

Cisco Switch example

```
Cisco(config)#interface gi1/0/48
Cisco(config-if)#switchport trunk encapsulation dot1q
Cisco(config-if)#switchport mode trunk
```

HP Switch example (create Port 48 as a tagged interface)

```
Procurve(config)#vlan 100
Procurve(config)#tagged 48
Procurve(config)#vlan 200
Procurve(config)#tagged 48
```

## 9.3.3 Install the Network Sensor

**Step 1: Switch from Ubuntu user to root**

```
genian@genian:~$ sudo su
[sudo] password for genian:
root@genian:/home/genian#
```

**Step 2: Update and upgrade packages**

```
root@genian:/home/genian# apt-get update
root@genian:/home/genian# apt-get upgrade
```

**Step 3: Install curl (required for install)**

```
root@genian:/home/genian# apt install curl
```

**Step 4: Install the Network Sensor with the following command**

```
curl -sSLk https://bit.ly/4fX6bQ8 | sudo PROMPT=1 SSHALLALOW=1 SSHPORT=22 TARGET=GNS␣
↪DEB=ztna LOCALE=en bash -
```

### 9.3.4 Configure the Network Sensor

**Step 1: Access Ubuntu and gnlogin**

After installation, access Ubuntu and gnlogin to perform initial setup.

```
genian@genian:~$ sudo su
[sudo] password for genian:
root@genian:/home/genian#
# Gain root privileges
root@genian:/home/genian# gnlogin
# Enter Genian Shell
```

**Note:** You must have root privileges to apply interface settings properly.

**Step 2: Configure the Network Sensor**

1. Enter global configuration mode with the enable command.
2. Enter configuration mode with the configure terminal command.
3. Set the interface IP address and subnet mask.
4. Set the interface default gateway.
5. Set the device default gateway.
6. Set the device DNS server.
7. Configure the Policy Server information by IP or Hostname.

```
genian> enable
Password: (For the enable password, contact Technical Support)
genian# configure terminal
genian(config)# interface [interface name] address [IP] [Subnet Mask]
genian(config)# interface [interface name] gateway [IP]
genian(config)# ip default-gateway [IP]
genian(config)# ip name-server [IP]
genian(config)# node-server IP [IP]
genian(config)# node-server Host [Hostname]
# If you configured interfaces during Ubuntu installation, some IP settings may␣
↪already exist.
```

**Note:** For configuring VLAN interfaces on a trunk interface, see *Adding and Deleting Network Sensors*.

### 9.3.5 Unsupported Hardware

If installation does not proceed normally, contact your partner engineer or Technical Support.

**Note:** In virtual environments, if the storage device or network interface is not recognized, change the storage type to SATA or change the network interface driver to an Intel family such as E1000.

## 9.4 Installing ZTNA Gateway

### 9.4.1 Deployment Models

You can install the ZTNA Gateway in two ways depending on your site's infrastructure setup.

### 9.4.2 Prepare the Environment

You need one or more public IP addresses to use the ZTNA Gateway.

### 9.4.3 Install ZTNA Gateway

#### Install Gateway on-premises

You can install the ZTNA Gateway on a physical system or a virtual machine.
Refer to *Install Ubuntu OS* to prepare **Ubuntu OS 24.04.4 LTS**.
If using a **sensor install token**, refer to *Token-based Policy Server access* for values to input.

**Note:**

You can install the ZTNA Gateway on a virtual machine.
ZTNA supports various hypervisors such as VMware, VirtualBox, and XenServer.

**Step 1: Switch to the root account**

```
genian@genian:~$ sudo su
[sudo] password for genian:
root@genian:/home/genian#
```

**Step 2: Update and upgrade packages**

```
root@genian:/home/genian# apt-get update
root@genian:/home/genian# apt-get upgrade
```

**Step 3: Install curl (required for installation)**

```
root@genian:/home/genian# apt install curl
```

**Step 4: Install ZTNA Gateway**

```
curl -sSLk https://bit.ly/4fX6bQ8 | sudo PROMPT=1 SSHALLOW=1 SSHPORT=22 TARGET=GNS␣
↪DEB=ztna LOCALE=en bash -
```

- Log in to Web UI, go to [System] -> [System Management].
- Select the newly added unapproved sensor and approve it via [Select Action] -> [Approve Unapproved Sensor].

### Install Gateway in Cloud-Managed environment - Manual via CLI

Create an instance for ZTNA Gateway per your cloud provider's guide.
Use an Ubuntu 24.04 image for the instance.
If using a **sensor install token**, refer to *Token-based Policy Server access* for values to input.

After creating the instance, connect via SSH and follow the steps below.

**Step 1: Switch the Ubuntu user account to the root account.**

```
genian@genian:~$ sudo su
[sudo] password for genian:
root@genian:/home/genian#
```

**Step 2: Update and upgrade packages**

```
root@genian:/home/genian# apt-get update
root@genian:/home/genian# apt-get upgrade
```

**Step 3: Install curl (required for installation)**

```
root@genian:/home/genian# apt install curl
```

**Step 4: Install ZTNA Gateway**

```
curl -sSLk https://bit.ly/4fX6bQ8 | sudo PROMPT=1 SSHALLOW=1 SSHPORT=22 TARGET=GNS␣
↪DEB=ztna bash -
```

- Log in to Web UI, go to [System] -> [System Management].
- Select the newly added unapproved sensor and approve it via [Select Action] -> [Approve Unapproved Sensor].

### Install Gateway in Cloud-Managed environment - Automatic via Web UI

To use automatic installation through the Web UI, first register a Cloud Provider and a Site. Refer to *Cloud Provider settings* and *Site settings*.

1. Access the Web UI console: `https://(ZTNA Policy Server IP):8443/`
2. From the top menu, click **System** -> **Cloud Provider Management**.
3. Click **Tasks** -> **Create** and enter credentials for each cloud.
4. In the left menu, go to **System** -> **Site** and create a site.
5. Go to **System** -> **System Management**, then **Tasks** -> **Add ZTNA Gateway**.

- Site name: Specify the previously created site.
- AMI / Image: Selected automatically based on site settings.

- Instance Type: Choose instance type (recommended: t2.medium or higher, or cloud recommended spec).
- Size: Set disk size (recommended: 64GB or higher).
- Subnet ID: Automatically assigned based on site settings.
- Key pair: Set the key pair for SSH to the Gateway instance.

6. Click **Check init** to confirm initialization, then click **Create**.
7. Verify instance creation in the cloud console (e.g., AWS EC2, Linode, OCI).
8. In the Web UI, go to [System] -> [System Management], select the newly added unapproved sensor, and approve it via [Select Action] -> [Approve Unapproved Sensor].

## 9.5 Administration Console

Genian ZTNA provides two types of management consoles. A command-line console that provides system settings such as basic service configuration and network configuration, and a Web console that provides all other management and policy features.

### 9.5.1 Web Console

The access method of the web console is different according to the deployment type of the policy server.

#### On-Premises

1. Open up **Web Browser** and navigate to the following link
2. Copy and paste link below into browser
3. Replace **Policy Server Management IP Address:8443** with actual IP address

```
https://"Policy Server Management IP Address:8443"/ (e.g. https://192.168.50.10:8443/)
```

#### Cloud

1. Open up **Web Browser** and navigate to the following link
2. Copy and paste link below into browser
3. Replace **Cloud Policy Server Name** with actual registered name of Cloud Policy Server

```
https://"Cloud Site Name"/ (e.g. https://nac.genians.net/)
```

### 9.5.2 CLI Console

#### 1. CLI console access through SSH access program

The CLI (Command Line Interface) console can be accessed through SSH (default port: 22).

```
ssh "policy server management IP" -p 22  (e.g. : ssh 192.168.50.10 -p 22)
```

**Note:**

Cloud-managed policy server does not provide SSH command-line console.

#### 2. CLI console access through SSH connection from the web console

1. Go to **System** on the top panel.
2. Select **System** from the **System** item on the left.
3. SSH connection destination IP address right 🗔 Click the icon.
4. SSH connection is performed using Username and Password in the pop-up window.

Genian ZTNA by default does not allow for SSH access to the appliance until the Administrator allows for this access by adding IP Address or Network Address/CIDR.

See: "Allow Remote Access via SSH" under *Initializing the System*

## 9.6 Installing License

When Genian ZTNA is installed, it works by default as Free Version. Free Version has the following restrictions.

- Only Basic Edition functions are provided. (Monitoring only)
- Up to 300 nodes can be managed.
- Remote sensor can not be connected. (All-in-One only)

If you require Visibility and Control, then you will need to obtain a license for the Professional or Enterprise Edition. You can get a trial license to experience the Professional/Enterprise Edition for 30 days by going to the Trial License Page

**Note:** License only required on On-Premises Policy Server. Cloud Managed service does not require license

### 9.6.1 Find Server ID

1. Go to **System** in the top panel
2. Go to **System > License** in the left **System Management** panel
3. Find **Server ID**

### 9.6.2 Get Trial License

1. Go to Trial License Page
2. Find **Server ID** section and add in your Server ID found on your Policy Server.
3. Enter **Full Name**, **Company Name**, and **Email**
4. Click **Get Trial License**
5. Copy **License** text from —–BEGIN CERTIFICATE—– to —–END CERTIFICATE—– (*Include both Begin and End Certficate Lines*)

### 9.6.3 To Install License

1. Go to **System** in the top panel
2. Go to **System > License** in the left **System Management** panel
3. Find **License** section and paste in the **License**
4. Click **Apply**

### 9.6.4 Transfer License to a Different Server ID

1. Login to my.genians.com and locate the existing license
2. In the search text box, enter the existing server ID and click **Search**
3. Under the **License Reissuance** field, enter the new server ID you would like to transfer the license to then click the **Reissue** button
4. You should see a **Success** pop-up message if the operation was successful
5. Search for the old server ID to confirm there is no longer an entry for it
6. Search for the new server ID and confirm the license has been transferred
7. Click the **Download** button and install the license on the new server following the instructions above

## 9.7 Installing Agent

**Agent** not only assists in determining the posture of the endpoint device, but can also collect system information, access control, and authenticate users. The Agent can be installed onto **Windows** and **MacOS** either manually or by **Agent Not Installed Enforcement** Policy. Once installed, the Agent then communicates with the Policy Server keeping device compliant with policies.

### 9.7.1 Installing Windows Agent

You can install **Agent** on Windows devices through GPO, Captive Web Portal (CWP), or manually using removable storage media

#### Install Windows agent

- *Download and install via agent download page*
- *Installing the agent via CWP*
- *MSI packages for installation via Active Directory GPOs*
- *Installing the agent from the Microsoft App Store*
- *Verify Windows Agent installed*
- *Where To Find Agent Logs On Windows Device*

#### Download and install via agent download page

1. Download Agent
   - https://(*IP or FQDN*)/agent
2. Choose Agent: DO NOT change the filename to avoid name conflicts
   - Windows installer version: GnUpdate_(*IP or FQDN*).exe
3. If prompted, provide the IP or FQDN of your Policy Server.

**Note:** If the user does not have the file installation permission, the installer can not be executed.

#### Installing the agent via CWP

Genian ZTNA enforcement policy can be enabled to redirect the user to the CWP for network access when the agent is not installed. In the CWP message, click the Install Agent button to download and install the Agent

To enable agent install by captive web portal:

1. Go to **Policy** in the top panel
2. Go to **Enforcement Policy**
3. Click the **Agent Not Installed** policy in the view pane.
4. Under the **General** section, change the Status to **Enabled**
5. Click **Update** at the bottom of the screen.

6. Click **Apply** in the top right corner of the screen.

Nodes under this enforcement policy are by default directed to a captive web portal with instructions on how to download the agent.

## MSI packages for installation via Active Directory GPOs

### Downloading MSI File

From the Web Console:

1. Navigate to the **System** Tab on the top of the Screen, then select **Genian Software** from the left menu panel.
2. In the main view pane, find Genian ZTNA Agent for Windows. On the far right of the row, click the **MSI** link to download.

### Deploying Agent MSI via Active Directory GPOs

**Note:** The Agent Execution Account may need elevated privilege for successful agent deployment and operation.

1. Go to **Policy** in the top panel
2. Go to **Node Policy**
3. Click "Node policy ID" where do you want to apply the policy.
4. Find the **Agent Policy** section
5. Select **Execution Account** and "Computer Logon account": in the checkbox
6. How to set up to deploy the MSI Package via AD

### To configure GPO in Active Directory

Describes how to set up a GPO that can deploy the Genian Agent MSI in AD.

### Step 1. Create a shared folder for the deploying MSI files

- Copy the Agent MSI file from Genians to a shared folder or set the folder that contains the file as a shared folder

### Step 2. Open the Group Policy Management and to make the GPO

- **Run** > **gpmc.msc** or **Start** > **Administrative Tools** > **Group Policy Management** in Window server
- Expand the **[domain name]** on the left panel > Click the **Group Policy Object** on the mouse right button > Click the **New** > Put the **Name(ex. genian)** > **OK**
- Click the **genian** GPO on right mouse button > **Edit** You can see the **Group Policy Management Editor**

### Step 3. To configure the Group Policy Management Editor

- Expand the **Policies** and **Software Settings** folder in left panel > click the **Software installation** > Click the right mouse button in right panel and click the **New** and **Package**
- To move on shared folder path like (ex. \[domain]Share folder). Set the folder permissions as **Authenticated = Read, Domain Computers = Read, System = Full Control**
- Select the Agent MSI file > select **Advanced** in **Deploy Software popup**
- click the **advanced** > check the **Ignore language when deploying this package** > **OK**

### Step 4.To apply the GPO policy in Group Policy Management

**Note:** GPOs can contain both **computer** and **user** sets of policies.

```
The **Computer section** of a GPO is applied during boot.
The **User section** of a GPO is applied at user login.
```

- Click the **Computers** or **user** folder on the mouse right button in left panel > click the **Link an Existing GPO** > Select the **genian GPO**

### Step 5. Verification

- **run** > **cmd** > put the command **gpupdate /force**
- Check the **GnAgent.exe, GnPlugin.exe, GnStart.exe** process in the **task manage**
- Check for Agent files existent like **GnAgent.exe, GnPlugin.exe, GnStart.exe** in C:Program FilesGeniGenian

### Installing the agent from the Microsoft App Store

The Genian ZTNA agent can be installed from the Microsoft App Store following the steps below:

1. From the search menu in Windows type in **windows** and click on **Microsoft Store App** when it appears
2. In the search box, type in **genian** and select the Genian ZTNA Agent App, then click **Open**
3. Enter the FQDN or IP of your policy server in the **Policy Server IP/Domain" text box, then click **Okay**
4. The ZTNA agent should install and connect with your Policy Server

### Verify Windows Agent installed

1. Select **Management > Node**
2. Click **NT AG SS** column in Nodes window (*If a node has an installed Agent, the Agent icon will show*)

### Genian Agent Options On Windows Device

1. Go to **Systray** of Windows device
2. Find and right-click on **Genians Agent Icon**
3. Listed options allow you to do the following:
   - **Read Notice:** Shows current notices from the Administrator
   - **Read Message:** Shows current messages from the Administrator
   - **View My Status:** Shows the devices current **Captive Web Portal (CWP)** page
   - **Login (L):** Allows user to log in and upon successful login displays CWP page
   - **Logout (O):** Allows user to log out
   - **View User Information:** Allows user to view account information upon successful login
   - **View Network Connections:** Allows user to view the devices active network connections
   - **View USB Information:** Allows user to view the devices USB information
   - **Delete Agent:** (*User is unable to delete the installed Agent. This must be done by the Administrator*)
   - **About Genian Agent:** Allows user to see current information about installed Agent

### Where To Find Agent Logs On Windows Device

1. Open **File Explorer** on Windows device
2. Go to **C:Program FilesGeniGenianLogs**
3. Sort by **Date modified**

### Installation Specifications

| Disk | Memory |
|---|---|
| 30~40MB | 20~30MB |

### Windows Support List

See: *Supported Operating Systems and Plugins*

## 9.7.2 Installing macOS Agent

You can install **Agent** on macOS devices through GPO, Captive Web Portal (CWP), or manually using removable storage media

### Install macOS Agent

1. Download Agent
   - https://(*IP or FQDN*)/agent
2. Choose Agent: DO NOT change the filename to avoid name conflicts
   - macOS version: GnAgent_(*IP or FQDN*).pkg
3. If prompted, provide the IP or FQDN of your Policy Server.

### Verify macOS Agent Installed

1. Select **Management > Node**
2. Click **NT AG SS** column in Nodes window (*If a node has an installed agent, the Agent icon will show*)

### Installation Specifications

| Disk | Memory |
|---|---|
| 20~30MB | 30~60MB |

### macOS Support List

See: *Supported Operating Systems and Plugins*

## 9.7.3 Installing Linux agent

### Installing the Linux Agent over CWP

There are several ways to install agents in Genian ZTNA.

This is the guide for how to install the agent by accessing the CWP page.

1. Access the CWP page. https://*policy_server_IP-or-cloudsite_name*/agent
2. Select the Linux icon from the OS-specific agent icon and download the file.
3. Open **Terminal** in your Linux distribution and navigate to the **Download** folder. (Based on Ubuntu)
4. **Run the installer in the download directory as follows:**
   - cd ~/Download
   - chmod 755 lnxagent_*Serveraddress*
   - sudo ./lnxagent_*Serveraddress*
5. If prompted, provide the IP or FQDN of your Policy Server.

**Note:**

- Depending on the Linux distribution, the download path for the Linux Agent installer may vary.
- The installer cannot run if the user does not have permission to installer, so it must be run as an administrator. The process will automatically run when the file ends.

- This installer may also be obtained and distributed via other means.

### Verify Linux Agent Installation

1. Connect to Web Console.
2. Go to the **Management > Node** menu.
3. Access the IP of the node you wish to check.
4. If the agent icon is displayed on the Node List screen, the installation and information registration are completed normally.

### Linux Agent Key Paths

- **Open Terminal in your Linux distribution to view the log files below.**
    - Installation path: /opt/genians/nac
    - Log path: /var/log/genians
    - Configuration file path: /opt/genians/nac/gnconf/gndata

### Supported OS for Linux Agent

See: *Supported Operating Systems and Plugins*

## 9.7.4 Deleting Agent

You can uninstall the Agent on the endpoints either by using a Node Policy which allows you to group many devices together or by using an Authentication Code which allows you to delete an individual agent.

### Delete Agent Using Policy

This method is ideal for deleting the agent from a large number of devices, without end user involvement.

1. Create a **Node Group** to select which nodes to delete agent.
2. Create a **Node Policy** to delete agent from the selected nodes.
    - Under: **Policy Preferences** find the **Agent Policy** section and set the **Agent** drop down menu to **Delete**.
3. After creating the node policy, click the **apply** option in the top right corner.

This will automate the deletion of the agent from the designated devices when the node policy updates on the agent.

**Note:** To uninstall a Windows Agent that was deployed via GPO, select the GPO for software deployment, select Computer Configuration, and select edit. Find the Genians Agent under the Computer Configuration menu, and right click to select All Tasks > Remove.

### Delete Agent From Tray Icon

This option is available to end users if it has been enabled on the Policy Server by the administrator.

To Configure see: **Agent Deletion Method** in: *Configuring Agent Defaults*

Deleting as **Endpoint user**:

1. Go to the task bar on Windows or OSX machine and find the Genians logo.
2. Right click the logo and select the ***Delete Agent(D)** option.
3. If prompted for a code, see the next section in this document.

### Delete Agent Using Authentication Code

This option is ideal for a user to request agent removal. An administrator can approve this request.

Deleting as **Endpoint user**:

1. Go to the task bar on Windows or OSX machine and find the Genians logo.
2. Right click the logo and select the ***Delete Agent(D)** option.
3. find the **Agent Code** in the pop up window, and provide it to your Genians ZTNA Administrator who will use it to generate an **Authentication Code**.
4. Enter the **Authentication Code** provided into the designated form, and click the **Delete** button.

Claiming ***Authentication Code** as an **Administrator**

1. Log in to Policy server Management console.
2. Mouse over the **Management** tab on the menu bar and select the **Request** option underneath.
3. In the tree panel on the left of the page, find **Agent Authentication Code**, and select **Generator**
4. Enter the **Agent Code** supplied by the endpoint user and click **Generate** button.
5. An **Authentication Code** will be displayed. Provide this code to the end user.

**Note:** Authentication Code based deletion method is still possible when endpoint is offline, as long as policy server is active.

### Delete Agent When Policy Server Is No Longer Available

The Policy Server used to install the agent is needed to delete the agent. If this Policy Server is no longer available, a new policy server is needed.

1. Install new Policy Server.
2. Reinstall Agent from Policy Server using standard agent installation. This will overwrite the existing agent.
3. Delete the agent using Node Policy or Authentication Code.

CHAPTER

TEN

# MONITORING NETWORK ASSETS

You can monitor network assets by the Nodes themselves or by monitoring IP Addresses, Switches, and Wireless LAN

## 10.1 Understanding Network Monitoring

### 10.1.1 Getting Visibility of Network and Endpoint

Network access control is generally established through the following steps.

- Obtain visibility of assets through network discovery and information gathering
- Classify the collected assets according to security policy and status
- Establish network access control policies for classified objects

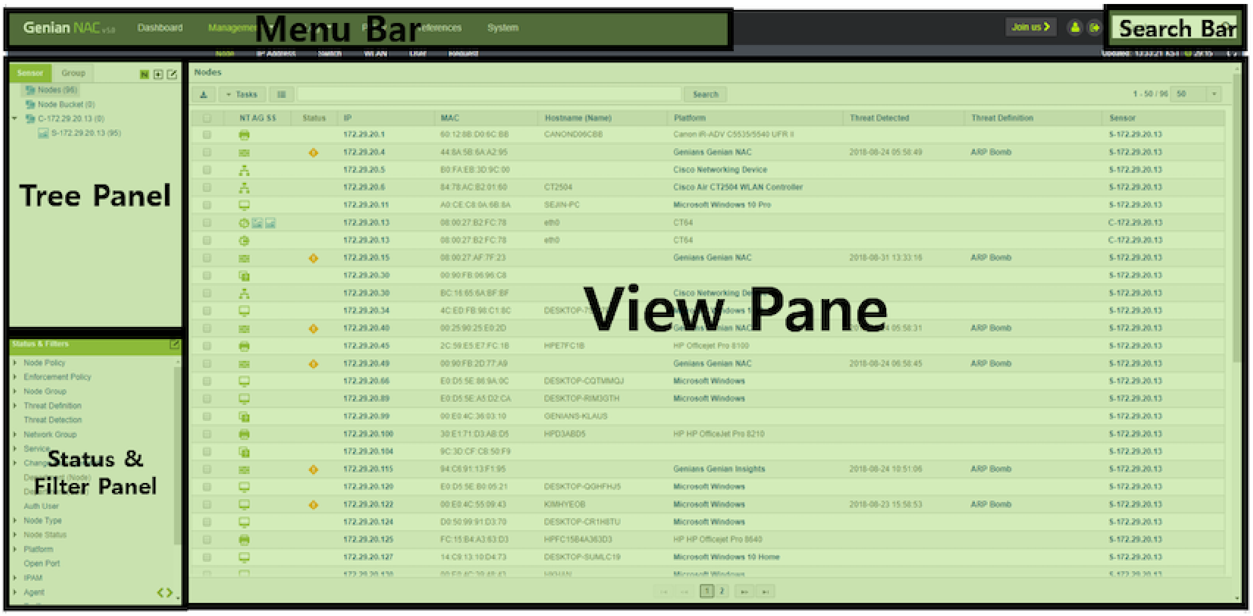
Genian ZTNA collects information of various network assets through network sensors and agents and provides real time visibility to network and endpoints including:

- Network Node
- Endpoint
- IP Address
- Switch / Port
- Wireless LAN

The network sensor and the agent monitor the management target network or the endpoint in real time and transmit the new information or the changed information to the policy server. The administrator can inquire the information of the entire management target network and the endpoint through the management console provided by the policy server.

### 10.1.2 Management Menu

The management menu on the administrator web console is for searching information collected through network sensors and agents. Each management screen is divided into three areas. The Tree Panel and Status & Filter Panel on the left serve to select the target objects to be displayed on the right View Pane.



| □ | NT AG SS | Status | IP | MAC | Hostname (Name) | Platform | Threat Detected | Threat Definition | Sensor |
|---|---|---|---|---|---|---|---|---|---|
| □ | | | 172.29.20.1 | 60:12:8B:D0:6C:B8 | CANOND06CBB | Canon iR-ADV C5535/5540 UFR II | | | S-172.29.20.13 |
| □ | | ◆ | 172.29.20.4 | 44:8A:5B:6A:A2:95 | | Genians Genian NAC | 2018-08-24 05:58:49 | ARP Bomb | S-172.29.20.13 |
| □ | | | 172.29.20.5 | B0:FA:EB:3D:9C:00 | | Cisco Networking Device | | | S-172.29.20.13 |
| □ | | | 172.29.20.6 | 84:78:AC:B2:01:60 | CT2504 | Cisco Air CT2504 WLAN Controller | | | S-172.29.20.13 |
| □ | | | 172.29.20.11 | A0:CE:C8:0A:6B:8A | SEJIN-PC | Microsoft Windows 10 Pro | | | S-172.29.20.13 |
| □ | | | 172.29.20.13 | 08:00:27:B2:FC:78 | eth0 | CT64 | | | C-172.29.20.13 |
| □ | | | 172.29.20.13 | 08:00:27:B2:FC:78 | eth0 | CT64 | | | C-172.29.20.13 |
| □ | | ◆ | 172.29.20.15 | 08:00:27:AF:7F:23 | | Genians Genian NAC | 2018-08-31 13:33:16 | ARP Bomb | S-172.29.20.13 |
| □ | | | 172.29.20.30 | 00:90:FB:06:96:C8 | | | | | S-172.29.20.13 |
| □ | | | 172.29.20.30 | BC:16:65:6A:BF:BF | | Cisco Networking De[illegible] | | | S-172.29.20.13 |
| □ | | | 172.29.20.34 | 4C:ED:FB:98:C1:8C | DESKTOP-7[illegible] | [illegible] Windows 1[illegible] | | | S-172.29.20.13 |
| □ | | ◆ | 172.29.20.40 | 00:25:90:25:E0:2D | | Ge[illegible] NAC | [illegible]4 05:58:31 | ARP Bomb | S-172.29.20.13 |
| □ | | | 172.29.20.45 | 2C:59:E5:E7:FC:18 | HPE7FC18 | HP Officejet Pro 8100 | | | S-172.29.20.13 |
| □ | | ◆ | 172.29.20.49 | 00:90:FB:2D:77:A9 | | Genians Genian NAC | 2018-08-24 06:58:45 | ARP Bomb | S-172.29.20.13 |
| □ | | | 172.29.20.66 | E0:D5:5E:86:9A:0C | DESKTOP-CQTMMQJ | Microsoft Windows | | | S-172.29.20.13 |
| □ | | | 172.29.20.89 | E0:D5:5E:A5:D2:CA | DESKTOP-RIM3GTH | Microsoft Windows | | | S-172.29.20.13 |
| □ | | | 172.29.20.99 | 00:E0:4C:36:03:10 | GENIANS-KLAUS | | | | S-172.29.20.13 |
| □ | | | 172.29.20.100 | 30:E1:71:D3:AB:D5 | HPD3ABD5 | HP HP OfficeJet Pro 8210 | | | S-172.29.20.13 |
| □ | | | 172.29.20.104 | 9C:3D:CF:C8:50:F9 | | | | | S-172.29.20.13 |
| □ | | ◆ | 172.29.20.115 | 94:C6:91:13:F1:95 | | Genians Genian Insights | 2018-08-24 10:51:06 | ARP Bomb | S-172.29.20.13 |
| □ | | | 172.29.20.120 | E0:D5:5E:B0:05:21 | DESKTOP-QGHFHJ5 | Microsoft Windows | | | S-172.29.20.13 |
| □ | | ◆ | 172.29.20.122 | 00:E0:4C:55:09:43 | KIMHYEOB | Microsoft Windows | 2018-08-23 15:58:53 | ARP Bomb | S-172.29.20.13 |
| □ | | | 172.29.20.124 | D0:50:99:91:D3:70 | DESKTOP-CR1H8TU | Microsoft Windows | | | S-172.29.20.13 |
| □ | | | 172.29.20.125 | FC:15:B4:A3:63:D3 | HPFC15B4A363D3 | HP HP Officejet Pro 8640 | | | S-172.29.20.13 |
| □ | | | 172.29.20.127 | 14:C9:13:10:D4:73 | DESKTOP-SUMLC19 | Microsoft Windows 10 Home | | | S-172.29.20.13 |
| □ | | | 172.29.20.130 | 00:E0:4C:20:4F:43 | HKHAN | Microsoft Windows | | | S-172.29.20.13 |

## Tree Panel

The Tree Panel allows you to select the target objects to be displayed on the View Pane as a sensor or as a group that meets the conditions specified by the administrator.

## Status & Filter Panel

The Status & Filter Panel provides more detailed filtering of selected objects in the Tree Panel. Based on various information gathered by Genian ZTNA, it is easy to select and display objects matching the information in the right view pane. Also, statistical information is provided through a graph or a table when the top of various categories provided is selected.

## View Pane

You can perform searches on the objects output through the search function provided at the top, or perform various tasks through the **Tasks** menu by selecting each item. Click on the link in the key column for each management menu to see more detailed information about the object. The key column for each management menu is as follows.

- Node: **IP**
- IP Address: **Sensor**
- Switch: Switch, **Port**
- WLAN: **MAC**

### 10.1.3 Troubleshooting

- *Genian ZTNA log collection method*
- *Genian ZTNA diagnosis Method*
- *Node is not displayed in Web Console*
- *Wrong Link State Displayed for Node*

## 10.2 Monitoring Network Nodes

You can monitor **Nodes** by grouping, filtering, and listing by various perspectives

### 10.2.1 Understanding Network Nodes

#### Network Nodes and Devices

A network node is a connection point that can be connected to an IP network and communicate with another system. A system uses IP address for remote network and MAC address for local network to communicate with other system. Genian ZTNA recognizes this IP and MAC address pair as one node.

A node is a logical concept different from a physical device. For example, a single device may have multiple IPs or MACs and thus be recognized as multiple nodes. E.g

- One device connected to the network via multiple LAN cards (wired LAN, wireless LAN)
- Multiple operating systems use different IP addresses through multiple boot on one device.
- Multiple IP / MAC pairs are used through a virtual machine on one device

Genian ZTNA automatically recognizes different nodes as connected to one device if:

- Nodes use the same MAC address
- Through the agent that multiple network adapters are installed on one device

This allows administrators to selectively provide node-based management view or device-based management view.

#### Detecting Network Nodes & Devices

Genian ZTNA detects nodes in the network through network sensors or agents. The network sensor recognizes the existence of the node through the ARP packet generated in the network. Because of its nature, ARP is broadcast over the network, so a network sensor can detect that a new network node is connected just by being connected to the network. It can also analyze Ethernet frames received over a broadcast packet such as DHCP to see if a new node is connected to the network.

Another way to recognize the node is to install the agent on the Endpoint system. The agent collects various information including the IP / MAC of the system and sends it to the policy server to be registered as a node.

Lastly, devices (MAC only) can be detected and registered through RADIUS authentication.RADIUS access-request supplies the MAC Address while accounting-request supplies the IP.

### Gathering Node Information

A network sensor uses a passive method of obtaining information through a packet such as a broadcast generated in a node and a method of actively collecting information through an open port of the node.

The passive method can collect information without affecting the node through the information contained in the packets periodically generated by the node, such as DHCP, NetBIOS, UPNP, and mDNS. The policy server can also gather node information like IP address, and connected SSID through RADIUS accounting.

In the active method, the network sensor first checks the service provided by the node through the port scan, and collects the information through the request according to each service. For example, if a node provides an HTTP service over the TCP 80 port, the sensor can request the top-level page to obtain information.

The information that is actively collected can set the target item and the collection period. For more information, see *Configure Collecting Networks and Node information*

The network sensor can also send WMI Queries to windows nodes to gather information about hardware, software and networking properties. See:

### WMI Node Info Scan

### Gathering Capabilities

### Hardware

- **Motherboard**
  - Chassis Type
  - Manufacturer
  - CPU Name
  - CPU Manufacturer
  - Revision
  - Battery
- **Memory Info**
  - Total
  - Used
  - % Used
- **Storage Devices**
  - Device Name
  - Device Type
  - Unique #
  - File System
  - Capacity
  - Used Capacity
  - % Used
- **USB Devices**

  - Class Name
  - Device Name
  - Manufacturer
  - State

### Operating System

- **Operating System**
  - Operating System Name
  - Version
  - Build Version
  - Service Pack
  - Most Recent Update Time
  - Language
  - User
  - Organization
  - Computer Name
  - Domain
  - Install Time
  - Uptime
- **User**
  - User Name
  - Account Type
  - Password Settings
  - Login Status
- **Screensaver**
  - Enabled/Disabled
  - Password Settings
  - Wait Time
  - Name

### Network

- **Interface**
  - Name
  - Connection Method
  - MAC
  - Device Name
  - Link
  - Speed
  - Promiscuity
- **IPv4 Settings**
  - Name
  - IPv4
  - IP/Netmask
  - Gateway
  - Primary/Secondary DNS
- **IPv6 Settings**
  - Name
  - IPv6
  - IPv6 Address
  - IPv6 Link Local

### Folder Sharing

- **Share Information**
  - Share Name
  - Type
  - Path
  - Details
  - Detection Time

### Printer

- **Printer**
  - Name
  - Device Name
  - Port Information

### Software

- **Software Information**
  - Program Name
  - Version
  - Path
  - Installation Date
  - Detection Time
- **Antivirus Information**
  - For Compatible AV Software, see: *Collecting Antivirus Software Information*
  - AV Name
  - Real Time Monitoring Status (Enabled/Disabled)

### Configuring WMI Node Info Collection

### Configure Pre-Requisite settings

1. Ensure that the target machines are domain joined.
2. Allow for endpoint/ domain accounts to respond to WMI Query.
3. Enter Bind DN and Password for privileged Domain account under **Preferences > Authentication Integrtation > LDAP Server**.

### Enable WMI Scan

1. Navigate to the **System** tab and select the desired sensor.
2. Select the **Sensor** tab, and then select the **Interface** you wish to configure.
3. Under **Node Information Scan**, enable **Port / Service Scan** and then enable **WMI Information Scan**

**Note:** The WMI scan only operates on nodes without an installed agent. If you wish to collect info with an agent, See: *Collecting Windows System Information using WMI*

## 10.2.2 Genian Device Platform Intelligence (GDPI)

### What is GDPI

BYOD, which uses a personal device in a business network, or IoT, in which all IT devices are connected to a network, makes todays networks more sophisticated and versatile than before. This puts a heavy burden on administrators responsible for IT security.

IT managers need to protect the network from vulnerable devices by allowing only authorized devices to connect to the network. However, it is not easy to identify and manage the various devices that are connected between many access points in an organization.

Genian ZTNA provides Device Platform Intelligence to make this task easier for administrators.

First, Device Platform Intelligence identifies the manufacturer, product name, and model name of devices connected to the network through various intelligent methods. Through the identified Device Platform, the administrator can inquire various information possessed by the device such as:

- Photos of the device
- Type of device connection (wired, wireless)
- End of Sale (EOS) status of the device.
- End of Life (EOL) status of the device
- Manufacturer
- Country of manufacturer
- Manufacturer Business Continuity Status
- Acquisition of manufacturer

This additional information makes it easier for administrators to manage IT by providing greater visibility into devices on their network.

### Device Platform and CVE

Common Vulnerabilities and Exposures (CVE) is a database of vulnerabilities in IT equipment and software provided by MITER. More than 1,000 new vulnerabilities are released each month. IT managers must identify vulnerabilities associated with IT devices they manage. Genian ZTNA can identify the IT devices in the network and show their CVEs to make network management easier.

### How to Detect Device Platform

Genian ZTNA will detect connected device platforms using various information collected by the **Network Sensor**. When a device connects to the network, packets are sent out and the device responds with one or more protocols. Genian ZTNA uses the following protocols to detect devices platform information

**Active Method:**

- HTTP / HTTPS header and body
- Web Browser User-Agent
- TELNET / SSH / SMTP banners
- Open Port
- SNMP OID / Description

- SIP
- and more

**Passive Method:**

- Web Browser User-Agent (using SPAN port)
- MAC Address
- Hostname
- DHCP Request
- UPNP
- HPSLP
- and more

Genian ZTNA is using our own, highly advanced platform database (GPDB) for detecting device platforms. GPDB has various patterns for matching against device information to ensure that platforms are accurately detected. To provide paramount accuracy, the GPDB is updated weekly so that the newest devices on the market can be quickly identified within the network. (*Weekly GPDB updates are for the Paid Edition Only. The Free Edition*'*s GPDB is updated monthly*)

### Node Types

Each Device Platform has a Node Type, such as:

- Policy Server
- Network Sensor
- Virtual Sensor
- Agent Sensor
- Switch Port
- Sensor Alias
- Virtual IP
- Wireless Sensor
- Undefined
- PC
- Mobile Device
- Server
- Network Appliance
- Wireless Device
- Router
- Switch
- Security Device
- Printer
- VOIP
- Other

You can browse or make policy based on this node type information.

### Genian Platform Database (GPDB)

GPDB is a database that stores device platform detection pattern and device platform information related to GDPI. This GPDB is constantly updated via Genians' device platform engineers. This makes it possible to detect new devices quickly without any additional work.

To check the time of the last updated GPDB

1. Go to **System > Genian Data**
2. See time of **Platform Information**

### See Device Platform Intelligence

You can see additional device platform information through Device Platform Intelligence page.

To see individual nodes information,

1. Go to **Management > Node** in the top panel
2. Find and click a desired **Platform** name of **Node**

### Define a Node Platform Manually

1. Go to **Management > Node** in the top panel
2. Select the desired node's **IP Address**

Under **General** tab

1. For **Platform**, click **Checkbox** to **Manually define**
2. Manually enter **Platform Name**
3. Click **Update**

**Note:** In Node View you will now see a Icon next to name in the Platform Column. This Icon will indicate this has been manually defined.

### Create a User-defined Node Type

1. Go to **Preferences** in the top panel
2. Go to **Properties > Node Type** in the left Preferences panel
3. Click **Tasks > Create**
4. Enter a **Name** and select an **Icon** (*Click **Add* to upload your own icon*)
5. Click **Save**

**Note:** A User-defined Node Type must be defined manually and added to the node.

1. Go to **Management > Node** in the top panel

2. Click on desired node **IP Address**

Under **General** tab

1. For **Node Type**, click **Checkbox** to **Manually define**
2. Select **Node Type**
3. Click Update

### Report Unknown/Wrong Platform Detection

If for some reason Genian ZTNA cannot detect the Platform of a device, one of the following could be the underlying reason:

- **Not enough information**: A device is not sending packets or is not responding to any request. This is possible if the OS has a Firewall active
- **No matching pattern in GPDB**: Node information has some evidence of a specific Platform, but the GPDB does not have that matching pattern yet.

In case there is no matching pattern in our GPDB, you can send that Nodes information to the Genian Cloud using the Report Wrong Platform dialog. Once Genians has received the report, our engineers will investigate the Platform pattern and update it to the GPDB.

### Disable Reporting Unknown Platform

By default, Genian ZTNA sends a Report Wrong Platform for unknown Platform Nodes every day. All sent information is readable from outside of the device. To deactivate sending a Report Wrong Platform to the Genian Cloud, follow these steps:

1. Go to **Preferences** in the top panel
2. Go to **General > Node** in the left Preferences panel

Under **Detection**

1. For **Reporting Unknown Platform**, select **Off**
2. Click **Update**

## 10.2.3 Browse/Search/Filter Nodes

### Sensor & Group Panel

The **Sensor & Group** panel allows the viewing of Nodes in a quick and organized manner. Click **Management > Node** in the top panel

- **Sensor tab**: All Nodes, Detected Networks, and the Sensors pertaining to each network are visible

  *(Clicking on a Sensor will show all the Nodes associated with that particular Sensor)*
- **Group tab**: All Nodes and Nodes categorized by their Node Group

### Status & Filter Panel

Nodes can be filtered by using our pre-defined filters in the **Status & Filters** panel

1. Click **Management > Node** in the top panel
2. Find **Status & Filters** in the left panel. Click **Main Category** then **Sub-Category**

*(Click on Main category just to see a summarized view of Nodes within categories)*

For Example: To view predefined filters with "Microsoft Windows" on a node managed by a specific Sensor:

1. Click **Management > Node** in the top panel
2. Go to **Sensor** tab in left panel. Click specific Sensor
3. Go to **Status & Filter** in the left down panel. Click **Node Group** > **Identification** > **Microsoft Windows**

You will see only "Microsoft Windows" nodes managed by a specific sensor on the main node view screen.

### Customize Status & Filter

You can hide unnecessary categories that are not in use

1. Click **Management > Node** in the top panel
2. Find **Status & Filters** in the left panel. Click **Edit** icon in top right corner of **Status & Filters** left panel
3. **Drag and Drop** unwanted categories from **Selected** to **Available**
4. Click **Update**

**Note:** Customized status & filters only affect the view of the current administrator.

### Find Nodes by Network Sensor

1. Go to **Management > Node** in the top panel
2. Go to **Sensor** tab in left panel
3. Click the search icon to use search
4. Input `Name` or `IP` of Network Sensor
5. Select specific Sensor
    - If no results are available, enter the blank and press Enter to confirm the entire sensor

**Note:** You will see the Nodes in the main Node view based off of the Network Sensors location.

### Edit and Create Subfolders for Multiple Sensors

1. Go to **Management > Node** in the top panel
2. Go to **Sensor** tab in left panel
3. Click **Edit Tree** icon at the top right corner
4. Select Sensor and Drag&Drop to reorginize of Network Sensor
   - In case you have many Network Sensors, you can create a subfolder by selecting Create option

### Find Nodes by Node Group

1. Go to **Management > Node** in the top panel
2. Go to **Group** tab in left panel
3. Under the site name, there are four **Node Categories** that contain **Node Groups** for you to select
   - **Identification**
   - **Categorization**
   - **Compliance**
   - **Uncategorized**

**Note:** These are provided by default, but you can create others by going to *Managing Node Groups*.

### Edit and Create Node Categories for Sensors and Node Groups

1. Go to **Management > Node** in the top panel
2. Go to **Group** tab in left panel
3. Click **Edit Tree** icon in the top right corner
4. **Right Click** on your site name to Create or Assign a **Sensor** or **Node Group**
   - In case you have many **Network Sensors**, you can create a subfolder by selecting **Create** option
   - Select Assign and toggle to see options for either **Sensor** or **Node Group**
5. Search and click **Checkbox**
6. Click **OK**

### List Nodes By Various Views

You can browse **Nodes** through various perspectives

1. Go to **Management > Node** in the top panel
2. Click the **menu** icon to the right of the **Tasks** button
3. Select **View Criteria** > **By Node** or **By Device**
4. View from the following perspectives:
   - **Overview**

- **Node View**
- **IPAM View**
- **Anomaly View**
- **OS Updates View**
- **Asset Management View**
- **Agent Action View**
- **Authenticated User View**
- **External Device View**
- **Device Life-Cycle View**

### Find Contextual Information

1. Go to **Management > Node** in the top panel
2. Find and click on desired **IP address** of **Node**
3. Find General information and other information to include:
   - If the agent is not installed
   - **General** - *IP, MAC, IPv6, IPv6 Link-local, Hostname, Platform, Platform Intelligence, Connection Type, User Authenticated, RADIUS Acct-Session,Platform CVE, Manufacturer CVE, and more*
   - **Device** - *Name, Device ID, Device Life-Cycle, Nodes for Device*
   - **Network** - *Traffic, WLAN, TCP Connections, Service, Open Port*
   - **Logs** - *Logs, Status Logs*
   - **IPAM** - *IP and MAC Policy*
   - **Policy** - *Authentication Policy, Hostname Policy, Node Management Options*
   - **Policy Status** - *Node policy, Enforcement Policy, Node Group, Anomaly Definition, Agent Action Compliance Statistics*
   - If the agent is installed, There are additional tabs. (*The information shown may vary depending on the plugin assigned*)
   - **General**
   - **Device**
   - **System** - *Motherboard, Memory, Disk, OS, Network Connections, Interface, Sharing, User Account, USB Device, Monitor, Printer*
   - **Network**
   - **Software** - *Antivirus Software, installed Program*
   - **OS Update** - *Windows OS Update*
   - **Logs**
   - **IPAM**
   - **Policy**
   - **Policy Status**

### Search Nodes by Contextual Information

To search from all nodes, or from the sensor/group selected in the tree panel, select the search bar from the top of the view pane and choose an attribute to search from the drop down list, specify the MYSQL operators, and define your search term.

- Supported Node Attributes Include:
- **IP**
- **MAC**
- **Status**
- **Node Type**
- **Node Policy**
- **Enforcement Policy**
- **Domain**
- **Authenticated User Username**
- **Authenticated User Full name**
- **Department**
- **Hostname**
- **Node name**
- **Node Description**
- **Platform**
- **Device Name**
- **Device Description**
- **Switch**
- **Switch Port**
- **Connected SSID**
- **Hardware Info**
- **Software Info**
- **Detected Anomaly**
- **Open Port**

And many more.

## 10.2.4 Tagging Nodes

### Understanding Tags

A **Tag** is a custom description that is applied to a Node (MAC + IP) or Device (MAC)to help manage them. One or more identifying **Tags** can be applied to a node or device. **Tags** may also be applied automatically through the log function, or used as a grouping condition.

**Node Tags** apply to a MAC+IP address pair. They are suitable for tracking or applying policy to a specific MAC address and a single IP address that it uses. Because a **node tag** applies to a MAC+IP address pair, a tag will not follow a device when it changes IP addresses, due to a change in static IP, DHCP assigned IP, or a network segment change. The changed IP address and the MAC address are considered to be a separate node.

In contrast, **MAC Tags** will apply to all nodes with the specific MAC address. This makes MAC tags ideal for tracking and controlling devices which may regularly change IP addresses, such as DHCP devices, or mobile devices that regularly change networks.

### Create Tag

1. Go to **Preferences** in the top panel
2. Go to **Properties > Tag**
3. Click **Tasks > Create**
4. For **Name**, type unique name
5. For **Description**, describe what this Tag is for
6. For **Color**, click choose desired color and click **OK**
7. For **Schedule**, this is optional for Lifetime and Expiration
8. If you assign this tag to a separate administrator, check the administrator role entry and select Administrator.
9. Click **Save**

### Tag for Individual Node

1. Go to **Management > Node** in the top panel
2. Find and click on desired **IP address** of **Node**
3. Move to bottom tag of panel
4. Enter the category, name, assignment, description, and so on and click the `ADD` button.
5. Click **Update** Top button

### Tag for Multiple Nodes

1. Go to **Management > Node** in the top panel
2. Find and click **Checkbox** of desired Nodes
3. Click **Tasks > Node and Device > Edit Node Tags**
4. Select **Assign Selected Tags** from the drop-down in the upper left corner of the **Edit Tag Settings** panel
5. Find and click **Checkbox** of desired **Tag** (*You can choose more then one*)
6. Click **Save**

**Note:** In this panel you can select options from the drop-down to edit current Tag Settings.

### Tag for MAC

1. Go to **Management > Node** in the top panel
2. Click **IP address** of the desired MAC Address
3. Move to bottom tag of panel
4. Enter the category, name, assignment, description, and so on and click the `ADD` button.
5. Click **Update** Top button

**Note:** When assigning a tag to a specific MAC address, all nodes with that MAC address will automatically be tagged as well.

### Untag for individual Node

1. Go to **Management > Node** in the top panel
2. Find and click on desired **IP address** of **Node**
3. Click **Delete** for the tag you want to delete in the bottom right corner of the panel.
4. Click **Update**

### Untag for Multiple Nodes

1. Go to **Management > Node** in the top panel
2. Find and click **Checkbox** of desired Nodes
3. Click **Tasks > Node and Device > Edit Node Tag Settings**
4. Select **Remove Selected Tags** from the drop-down in the upper left corner of the **Edit Tag Settings** panel
5. Find and click **Checkbox** of desired **Tag** (*You can choose more then one*)
6. Click **Save**

**Note:** Select **Remove All Tags** to remove all tags from the node.

### Untag for MAC

1. Go to **Management > Node** in the top panel
2. Click **IP address** of the desired MAC Address
3. Find and click on desired **IP address** of **Node**
4. Click **Delete** for the tag you want to delete in the bottom right corner of the panel.
5. Click **Update**

### Tagging with Log Filter

You can automatically tag or untag a node when a specific log occurs.

- For more information on creating log filters. See : *Creating Log Filter*
- For more information on Tagging with log filter. See: *Tagging Assets Using Event*

## 10.2.5 Managing Nodes

### Adding Nodes

Genian ZTNA automatically detects active nodes and registers them in the node list. Also, You can pre-register and use a node when you allow or deny a node before the node has access to the network.

1. Go to **Management > Node** in the top panel
2. Click **Tasks > Node and Device > Add Node**
3. Fill out the **Add Node** up to the panel.

You can register the node by entering IP only, MAC only, or both.(*Other values are optional*)

1. **IP** as `IP address`
2. **Additional IP** Select this when you want to register multiple consecutive IP nodes.
3. **IP Policy Select when you want to use a specific IP policy.**
    - **Allow IP**
    - **Allow IP for Specific MACs**
4. **Start** Select the start date and time in the calendar. Set the availability start period for the node.
5. **End** Select the end date and time in the calendar. Set the availability end period for the node.
6. **IPAM Policy for New Node**
    - **Allow MAC**
    - **Enable Conflict Prevention**
    - **Enable Change Prevention**
    - **Enable Conflict Prevention / Change Prevention**
7. **MAC** as `MAC address`
8. **MAC Policy** Select when you want to use a specific MAC policy.
9. **Start** Select the start date and time in the calendar. Set the availability start period for the node.

10. **End** Select the end date and time in the calendar. Set Set the availability end period for the node.
11. **Sensor** The node selects the location of the sensor to be registered.
12. **Node Type** Select the type of node to be registered.
13. **Node Delete-Prevention** Select whether the node can be deleted. `on` or `off`
14. Configure additional fields (if applicable)
15. Click **Save**

### Add Multiple Nodes

You can register multiple nodes at once using CSV file.

1. Go to **Management > Node** in the top panel
2. Click **Tasks > Node and Device > Import Nodes**
3. Click **Select file CSV** menu in **Import Nodes** up to the panel.
4. Select the CSV file that you created for the format on your file explorer.
5. Select the appropriate **Sensor** from the drop-down menu where the node will be registered.
6. Click **Import**

**Note:** If the format in the CSV file is not correct, the node is not registered.

### Remove Node

You can delete inactive Node data to better organize the networks Node view. You can delete inactive Nodes through policies, or manually delete Nodes as they are no longer found on the network.

### Manually Remove Inactive Nodes

1. Go to **Management > Node** in the top panel
2. Find desired inactive Nodes. Click **Checkbox**
3. Click **Tasks > Node and Device > Remove Node**

**Warning:** If a connected and running node is accidentally deleted, that node will instantly re-register.

### Remove Inactive Nodes Through Policy

1. Go to **Policy** in the top panel
2. Go to **Policy > Node Policy** in the left Policy panel
3. Find and click **[Policy Name]** in the Node Policy panel
4. Find **Management Policy > Deleting Down Node** in the Node Policy panel
5. Set a time for deleting Nodes after a period of inactivity : `30` (*If a Node is offline for a certain period of time, it will be deleted automatically. Default is 30 days*)
6. Click **Update**
7. Click **Apply** in top right corner

### Remove Outdated Node

The Policy Server keeps Node information by default up to 3 days after an IP has been changed.

1. Go to **Preferences > General > Node**
2. Find **Lifetime > Keeping Outdated Node** in the Node
3. Set a time for deleting Nodes after a period of outdated Node information by IP address change : `3` (*Default is 3 days*)
4. Click **Update**
5. Click **Apply** in top right corner

### Monitoring Node Host Names

New Nodes can be screened for compliance with a host name policy.

You can define the allowed host name for nodes per their Node Policy. Criteria for allowed node policy can be constructed based off authenticated User Attributes , IP address or regex.

1. Go to **Policy** in the top panel #. Go to **Policy > Node Policy** in the left Policy panel
2. Find and click **[Policy Name]** in the Node Policy panel
3. Find **Management Policy > Hostname Policy for New Node** and select **On**.
4. Enter your standard hostname, or click **Use Template** to define a compliant host name scheme.

Windows host names may also be changed using the Change Computer Name plugin.

See: *Changing Computer Name*

### Using Node Bucket

The Node bucket is a a grouping tool that can be used for various administrative purposes such as testing or monitoring. It cannot be used for Policy.

### Add to Node Bucket

1. Go to **Management > Node** in the top panel
2. Find the desired node(s) and Click the **Checkbox** on the left of the entry.
3. Click **Tasks > Node and Device > Add To Node Bucket**
4. Click **Ok** (*Nodes added to your Node Bucket will appear in the Management > Node view*)

### Remove from Node Bucket

1. Go to **Management > Node** in the top panel
2. Go to **Sensor Tab > Node Bucket** in the left panel
3. Find **Node** from **Node Bucket** window. Click **Checkbox**
4. Click **Empty** button in top right (*To clean the entire Node Bucket. Click Empty All*)

## 10.2.6 Managing Node Groups

### Creating a Node Group

A **Node Group** is a group of **Nodes** that are similar to each other based off of certain conditions. **Node Groups** allow you take action on many **Nodes** at once versus the same action on many individual **Nodes**.

Genian ZTNA provides two types of **Node Groups**:

- **Policy Group**: is group based on Node-related information such as Node type, IP/MAC information, User information, Authentication, and more.
- **Node Group**: is group based on the Node status, measured by Node Policies and the outcome of associated conditions.

Only **Policy Groups** may be linked to **Node Policies**, while all group types may be linked to **Enforcement Policies**

1. Click **Policy** in the top panel
2. Go to **Group > Node** in the left Policy panel
3. Click **Tasks > Create for Node Policy** or **Create**

Under **General**

1. For **Category**, Choose default or Create New (*This allows you to categorize your Node Groups*)
2. For **ID**, type unique name
3. For **Description** (*Brief description of what this Node Group is for*)
4. Set the **Risk score**.

- The **Risk Score** is set to the risk score of the node as a percentage of the sum of the total score of the node group to which the node belongs, relative to the sum of the total scores of the node groups that have risk scores set.
- The **Risk Level** nodes are risk leveled into the four tiers below based on their risk score.
  - 76-100: Critical
  - 51-75: High
  - 26-50: Medium
  - 0-25: Low

5. For **Status**, **Enabled**
6. Enter the following in Condition section:
   - Boolean: "**AND**" or "**OR**" (*"AND" all conditions have to apply. "OR" any of the conditions have to apply*)
   - Settings: Click **Add** (*These are the various conditions to be applied for proper grouping*)
7. Click **Add**
8. Click **Save**
9. Click **Apply** in top right corner

## Node Group Settings

### Favorite a Node Group

To pin a node group to the top of the list, you can **Star** a node group by clicking the **Star** to the left of the node group name in the view pane.

### Edit Node Group Category

You can change the **Name** or **Link Color** of a node group category to make them more easily recognized.

1. Click the Category name in the left panel.
2. Click **Tasks > Update Category**
3. Fill in the desired **Name**
4. Click the **Color** form to enter the desired Hex Color code, or use the included selector tool.
5. After selecting, click **Ok**
6. Click **Update**

### Bulk Risk Score Settings

1. Select multiple node groups that need risk score settings.
2. Click **Tasks > Bulk Risk Score Settings**.
3. The risk score bulk setting popup dialog provides a description of the node risk score criteria and the ability to set scores in bulk for all selected node groups.
4. The selected node group name, number of nodes, before and after risk scores are displayed in list format.

### Import / Export Node Group in JSON Format

Genian ZTNA Supports importing and exporting node group configurations in json format.

To import or export a node group in json format:

1. Click **Policy** in the top panel
2. Go to **Group > Node** in the left Policy panel
3. Click **Tasks > Export Node Group** (select node group) or **Import Node Group**

## 10.2.7 Node Details

Genian ZTNA displays node detail information and policy status in the Web Console. Node-Details included Network Sensor collected information, Agent collected information and Node Policy status.

In Node-Details, Administrator can check the node policy status, run node tasks and run agent tasks.

### How to check Node-Details

1. Go to **Management > Node** in the top panel
2. Choose Node and Click Node's **IP**
3. Check **Node Details**

| List(tab name) | Collecting from | Collected information |
|---|---|---|
| Node | Network Sensor | IP, MAC, Status, Platform Intelligence information |
| Device | Network Sensor | Nodes for Device, Device Life-Cycle |
| Network | Network Sensor | Service, Open port |
| | Agent Plugin (Collect network information, Inspect TCP Connections, Contorl WLAN) | Traffic, WLAN, TCP Connections |
| System | Agent Plugin (Collect Hardware Information, Collect Monitor Information, Control Network Folder Sharing, Collect System Information Using WMI, Control Personalization) | Hardware information, OS, Network Connections, WMI Status, etc. |
| Software | Agent Plugin (Collect Software Information) | Programs, Antivirus Software |
| OS Update | Agent Plugin (Update Windows, Update macOS) | OS update information |
| Policy | Policy Server | IP Policy, MAC Policy, Node(IP+MAC) Policy |
| Policy Status | Policy Server | Node Policy, Enforcement Policy, Node group, Node group Risk Score, Security Level, Agent Action Compliance Statistics, etc. |
| Malware | Agent Plugin (Collect Malware Information) | Malware information |
| Logs | Policy Server(Log Server) | Audit logs based on node information(IP+MAC) |

## 10.2.8 Security Level

By setting security levels on node information, you can efficiently manage the distinction and access restrictions for each node based on their security level. Through this configuration, you can apply appropriate security policies according to the importance of each node and control access between nodes.

### Levels

Security levels are divided into default security levels and user-defined security levels. Each security level has a priority set according to its importance. This priority is expressed as a number, and the lower the number, the higher the importance.

- **Default Security Levels**
  - Confidential: The highest priority (most important)
  - Sensitive: Lower priority than confidential
  - Open: Lower priority than sensitive
- **User-defined Security Levels**

  Users can define custom security levels by specifying priority, name, and level color, allowing them to create their own security levels.

### Table Details

- **Name**
  - Displays the name of the security level.
- **Preview**
  - The preview tag is created by the first two characters defined in the name column.
  - For example, "TEST" → only "TE" is displayed, "테스트" → only "테스" is displayed.
- **Node Count**
  - The number of nodes refers to the total number of nodes in the node groups (role, location, risk, Compliance) associated with the security level.
- **Node Groups**

  Node groups are divided into three categories below, and one node group can belong to multiple categories. For example, the node group "PC" can belong to the role, location, and risk categories simultaneously.

  - **Role:** (Currently undefined)
  - **Location:** (Currently undefined)
  - **Risk:** (Currently undefined)
- **Security Compliance**
  - **Compliance:** (Currently undefined)
- **Description**
  - The description provides additional or separate explanations for the security level.
- **Priority**
  - Priority means that a lower number indicates greater importance, so the items are listed in descending order. You can change the rank using the 'up' and 'down' buttons.

### User Function Guide

Security Level Page Location : Policies > Governance > Security Level

**Create Security Level**

A new security level can be added. To add a security level, the name and priority are mandatory fields that must be entered when creating the security level. The name is a critical identifier for the security level, and the priority is represented by a number indicating the importance of the security level. Higher numbers indicate higher importance.

1. Click **Select Action** and choose **Create** from the dropdown menu.
2. After clicking **Create**, a form to create a security level will appear. Fill out the form.
3. After filling out the form, click the **Create** button.

---

**Note:**

- **Node Groups:** The left box for role, location, and risk displays a list of existing node groups, while the right box shows the list of assigned node groups.
- **Security Compliance:** The compliance items are from the list created in Policies > Governance > Security Compliance. If the list does not exist, you must first create the security compliance.

**Delete Security Level**

Users can freely delete created security levels.

**Note:** Default security levels cannot be deleted.

**1.** Select the security level to delete by checking the checkbox in the first column of the table.

**2.** Click **"Select Action"** and choose **Delete** from the dropdown menu.

**3.** After clicking **Delete**, a modal window will appear asking for confirmation. Click "Delete" to confirm or "Cancel" if you do not want to delete.

**Edit Security Level**

The contents of an existing security level can be modified by the user.

**1.** Click the **security level** in the table that needs to be edited.

**2.** After clicking the security level, a form will appear with the information for modification. Enter the new information.

**3.** After entering the new information, click **Edit** to modify the existing details of the security level.

**Note:** After creating, editing, or deleting a security level, a "Apply Changes" button will blink in the page menu. When this happens, click "Apply Changes" to review the modifications, then click "Apply Policy" to save the changes.

**Search for Security Levels**

You can easily find specific security levels by entering a search keyword. The search box offers filters such as "Quick Search", "Name", and "Node Group" for searching by these criteria.

**Filters**

**Quick Search:** The search keyword will be matched with the security level's name.

**Name:** The search keyword will be matched with the security level's name.

**Node Group:** The search keyword will be matched with the security level's node group.

### Status & Filters

- In Management > Node > Status & Filters, you can view the status of security levels.
- Click on the security level to view the status of the number of nodes in the security level in Pie Chart format.
- The security level submenu provides a link to view the node list by security level.

### 10.2.9 Risk Level

Risk level allows you to identify the risk level of nodes by setting risk scores for node groups. The risk level of a node is determined by summing the risk scores of the node groups to which the node belongs.

#### Level Definition

- **Critical (76-100):** Nodes with a sum of risk scores between 76 and 100 from node groups
- **High (51-75):** Nodes with a sum of risk scores between 51 and 75 from node groups
- **Medium (26-50):** Nodes with a sum of risk scores between 26 and 50 from node groups
- **Low (0-25):** Nodes with a sum of risk scores between 0 and 25 from node groups

#### Risk Score Setting

Risk scores for node groups can be set in two ways.

**Risk Score Setting in Node Group Management**

Risk score settings can be configured on the node group detail page at Policy > Groups > Node (node group).

Select multiple node groups from the node group list, click the **Tasks** button, and then click **Bulk Risk Score Settings** to open the risk score bulk setting page.

**Risk Score Setting in Policy Management**

Risk scores can be set at Policy > Governance > Risk Score.

**1.** Click the node group selection button at the bottom of the node group table displayed on the right side of the screen to add node groups whose settings you want to change.

**2.** When you change the risk score of an added node group, you can check the updated values in the statistics preview table on the left. Click the node count in the preview table to view the list of target nodes by grade.

**3.** Click the **Reset** button at the top of the node group selection table to reset the risk scores of node groups.

**4.** To apply different risk scores without changing existing settings, click the **Add Tab** button on the right side of the tab to add a tab and set risk scores.

**5.** To apply the changed risk scores, click the **Apply Risk Score** button to reflect the risk scores applied to the current tab.

**6.** Click **Apply Policy Changes** at the top right of the screen.

#### Status & Filters

In Management > Node > Status & Filters, you can view the risk level status and the list of nodes for each grade.

## 10.3 Monitoring IP Address

The **Network Sensor** monitors IP Addresses and presents the usage status of the IP Address in real-time through the intuitive Matrix view.

### 10.3.1 Browsing Sensor IP Status

You can browse through **Network Sensors** and see current status from the **IPAM** panel.

#### To Find the Overall Status of IP usage by Network Sensor Per Network

1. Go to **Management > IP Address** in the top panel
2. Click on **name of Network Sensor** in the left IPAM panel

### 10.3.2 Browsing IP Status Using Matrix View

You can browse **IP usage** and see **current status** from the Matrix view.

#### Find how IP Addresses are being used for each Network Segment

1. Go to **Management > IP Address** in the top panel
2. Click on **name of Network Sensor** in the left IPAM panel

#### Find Details

1. Go to **Management > IP Address** in the top panel
2. Click on **name of Network Sensor** in the left IPAM panel
3. Mouse over an **IP Address block** to see more information

## 10.4 Monitoring Switch

You can see how many devices are connected to specific Switch ports, connection status (*up/down*), port-level security status, 802.1x information, traffic, utilization, and more.

### 10.4.1 Browsing Switches

To identify a **Switch**, Genian ZTNA sends out an **SNMP request**. If the response to the request comes back with an OID (dot1dBaseBridgeAddress(1.3.6.1.2.1.17.1.1)), then Genian ZTNA labels that **MAC Address** as a **Switch**. If switches are not identified with the public community string you will need to check the community string configuration or run a SNMPWALK to verify switch is responding properly.

### Set Node Scan Interval On Network Sensor

1. Go to **System** in the top panel
2. Go to **System > Sensor** in the left System Management window
3. Click **Network Sensor IP**

Under **Settings** tab:

1. Click **Sensor Settings**

Under **Node Information Scan**:

1. For **Update Interval**, edit time interval (1 minute - 1 year)
2. Click **Update**

### Set SNMP Settings For SNMP Scan

1. Go to **Preferences** in the top panel
2. Go to **General > Node** in the left Preferences window

Under **SNMP**:

1. Click **Add** for SNMP settings

1. For **SNMP Version** select `Version 2c` or `Version 3`
2. In Version 2, enter read/write community string(*e.g. public,private*) For **Community**
3. In Version 3, enter **Username** and Select the appropriate **Security Level**
4. There are `NoAuth/NoPriv`, `Auth/NoPriv`, and `Auth/Priv` in the **Security Level**

1. For **Collecting Network Information**, needs to remain **On** (*If set to Off SNMP information will not be collected*)
2. For **Update Interval**, edit time interval (*5 minutes – 1 year*)
3. For **Time Object**, specify time object
4. Click **Scan Now** button for SNMP to scan instantly

### Use SNMPWALK on Windows machine To Verify Switch Response

**Note:** If a Switch fails to populate in Switch List, first check Switch Community strings on switch, then run a SNMPWALK.

1. Login to your **Switch** and verify it's SNMP Community strings
2. Verify Genian ZTNA has correct **SNMP Community strings** set
3. Using Windows machine and Net-SNMP do the following:
   - Download **Net-SNMP** for Windows (*Set the default folder location to C:Net-SNMP to easily locate it*)
   - Open **Command Prompt** and change directories. Type **cd /Net-SNMP/bin**
   - Run the snmpwalk using this command: **snmpwalk -Os -c public -v 2c "Switch-IP" .1.3.6.1.2.1.17.1.1** (*e.g. snmpwalk-Os -c public -v 2c 192.168.50.5 .1.3.6.1.2.1.17.1.1*)

- Should display **mib-2.17.1.1.0 = Hex-STRING: XX XX XX XX XX XX** (*This determines that the switch is responding properly to SNMP Requests*)

### Configure Switch Specific Information

**Note:** To enable switchport blocking enforcement, a write community or an SNMPv3 user with write permissions must be used. For more info see *Configuring Switch Port Control*

1. Go to **Management > Switch** in the top panel and click **Switches** folder in the left Switch Management window.
2. Find and click desired **Switch** name in the main Switches window
3. By SNMP Data Collection , select **On** or **Off**.
4. Select SNMP **Version 2c** or **Version 3**.
5. Enter the Community strings in the **Read/Write Community** fields or enter the **SNMP V3 Security information**.
6. Click **Update**

## 10.4.2 Switch Ports

### Browsing Switch Ports

The **Switch Port** List provides detailed information about every **Switch Port** detected on the network. The **Switch Port List** can be viewed by going to the **Switch Management Panel** in the top left, and clicking on Switch Ports.

### Contextual Information

1. Go to **Management > Switch**
2. Find and click on desired **Switch Name**
3. Find information such as:
   - **Switch** - Hostname of Switch
   - **Port** - Port Number of Switch
   - **Description** - Description of port
   - **Authenticated User** - Authenticated user's Full Name through connected switch port
   - **Hostname** - Hostname of node through connected switch port
   - **IP / MAC** - IP / MAC through connected switch port
   - **Nodes** - The number of nodes through connected switch port
   - **MACs** - The number of macs through connected switch port
   - **Connection Type** - Connection type through connected switch port
   - **Link** - Link On Green icon, Link Off Gray icon
   - **Admin Down** - Indicates port shutdown.
   - **Duplex** - Link Duplex

- **Speed** - Link Speed
- **Traffic** - bps through connected switch port
- **Utilization** - Port utilization `%`
- **VLAN ID** - VLAN ID assigned to the port
- **Trunk Port** - Show if trunk port is enabled `trunk` or blank
- **Port Security Settings** - Status of Port Security settings `On` or `Off`
- **802.1x Settings** - Status of 802.1x settings `Enable` or blank
- **Auth MACs** - The number of Authenticated MAC address

### Add to a Node Bucket

1. Go to **Management > Switch** in the top panel
2. Find **Switch Ports** to add. Click **Checkbox** (*Make sure that port has at least 1 node connected*)
3. Click **Tasks > Add To Node Bucket**
4. Click **Ok** (*Nodes added to your Node Bucket will appear in the Management > Node view*)

### Remove from a Node Bucket

1. Go to **Management > Node** in the top panel
2. Go to **Sensor Tab > Node Bucket** in the left panel
3. Find **Node** from **Node Bucket** window. Click **Checkbox**
4. Click **Empty** button in top right (*To clean the entire Node Bucket. Click Empty All*)

### Searching Switch Ports

You can search **Switches** and their information using the **Search Bar** located at the top of the main panel. Details that can be searched are Switch Name, Port, Description, Auth User, Hostname, or the Number of MACs/Nodes.

### Changing Switch Port Description

1. Go to **Management > Switch** in the top panel
2. Find and click **Switch Port** in the **Port** column

Under **General** tab

1. For **Description field**, enter a description
2. Click **Update**

#### Changing Switch Port VLAN ID

1. Go to **Management > Switch** in the top panel
2. Find and click **Switch Port** in the **Port** column

Under **General** tab

1. For **VLAN ID**, enter a number
2. Click **Send SNMP Command**

#### Changing Switch Port Default VLAN

1. Go to **Management > Switch** in the top panel
2. Find and click **Switch Port** in the **Port** column

Under **General** tab

1. For **Default VLAN**, enter a number. When a node attached to a switchport falls under an Enforcement Policy where switch port VLAN assignment is not specified, the switch port will be set the the **Default VLAN**. Enter **0** as the **Default VLAN** to perform no change to the Switch Port.
2. Click **Set**

**Note:** In order to change a Description, or VLAN ID the read/write Community string or an SNMPv3 Username with write permissions for that Switch must be specified.

### 10.4.3 Troubleshooting

- *Cisco Switch-port Information Is Not Showing*

## 10.5 Monitoring Wireless LAN

Network Sensors with built-in Wireless Adapters scan the network and detect all Internal and Neighboring wireless SSIDs. The Policy Server communicates with the installed Agent on the endpoints to leverage their built-in Wireless Adapters to collect SSID information as well as Internal SSIDs. You can browse and search through the WLAN view and create groups for monitoring, managing and enforcing policies. (*Without a Wireless Adapter you will not detect any WLAN SSIDs*)

### 10.5.1 Browsing SSIDs

You can find any wifi-enabled devices and list them by **Network Sensor** or **WLAN AP** status (*SSID usage, security status, frequency, 802.11 protocol, signal strength, detected date, connected wireless devices, etc.*)

### View All the Detected SSIDs on your Network

1. Go to **Management > WLAN** in the top panel

### Customize Table Columns

1. Click **Tasks** in the top left of the WLAN Node list
2. Select **Edit Columns**
3. Move column topics from **Available** to **Selected** to add to the **WLAN List**
4. **Drag** and **Drop** columns to change the display order
5. Click **Update**

### Searching SSIDs

You can search **SSIDs** and their information using the **Search Bar** located at the top of the **Management > WLAN** main panel. Details that can be searched are **SSID, MAC Address**, **Vendor**, and **Security Settings**.

### WLAN Status and Filters

WLANs can be viewed by pre-defined filters in the Status & Filters section.

### Viewing Stations

**Stations** also referred to as **STA**, are devices that have the capability to use the 802.11 protocol. These can be fixed, or mobile.

### View Station Details

1. Go to **Management > WLAN** in the top panel
2. Find **Stations** column in the main **WLANs** window. Click **Stations** to sort column (*This will sort the column based off of a number of Stations for each MAC Address*)
3. **Click the Number in the Stations column of the desired device**
    - You can now view all Stations for MAC Address and change view between **External/Internal**
    - Use the **Search bar** to find specific **Stations** (*Searches can also be filtered between External/Internal or Internal*)

### Finding SSID Physical Location

In a BYOD environment, unknown devices appear at any given time, and when they do, it is the Network Administrators job to track them down. To figure out what devices are in or outside of a network, various different steps are needed to locate that device's physical location.

### Discover what SSID a Device belongs to

If a rogue device shows up on the network, the first step to tracking it down is to find which SSID it is connected to.

1. Go to **Management > Node** in the top panel
2. Click the **IP Address** of the desired node
3. In the **General** tab, under **SSID Connected**, click the **SSID** displayed

All information relevant to that SSID is now displayed in the main panel.

### View the Signal Strength of a Device

A devices relative location can be determined by monitoring the signal strength to figure out which direction and how close it is. The stronger the signal, the closer the device.

The signal strength is depicted in two ways:

- **Color/Icon**: Red means weak, Orange means not an ideal signal, and Green means a strong signal connection
- **dBm**: This is the decibel strength of the signal. The lower the numbers, the closer the stronger the signal and closer the device

The device can now be tracked down to a relative location. The device can then be looked for or employees can be inquired about the device until it is found.

## 10.5.2 Detecting Internal SSID

SSIDs are differentiated in the list from **Internal** to **Neighboring APs**.

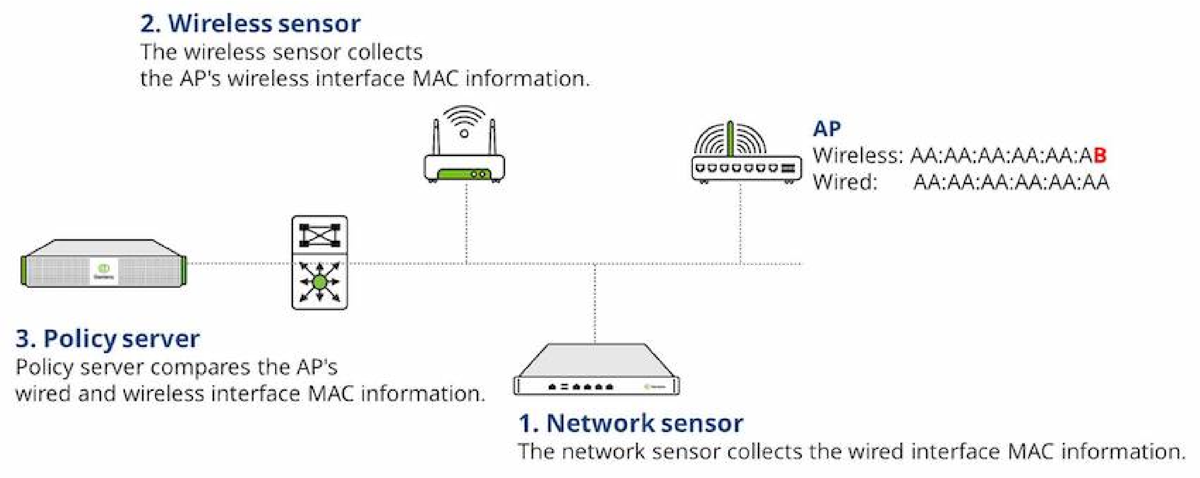
### Show Internal SSIDs

1. Go to **Management > WLAN** in the top panel.
2. Find and click column labeled **Internal** in the main WLANs window. All internal APs will be identified with a checkmark in this column.

### How to Find an Internal AP

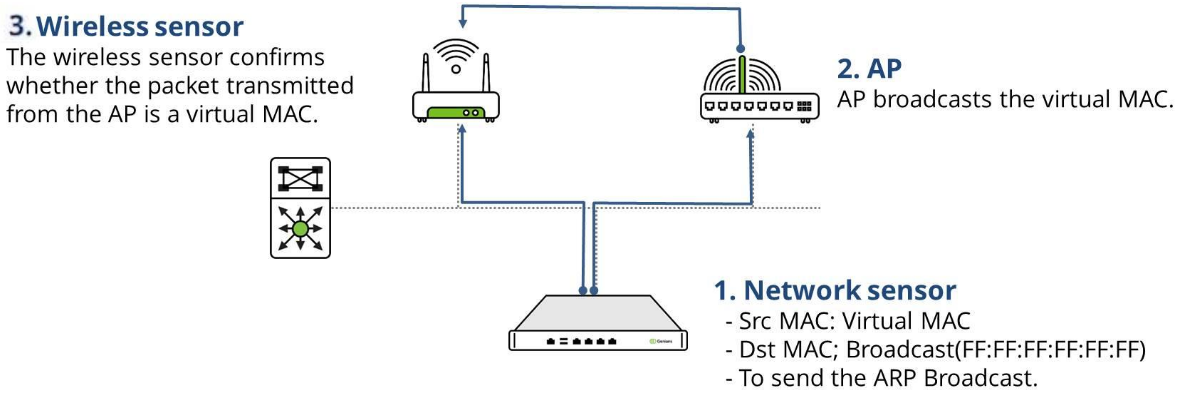
The AP detected by the Genian ZTNA Agent and the wireless sensor can be distinguished as an internally connected AP by several criteria. The Internal AP detection method is as follows:

**MAC Similarity Check**


2. Wireless sensor
The wireless sensor collects
the AP's wireless interface MAC information.
AP
Wireless: AA:AA:AA:AA:AA:AB
Wired: AA:AA:AA:AA:AA:AA
3. Policy server
Policy server compares the AP's
wired and wireless interface MAC information.
1. Network sensor
The network sensor collects the wired interface MAC information.

1. The network sensor collects the wired interface MAC information of the internally connected AP.
2. The wireless sensor collects the AP's wireless interface MAC information and sends it to the policy server.
3. Policy server compares the AP's wired and wireless interface MAC information and if they are similar, it determines that the access point is internal.

**Packet broadcasting**


3. Wireless sensor
The wireless sensor confirms
whether the packet transmitted
from the AP is a virtual MAC.
2. AP
AP broadcasts the virtual MAC.
1. Network sensor
- Src MAC: Virtual MAC
- Dst MAC; Broadcast(FF:FF:FF:FF:FF:FF)
- To send the ARP Broadcast.

1. The network sensor broadcasts a virtual MAC to the network.
2. At this time, AP connected to the internal network broadcasts the virtual MAC received from the network sensor to the AP's wireless band.
3. The wireless sensor is monitoring the wireless network and when the wireless sensor receives the virtual MAC from the AP, it judges the AP as the internal AP.

**Agent**

1. The Agent collects all network interface information on user device.
2. This information is checked for matches against known network interface MAC addresses.

**SNMP with wireless controller**

1. Information is collected from wireless controller using SNMP.
2. This information is checked for matches against known MAC addresses from the wireless controller.

### 10.5.3 Creating Wireless Groups

A **Wireless Group** is any detected amount of **SSIDs** that are grouped together due to conditions or properties that have been set as identifiers. This is to help Network Administrators quickly navigate to specific **SSIDs** or **Categories** when dealing with a large quantity of SSIDs.

#### Create a WLAN Group

1. Go to **Policy** in the top panel
2. Go to **Group > WLAN** in the left Policy panel
3. Click **Tasks > Create**

Under **General**:

1. For **ID**, enter a unique name
2. For **Description**, type what this group consists of
3. For **Status**, select **Enabled** from the drop-down list.
4. For **Generating Logs** turn **On** to show logs when SSIDs are added to the group

Under **Condition**:

1. For **Boolean Operator**, choose **AND** to match all conditions, or **OR** to match any conditions
2. For **Conditions** click **Add** to add conditions

Under **Settings**:

These are conditional settings that allow you to be specific in identifying SSIDs:

1. For **Criteria**, you can select MAC, Protocol, SSID, Security Settings, Tag, and more
2. For **Operator**, allows you to choose equal to, not equal to, contains, does not contain, and more
3. For **Value**, type in some value to match what your searching for
4. For **Description**, type what this condition does
5. Click **Add**
6. Click **Save**

#### Assign a WLAN Tag

You can Tag SSIDs to help categorize them and to build Policies using these Tags:

1. Go to **Management > WLAN** in the top panel
2. Find and click **Checkbox** of desired **SSIDs**
3. Click **Tasks > Edit WLAN Tag Settings**

Under **Assign WLAN Tag**

1. In drop-down select **Assign Selected Tags**
2. Click **Checkbox** of tag to apply
3. Click **Save**
4. Click **Apply**

### Assign a WLAN Group

You can group SSIDs that are similar to each other based off of Tags, SSID Name, Vendor, Security Settings, Protocol, and more.

1. Go to **Management > WLAN** in the top panel
2. Find and click **Checkbox** of desired **SSIDs**
3. Click **Tasks > Edit WLAN Group Settings**

Under **Assign WLAN Group**

1. For **Action**, select **Add** or **Remove**
2. For **WLAN ID**, select **SSID, MAC,** or **MAC+SSID**
3. For **WLAN Group**, group to associate to
4. Click **Save**
5. Click **Apply**

### Group by Network Sensor

If you have many Network Sensors, it is difficult to manage all of these in one list. Here you have the ability to create groups and assign **Network Sensors** to them.

1. Go to **Management > WLAN** in the top panel
2. Click **Edit Tree icon** in the top right corner
3. Right click on either **WLAN AP** or **WLAN Client**, click **Create** (*New node group will appear for you to rename*)
4. Right click on newly created group and click **Assign**
5. Search for **Network Sensor** and select each **Checkbox** you want to add to this group
6. Click **OK**

**Note:** If you have a presence around the world you can create **Country Groups** and add **Network Sensors** that are located within those countries.

## 10.6 Managing Dashboards

Dashboards are a collection of Widgets. Dashboards give you an overview of the reports and metrics that are most important to you. You can personalize Dashboards by customizing Widgets. By default, Genian ZTNA provides over 100 Widgets which are categorized by the following groups.You can add, delete, customize and share your dashboards depending on your requirements.

### 10.6.1 Create Dashboards

1. Click **Add Tab** on the right side of the tabs on the main screen.
2. In the Add Dashboard Tab window, enter **Tab Name**.
3. Click **Confirm**.

### 10.6.2 Remove Dashboards

1. Hover your mouse over the name of the tab you want to delete.
2. Click the **Delete** next to the name.
3. **Confirm** in the confirmation window.

### 10.6.3 Add a Widget to Dashboard

1. Go to **Dashboard** in the top panel.
2. Click **Tools > Add Widget**.
3. Find **Category** section in the Add Widget window. Select **Category**.
4. Find **Widget** section in the Add Widget window.
5. Click **Add Widget**.

### 10.6.4 Arrange Widgets

Widgets can be grabbed by the title bar and dragged to the desired location.

### 10.6.5 Customize the Settings of a Widget

Hovering over a widget will make a gear icon appear in the upper right corner of the widget. Clicking the gear icon will display that widget's settings. Setting changes can be applied to the widget by clicking Save when finished.

### 10.6.6 Delete a Widget

1. Go to **Dashboard** in the top panel.
2. Find **Widget** and hover over the title bar.
3. Click **X**.
4. Click **Confirm**.

### 10.6.7 Creating a Sensor Map

To monitor and customize Sensor Placement globally using Google Maps.

- To use Sensor Map, you must obtain the Google Maps API Key.
- For use, please follow the API Key issue guidelines.

1. Click **Add Tab** on the right side of the tabs on the main screen.
2. In the Add Dashboard Tab window, enter **Tab Name**.
3. Activate **Sensor Map**.
4. Click **Confirm**.
5. Enter the issued **API Key**.
6. Click **Confirm**.

### 10.6.8 Place a Sensor on Sensor Map

1. Go to **Sensor Map** tab.
2. Find **Menu** icon in the upper right corner of the main panel.
3. Find **Sensor bubble** and drag it to the desired location.

### 10.6.9 Export Dashboards

You can export Dashboards into several formats:

1. Click **Dashboard** in the top panel
2. Select **Dashboard** tab you choose to export
3. Click **Export icon** and a popup window will be displayed.
4. Select an export file type.
5. Select whether to show the report title page.
6. Set the page size.
   - You can select A4,A3,A2,B4,B3,B2,LETTER page size by PORTRAIT/LANDSCAPE.
   - Custom horizontal and vertical size settings allow you to output all widgets that appear in the dashboard on a single page.
7. Click **Export**.

### Creating Mobile Platform Detection Widget

Administrators can create Mobile Platform Detection Widget for monitoring Mobile devices.

#### Step 1. Create Mobile platform Node Group

Please refer to *Managing Node Groups* for create new node group

**Create Android Nodegroup**

- Node Group Type : Status Group
- **Group Condition**
  - Criteria : OS
  - Value : Android

**Create Iphone OS Nodegroup**

- Node Group Type : Status Group
- **Group Condition**
  - Criteria : OS
  - Value : iPhone OS

#### Step 2. Assign Node Group to Widget

1. Go to **Dashboard** in the top panel.
2. Click **Tools > Create Dashboard**.
3. Find **Node** in Categories list.
4. Find **Node Group** or **Node Detection Statistics by Node Group**.
5. Click **Add Widget**.
6. Find Node Group on left side and move to **right**.
7. Configure View Name, Update Interval, Value Font Size, Lable Font Size.
8. Click **Save**.

## 10.7 Genian ZTNA Monitor(for Mobile)

Genian ZTNA can check the status on Mobile through Genian ZTNA Monitor. It also provides real-time information to the administrator through **Push Alarm.**

### 10.7.1 Receive alarms via Mobile App

#### Support Feature

1. Push alarm when detecting new node.
2. Push alarm when IP application occurs.

#### Setting method

1. Login after running Genian ZTNA monitor
2. Administrator push token registration confirmation

- Accessing Web Console via WebBrower > Management > User > Admin ID accessed by App Click > Administrator Tab> Notification > Confirm items added to administrator Push Token.*

**Note:** **Install method App** : Install "Genian ZTNA monitor" app on mobile device (Android and IOS support)

## 10.8 Managing Nodes in the Cloud

As cloud infrastructure expands, the importance of ensuring security visibility and asset integration increases. Especially in a Zero Trust security environment like Genians ZTNA, real-time collection and monitoring of cloud resources form the foundation of security policies. The Genian ZTNA Cloud Collector can be enabled to collect information on IP-supported nodes within a cloud environment. On a configured schedule, the Cloud Collector queries the Cloud Service Provider to identify nodes in the designated environment and other critical cloud-related details.

### 10.8.1 Cloud Environment Configuration

Prior configuration is required to use the Cloud Collector. Please follow the steps below to complete the setup before use.

1. *Cloud Provider Management*
2. *Site Management*
3. *Collector*

### 10.8.2 Cloud Node Detection Check

This page allows you to search nodes registered by sensors using various status views and filters.

1. From the top menu, go to Management > Node.
2. In the left pane, click the site name created in the previous steps.
3. All resources in the previously specified VPC and subnet will appear as nodes.
4. Detailed cloud resource information for discovered nodes can be viewed through the node information. Go to Management > Node, click the node's IP, and scroll down to the Cloud section to see more details.

**Note:** For information on node discovery, grouping, and monitoring, refer to Network Node Monitoring.

## 10.9 Network Traffic

### 10.9.1 Enabling Netflow Agent

Genian ZTNA can monitor network traffic by utilizing the Netflow Agent function of a sensor. This flow information of connected devices provides enhanced Network Observability which is a crucial component for enforcing ZTNA policies. Once enabled, the Netflow Agent will log flows of all traffic flowing through the sensor. Information logged in flows includes but is not limited to:

- **Source IP Address**
- **Destination IP Address**
- **Protocol (UDP/TCP)**
- **Source Port**
- **Destination Port**
- **Application**
- **Geolocation Data**
- **User (which user the flows are associated with)**
- **Number of Packets**
- **Number of Bytes**
- **Flow Start (date/time)**
- **Flow End (date/time)**

**Note:** In order to see flows utilizing the Netflow Agent, traffic from an endpoint must be flowing through a network sensor. To route traffic through a sensor, following the instructions below to deploy a cloud gateway and ZTNA client.

*Managing Nodes in the Cloud*

*Controlling Access to Cloud Resources*

To enable the Netflow Agent on the network sensor:

1. Go to **System > Sensor** in the top panel
2. Click on **Edit Sensor Settings** for the tap_1 sensor interface
3. Scroll down to **Traffic Monitoring** section and toggle **Netflow Agent** to **On**
4. Click **Update** at the bottom of the page

To test and validate that flow data is being collected and logged:

1. Go to **Log > Flow** in the top panel
2. Flows should be populated for any traffic routing through the network sensor

**Note:** Only flows for connected ZTNA clients will be logged.

To view connected ZTNA clients:

1. Go to **System > Site** in the top panel

2. Under the ZTNA - Client column, click on the **(*)** link to view connected clients
3. Flows from these clients should be visible in the flow logs

To view summary information for flow data:

1. Go to **Dashboard** in the top panel
2. Click on **Flow Data** tab in Dashboard
3. View various widgets including Top Traffic by Source IP, Destination IP, User, etc.

CHAPTER

ELEVEN

# CONTROLLING NETWORK ACCESS

**Note:** This feature required Professional or Enterprise Edition

Based on the information collected through the network sensor and the agent, a policy can be established to restrict network use by the non-compliant device. Enforcement policies can be applied in a variety of ways.

## 11.1 Understanding Access Control Policy

Genian ZTNA uses 3 main policies to control network access, **IP/MAC Policy**, **Node Policy**, and **Enforcement Policy**.

### 11.1.1 IP/MAC Policy

IP and MAC features allow an administrator to manually or automatically control a devices IP address, and to allow / deny network access based off of IP or MAC address.

To use these features in Genian ZTNA, you must configure the network sensor(s) in enforcement mode and enable an IP/MAC policy. This section will explain how to enable IPAM policy, enforce Conflict/Change Prevention, and set up time allowances for IP/MAC addresses.

#### Preparing Access Control using IPAM

You can enable enforcement by enabling the **Unauthorized Device** default policy, and changing the default policies on each individual sensor.

#### To Enable "Unauthorized Device" Policy

By default, the “**Unauthorized Device**” enforcement policy is disabled. Before controlling nodes using the Policy, the enforcement policy for “**Unauthorized Device**” must be enabled.

1. Go to **Policy** in the top panel
2. Go to **Enforcement Policy** in the left Policy panel
3. Click **Unauthorized Device** name in the Enforcement Policy window
4. Find **General > Status** section to **Enabled**
5. Click **Update**
6. Click **Apply** in top right corner

### To Change Sensors IPAM Default Policy

The Default Policy can be changed on each sensor's settings

1. Go to **System** in the top panel
2. Go to **System > Sensor** in the left System Management panel
3. Click the desired sensor's **IP Address**
4. Click the **Settings** tab and click **Sensor Settings**
5. Find **IPAM Policy** section, change **IPAM Policy** for **New Node** accordingly
6. Click **Update**

Options for New node policy are as follows:

- **Deny MAC**: Deny a MAC Address
- **Deny IP**: Deny an IP Address
- **Deny IP/MAC**: Deny an IP and MAC Address
- **Allow**: Allow an IP and MAC (default)
- **Enable Change Prevention**: Enable IP Change Prevention for a node's IP/MAC
- **Enable Conflict Prevention**: Enable IP conflict Prevention for a node's IP/MAC

### Changing IPAM Policy

You can also manually allow or deny from Node List and Matrix View.

the following IPAM options are available when selecting nodes from the node view or IP's from the matrix view

### To Allow or Deny IPAM from Node List

1. Go to **Management > Node** in the top panel
2. Click **Checkbox** of the **desired node** in the Node window
3. Click **Tasks > IP/MAC Policy**
4. Select the desired **options:**

- **Deny IP**
- **Allow IP**: Allow an IP Address, but do not reserve the IP address.
- **Allow IP for Specific MACs**: Allow an IP Address, and reserve it to a specific MAC address. (Additional MACs may be added by selecting the node, and editing under the IP Policy section.)
- **Enable Hostname Policy for IP** (Require host name to meet the Hostname Policy defined in the node policy. See: *Managing Nodes* )
- **Remove Hostname Policy for IP**
- **Time Restriction for IP**: Set allowed time period for IP.
- **Edit IPAM New Node Policy for Reserved IP**: (Choose: Allow MAC, Enable Conflict Prevention, Enable Change Prevention, or Enable Conflict Prevention/Change Prevention)
- **Edit IP Purpose** (Choose: Dynamic, Static, or Temporary IP Address)

- **Deny MAC**
- **Allow MAC**: Allow an IP Address, but do not mandate an IP address.
- **Allow MAC - Current IP for Current Sensor**: Allow a MAC Address, and mandate a specific IP address on a specific sensor managed network.
- **Allow MAC - Current IP for All Sensors**: Allow a MAC Address, and mandate a specific IP address.
- **Time Restriction for MAC**: Set allowed time period for MAC.
- **Deny IP/MAC**: Deny an IP and MAC Address
- **Allow IP and MAC**: Allow an IP and MAC
- **Enable Conflict/Change Prevention**: Enable IP Change and conflict Prevention for a node's IP/MAC

### To Allow or Deny IPAM from Matrix View

1. Go to **Management > IP Address** in the top panel
2. Click on the desired **Sensor's Name**
3. Find **IP Address Square** and click to **highlight square**
4. Click **Tasks**
5. Select the desired **options:**

- **Add Node**
- **Remove Node**
- **Deny IP**
- **Allow IP**: Allow an IP Address, but do not reserve the IP address.
- **Allow IP for Specific MACs**: Allow an IP Address, and reserve it to a specific MAC address.
- **Enable Conflict/Change Prevention**: Enable IP Change and conflict Prevention for a node's IP/MAC
- **Edit IPAM New Node Policy for New Node Settings** (Choose: Allow MAC, Enable Conflict Prevention, Enable Change Prevention, or Enable Conflict Prevention/Change Prevention)
- **IP Time Allowance**
- **Assign User IP Ownership**
- **Assign Department IP Ownership**
- **Define IP Purpose** (Choose: Dynamic, Static, or Temporary IP Address)

**Note:** Denied IP/MAC Addresses are highlighted in light red with the text of the IP Address having a strikethrough

### Configuring IP Change Preventions

You can prevent users from changing their IP Address. Changing an IP can lead to conflicts or compromising issues where users can gain privileges they were not intended to have. For instance, an Administrator could have a designated IP Address set up to allow internet access, while all others are blocked. If an employee is able to change their IP to that designated address, then that employee will gain internet access when they are not allowed to.

### How IP Change Prevention Works

The Sensor watches and analyzes packets that are being sent from each device. When a new node is detected, the Sensor sends a gratuitous ARP request. If a machine receives an ARP request containing a source IP that is different than the previously used IP for that MAC, then it knows a change has occurred, and the offending node will be enforced against.

### To Enable IP Change Prevention

1. Go to **Management > Node** in the top panel
2. Click on the desired node **IP**
3. Click **Policy** tab
4. Find **MAC Policy** section, click **Allow MAC - Enable Change Prevention (Choose: Specific Network or All Networks)**
5. Enter **IP Address(es)** in the form below to allow them to be used the selected device.
6. Click **Update**

### To Disable IP Change Prevention

1. Go to **Management > Node** in the top panel
2. Click on the desired node **IP**
3. Click **Policy** tab
4. Find **MAC Policy** section, click **Allow MAC – Disable Change Prevention**
5. Click **Update**

> **Warning:** This feature should only be used on nodes using a static IP to avoid accidental blocking.

### Configuring IP Conflict Prevention

You can prevent users from using an IP Address that is already assigned to another device. IP conflicts can result in routing issues, or users can gaining privileges they were not intended to have. For instance, an Administrator could have a designated IP Address set up to allow internet access, while all others are blocked. If an employee is able to change their IP to that designated address, then that employee will gain internet access when they are not allowed to.

### How IP Conflict Prevention Works

The Sensor watches and analyzes packets that are being sent from each device. When a new node is detected, the Sensor sends a gratuitous ARP request. If a machine receives an ARP request containing a source IP that is reserved for another MAC address, a conflict is identified, and the offending node will be enforced against.

### To Enable IP Conflict Prevention

1. Go to **Management > Node** in the top panel
2. Click on the desired node **IP**
3. Click **Policy** tab
4. Find **IP Policy** section, select **Allow IP – Enable Conflict Prevention**
5. Enter **MAC Address(es)** in the form below to allow them to use the **IP**.
6. Click **Update**

### To Disable IP Conflict Prevention

1. Go to **Management > Node** in the top panel
2. Click on the desired node **IP**
3. Click **Policy** tab
4. Find **IP Policy** section, select **Allow IP – Disable Conflict Prevention**
5. Click **Update**

### Allowing IP/MAC Based On Time

You can allow an IP Address for a designated period of time (Date, Hours, and Minutes) to ensure temporary access is granted. When that time is up, the IP Address becomes denied and blocked from the network until another allowance or privilege is set.

### Configure an IP Allowance Time

1. Click **Management > Node** in the top panel
2. Click the desired **IP Address**
3. Click **Policy** tab
4. Find **IP Policy** section, Locate **Start** and click the form to edit date and time settings
5. Locate **End** and click the form to edit date and time settings
6. Click **Update**

### Configure an MAC Allowance Time

1. Click **Management > Node** in the top panel
2. Click the desired **IP Address**
3. Click **Policy** tab
4. Find **MAC Policy** section, Locate **Start** and click the form to edit date and time settings
5. Locate **End** and click the form to edit date and time settings
6. Click **Update**

## 11.1.2 Node Policy

**Node Policies** are mainly used for collecting information from Nodes, and managing their network presence while they are in a compliant state. **Node Policies** allow you to establish **Authentication Policies** based on User, Node, and Authentication method, as well as to define the standard operation of the endpoint agent and more.

To configure a Node Policy, create or use existing **Node Groups** (*Managing Node Groups*)

Next, navigate to **Policy > Node Policy** and select **Tasks > create**.

Follow the Policy creation prompts to apply the policy to groups and configure options.

**See:**

- *Configuring User Authentication Options*
- *Configuring Agent Settings by Node Policy*
- *Managing Nodes*

## 11.1.3 Enforcement Policy

While Node Policy collects node information and evaluates status, Enforcement Policy allows/blocks network access based on those results and performs additional actions. Additional actions include redirecting to CWP for policy compliance or controlling endpoints via the Agent.
To apply an Enforcement Policy, create the necessary Node Groups in *Managing Node Groups*, then assign the Node Group to the Enforcement Policy to apply it to the nodes included in that group.

Enforcement Policy consists of the following two components for Attribute-Based Access Control (ABAC).

### Compliance Policy

This defines "what to block when non-compliant". It sequentially checks Compliance that a node accessing the network must comply with.

- Regulations are evaluated from top to bottom, and the first matching Enforcement Policy is applied to the node.
- If no Enforcement Policy matches, the Permission Policy is applied.
- Enforcement Policy and Permission Policy are not applied simultaneously.

### Permission Policy

This defines "what can be done". It declaratively grants services/permissions accessible to nodes that have complied with all Enforcement Policies.

- Uses a permission-centric node assignment model. A single node can have multiple permissions simultaneously.
- There is no policy order; the node is granted the union of permissions from all Permission Policies it belongs to.

### Creating Permissions

### Understanding Permissions

Permissions allow you to define Node Access based off of a combination of Network, Service, Time, and Process objects. Out of the box Genians has 2 Permissions that are used in our pre-defined Enforcement Policies. These are **PERM-ALL** and **PERM-DNS**.

- **PERM-ALL**: Allow all services on all networks
- **PERM-DNS**: Only allow DNS service on all networks

(*You can create custom Permissions but you first need to understand about the Network, Service, Time, and Process objects and how to edit and create them*)

- **Network** - A rule that identifies certain networks and allows you to define access based off of IP/Netmask, IP Range. Fully qualified domain names may also be used to block or allow specific websites. Node Groups may also be used as a network object.
- **Service** - A rule that identifies services to allow you to define access through several protocols and ports.
- **Time** - A rule used to create different access times to either allow during certain days and hours, or deny during certain days or hours.
- **Process** - A rule that identifies specific processes running on controlled terminals. You can define access by specifying the full executable file path and process information, and enter a description of the process's purpose and objectives.

(*Exclude checkbox is used to as a **NOT Operator**. e.g. For a defined Network, checking the box for Exclude allows Nodes to access ALL networks other then this one*)

**Important:** Permission is applicable only to ARP Enforcement, Port Mirroring enforcement, and in-line enforcement.

### Step 1. Create A Custom Network Object

**Note:** Node Groups may also be used as Network Objects. To enable, go to **Preferences > Beta Features**, then skip to **Step 4** to configure to a permission.

1. Go to **Policy** in top panel
2. Go to **Object > Network** in left Policy panel
3. Click **Tasks > Create**
4. Enter the following:

- **ID**: Unique-Name (*e.g. Guest Network*)
- **Group**: Select Group or Groups to apply to this Network Object
- **Network IP/Netmask, Range, or FQDN + DNS TTL**

5. Click **Create**
6. Click **Apply**

### Default Network Objects

- **@LOCAL** - Is an object representing the local network of each intended sensor interface. A local server can be accessed by anyone on the local network but outside access is denied.
- **@MANAGED** - Is combined networks from ALL Network Sensors. If New Network Sensors are added then those networks are automatically added and included into the @MANAGED group.

Example:

| Network Sensor | IP Address |
|---|---|
| Sensor 1 | 192.168.10.10 |
| Sensor 2 | 192.168.20.10 |
| Sensor 3 | 192.168.30.10 |

A Node connects with IP: 192.168.10.100

If the Node is allowed and the Network object is LOCAL Group: A(192.168.10.100) Perm Destination Network: Local The node can only connect to the Network range 192.168.10.0/24

The Node is allowed and the Network object is MANAGED Group:A(192.168.10.100) Perm Destination Network: Manage The node can only connect to the Network ranges in 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24

### Step 2. Create A Custom Service Object

1. Go to **Policy** in top panel
2. Go to **Object > Service** in left Policy panel
3. Click **Tasks > Create**
4. Enter the following:
   - **ID**: Unique-Name (*e.g. Port 80*)
   - **Group**: Select Group or Groups to apply to this Network Object
   - **Service Port**: Select a Protocol and Operator to choose ports (*e.g. For Port 80: TCP/ = 80, and TCP/ = 8080*)
5. Click **Update**
6. Click **Apply**

### Step 3. Create A Custom Time Object

1. Go to **Policy** in top panel
2. Go to **Object > Time** in left Policy panel
3. Click **Tasks > Create**
4. Enter the following:
   - **ID**: Unique-Name (*e.g. Business Hours for Guests*)
   - **Group**: Select Group or Groups to apply to this Network Object
   - **Time**: Specific Date or Range of Days and Hours (*e.g. Time: 0800-1800, Days: Monday-Friday*)
5. Click **Create**
6. Click **Apply**

### Step 3.5. Create A Custom Process Object

1. Go to **Policy** in top panel
2. Go to **Object > Process** in left Policy panel
3. Click **Tasks > Create**
4. Enter the following:
   - **ID**: Unique-Name (*e.g. Web Browser*)
   - **Group**: Select Group or Groups to apply to this Process Object
   - **Process Information**: Enter the complete executable file path and process information (*e.g. C:Program FilesInternet Exploreriexplore.exe*)
   - **Process Description**: Enter a description of the process purpose and objectives
5. Click **Create**
6. Click **Apply**

### Step 4. Create A Permission

1. Go to **Policy** in top panel
2. Go to **Object > Permission** in left Policy panel
3. Click **Tasks > Create**
4. Enter the following:
   - **ID**: Unique-Name
   - **Description**: Some description to help understand what the Permission does
   - **Settings**: Select and edit Network, Service, Time, and Process objects.
   - **Exclude**: Is used as a NOT Operator
5. Click **Create**
6. Click **Apply**

### Creating and Viewing Enforcement Policy for Nodes

**Enforcement Policies** work in a similar fashion to sorting in a mail room. All Nodes flow through a Priority List of **Enforcement Policies** to decide how much access they are allowed and which Groups they fit into. (*When creating custom Enforcement Policies, or re-arranging your Enforcement Policy list, two Enforcement Policies are required to stay where they are*)

- **Blocking Exceptions**: A custom Enforcement Policy cannot be placed above the Blocking Exceptions, or the Exceptions will not be properly applied
- **Default Policy**: A custom Enforcement Policy cannot be placed below the Default Policy, as these are the bottom baselines for Enforcement

### To Create An Enforcement Policy

1. Go to **Policy** in the top panel
2. Go to **Policy > Enforcement Policy** in the left Policy panel
3. Click **Tasks > Create**
4. **Action** tab click **Next**
5. **General** tab create an **ID** and enter brief **Description** to identify what the Policy does (*Priority stays as default. Status should be Enabled*) Click **Next**
6. **Node Group** tab select the **Node Group** that was created, move to **Selected** section and click **Next**
7. **Permission** tab select **Available Permission** and move to **Selected** and click **Next**
8. **Redirection** tab is optional to set **CWP** and **Switch Block options**. Click **Next**
9. **Agent Action** tab is **optional** to add **Agent Actions**
10. Click **Finish**

### Viewing Enforcement Policy Utilization

Widgets displaying enforcement stats can be viewed by clicking **Policy** from the top panel and then selecting **Policy > Enforcement Policy** from the left Policy panel.

The two widgets displayed are:

- **Sensor Operation Mode Status Statistics**: Shows how many Sensors are Up and how many are in Monitoring or Enforcement Sensor Operating Mode
- **Nodes Denied Status**: Shows percentage of nodes denied out of all detected nodes

### To See Enforcement Status on Node Management Page

The *Enforcement Status* of a Node can be found by on the **Node Management** page, which can be viewed from the top panel by clicking **Management > Node**

- **Enforcement Policy Column**: Shows which Policies are being enforced on that Node. If a Node has a Policy listed in **Orange**, that means that node is currently **Blocked** because it is not compliant with that Policy.

### To Group by Enforcement Policy

> Go to the **Status & Filters** window in the bottom left corner of the **Node Management** page. Select from the options under **Enforcement Policy**.

### Configuring Agent Action For Enforcement Policy

Enforcement Policy Agent Actions use the installed Agent to do various administrative tasks, allowing you to take various actions on endpoint devices. You can Control Network Interface, Control Power Options, Notify User, or more.

### To Configure Agent Action for Enforcement Policy

1. Go to **Policy** in the top panel
2. Go to **Enforcement Policy > Agent Action** in the left Policy panel
3. Click **Tasks > Create**
4. Find **Agent Action** section and configure the following options:
   - **OS Type** (*Windows, Linux, macOS*)
   - **Plugin** (***Windows example***)
     - **Control Network Interface** has various control settings of all Network Interfaces
     - **Control Power Options** allows you to control various Power Options of the Windows machine
     - **Notify User** allows you to notify user and keep them informed of the current Enforcement Policy
   - **Execution Interval**
   - **Language**
   - **OS Edition**
5. Click **Create**
6. Click **Apply** in top right corner

### To Apply or Remove an Agent Action from an Enforcement Policy

1. Go to **Policy** in the top panel
2. Go to **Enforcement Policy** in the left Policy panel
3. Find and click name of **desired Enforcement Policy**
4. Find **Agent Action** section and click Assign
5. Click and drag agent actions to or from the **Selected** column, double click them, or highlight them and user the arrow buttons.
6. Click **Add**
7. Click **Update**
8. Click **Apply** in top right corner

### Delete Agent Action

1. Go to **Policy > Enforcement Policy > Agent Action**
2. Find and click **Checkbox** of **desired Agent Action** to delete
3. Click **Tasks > Delete**
4. Click **Apply** in top right corner

## 11.1.4 RADIUS Policy

RADIUS Policy is used to approve/deny user authentication attempts via RADIUS (wireless and wired) and perform additional actions.
These additional actions include configuring ACL, VLAN, Session timeout, and Filters on the switch port where the allowed node is connected.

To configure the policy, you must use an existing User Group or create a new one.

Next, navigate to **Policy > RADIUS Policy > Tasks > Create**.

Follow the policy creation procedure to assign a *User Group* to the policy, add conditions, and configure detailed policy settings.

### RADIUS Policy Settings

This guide explains the condition settings and policy settings required to configure a RADIUS policy.

### Condition Settings

Condition settings define the targets to which the policy applies.
You can specify policy targets using connection information.

#### Available Attributes

| Attribute Item | Description |
|---|---|
| User-name | Authenticated User Name |
| Calling-Station-Id | MAC address of the requesting device |
| Called-Stastion-Id | MAC address of the connected device (AP) |
| Called-Station-SSID | SSID of the connected device (AP) |
| Framed-IP-Address | IP address of the connected device |
| NAS-Port | Physical port number of the connected device |
| NAS-Identifier | Hostname of the connected device |
| Service-Type | Type of service to request or provide (login, callback login, authentication, etc.) |
| Fiter-Id | Name of the filter list for the connected user |
| Login-IP-Host | System to connect to when using login service attributes |
| Class | |
| Vendor-Specific | Manufacturer name of the connected device |
| NAS-Port-Type | Type of connected port (wireless-802.11, ethernet, adsl, etc.) |
| Connect-Info | |
| NAS-Port-ID | Port of the connected device |
| Aruba-User-Role | User role name of Aruba AAA profile |
| Aruba-Essid-Name | Aruba ESSID (Network consisting of one or more APs using the same SSID) |

### Policy Settings

This item configures the policy to apply to authenticated users.
By default, it is set to allow/deny authenticated users.
You can grant additional attributes to authenticated users.

#### Additional Attributes

| Attribute Item | Description | Example |
|---|---|---|
| VLAN Number/Name (Tunnel-Private-Group-Id) | VLAN Assignment | Number 1~4092 |
| Cisco-AVPair(ip:inacl) | ACL setting for Inbound packets | permit ip host 192.168.1.203 any |
| Cisco-AVPair(ip:outacl) | ACL setting for Outbound packets | deny ip host 192.168.1.203 any |

continues on next page

Table 2 – continued from previous page

| Attribute Item | Description | Example |
|---|---|---|
| Cisco-AVPair(security-group-tag) | Security Group Tag | |
| Cisco-AVPair(url-redirect-acl) | ACL name created on Cisco device | |
| Cisco-AVPair(url-redirect) | Redirect Address | http(s)://IP or DOMAIN |
| Cisco(AVPair) | Cisco AVPair Attribute | String |
| Filter-ID | ACL name configured on the access device | |
| NAS-Filter-Rule | ACL List Setting | permit in tcp from any to any |
| Session-Timeout | Session termination value after authentication | Seconds |
| Termination-Action | Action after session expiration | 1 (Re-authenticate),<br>0 (Terminate) |
| Manual Input | Direct input of detailed attribute values | String |

After completing the Basic Settings, Condition Settings, and Policy Settings, click the Update button at the bottom.

For attribute items, please refer to the RFC2865 document.

## 11.2 Policy Enforcement Methods

You need a way to control devices that violate network policies defined by your organization. Genian ZTNA provides multiple layers of enforcement methods from Layer 2 network control to agent-based. Depending on your network environment or security requirements, you can leverage the following options:

### 11.2.1 ARP Enforcement

Controlling network access according to the status of devices in the internal network has always been a challenge. Setting ACLs on routers to control access between internal networks can provide only a simple access control.

ACLs can be difficult to enforce in a DHCP environment where devices move frequently or devices that use IP change frequently. Moreover, access control between multiple devices connected to the same sub-net is the most challenging task and there are not many solutions.

A possible choice is to apply the Port based Access Control function using 802.1x to the switch port to which the device is connected. However, 802.1x can be expensive, requiring large network configuration changes, such as replacing unsupported devices and and converting to a single vendor for networking equipment.

In addition, because all network devices do not support 802.1x, manual configuration is frequently required for each switch port. In an enormous enterprise network, setting an exception list for 802.1x for each switch port is complicated and time consuming.

Another option is to use network access control with ARP Enforcement. ARP Enforcement uses the characteristics of the ARP protocol to perform access control. The device conducting the enforcement impersonates other network endpoints in order to intercept traffic.

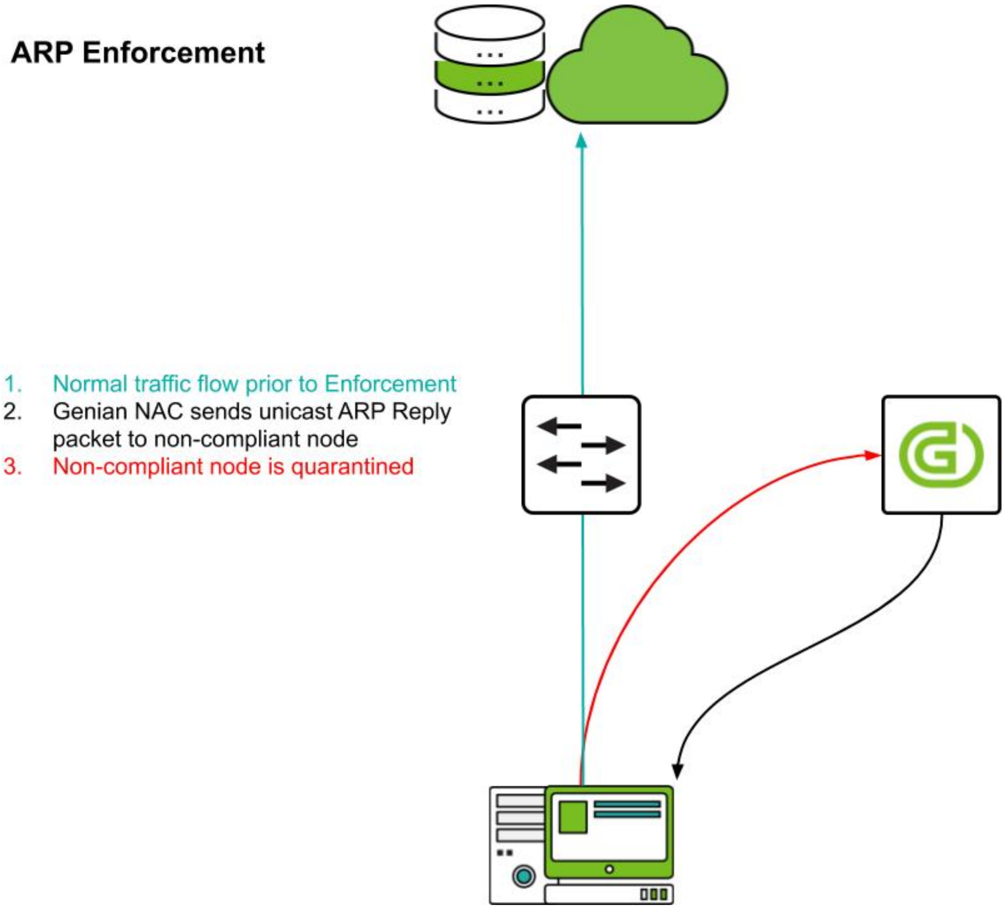
Genian ZTNA performs ARP Enforcement using the following procedure.

- The device to be blocked generates an ARP request.

- The network sensor responds to the request with its own MAC.
- The device to be blocked transmits the packet to the network sensor.
- The network sensor drops according to the access control policy or delivers it to the actual destination.

If the target device attempts to bypass this enforcement by setting static ARP, a bidirectional enforcement function is provided to control the reply packet generated from the communication target such as gateway, and static ARP setting can be blocked through Agent.

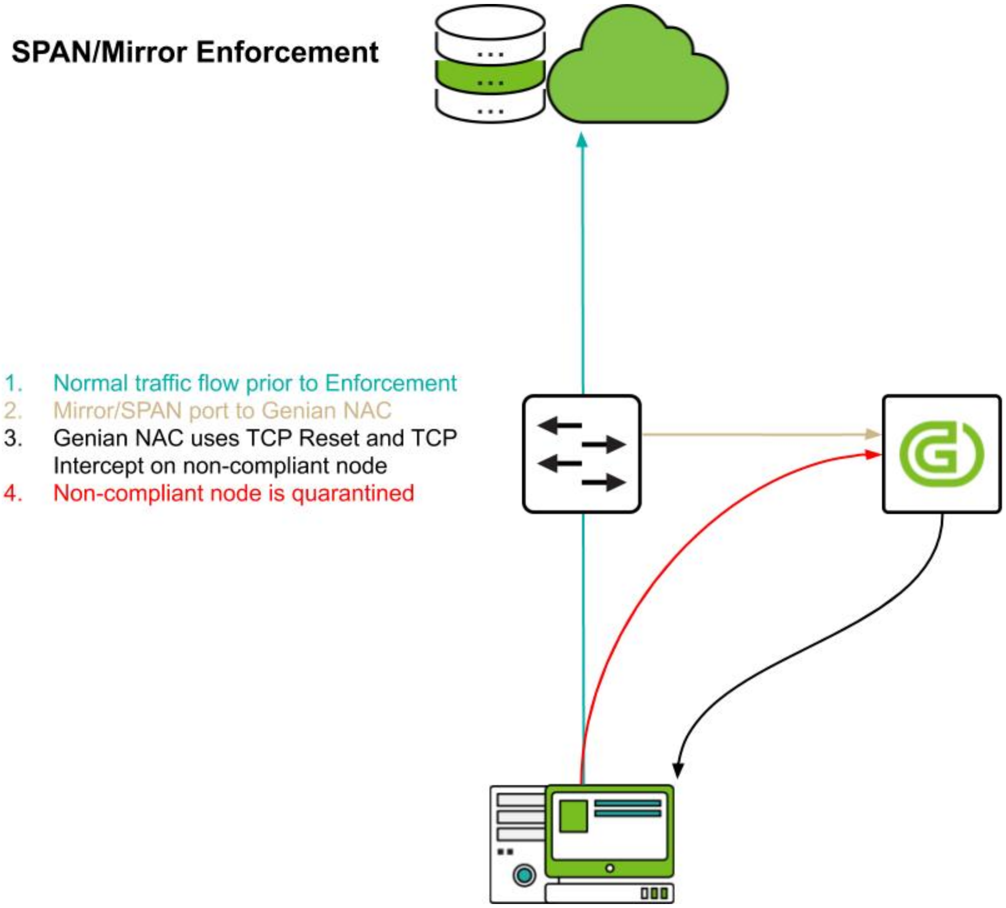
Genian ZTNA has a built-in RADIUS server for 802.1x and ARP Enforcement via network sensor, so users can select the option best for their network environment.


ARP Enforcement
1. Normal traffic flow prior to Enforcement
2. Genian NAC sends unicast ARP Reply packet to non-compliant node
3. Non-compliant node is quarantined

### 11.2.2 Port Mirroring (SPAN)

Genian ZTNA uses Port Mirroring (SPAN in Cisco) as a way to provide access control with minimal network configuration changes. It monitors newly connected sessions through Mirroring port and blocks connection by transmitting TCP RST or ICMP Destination Unreachable packet.

To do this, you need to transfer the traffic to Genian ZTNA using a Port Mirroring supported switch or a Network TAP device.


SPAN/Mirror Enforcement
1. Normal traffic flow prior to Enforcement
2. Mirror/SPAN port to Genian NAC
3. Genian NAC uses TCP Reset and TCP Intercept on non-compliant node
4. Non-compliant node is quarantined

Genian ZTNA offers two types of port mirroring modes.

**Global Mirror Sensor**

The Global Mirror Sensor can perform information collection and access control. In general, it is located in the boundary network connected to the Internet, and access control is performed while monitoring all the internal traffic.

In this setup, is recommended to use a separate network sensor with high performance hardware because it controls all nodes while monitoring all traffic generated in the network.

**Local Mirror Sensor**

Unlike the Global mirror, the local mirror sensor can only control packets passing through a specific network segment at that location. To solve this problem, it is possible to add a mirroring port to the network sensor installed in each end network. This makes it possible to control connections occurring within the local network.

Since the local mirror sensor is only monitoring and controlling one network segment, it can be operated in the hardware of relatively low specification as compared with the global mirror sensor.

### 11.2.3 802.1x (RADIUS)

802.1x port based access control is the most ideal access control method that can be applied in enterprise wireless LAN environment. User-based authentication allows only authorized users to access the network. Also, depending on the compliance status of the device, it is possible to connect to a specific VLAN or forcibly release a connected connection.

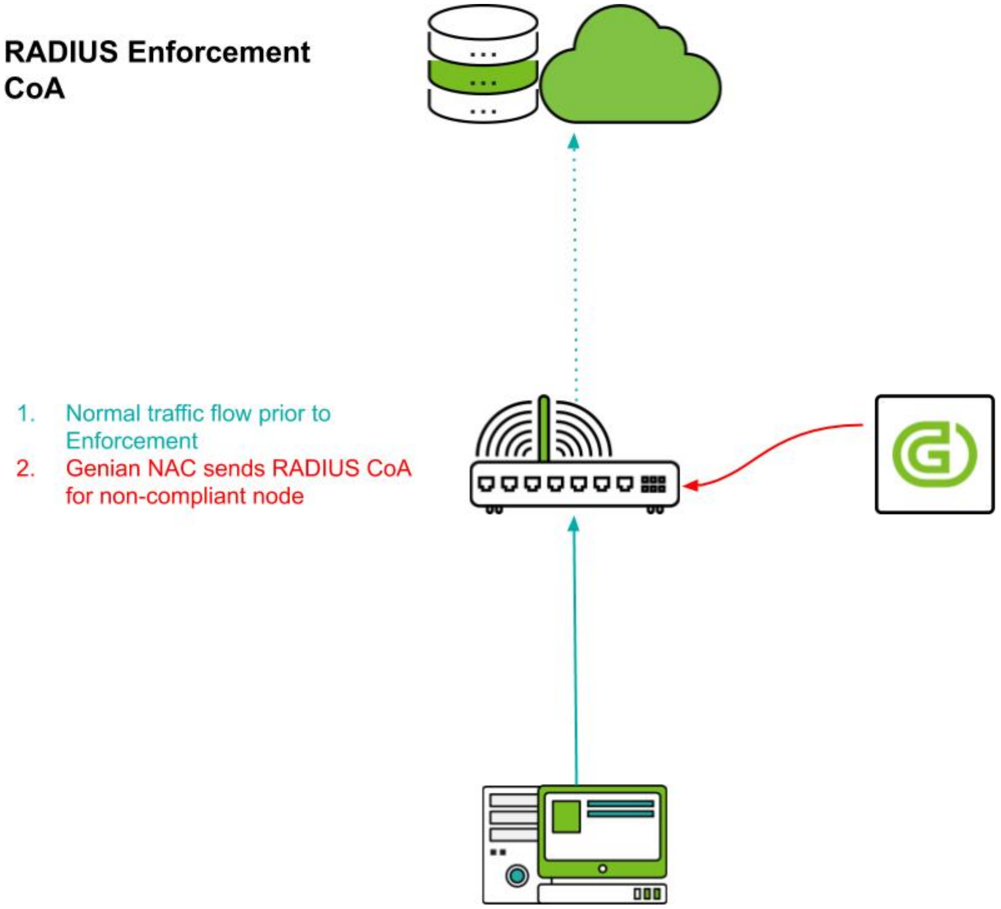
This requires a user device that supports 802.1x, a network access device such as an 802.1x-capable access point or switch, and a RADIUS server. Genian ZTNA provides a built-in RADIUS server and provides the following access control functions.

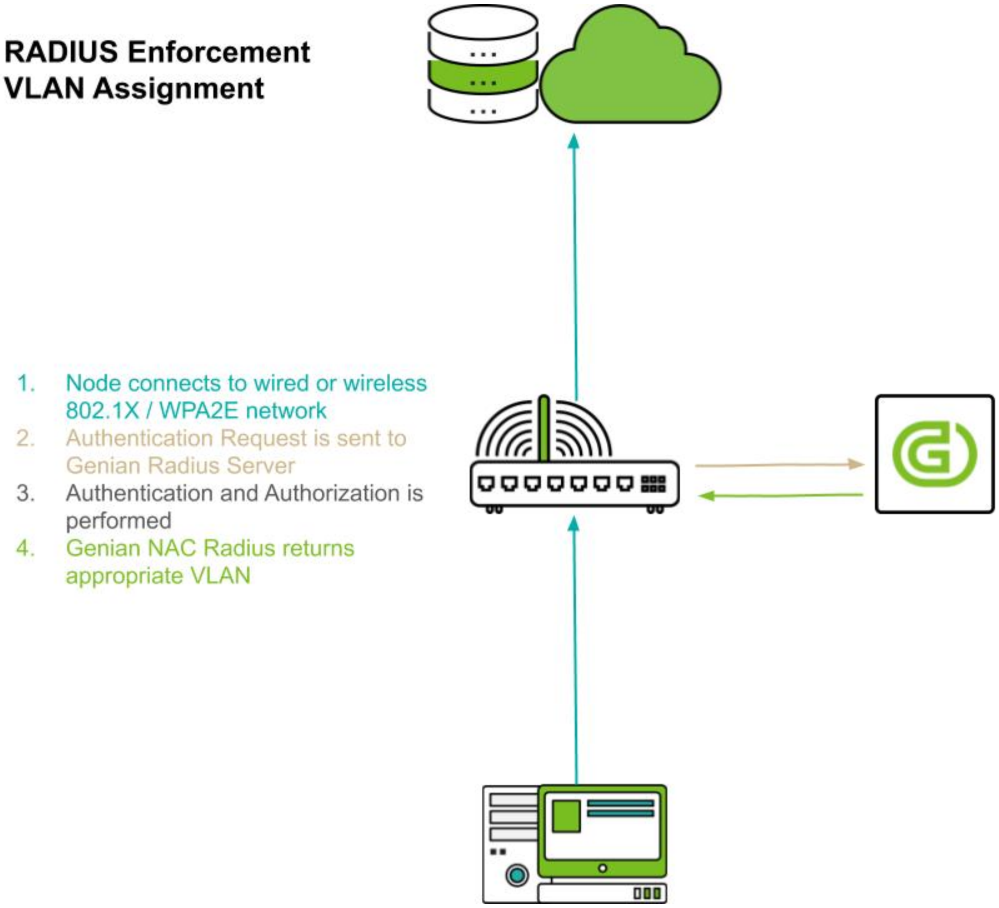
**User Authentication**

802.1x allows access to the network through user-based authentication instead of a weak authentication method such as a shared secret. For more information about User Authentication, see *Configuring RADIUS Enforcement*

**VLAN Assignment & Reassignment**

Devices can be assigned to a VLAN upon connection based on Radius attributes (Standard or Vendor-specific.) If network access needs to be restricted due to device state changes, the device can be terminated using a RADIUS CoA (Change of Authorization). The disconnected device will try a new connection and connect to the isolated VLAN at this time to securely isolate the device from the network. To do this, the access point or switch must support the *RFC 5176 - Dynamic Authorization Extensions to RADIUS* standard.


RADIUS Enforcement
CoA
1. Normal traffic flow prior to Enforcement
2. Genian NAC sends RADIUS CoA for non-compliant node

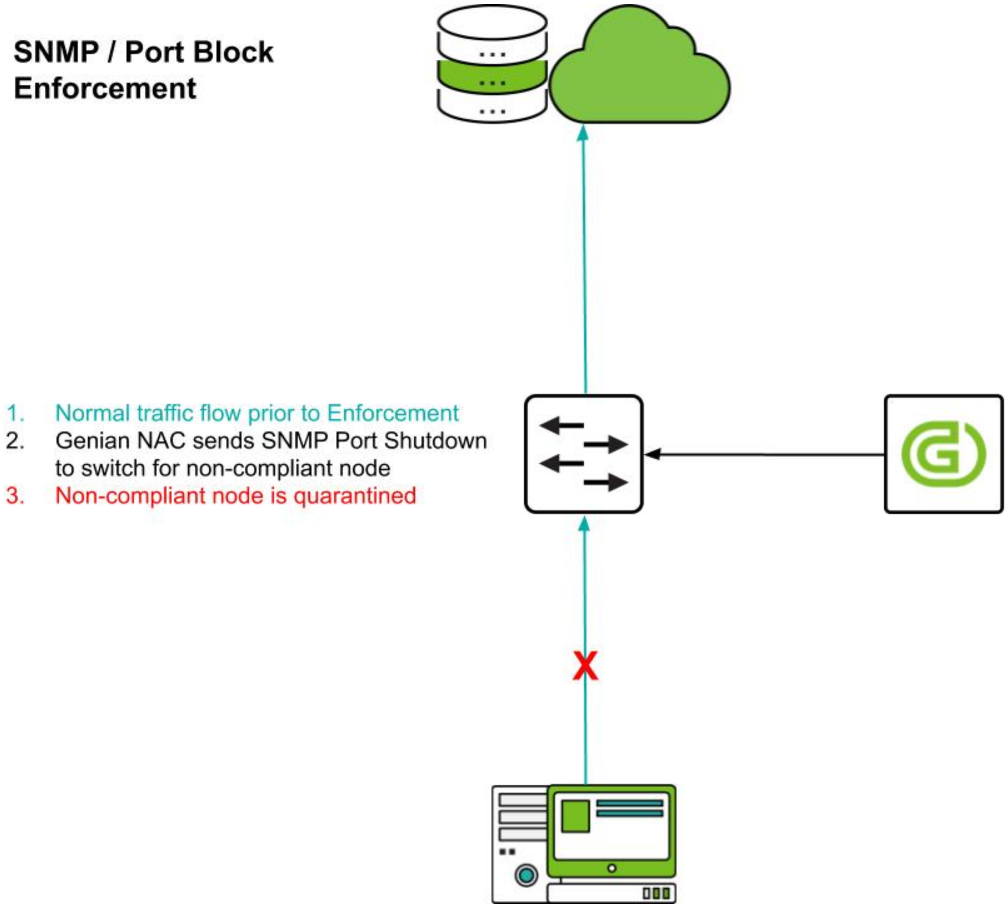

RADIUS Enforcement
VLAN Assignment
1. Node connects to wired or wireless 802.1X / WPA2E network
2. Authentication Request is sent to Genian Radius Server
3. Authentication and Authorization is performed
4. Genian NAC Radius returns appropriate VLAN

### 11.2.4 DHCP

Genian ZTNA can allocate or not allocate IP according to IP / MAC policy through built-in DHCP server. This prevents unauthorized devices from accessing the network or assigns a fixed IP address to devices with a specific MAC address.

### 11.2.5 Switch Port Block

If you use a switch that supports SNMP, Genian ZTNA will collect SNMP and switch and port information connected to each node. This information can be used to shut down the switch port according to the security policy of the device. Switch port block is done via SNMP Write. The switch MUST provide a writable *SNMP MIB-2 ifAdminStatus* property.

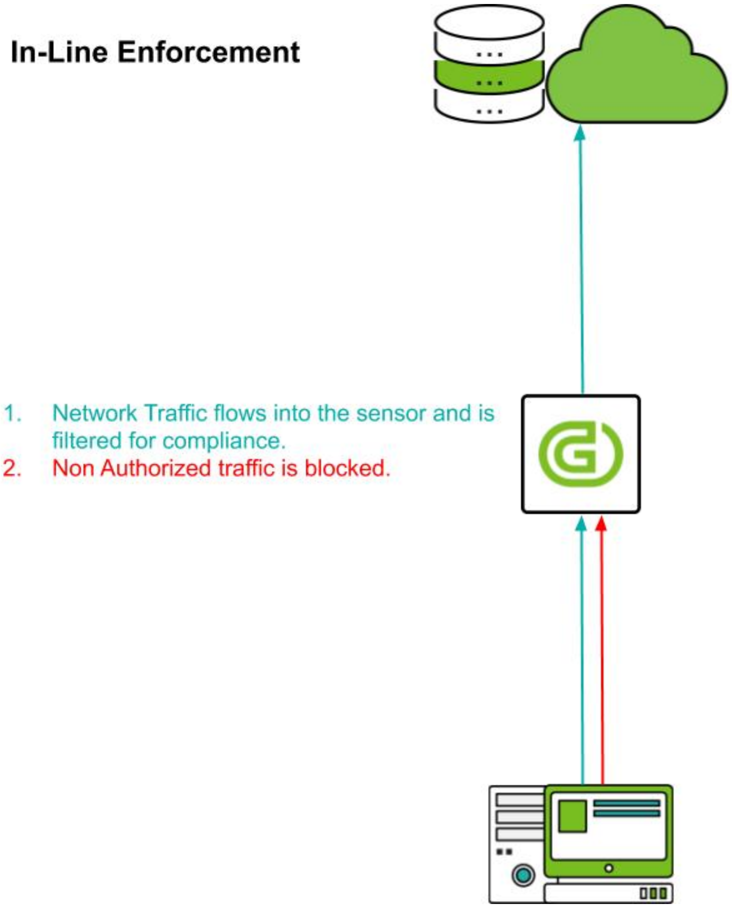

SNMP / Port Block Enforcement
1. Normal traffic flow prior to Enforcement
2. Genian NAC sends SNMP Port Shutdown to switch for non-compliant node
3. Non-compliant node is quarantined
X

### 11.2.6 Inline packet filtering

To apply the access control policy determined by the enforcement policy, you can use a dual-homed packet filtering device between the two networks. This works the same way as a firewall. Two network interfaces operate as gateways in each network, and in the process of forwarding packets, it checks the policy and drops unauthorized packets.

Unlike the out-of-band method such as ARP or Port Mirroring method, it provides higher security because it checks the security policy against all packets passing through and transfers only allowed packets. However, this inline device is subject to security policy checks on every packet it passes through, which can cause packet transmission delays. In addition, access control policies can not be applied to packets that do not pass through this inline device. Therefore, you need to be careful about where you will install it before deployment.

For inline packet filtering, network sensor software must be installed on hardware that has two or more network interfaces. When the sensor operation mode is set to 'inline' through the setting, the security policy is applied to the received packet and then forwarded to another interface in the system according to the routing table.

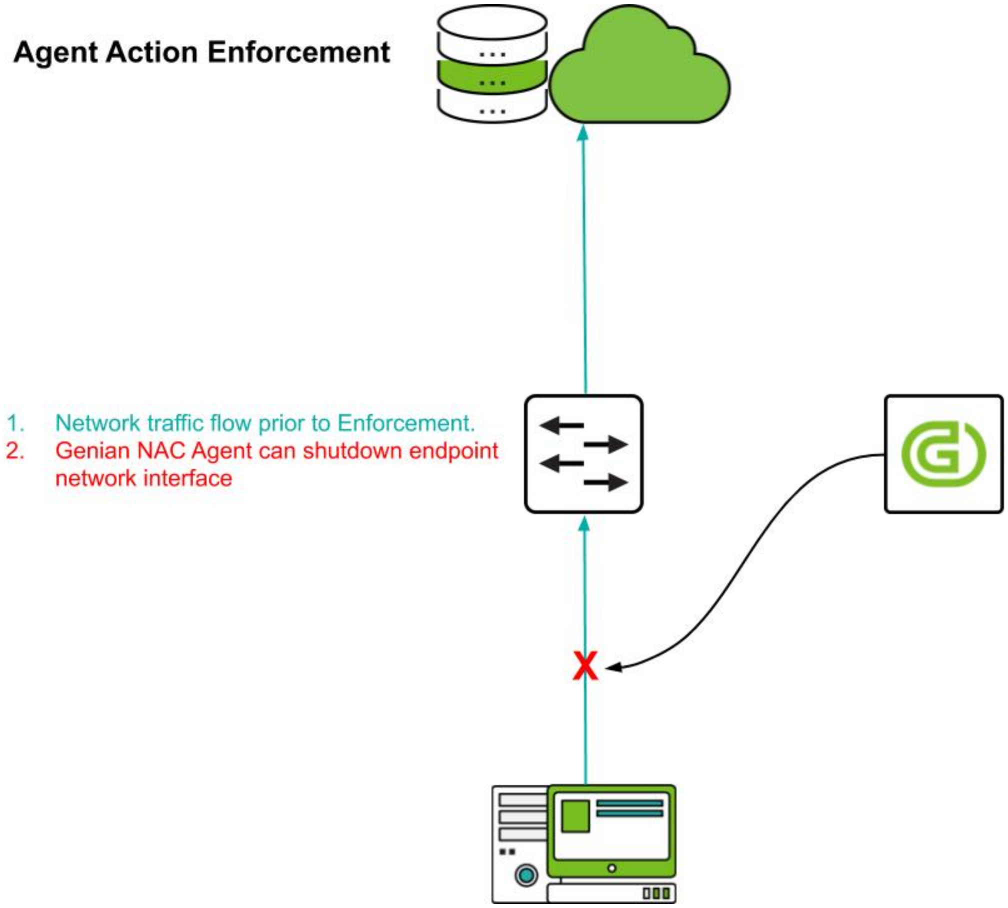

In-Line Enforcement
1. Network Traffic flows into the sensor and is filtered for compliance.
2. Non Authorized traffic is blocked.

### 11.2.7 Agent Action

Depending the node policy, and enforcement policy, applied, the following agent actons can be used to control an endpoint:

- *Control Windows Firewall*
- *Controlling Network Interface*
- *Controlling WLAN*
- *Shut Down System*
- *Notify User*

**Note:** If you use wired/wireless network interface control to control your device, you might not be able to communicate with the policy server and receive a new policy assignment.


Agent Action Enforcement
1. Network traffic flow prior to Enforcement.
2. Genian NAC Agent can shutdown endpoint network interface
X

## 11.3 Configuring ARP Enforcement

Network Sensor by default is configured to passively collect information and forward it to the Policy Server. This information assists in identifying the endpoints information, allowing you to build groups and policies. Network Sensor Operating Mode needs to be changed from Monitoring to Enforcement which allows the Policy Server to enforce policies and control endpoints access onto the network using ARP Enforcement.

For more information. See *Policy Enforcement Methods*

**Note:** ARP Enforcement may trigger security alerts from IDS or EDR products, see: *ARP Enforcement does not block network access*

### 11.3.1 Enabling ARP Enforcement

You can enforce policies by activating the **Network Sensor**. The Network Sensor has two types of **Sensor Operating Modes**. By default, the **Network Sensor** is set to **Monitoring** mode.

To activate the Network Sensor enforcement:

1. Go to **System** in the top panel
2. Select the desired sensor's **IP Address** for activating enforcement
3. Click the **Sensor** tab
4. Click the **Interface** of the sensor you wish to activate.
5. For **Sensor Mode**, select **Host**
6. For **Sensor Operating Mode**, change to **Enforcement**
7. Configure optional **Enforcement Exceptions** Unmanaged IP ranges.
8. Configure **Managed IP Control** Range
9. Click **Update**

## 11.4 Configuring Mirror Mode

Mirror Mode monitors newly connected sessions through Mirroring port and blocks connection by transmitting TCP RST or ICMP Destination Unreachable packet.

Mirror mode requires at least two NICs. One NIC assigns an IP to manage the sensor and the other as an unnumbered NIC for Packet Monitoring.

For more information. See *Policy Enforcement Methods*

### 11.4.1 Global Mirror

The Global Mirror sensor monitors all Nodes.

1. Go to **System** in the top panel
2. Go to **System > Sensors** in the left System Management panel
3. Select the desired sensor's **IP Address** for Mirror
4. Click **Sensor** tab
5. Click the interface desired to use in mirror mode. **eth1** *There is no IP assigned to this interface*
6. Select **Mirror** in **Sensor Mode**
7. Select **Global** in **Mirror Operating Scope**
8. For **Sensor Operating Mode**, change to **Enforcement**
9. Click **Update**

**Note:** If you use Global Mirror only, the agent must be installed on the endpoint because it is not registered as a node.

### 11.4.2 Local Mirror

You can use it with **Host** mode sensor to gather more information. Available in the same equipment as **Host** mode sensor.

1. Go to **System** in the top panel
2. Go to **System > Sensors** in the left System Management panel
3. Select the desired sensor's **IP Address** for Mirror
4. Click **Sensor** tab
5. Click the interface desired to use in mirror mode. **eth1** *There is no IP assigned to this interface*
6. Select **Mirror** in **Sensor Mode**
7. Select **Local** in **Mirror Operating Scope**
8. For **Sensor Operating Mode**, change to **Enforcement**
9. Click **Update**

**Note:** Local Mirror can additionally use Traffic Monitoring.

1. Find **Traffic Monitoring** section
2. **Collection Interval** `0` is disable, minimum `10` **seconds**, maximum `1` **day**
3. **Time for Average** minimum `10` **seconds**, maximum `1` **day**, Initial value is `5` **minutes**
4. **Minimum Update Value** KB/s unit, the minimum value to update the traffic information, Initial value is `30` KB/s
5. **Update Fluctuation** % unit, the minimum fluctuation percentage rate, Initial value is `30` %
6. **Destination based Status Collection** Select **On** or **Off**, collect the traffic information based on the destination

## 11.5 Configuring RADIUS Enforcement

Genian ZTNA includes a built in RADIUS server for use with wireless and wired 802.1x authentication (credential or client certificate), or MAC/MAB Authentication (based on MAC Address only).

In order for the Genian ZTNA RADIUS server to accept authentication requests from RADIUS clients/authenticators (switches, controllers, access points, etc), they must first be added as a known RADIUS client. See the instructions below to add RADIUS clients to the RADIUS server.

The RADIUS server can also register devices into the policy server database. IP addresses and other information can be collected through RADIUS accounting.

### 11.5.1 Enable Built-In RADIUS Server

1. Go to **Preferences** in the top panel.
2. Go to **Service > RADIUS Server** in the left panel.

Under **RADIUS Secret**

1. For **Shared Secret Key**, enter the shared secret key for RADIUS the client/authenticator. This must match what is configured on the switch, controller or access point.

2. For **RADIUS Client IP**, enter the IP address or addresses. Each entry must be on a separate line. Individual IPs and CIDR notation for subnets are supported.

Under **Authentication Server**

1. For **Generating Accounting**, select **On** to allow for node information collection, if the RADIUS Clients do not support accounting.

For information on RADIUS Accounting from External RADIUS Servers, see: *Single Sign-On*

## 11.5.2 802.1X Authentication

802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server.

The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator.

The authenticator is a network device, such as an Ethernet switch, wireless controller or wireless access point. The authenticator acts like a security guard to a protected network. The supplicant is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized.

With 802.1X port-based authentication, the supplicant provides credentials, such as username/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

### Configuring 802.1x

### EAP Settings

Different configurations are required based upon which database user credentials are being checked against.

### Active Directory or Genians Local Directory (Internal Database)

1. Go to **Preferences** in the top panel
2. Go to **Service > RADIUS Server** in the left panel
3. Under **Authentication Server**
4. Under **EAP Authentication > Default EAP-PEAP**, Select **MSCHAPv2**
5. Click **Update**

**Note:** If EAP is disabled, NTLM Auth PAP will be used by default.

### LDAP (or other legacy directory)

1. Go to **Preferences** in the top panel
2. Go to **Service > RADIUS Server** in the left panel
3. Under **Authentication Server**
4. Under **EAP Authentication > Default EAP-PEAP**, Select **EAP-GTC**
5. Click **Update**

**Note:** The above LDAP authentication configuration requires the Genian ZTNA agent on the endpoint as native support for GTC is typically not available in supplicants by default.

### EAP-TLS

When you use EAP with a strong EAP type, such as TLS with smart cards or TLS with certificates, both the client and the server use certificates to verify their identities to each other.

1. Go to **Preferences** in the top panel
2. Go to **Service > RADIUS Server** in the left panel
3. Under **Authentication Server**
4. Under **EAP Authentication > EAP-TLS**, Select **On**
    1. Click **Upload** button to the right of the **CA Certificate** to upload the certificate of the CA.
    2. Click **+** button on CA certificate window, Select the certification file of the CA.
    3. **CACert Information** allows you to check the information of the saved CACert.
5. Click **CreateServerCertificate** button to the right of the **Server Certificate**
    1. Input the **Common Name** like `nac.genians.com`, The fully qualified domain name (FQDN) of your server or IP of the server. This must match exactly what you type in your web browser or you will receive a name mismatch error.
    2. Input the country code as **Country** like `US`, The two-letter ISO code for the country
    3. Input the name of organization as **Organization** like `Genians Inc.`
    4. Input the Email as **Email** like `admin@genians.com`, An email address used to contact your organization.
    5. Click **Generate CSR**
    6. Copy All text in the box to the right of the **Certificate Signing Request**
    7. Send a request to the CA server, issue a server certificate, open a BASE64 encoded file, and copy and paste the text in the box to the right of the **Certificate**
    8. Click **Register**
    9. **ServerCert Information** allows you to check the information of the saved ServerCert.
6. Input Certificate Revocation List point as **CRL distribution point**, If you do not verify the CRL, you do not need to enter it.
7. Input Online Certificate Status Protocol Responder URL as **OCSP Responder URL**, If you do not use OCSP, you do not need to enter it.

8. Click **Update**

**Note:** To use EAP-TLS, the user must also obtain a certificate from the same CA server or trusted CA server that issued the certificate to the server.

**Attention:** Issuance, revocation and management of server certificates and user certificates are managed through an external CA server.

### Cisco Switch RADIUS Configuration Settings

1. Switch AAA and 802.1X Settings

Configure global AAA RADIUS and 802.1X settings, define RADIUS server and enable RADIUS Change of Authorization (CoA).

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa session-id common
aaa accounting update newinfo periodic 10

radius server {radius server name}
 address ipv4 {radius server ip} auth-port 1812 acct-port 1813
 key {radius secret key}

radius-server vsa send authentication
ip radius source-interface X (Layer 3 management interface)

aaa server radius dynamic-author
client

server-key {radius secret key}

port 3799
auth-type any

dot1x system-auth-control
ip device tracking
```

2. Interface 802.1X Settings

Configure 802.1X and mab on the interface along with associated timers and authentication modes.

```
dot1x port-control auto
authentication port-control auto
mab
dot1x pae authenticator
dot1x timeout quiet-period 10
dot1x max-reauth-req 1
dot1x radius-attributes vlan static
dot1x host-mode multi-auth
```

**Note:** Two port-control commands are provided since various Cisco IOS versions use different commands. Choose the appropriate command for your version.

**Note:** "mab" is configured to allow devices that do not support a supplicant to authenticate via MAC Authentication.

**Note:** Refer to Cisco documentation for more information on timers and authentication modes.

### 11.5.3 MAC Authentication Bypass (MAB)

Not all devices support 802.1X authentication. Examples include network printers, Ethernet-based electronics like environmental sensors, cameras, and wireless phones. For those devices to be used in a protected network environment, alternative mechanisms must be provided to authenticate them.

For wired networks, when Mac Authentication/ MAB is configured on a port, the port will first try to check if the connected device is configured for 802.1X (has an active supplicant), and if no response is received from the connected device, it will try to authenticate with the RADIUS server using the connected device's MAC address as the username and password. You may also configure switch ports to only perform MAC authentication (speeding up the process) or in many cases, the option to change the authentication order is also available (MAC authentication first followed by 802.1X authentication). This will vary by switch vendor.

For wireless networks, the authentication method is typically set on a per SSID basis and is either 802.1X/WPA2E or MAC authentication but not both.

#### Configuring MAC Authentication (MAB)

Genian ZTNA can select the MAC address to be allowed on the network through a specified Node Group. If the MAC address that is requested to be authenticated exists in the Node Group, the authentication is allowed; otherwise, the authentication is denied.

1. Go to **Preferences** in the top panel
2. Go to **Service > RADIUS Server** in the left panel
3. Under **Authentication Server**
4. For **MAC Authentication**, select **On** for enable MAC Authentication bypass (MAB)
5. For **Node Group**, select Node Group for allow MAC authentication
6. Click **Update**

No endpoint supplicant configuration is required for MAC Authentication (MAB).

### 11.5.4 Authorization

AAA refers to Authentication, Authorization and Accounting. Once an endpoint device successfully authenticates to a network, authorization is optional.

Authorization is a method to authorize the device a specific level of access (such as a VLAN or ACL) or apply other attributes to the device that control certain aspects of connectivity (such as QoS attributes).

The Genian ZTNA RADIUS Server supports authorization in the form of initial VLAN assignment. Additional access controls are available with Genian ZTNA outside of the RADIUS server as well (ACLs via ARP Enforcement, etc).

#### Configuring Authorization

Authorization can be completed at the time of initial authentication based on AD/LDAP group membership or RADIUS attributes included in the authentication request. Authorization can also be facilitated by RADIUS CoA after authentication has been completed based on other criteria such as node group, noncompliance with a policy, change in status, etc.

#### Configure Initial Authorization

Genian ZTNA provides the ability to specify an attribute for a device when it connects to the network. This can be used for assigning a VLAN, ACL or other attribute based on an attitribute of the node authenticating, such as User-Name. Additonally this feature can be used to selectively deny authentication requests.

1. Go to **Policy** in the top panel.
2. Go to **Policy > RADIUS Policy** in the left panel.
3. Click **Tasks > Create**
4. For **General**, input **Name**, **Priority**, and activation **Status**.
5. For **Conditions**, select **Attribute**.
6. Select **Operator** and **Value**.
7. Click **Add** button.
8. For **Policy**, choose to **ACCEPT** of **REJECT** Authentication Requests that match the attribute conditions.
    - If **ACCEPT**, Select **Additional Attributes** to apply to the Node / User.
9. Click **Add** button.
10. Click **Create** button.

**Note:** You can use RADIUS attributes such as *User-Name, Calling-Station-Id, Called-Station-Id, Framed-IP-Address, NAS-IP-Address, NAS-Port, Service-Type, Filter-Id, Login-IP-Host, Class, Vendor-Specific, NAS-Port-Type, Connect-Infox, NAS-Port-ID, Aruba-User-Rolex, Aruba-Essid-Name*

**Attention:** RADIUS client devices must support the RFC2868 IEEE 802.1X standard for client authentication.

### Enable CoA (Change of Authorization)

If a device changes status after being authenticated to the network, such as violating a configured policy, the network access for the device can be restricted or denied using various RADIUS attributes. This is provided through a standard called CoA (Change of Authorization, RFC 5176 - Dynamic Authorization Extensions to RADIUS standard).

The CoA will disconnect the device from the network at which point the device will attempt to reconnect. The RADIUS server will then return the desired attribute.

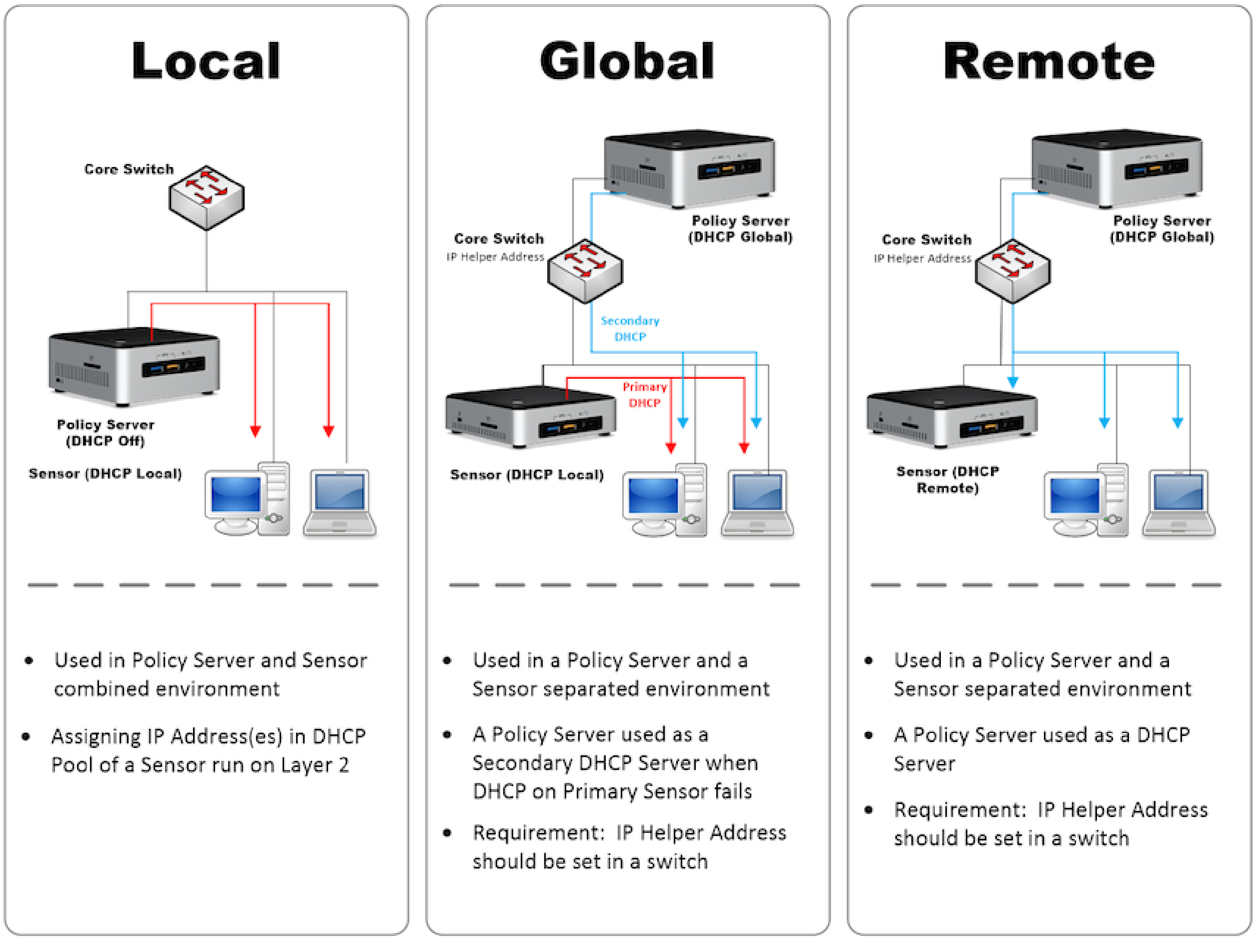
1. Go to **Policy** in the top panel.
2. Go to **Policy > Enforcement Policy** in the left panel.
3. Click name of enforcement policy to disconnect connection.
4. Under **Enforcement Options > RADIUS Control**.
5. For **RADIUS CoA**, select **On**.
6. For **CoA Commands**, select **Terminate Session** for a standard attribute or select another Vendor Specific Attribute (VSA).
7. For **Vendor-Specific-Attribute**, Enter the VSA value (for example, `Nas-filter-Rule = 'permit in tcp from any to any 23'`).
8. Click **Update** button.
9. Click **Apply** in the right top.

## 11.6 Configuring DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on IP networks. The DHCP is controlled by the Policy Server/Sensor that dynamically distributes network configuration parameters, such as IP addresses. You will be able to configure and manage the Built-In DHCP Options and configure Policy Server/Sensor to utilize the three DHCP Services. (Local, Remote, and Local & Remote)

If you need to make custom configuration changes to a Network Sensor that is already in operation then you would use the **System > Sensor > Sensor Settings** option.

Depending on your requirements you have three options for DHCP. (**Local**, **Remote**, and **Local & Remote**)



- Used in Policy Server and Sensor combined environment
- Assigning IP Address(es) in DHCP Pool of a Sensor run on Layer 2

- Used in a Policy Server and a Sensor separated environment
- A Policy Server used as a Secondary DHCP Server when DHCP on Primary Sensor fails
- Requirement: IP Helper Address should be set in a switch

- Used in a Policy Server and a Sensor separated environment
- A Policy Server used as a DHCP Server
- Requirement: IP Helper Address should be set in a switch

### 11.6.1 Configuring DHCP Services

- *Configuring DHCP Server*

### 11.6.2 Assign fixed IPs to devices

Genian ZTNA supports fixed DHCP IP allocation to analyze many environments to support situations in which some devices in the DHCP environment need to have static IP allocation.

1. Go to **Management** in the top panel
2. Check the left side check box of the terminal to assign a static IP.
3. Click Select **Task** > IP/MAC Policie > Enable Conflict/Change Prevention

- When you set conflict protection and change prevention, the IP is assigned only to the setup device.

### 11.6.3 Managing DHCP Leases

It is a function to inquire and delete the DHCP IP assigned to the device by the DHCP server. This feature is only available through the CLI(Command Line Interface).

**Show DHCP Lease status**

```
genian# show dhcp lease all
IP Address      MAC               Expire              Interface
--------------- ----------------- ------------------- -----------
172.29.30.152   00:24:21:3D:65:C4 2018-08-06 20:10:13 eth0
172.29.30.154   00:90:FB:26:7D:24 2018-08-06 19:10:24 eth0
172.29.30.155   AC:3C:0B:3C:01:70 2018-08-06 20:10:21 eth0
```

**Clear DHCP Lease status**

```
geinian# clear dhcp lease ip 172.29.30.152
genian# show dhcp lease all
IP Address      MAC               Expire              Interface
--------------- ----------------- ------------------- -----------
172.29.30.154   00:90:FB:26:7D:24 2018-08-06 19:10:24 eth0
172.29.30.155   AC:3C:0B:3C:01:70 2018-08-06 20:10:21 eth0
```

## 11.7 Configuring Switch Port Control

Configuring Switch Port Control by Enforcement Policies or manual action starts with the configuration of SNMP, which will provide the information and access necessary for port blocking. For basic switch setup, see: *Browsing Switches*.

### 11.7.1 Enable Switch Port Control on Enforcement Policy

The target of the switch port control is determined by the Enforcement Policy. If you want to control switch ports for specific nodes, you need to create an enforcement policy that targets those nodes and then configure the switch port blocking setting.

1. Click **Policy** in the top panel
2. Go to **Policy > Enforcement Policy** in the left panel
3. Click desired **ID** for enabling switch port blocking

Under **Enforcement Options > Switchport Control**

1. For **Control Port with SNMP**, select **None**, **Shutdown**, or **VLAN**
2. For **SNMP Write Community**, enter default write community string, or an SNMPv3 user and password(s). If this setting is empty, will use switch's own setting.
3. Configure Specific options:
   - For **Port Shutdown**: configure the following:

     **Description**: enter text for appending to SwitchPorts existing description.

     **MAC Threshold for Disabling**: if a SwitchPort has more than this number of MACs associated, it will not blocked.

     **Description for Exception**: If a SwitchPort Description partially matches a term entered here, it will not be shut down.

   - For **Port VLAN**: Enter the **VLAN ID** to be assigned.

4. For **MAC Threshold for Disabling**, if a switch port has more than this number of MACs, it will not blocked.
5. For **Description**, enter text for appending to switch port's existing description.
6. Click **Update**

### 11.7.2 Switch Port Manual Control

You can manually control **Switch Ports** in the web UI undr **Management > Switch**.

1. Go to **Management > Switch** in the top panel
2. Click on **Port** in the main **Switch Ports** window
3. Configure one or more of the following:
   - **Admin Down**: Check or uncheck the box to change the port link status.
   - **VLAN ID**: Enter a VLAN ID for the port.
4. Click **Send SNMP Command**

## 11.8 Configuring Wireless Access Control

Genian ZTNA has features aimed at addressing the most common concerns relating to wireless network administration.

### 11.8.1 Detecting Rogue Access Points

Rogue access points within your networks, can be easily identified, and blocked. Any devices and users associated with use of the rogue access point can also be identified.

### 11.8.2 Unauthorized Network Connections

The wireless sensor is capable of detecting when devices connect to an SSID that does not belong to your organization. This makes it easy to block devices that may have been compromised and easily identify users who are breaking device usage policies.

A nodes connected SSID can be seen in the Node Management window, the WLAN Management window or in the Logs section.

Both **Rogue Access Points** and **Unauthorized Connections** can by identified in the following locations:

- *Browse/Search/Filter Nodes*
- *Monitoring Wireless LAN*
- *Managing Logs and Events*

### 11.8.3 SSID Whitelisting

Using information collected about SSIDs in your area, you can create an SSID whitelist. Through use of the endpoint agent (Windows), connections to any SSID not on the white list can be disabled.

**See:**

- *Controlling WLAN*

### 11.8.4 Wlan Client Provisioning

By configuring the connection settings for your preferred wireless networks on the Policy Server, the correct network configuration can be automatically distributed to end user devices through use of the endpoint agent (Windows).

**See:**

- *Configuring Wireless Connection Manager*

## 11.9 Configuring ZTNA Gateway Options

**Note:** This section assumes you have already installed a ZTNA Gateway. For ZTNA Gateway installation instructions refer to the link below.

See *Installing ZTNA Gateway*

### 11.9.1 Enable ZTNA Client Option

See *Enable ZTNA Client in Cloud Site*

#### ZTNA Client Split Tunneling Option

The network address entered into the Access Network text box (ex 192.168.100.0/24) will be routed through the ZTNA Gateway while all other traffic will be routed out the local default gateway.

Default setting: If nothing is entered, then all traffic (0.0.0.0/0) will be routed through the ZTNA Gateway.

#### ZTNA Client Isolation Option

When enabled, connected ZTNA clients with different IP addresses or different usernames will not be able to communicate. ZTNA clients with different IP addresses but the same username will be able to communicate.

Default setting: Off. All ZTNA connected clients can communicate with each other.

### 11.9.2 Enable ZTNA Netflow Agent Option

See *Network Traffic*

### 11.9.3 Enable Cloud Collector Option

Ensure steps 10 and 11 in the link below have been completed for the appropriate Hub site.

See create-cloud-site

### 11.9.4 Enable Multi-Factor (MFA, 2FA, 2-step) Authentication for ZTNA Connection Manager

To enable MFA for clients connecting through the ZTNA Gateway, refer to the link below.

See *Enabling Multi-Factor Authentication for ZTNA Connection Manager (MFA, 2FA, 2-Step)*

## 11.10 Integrating External Systems

**Note:** This feature requires Enterprise Edition

Genan ZTNA can integrate with a variety of security vendors to establish security intelligence.

### 11.10.1 Integrating Palo Alto Networks Firewall

This guide provides an overview of integration with Palo Alto firewall. It includes the following information:

- *1. About This Guide*
- *2. Deployment of Genian ZTNA using PAN Firewall*
- *3. Configuring PAN Firewall for integration via XML API*
- *4. Configuring PAN Firewall for Integration via SYSLOG*

#### 1. About this Guide

This guide describes how Genian ZTNA engineers and enterprise operators can send information of user authentication to PAN firewall.

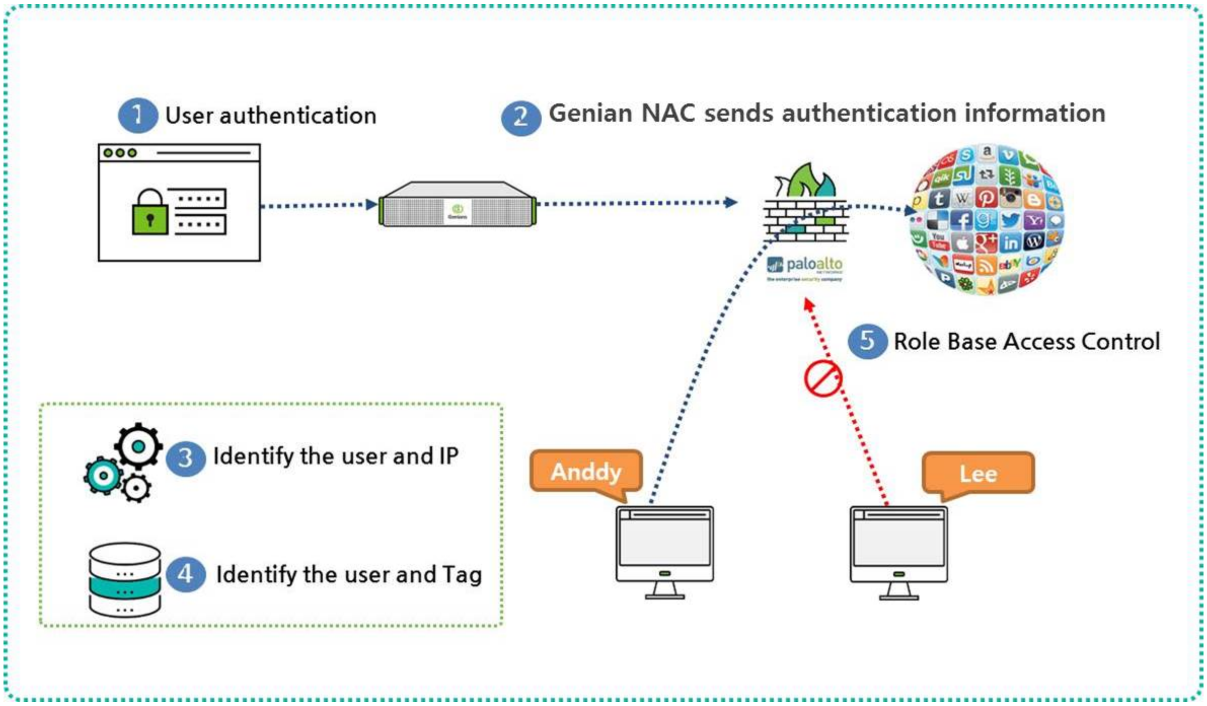
PAN Firewall generally requires that when a user changes a department or location, the IP information changes and the assigned permissions are modified accordingly. IP-based firewall policies do not know who is using an IP, but they can work with Genian ZTNA to get user information about an IP.

Based on this information, even if the user's department or location is moved and the IP information is changed, the user will be able to apply the authority assigned to each user without modifying the rule in the firewall. This efficiently improves administrator's internal infrastructure operation and security.

For more info about PAN firewalls , see https://docs.paloaltonetworks.com/pan-os

### 2. Deployment of Genian ZTNA using PAN Firewall

Genian ZTNA provides the integration of authentication. The PAN firewall refers to the IP and user authentication information provided by Genian ZTNA, and performs USER-ID mapping to enable access control by user role in the PAN Firewall.

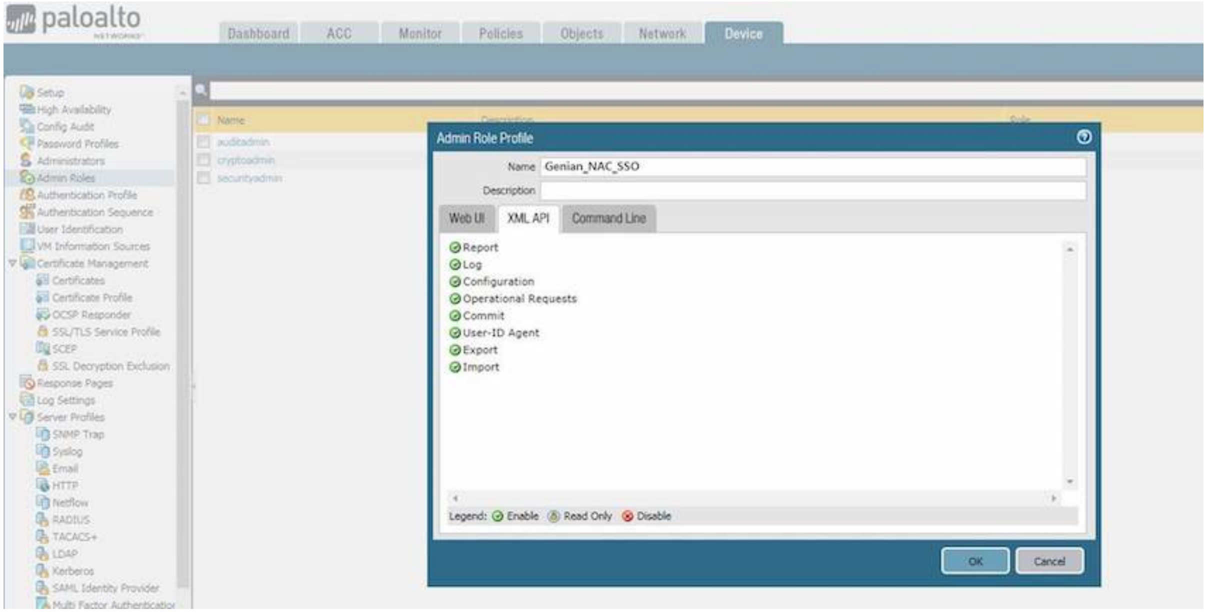

1 User authentication
2 Genian NAC sends authentication information
paloalto
5 Role Base Access Control
3 Identify the user and IP
4 Identify the user and Tag
Anddy
Lee

The authentication process is described below:

1. User Authentication in Genian ZTNA
2. Genian ZTNA sends authentication user and IP information to PAN firewall
3. The PAN firewall compares the authentication user and IP information it receives from Genian ZTNA with its own user ID table.
4. PAN confirms tag assigned to User-ID
5. Establish role-specific access control policy based on tag assigned to each user

## 3. Configuring PAN Firewall for integration via XML API

3.1 Create an Admin role on the PAN firewall. - Go to **Device** > **Admin Roles** > **Add** - Create the role **Name** Genian_ZTNA_SSO, under the **XML API** tab - Enable everything and validate it with **OK**



Admin Role Profile

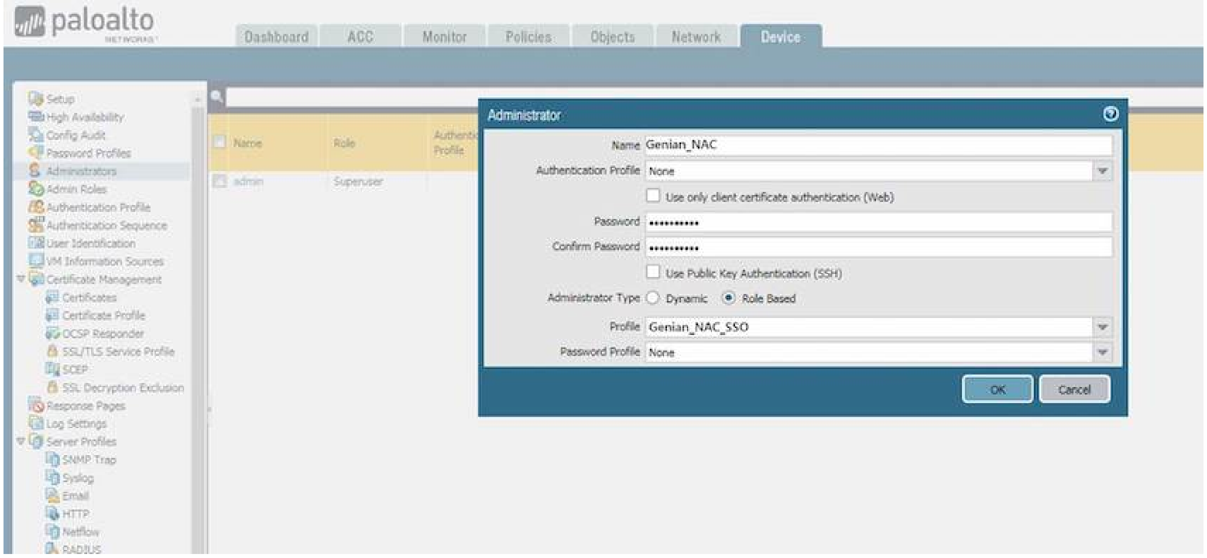
Name Genian_NAC_SSO

Description

✓ Report
✓ Log
✓ Configuration
✓ Operational Requests
✓ Commit
✓ User-ID Agent
✓ Export
✓ Import

Legend: ✓ Enable ● Read Only ⊗ Disable

3.2 Create an account for Genian ZTNA. Assign the SSO role to the account. - Enter a **Name**: Genian_ZTNA - Select the **Administrator Type**: Role Based - Select the **Profile**: Genian_ZTNA_SSO



Administrator

Name Genian_NAC

Authentication Profile None

□ Use only client certificate authentication (Web)

Password ••••••••••

Confirm Password ••••••••••

□ Use Public Key Authentication (SSH)

Administrator Type ○ Dynamic ● Role Based

Profile Genian_NAC_SSO

Password Profile None

3.3 Generate the XML Key. Go on this URL: **https://[ IP of PAN firewall]/api/?type=keygen&user=[username]&password=[password]** You can see the generated Key below:

```
**Script**
<response status = 'success'>
 <result>
     <key>LUFRPT1KbW80SU1hRXJuNk5XNHBudUhCNGMydE0rSUk9RFIzdEJ5RGcwWkRCVlhYMXl0Q1FPdz09
     </key>
 </result>
```

(continues on next page)

(continued from previous page)

```
</response>
```

3.4 Configure the Genian ZTNA for sending SYSLOG. Genian ZTNA uses filters in the audit log to integrate with XML.

- Go to **Log** in the top panel
- Go to **Log** > **Search** > **Advanced Search** > **Log ID** > **Check Authentication** > Click **Search** button in the left **Log** panel
- You will see the Log of Authentication user and then you click the "**save as**" button

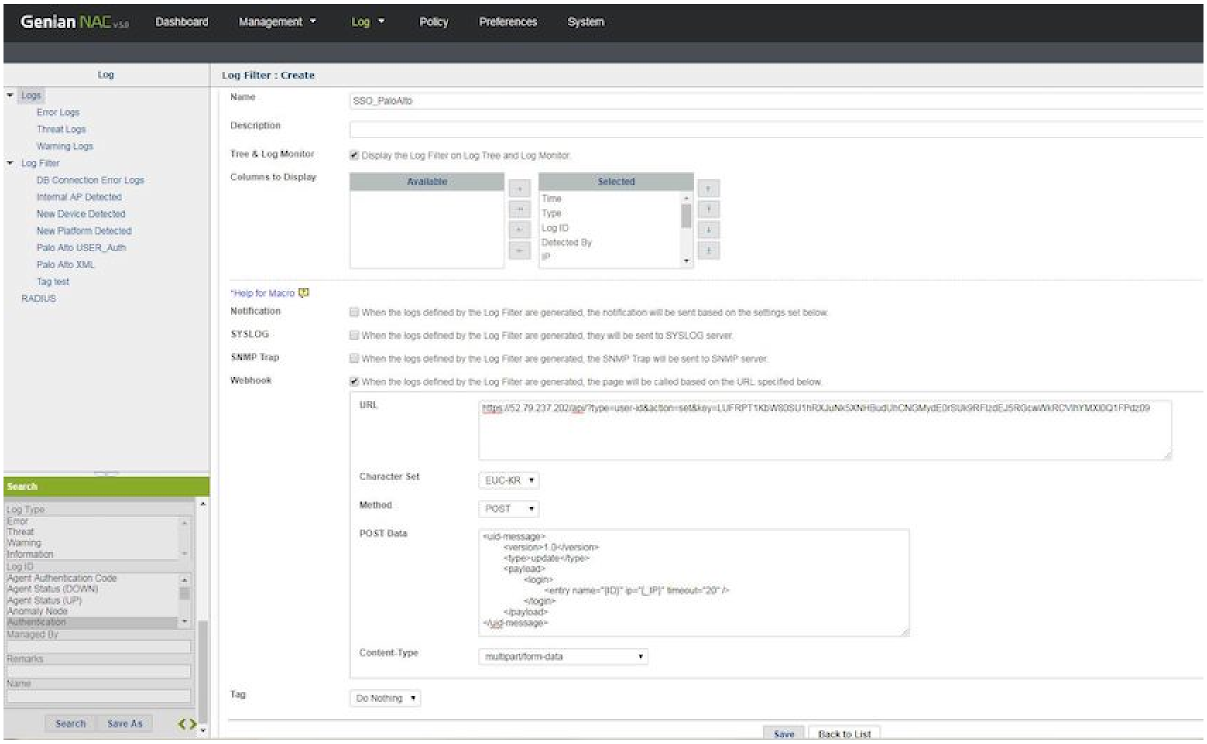
Enter a **Name**: SSO_PaloAlto Set the **Webhook URL:**

```
Call the PAN firewall XML
https://[IP of PAN firewall]/api/?type=user-id&action=set&
↪key=LUFRPT1KbW80SU1hRXJuNk5XNHBudUhCNGMydE0rSUk9RFIzdEJ5RGcwWkRCVlhYMXl0Q1FPdz09
```

Select a **character Set**: EUC-KR Select a **Method**: POST Enter the **POST Data**:

```
Script
<uid-message>
 <version>1.0</version>
 <type>update</type>
 <payload>
     <login>
         <entry name="{ID}" ip="{_IP}" timeout="20" />
     </login>
 </payload>
</uid-message>
```

Select a **Content-Type**: multipart/form-data



Log Filter : Create

Name: SSO_PaloAlto

Description:

Tree & Log Monitor: ☑ Display the Log Filter on Log Tree and Log Monitor

Columns to Display: Time, Type, Log ID, Detected By, IP

Notification: □ When the logs defined by the Log Filter are generated, the notification will be sent based on the settings set below

SYSLOG: □ When the logs defined by the Log Filter are generated, they will be sent to SYSLOG server

SNMP Trap: □ When the logs defined by the Log Filter are generated, the SNMP Trap will be sent to SNMP server

Webhook: ☑ When the logs defined by the Log Filter are generated, the page will be called based on the URL specified below

URL: https://52.79.237.202/api/?type=user-id&action=set&key=LUFRPT1KbW80SU1hRXJuNk5XNHBudUhCNGMydE0rSUk9RFIzdEJ5RGcwWkRCVlhYMXl0Q1FPdz09

Character Set: EUC-KR

Method: POST

POST Data:

```
<uid-message>
    <version>1.0</version>
    <type>update</type>
    <payload>
        <login>
            <entry name="{ID}" ip="{_IP}" timeout="20" />
        </login>
    </payload>
</uid-message>
```

Content-Type: multipart/form-data

Tag: Do Nothing

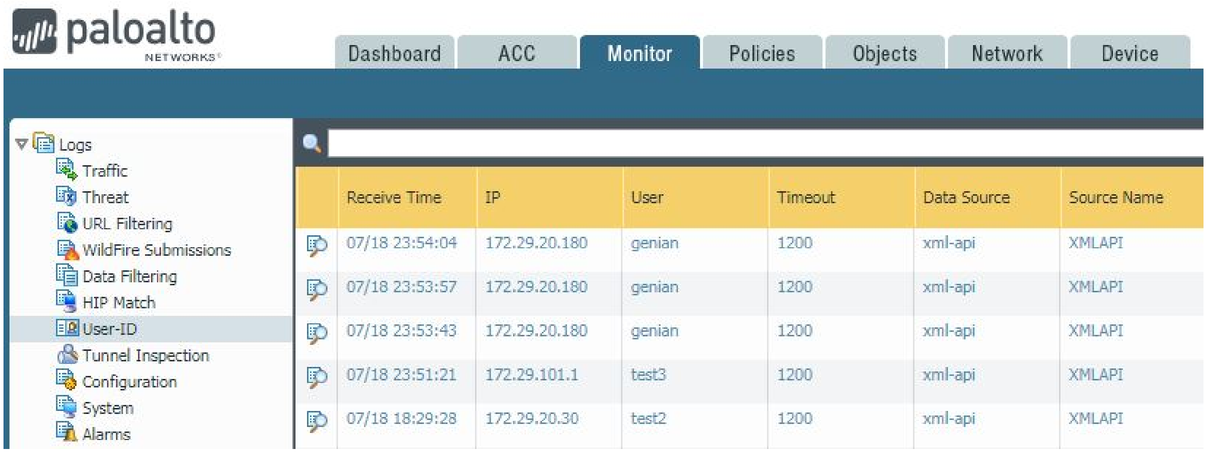
3.5 Configuring User Identification on Security Zones. PAN firewall policy rules use security zones to identify the Data traffic which flows freely within the zone, not flowing freely between the different zones until you define the allowed security policy rules. To enable enforcement of user identity, you must enable user identification in both the inbound and outbound zones that are passed by end-user traffic.

To enable User Identification - Go to **Network** > **Zone** - Select **Enable User Identification** and click **OK**

3.6 Verify that the firewall is successfully receiving login events from SSH and Web Console.

```
CLI Command
admin@PA-VM> show user ip-user-mapping all
IP                Vsys      From       User       IdleTimeout(s)    MaxTimeout(s)
--------------- ------      --------   ---------  --------------    -------------
172.29.101.1      vsys1     XMLAPI    genian          1111              1111
Total: 1 users
```

**WebConsole** - Go to **Monitor** - Go to **Logs** > **User-ID** in the left Monitor panel - You will see the list of authentication via Genian ZTNA



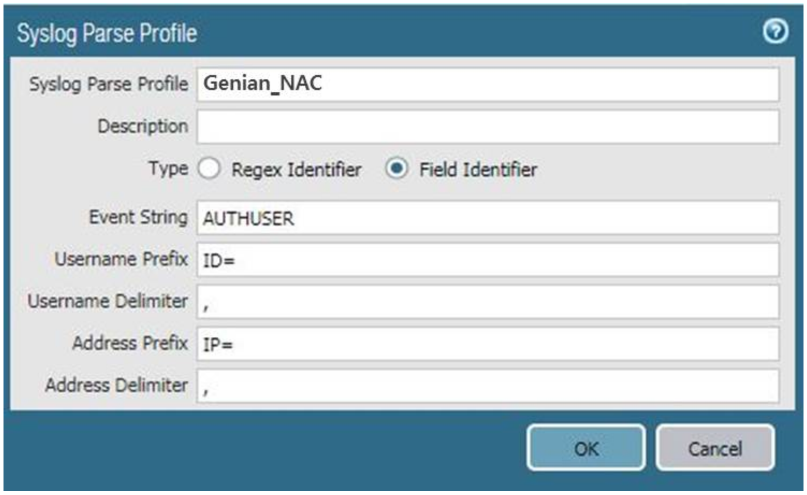
| Receive Time | IP | User | Timeout | Data Source | Source Name |
|---|---|---|---|---|---|
| 07/18 23:54:04 | 172.29.20.180 | genian | 1200 | xml-api | XMLAPI |
| 07/18 23:53:57 | 172.29.20.180 | genian | 1200 | xml-api | XMLAPI |
| 07/18 23:53:43 | 172.29.20.180 | genian | 1200 | xml-api | XMLAPI |
| 07/18 23:51:21 | 172.29.101.1 | test3 | 1200 | xml-api | XMLAPI |
| 07/18 18:29:28 | 172.29.20.30 | test2 | 1200 | xml-api | XMLAPI |

## 4. Configuring PAN Firewall for Integration via SYSLOG

4.1 Create a filter. The Palo Alto Firewall creates a log filter to distinguish authentication-related messages when receiving Syslog messages from Genian ZTNA.

- Go to **Device** on the top panel
- Go to User **Identification** > **User Mapping** > Click the Button look like **Gear** on PAN firewall **User-ID Agent Setup** Tab
- Go to Syslog **Filters** > **Add**

```
Enter values
Enter a Syslog Parse Profile: Genian_ZTNA
Enter a Event String: AUTHUSER
Enter a Username Prefix: ID=
Enter a Username Delimiter: ,
Enter a Address Prefix: IP=
Enter a Address Delimiter: ,
```


Syslog Parse Profile

Syslog Parse Profile: Genian_NAC

Description:

Type ○ Regex Identifier ● Field Identifier

Event String: AUTHUSER

Username Prefix: ID=

Username Delimiter: ,

Address Prefix: IP=

Address Delimiter: ,

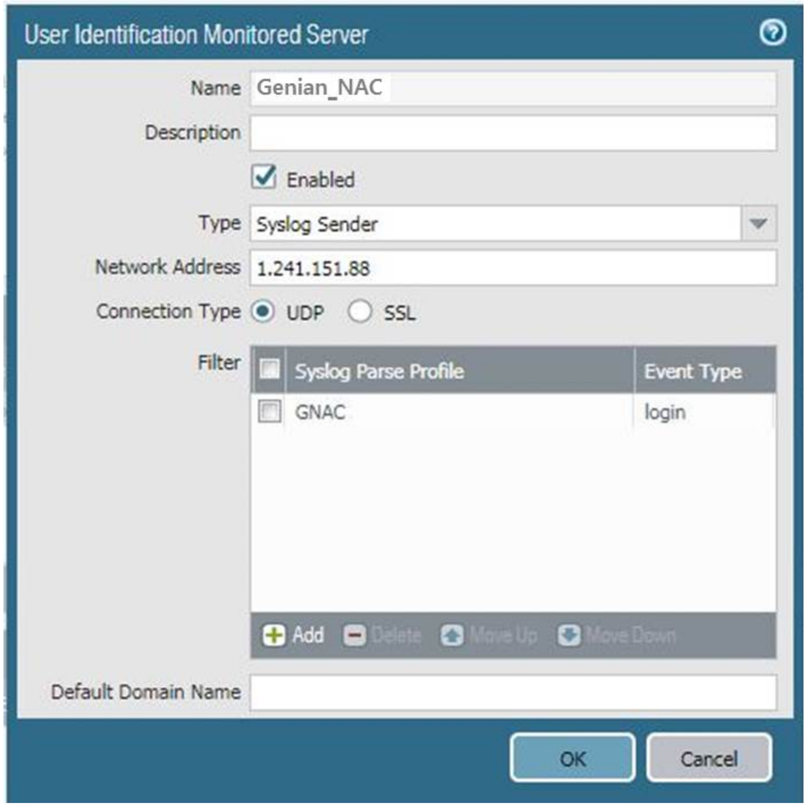
4.2 Specify the SYSLOG sender that the PAN firewall monitor.

- Go to **Device** > **User Identification** > **User Mapping** and **ADD** an entry to the Server Monitoring list

```
Enter values
Enter a Name to identify the sender
Make sure the sender Profile is Enabled (default is enabled)
Set the Type to Syslog Sender.
Enter the Network Address of the Genian ZTNA IP address
Select SSL(default) or UDP as the Connection Type
```

**Note:** The UDP protocol is unencrypted data. It is recommended to use of the SSL protocol.

The listening ports(514 for UDP and 6514 for SSL)



User Identification Monitored Server

Name: Genian_NAC

Description:

☑ Enabled

Type: Syslog Sender

Network Address: 1.241.151.88

Connection Type: ● UDP ○ SSL

Filter:

| □ Syslog Parse Profile | Event Type |
|---|---|
| □ GNAC | login |

Default Domain Name:

4.3 Enable SYSLOG listener services. It is able to listen to the SYSLOG from Genian ZTNA.

- Go to **Network** > **Network Profiles** > **Interface Mgmt** > **ADD** a new profile

```
Enter values
Enter a Name to identify the Network Profile: Allow Genian ZTNA
Check the User-ID SYSLOG Listener-SSL or User-ID SYSLOG Listener-UDP
Click OK to save the interface management profile
```

4.4 Assign the interface Management profile to the interface.

- Go to **Network** > **Interfaces** and edit the interface
- Go to **Advanced** > **other info** > select the **Interface Management Profile** > select the Allow Genian ZTNA > Click **Ok**
- **Commit**

4.5 Configure the Genian ZTNA for sending SYSLOG. Genian ZTNA uses filters in the audit log to integrate with SYSLOG.

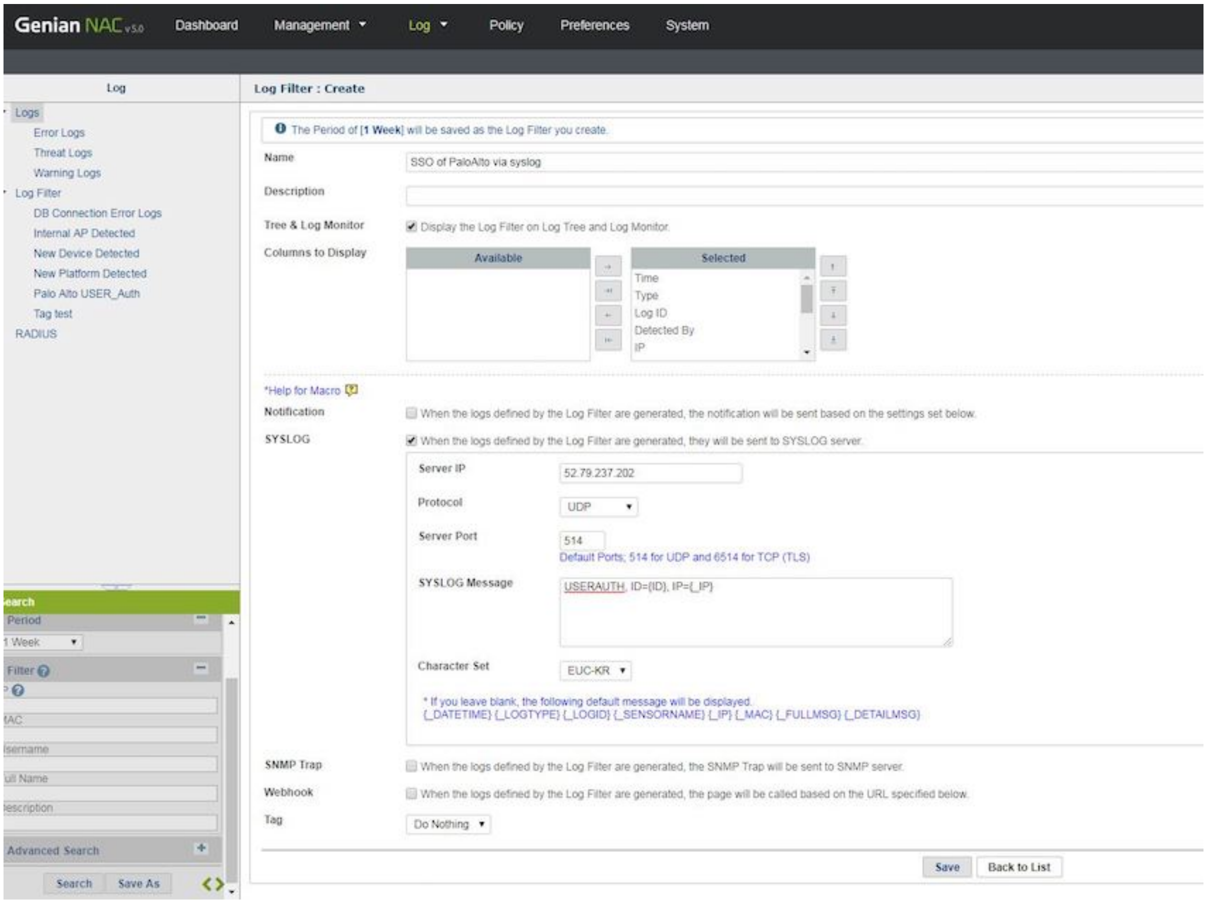
- Go to **Log** in the top panel
- Go to **Log** > **Search** > **Advanced Search** > **Log ID** > Check Authentication > Click **Search** button in the left Log panel
- You will see the Log of Authentication user and then you click the "**save as**" button

```
Enter values
Enter a Name
Enter a Server IP address[ Palo Alto IP]
Select the Protocol either UDP or TCP(TLS)
```

(continues on next page)

(continued from previous page)

```
Set a Server port(UDP for 514, TCP(TLS) for 6514)
Enter the SYSLOG Message: USERAUTH, ID={ID}, IP={_IP}
Click the Save
```



Log Filter : Create

The Period of [1 Week] will be saved as the Log Filter you create.

Name: SSO of PaloAlto via syslog

Description:

Tree & Log Monitor: ☑ Display the Log Filter on Log Tree and Log Monitor.

Columns to Display: Available / Selected: Time, Type, Log ID, Detected By, IP

*Help for Macro

Notification: ☐ When the logs defined by the Log Filter are generated, the notification will be sent based on the settings set below.

SYSLOG: ☑ When the logs defined by the Log Filter are generated, they will be sent to SYSLOG server.

Server IP: 52.79.237.202

Protocol: UDP

Server Port: 514

Default Ports; 514 for UDP and 6514 for TCP (TLS)

SYSLOG Message: USERAUTH, ID={ID}, IP={_IP}

Character Set: EUC-KR

* If you leave blank, the following default message will be displayed.
{_DATETIME} {_LOGTYPE} {_LOGID} {_SENSORNAME} {_IP} {_MAC} {_FULLMSG} {_DETAILMSG}

SNMP Trap: ☐ When the logs defined by the Log Filter are generated, the SNMP Trap will be sent to SNMP server.

Webhook: ☐ When the logs defined by the Log Filter are generated, the page will be called based on the URL specified below.

Tag: Do Nothing

Save | Back to List

4.5 Verify that the user mappings when users log in and out.

```
CLI command
admin@PA-VM> show user ip-user-mapping all type SYSLOG
IP                 Vsys       From      User            IdleTimeout(s)    MaxTimeout(s)
---------------  -----      -------   --------------------     --------------             
↪   -------------
172.29.101.1       vsys1      SYSLOGI    genian          2220                  2220
Total: 1 users
```

## 11.10.2 Integrating FireEye

This guide provides an overview of integration with FireEye. It includes the following information:

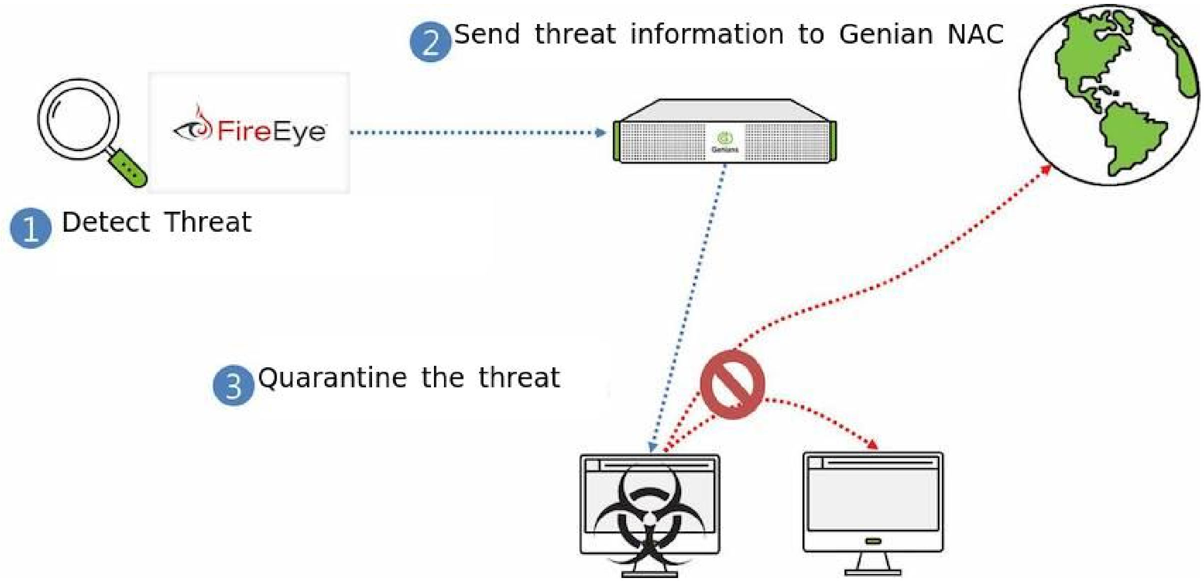
- *1. About This Guide*
- *2. Deployment of Genian ZTNA using FireEye*
- *3. Configuring FireEye for integration via SYSLOG*
- *4. Apply Genian ZTNA Policy based on FireEye Data*

## 1. About this Guide

The guide describes how to integrate Genian ZTNA and FireEye.

When a specific anomaly is detected by FireEye, FireEye sends anomaly information detected to Genian ZTNA through SYSLOG Genian ZTNA will be able to prevent the spread of anomalies by quarantine the anomaly target.

## 2. Deployment of Genian ZTNA using FireEye



1. FireEye detects the threatening device.
2. FireEye sends the anomaly information to Genian ZTNA via SYSLOG.
3. Genian ZTNA quarantines the device to prevent compromising other assets on the network. Other automated responses may also be configured.

## 3. Configuring FireEye for integration via SYSLOG

### 3.1 Configuration of Genian ZTNA

For Genian ZTNA to receive and use the information from FireEye, the internal SYSLOG server must be configured to properly extract node information from the incoming log. The `Type` and `Type Value` variables determine which information sources will be accepted, and how they will be categorized. The `IP Prefix` and `MAC Prefix`

1. Login into Genian ZTNA with the administrator account
2. Go to the **Preferences** tap on the top panel.
3. Go to the **General** > **Log** on the left panel.
4. **Add** the Filter in **Server Rules** in the middle of the center
5. Enter the content

<table>
<tr><td>Name</td><td>FireEye</td></tr>
<tr><td colspan="2">Filter | host</td></tr>
<tr><td colspan="2">Filter Value|[IP address of FireEye]</td></tr>
<tr><td>IP Prefix</td><td>src=</td></tr>
<tr><td>MAC Prefix</td><td>smac=</td></tr>
</table>

6. Click the **Add** button below and **Update** button

**3.2 Configuration of FireEye**

The FireEye appliances are very flexible regarding Notification output and support the following formats.

- CEF
- LEEF
- CSV

For our guide, we will use CEF Complete the following steps to send data to Genian ZTNA using CEF:

1. Log into the FireEye appliance with an administrator account
2. Go to the **Settings** tap on the top panel.
3. Go to the **Notifications** on the left panel
4. Click the **rsyslog** on the middle of the center
5. Check the "Event type" in the check box
6. Make sure **Rsyslog settings** are

```
Default format: CEF
Default delivery: Per event
Default send as: Alert
```

7. **Add Rsyslog server** on the middle of under > Enter the **Name** Genian ZTNA > Click on **Add Rsyslog Server** button
8. Enter the IP address of the Genian ZTNA in the IP Address field
9. Click the **Update** button below

**3.3 Verification**

1. Go to **Log** on the top panel of Genian ZTNA.
2. Messages from FireEye will show. The Sensor column data will show the IP of the FireEye system, and the Description column data will show a FireEye signature.

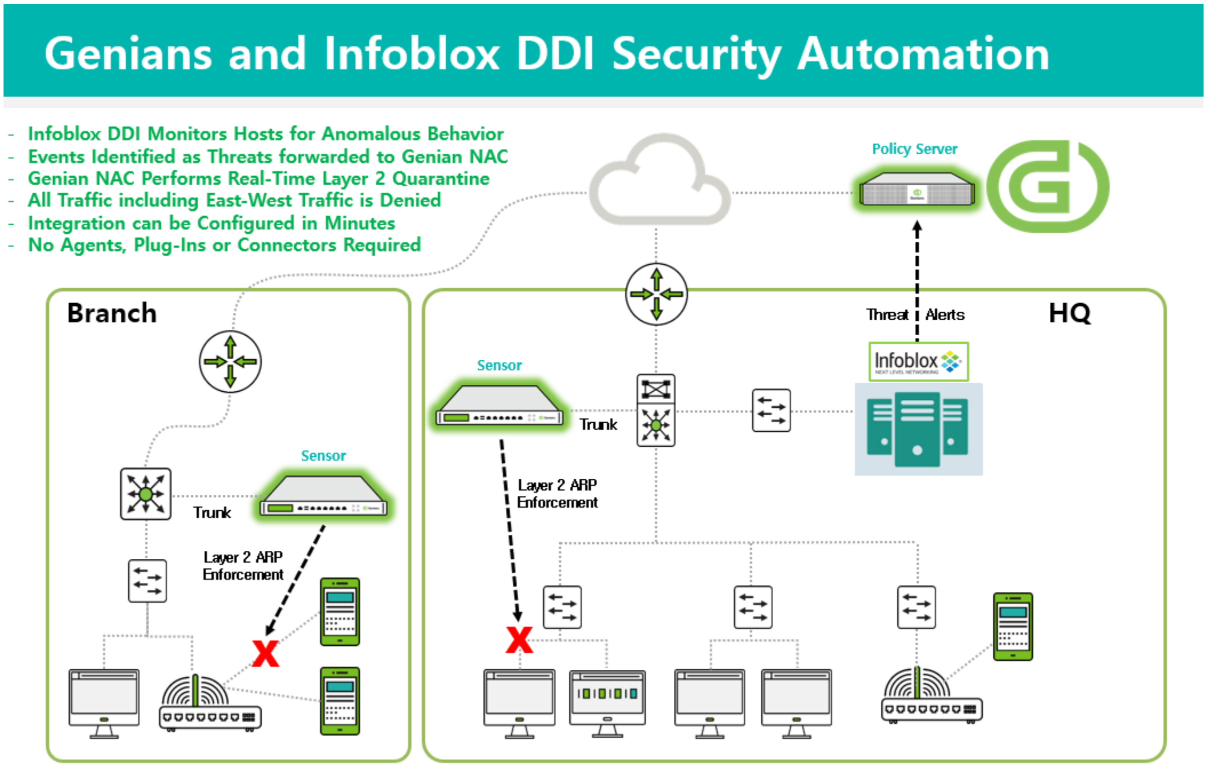
## 4. Apply Genian ZTNA Policy based on FireEye Data

Once Genian ZTNA is receiving SYSLOG data from FireEye, the device information contained in the log files can be used to automatically apply Tags to individual nodes. These tags can be used to group nodes for organizational, or policy purposes.

To apply policy through log tagging see: :*Tagging Assets Using Event*

### 11.10.3 Integrating Infoblox DDI

This document describes how to integrate Infoblox with Genian ZTNA using syslog. This integration provides the ability to extend the Infoblox DDI Response Policy Zone (RPZ) feature into the Enforcement capabilities of Genians ZTNA. A full video Webinar covering this integration along with a demo is available on the Genians YouTube Channel.



Genians and Infoblox DDI Security Automation

- Infoblox DDI Monitors Hosts for Anomalous Behavior
- Events Identified as Threats forwarded to Genian NAC
- Genian NAC Performs Real-Time Layer 2 Quarantine
- All Traffic including East-West Traffic is Denied
- Integration can be Configured in Minutes
- No Agents, Plug-Ins or Connectors Required

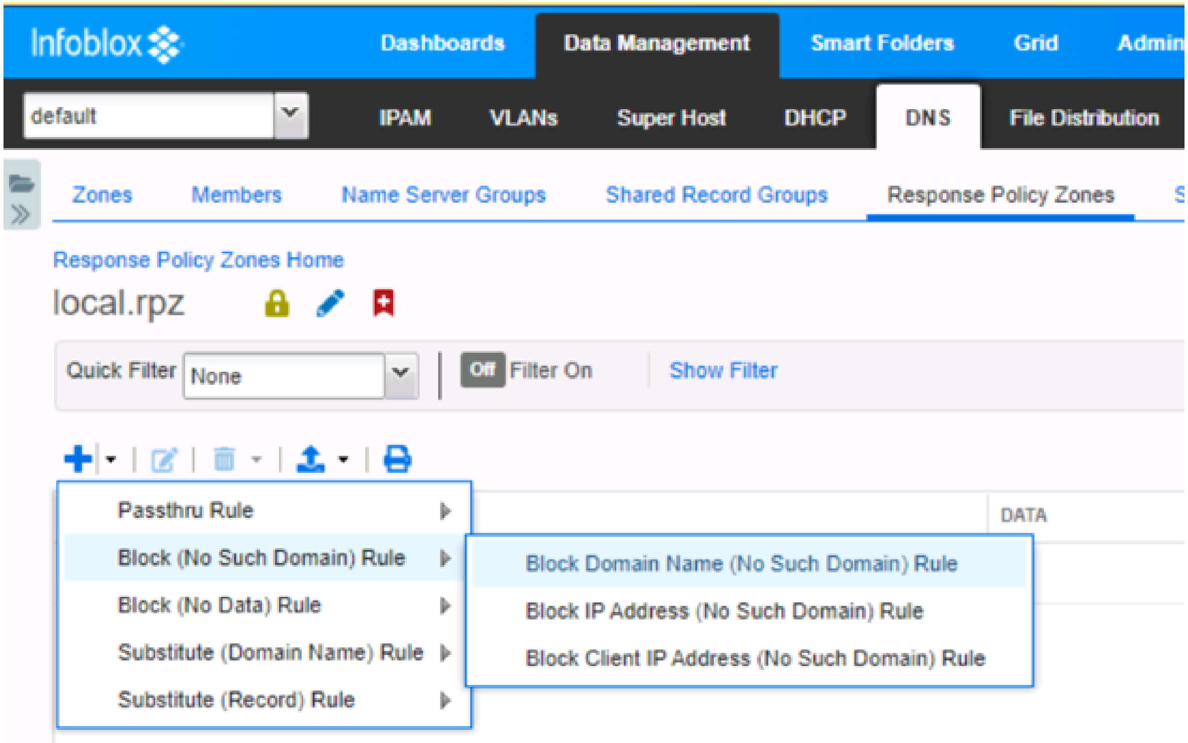
The main steps of this integration are as follows:

- Configure a domain to be blocked in Infoblox
- Export this blocking event to Genian ZTNA via syslog
- Configure Genian ZTNA to interpret this event, and apply enforcement to the impacted node.

### Infoblox Domain Blocking Configuration

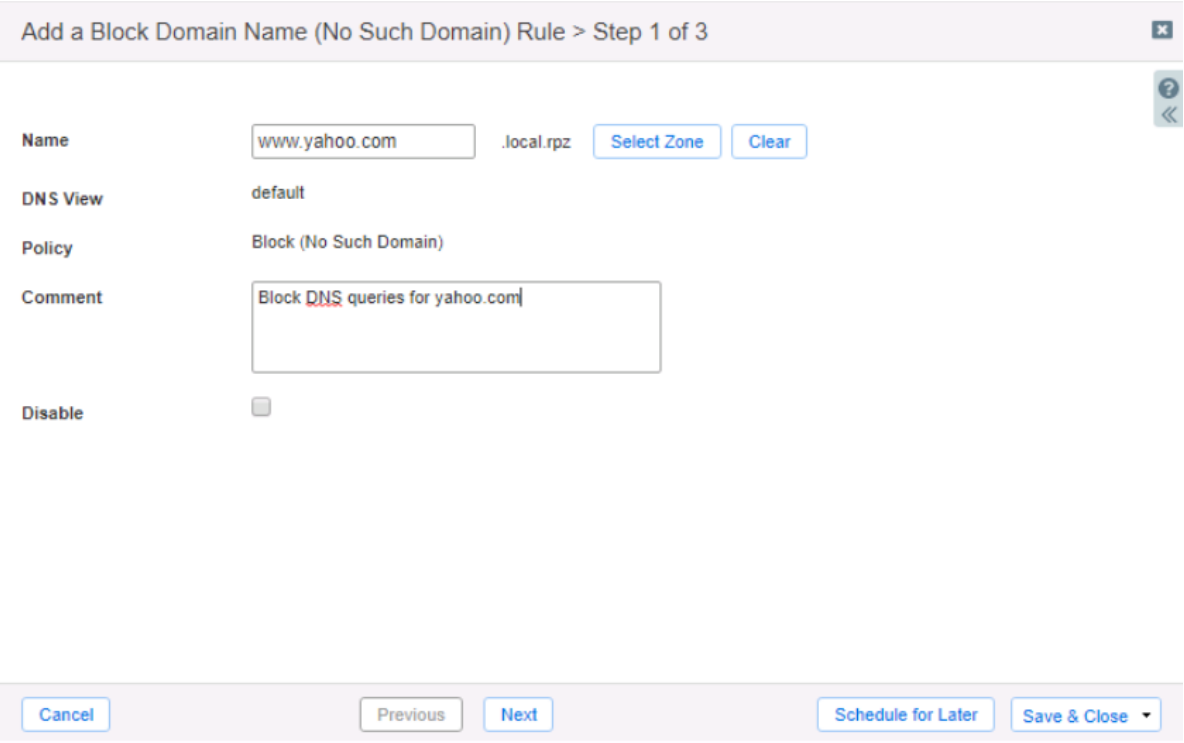
The steps below demonstrate how to configure and export critical RPZ events from Infoblox DDI to Genians via Syslog.

1. Navigate to **Data Management > DNS > Response Policy Zones > local.rpz**
2. Click **+** to add a new Block Rule for a Domain Name



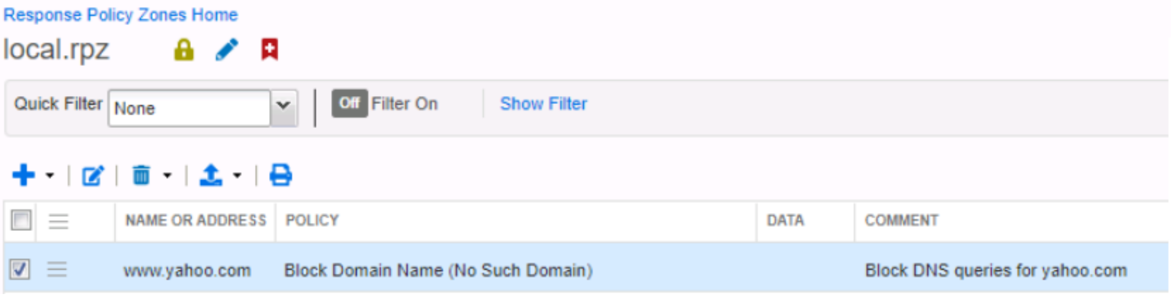
3. Enter a test domain name. In this example www.yahoo.com was used to simulate to simulate a Domain Name that is associated with a Malware Threat. Enter the Domain Name and a comment and then click Save & Close. No need to complete steps 2 and 3 in Infoblox.

**Note:** If your Infoblox Grid is already receiving Threat Intelligence from an external Threat Feed, then any sites listed as malware sites in that feed will also be blocked. Consult Infoblox documentation for additional details.



Add a Block Domain Name (No Such Domain) Rule > Step 1 of 3

| | |
|---|---|
| Name | www.yahoo.com .local.rpz |
| DNS View | default |
| Policy | Block (No Such Domain) |
| Comment | Block DNS queries for yahoo.com |
| Disable | □ |



Response Policy Zones Home

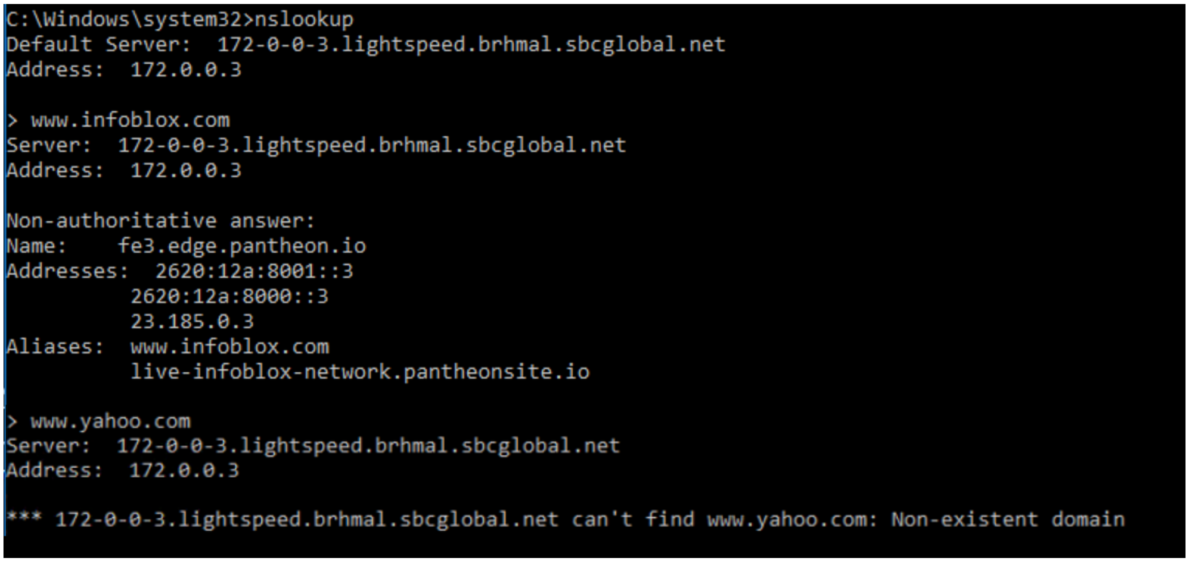
local.rpz

Quick Filter None | Off Filter On | Show Filter

| □ | NAME OR ADDRESS | POLICY | DATA | COMMENT |
|---|---|---|---|---|
| ☑ | www.yahoo.com | Block Domain Name (No Such Domain) | | Block DNS queries for yahoo.com |

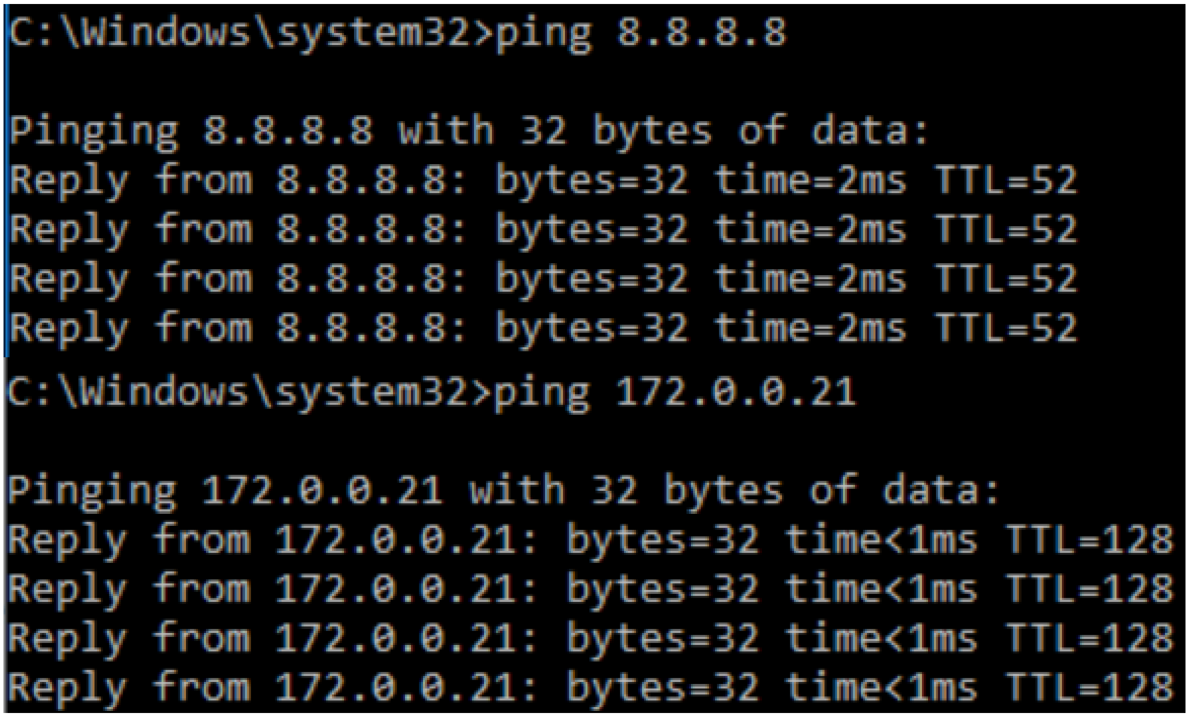
4. On a test machine subject to the previously configured Response Policy Zone, perform an nslookup on authorized domain (infoblox.com) and then perform an nslookup on unauthorized domain simulating malware site (www.yahoo.com).

5. Note Infoblox.com resolves fine but www.yahoo.com is returned as Non-existent domain. If you do not receive a Non-existent domain notification for the test malware site, consult Infoblox DDI documentation or support until the issue is resolved.



```
C:\Windows\system32>nslookup
Default Server:  172-0-0-3.lightspeed.brhmal.sbcglobal.net
Address:  172.0.0.3

> www.infoblox.com
Server:  172-0-0-3.lightspeed.brhmal.sbcglobal.net
Address:  172.0.0.3

Non-authoritative answer:
Name:    fe3.edge.pantheon.io
Addresses:  2620:12a:8001::3
          2620:12a:8000::3
          23.185.0.3
Aliases:  www.infoblox.com
          live-infoblox-network.pantheonsite.io

> www.yahoo.com
Server:  172-0-0-3.lightspeed.brhmal.sbcglobal.net
Address:  172.0.0.3

*** 172-0-0-3.lightspeed.brhmal.sbcglobal.net can't find www.yahoo.com: Non-existent domain
```

6. On the test machine, generate continuous pings to both an internal and external host. Note that even though Infoblox DDI has denied the domain from being resolved, the device still has network access, both to external and internal hosts:

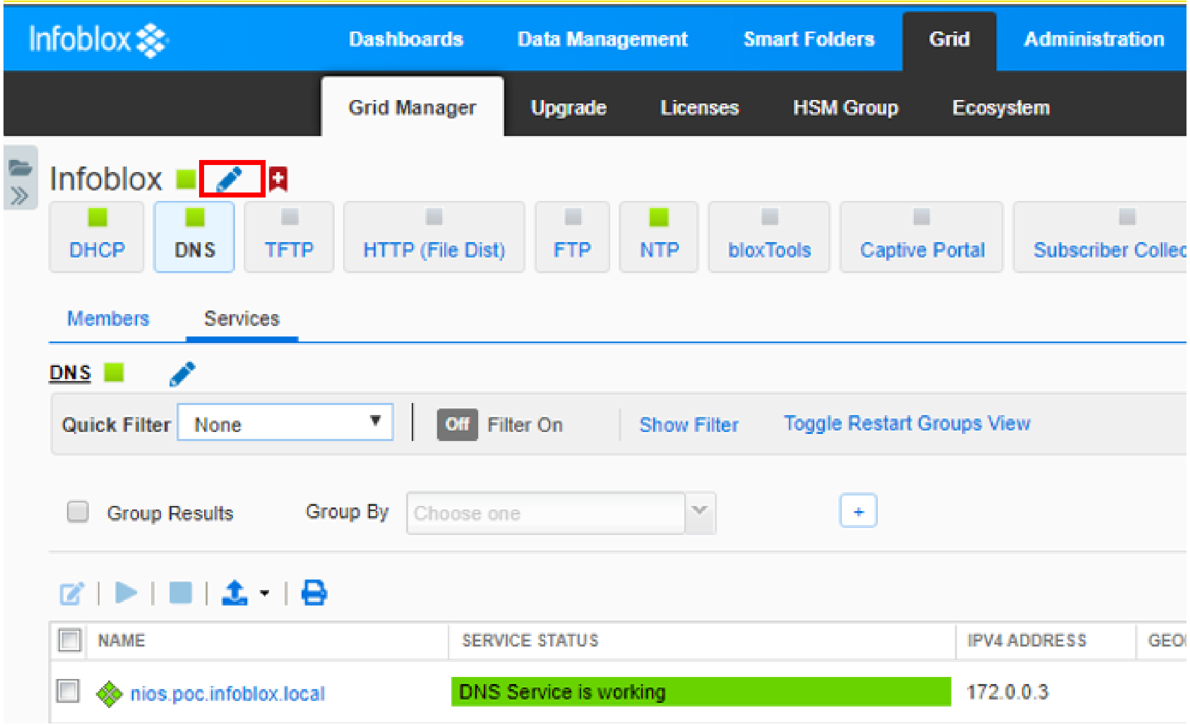


```
C:\Windows\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=2ms TTL=52
Reply from 8.8.8.8: bytes=32 time=2ms TTL=52
Reply from 8.8.8.8: bytes=32 time=2ms TTL=52
Reply from 8.8.8.8: bytes=32 time=2ms TTL=52
C:\Windows\system32>ping 172.0.0.21

Pinging 172.0.0.21 with 32 bytes of data:
Reply from 172.0.0.21: bytes=32 time<1ms TTL=128
Reply from 172.0.0.21: bytes=32 time<1ms TTL=128
Reply from 172.0.0.21: bytes=32 time<1ms TTL=128
Reply from 172.0.0.21: bytes=32 time<1ms TTL=128
```

7. Once the test above has been validated, perform the steps below to export Non-existent domain events to the Genian ZTNA Policy Server.

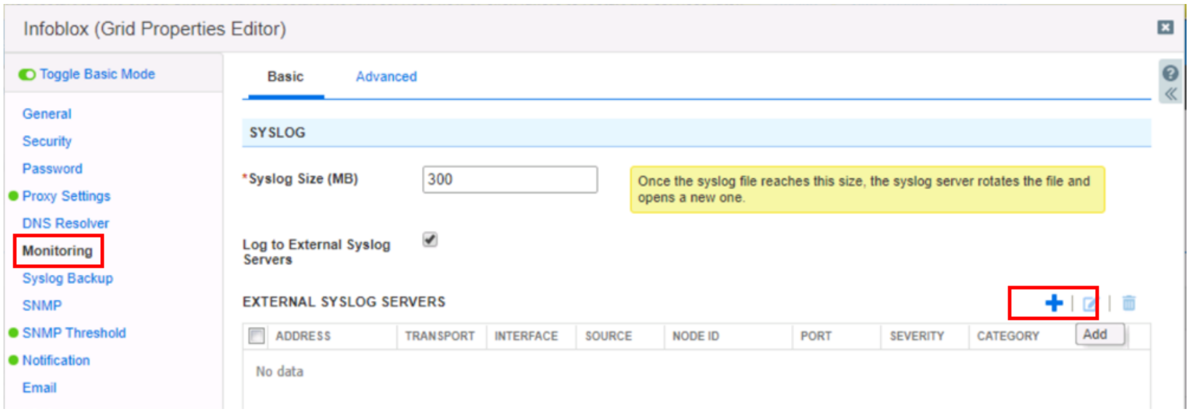
## Infoblox Event Export Configuration

1. Navigate to **Grid > Grid Manager** and click on the **edit** button next to Infoblox.



| ☐ | NAME | SERVICE STATUS | IPV4 ADDRESS | GEO |
|---|---|---|---|---|
| ☐ | nios.poc.infoblox.local | DNS Service is working | 172.0.0.3 | |

2. Click on **Monitoring** and then click the **+** button to add a new Syslog server.



*Syslog Size (MB): 300

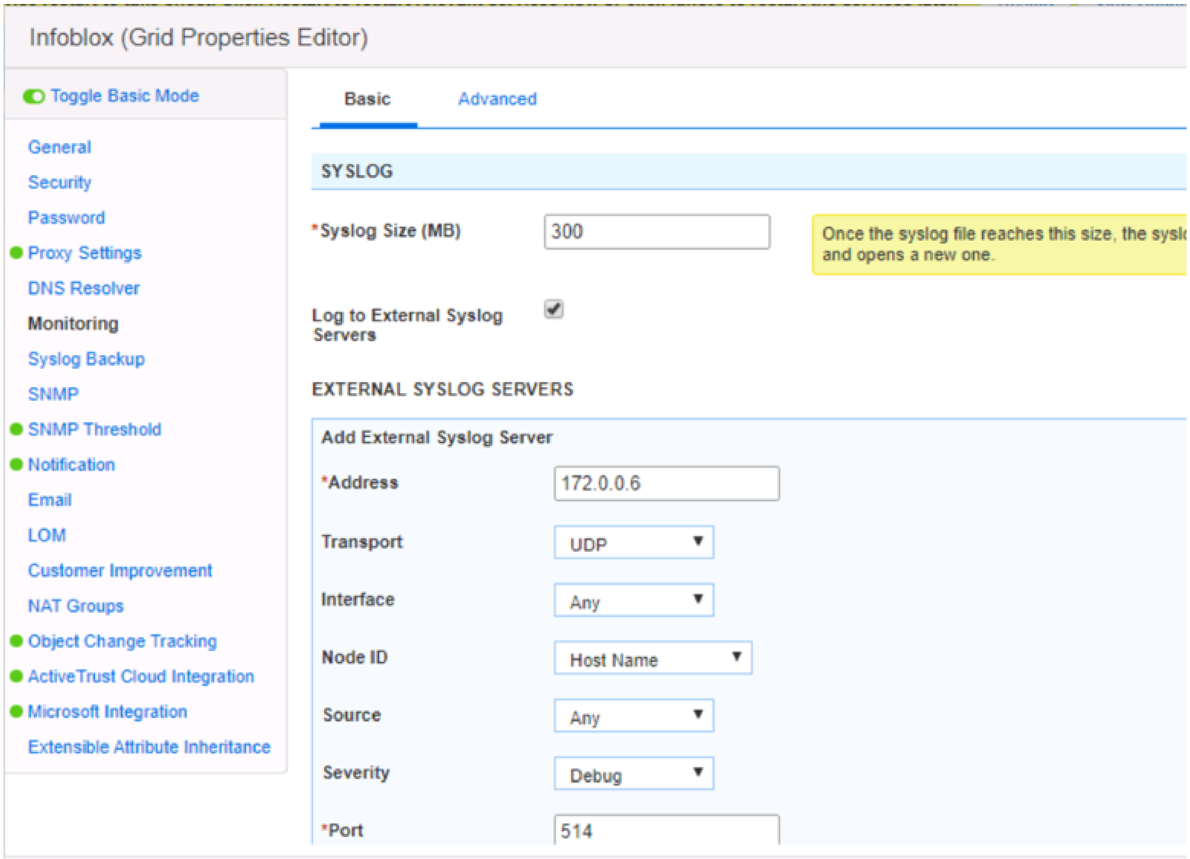
Once the syslog file reaches this size, the syslog server rotates the file and opens a new one.

Log to External Syslog Servers ☑

| ☐ | ADDRESS | TRANSPORT | INTERFACE | SOURCE | NODE ID | PORT | SEVERITY | CATEGORY |
|---|---|---|---|---|---|---|---|---|
| | No data | | | | | | | |

3. Check the **Log to External Syslog Servers** box and click the **+** button to add a new server.

4. Enter the IP of the Genian ZTNA Policy Server, select **UDP**, **Any** for Interface, **Host Name** for Node ID, **Any** for Source, **Debug** for Severity and **514** for Port. Restart service in Infoblox DDI if prompted.



Infoblox (Grid Properties Editor)

SYSLOG

*Syslog Size (MB): 300

Once the syslog file reaches this size, the sysl
and opens a new one.

Log to External Syslog Servers: ☑

EXTERNAL SYSLOG SERVERS

Add External Syslog Server

*Address: 172.0.0.6

Transport: UDP

Interface: Any

Node ID: Host Name

Source: Any

Severity: Debug

*Port: 514

## Genian ZTNA Syslog Server Configuration

A Server Rule set must be added before receiving syslogs. We will configure a server rule based on the format of the Infoblox message to extract information about the device to be blocked. In this integration, we will use the IP address.

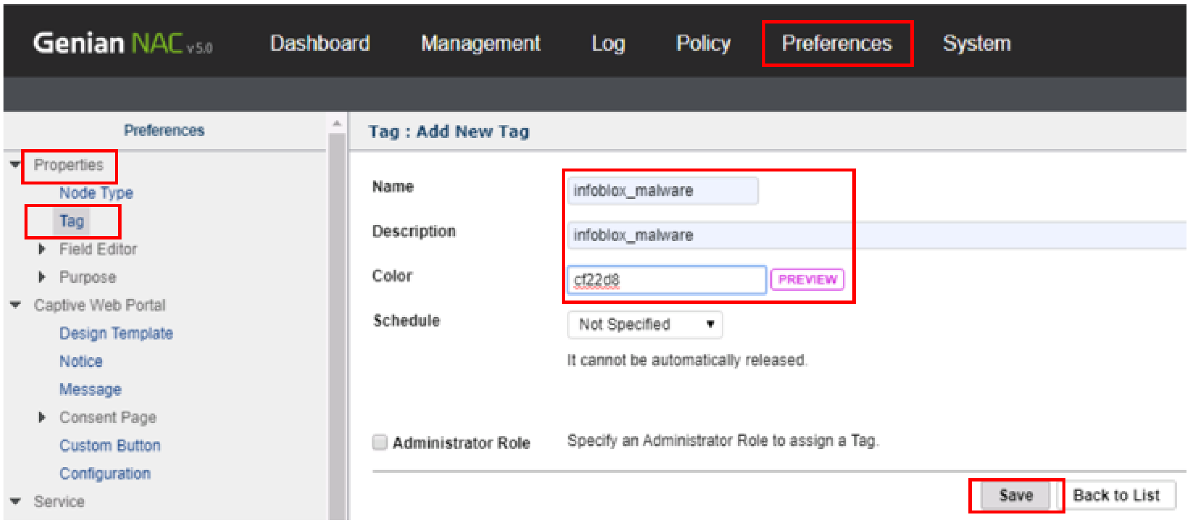
These options may be found under **General > Log** in the **Preferences** section.

1. Click the **Add** button to the right of the **Server Rules** label, and fill out the pop-up form.
2. Enter a name for the Rule.
3. For **Filter**,select a variable by which to evaluate incoming syslogs for allowance. Select from **Program** , **Host**, **Match**, or **Netmask.**
4. Define a **Filter Value.** If the **Filter** variable of the imported syslog matches the **Filter Value** , the syslog will be merged into the policy server logs. Enter the appropriate network or program information so that the message from your Infoblox system will be recognized.
5. Define **src=** as a prefix for **IP** values. This prefix will trigger the filter to import the value immediately following as an IP Address, allowing Genian ZTNA to identify the device using that IP.
6. Define the character set which the syslogs will be imported in.
7. Click **Add** at the bottom of the pop-up window.
8. Click **Update** at the bottom of the Log Preferences page.

Now the message from the Infoblox system will be correllated with the nodes detected by Genian ZTNA.

## Genian ZTNA Tag and Policy Configuration

1. Navigate to **Preferences > Properties > Tag** and create a tag called "infoblox_malware" then click **Save**. This tag will be linked to a log filter and eventually to an Enforcement Policy in future steps.



Tag : Add New Tag

Name: infoblox_malware

Description: infoblox_malware

Color: cf22d8 PREVIEW

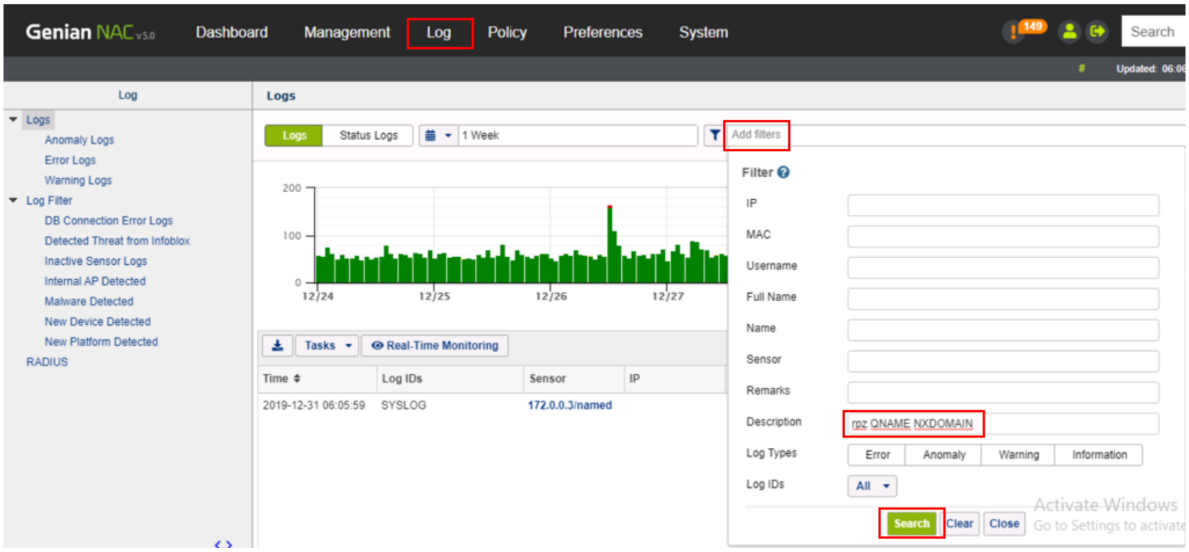
Schedule: Not Specified

It cannot be automatically released.

□ Administrator Role: Specify an Administrator Role to assign a Tag.

Save | Back to List

2. Click on **Log** and then **Add filters**. Critical RPZ syslog alerts from Infoblox DDI include the key words "rpz QNAME NXDOMAIN". Type these words into the Description field of the log filter and click **Search**.



Filter

IP:

MAC:

Username:

Full Name:

Name:

Sensor:

Remarks:

Description: rpz QNAME NXDOMAIN

Log Types: Error | Anomaly | Warning | Information

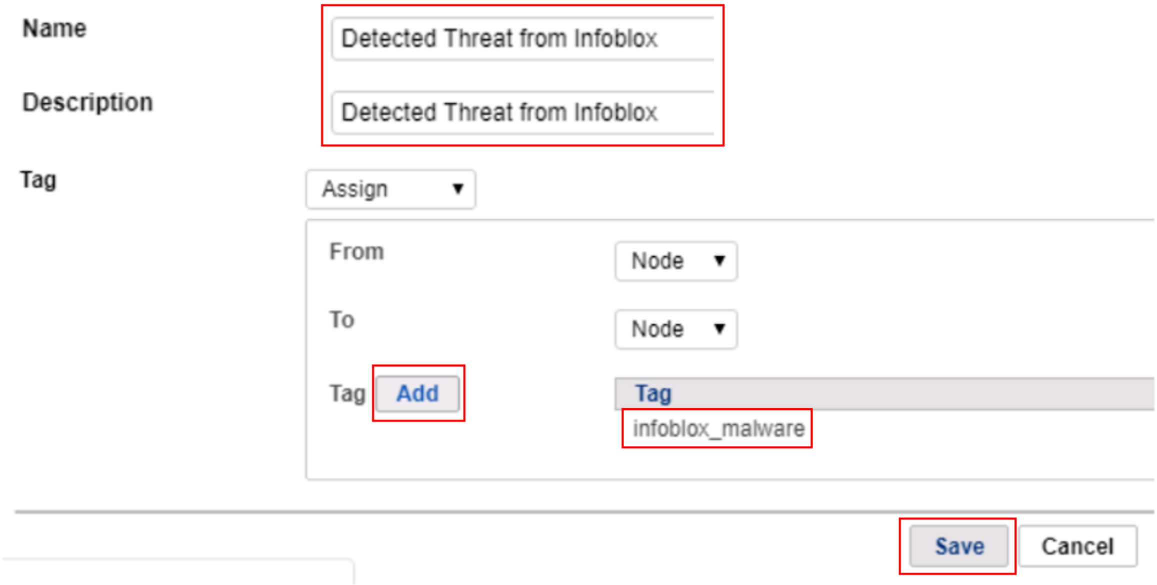
Log IDs: All

Search | Clear | Close

| Time | Log IDs | Sensor | IP |
|---|---|---|---|
| 2019-12-31 06:05:59 | SYSLOG | 172.0.0.3/named | |

3. The search results should show a syslog alert from Infoblox DDI showing rpz QNAME NXDOMAIN for www.yahoo.com. This alert was generated from the previous test on [Win-Client1]. Click Save to save as a log filter.

4. Give the log filter a name, description and add the previously created "Infoblox_malware" tag then click **Save**. In this example, we will apply the tag to the node (MAC+IP), though log filters can also apply tags to MACs, Users, or WLANs.


Name: Detected Threat from Infoblox

Description: Detected Threat from Infoblox

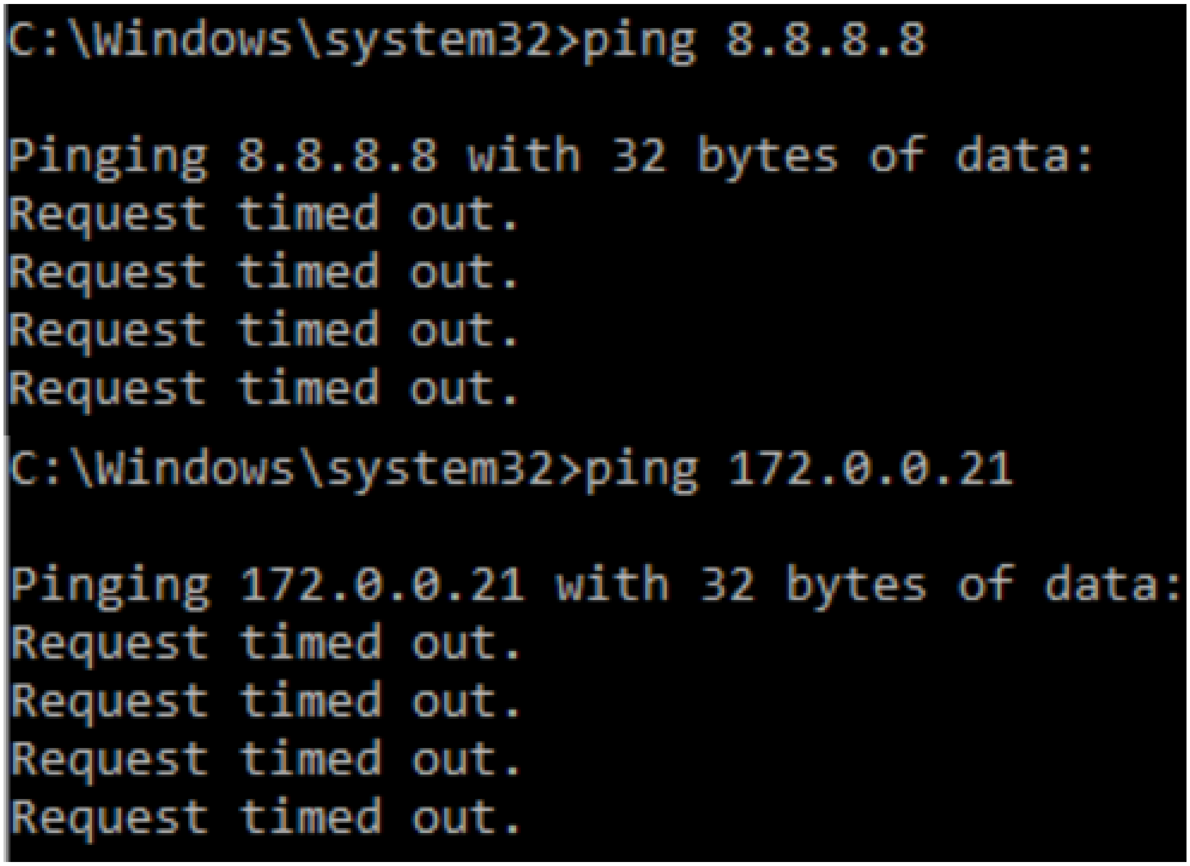
Tag: Assign

From: Node

To: Node

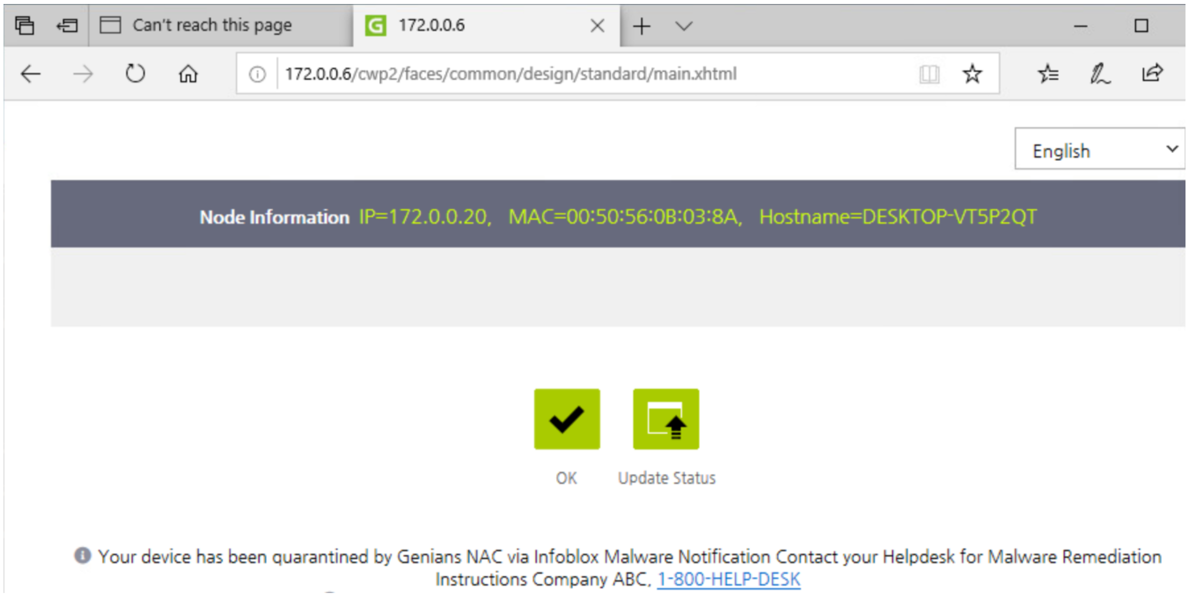
Tag: infoblox_malware

5. Navigate to **Policy > Group** then click **Tasks > Create** to create a new Node Group. Under General enter an ID and Description and set the Status to Enabled. Under Condition, click **Add** to add the previously created “Infoblox_malware” tag then click **Save**.
6. Navigate to **Policy > Enforcement Policy** then click **Tasks > Create** to create a new Enforcement Policy. Follow the wizard to create a new Enforcement Policy. Select the previously created “Infoblox_quarantine” Node Group, do not select any permissions (all access will be blocked by default), enable Captive Portal and enter a message to be displayed to the end user.
7. With all configurations now in place, the Genians Network Sensor must be switched from Passive to Active mode to facilitate the Layer 2 quarantine of non-compliant nodes on the network. Navigate to **System > Sensor > Edit Sensor Settings** and set the Sensor Operating Mode to Active then click Update at the bottom of the page.
8. To test the integration, from the test machine open a browser and navigate to www.yahoo.com. The page should not load. As a result of Infoblox enforcement DNS cannot be resolved, and no captive portal will be shown.
   - However, behind the scenes, a rpz QNAME NXDOMAIN syslog alert has been sent from Infoblox to Genians and the host has been Layer 2 quarantined on the network. The test machine should no longer be able to ping external or internal hosts.



```
C:\Windows\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
C:\Windows\system32>ping 172.0.0.21

Pinging 172.0.0.21 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

9. In the browser of the test machine, navigate to Infoblox.com and the Genians Captive Portal will be displayed with your message. Both the page design and contents may be customized, this is just a generic template.



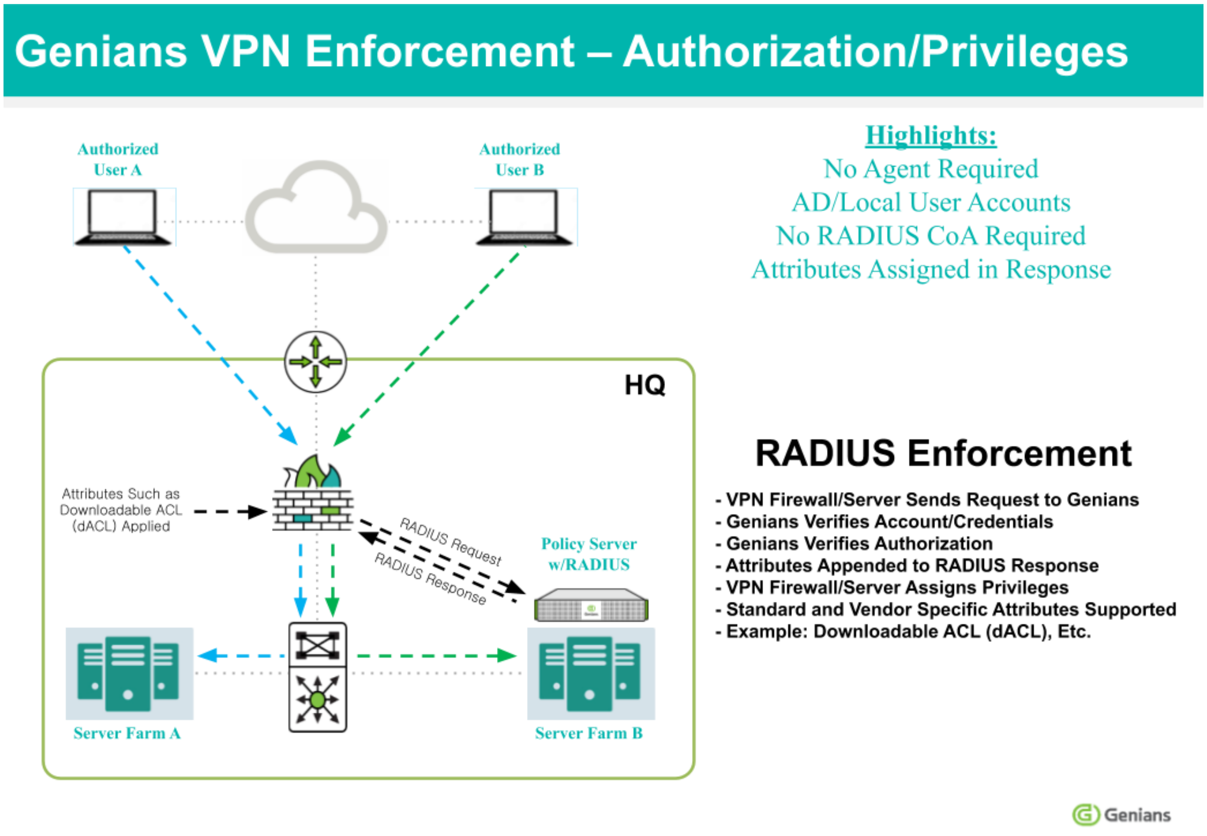
Node Information IP=172.0.0.20, MAC=00:50:56:0B:03:8A, Hostname=DESKTOP-VT5P2QT

Your device has been quarantined by Genians NAC via Infoblox Malware Notification Contact your Helpdesk for Malware Remediation Instructions Company ABC, 1-800-HELP-DESK

**Note:** Pages using HTTP Strict Transport Security (HSTS) will not allow a Captive Portal to be displayed. Navigate to another site if you see an HSTS error.

### 11.10.4 Integrating Cisco ASA - Applying Dynamic ACLs

If users are accessing your network using Cisco ASA (or a comparable solution) as a VPN gateway, you can use the Genians RADIUS Server to apply a dACL to perform role based access control to various network resources.



Genians VPN Enforcement – Authorization/Privileges

Highlights:
No Agent Required
AD/Local User Accounts
No RADIUS CoA Required
Attributes Assigned in Response

RADIUS Enforcement

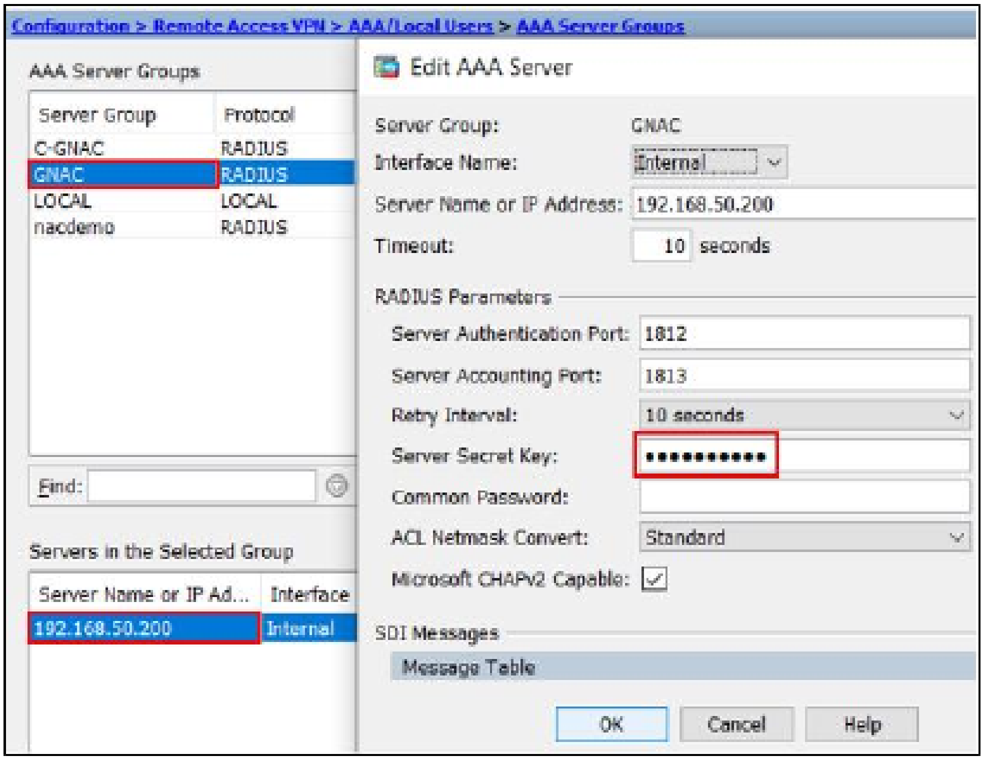
- VPN Firewall/Server Sends Request to Genians
- Genians Verifies Account/Credentials
- Genians Verifies Authorization
- Attributes Appended to RADIUS Response
- VPN Firewall/Server Assigns Privileges
- Standard and Vendor Specific Attributes Supported
- Example: Downloadable ACL (dACL), Etc.

#### Integrating the Radius Server

First, ensure that the RADIUS Server is properly configured, and that your settings are compatible with your VPN environment.

See: *Configuring RADIUS Enforcement*

Next, configure Genian ZTNA as an Authentication Server in your VPN settings, by entering the **Shared Secret**, **Server Address**, **Authentication Port**, **Accounting Port**, and other info, as shown in the example below:



Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

AAA Server Groups

| Server Group | Protocol |
|---|---|
| C-GNAC | RADIUS |
| GNAC | RADIUS |
| LOCAL | LOCAL |
| nacdemo | RADIUS |

Find:

Servers in the Selected Group

| Server Name or IP Ad... | Interface |
|---|---|
| 192.168.50.200 | Internal |

Edit AAA Server

Server Group: GNAC
Interface Name: Internal
Server Name or IP Address: 192.168.50.200
Timeout: 10 seconds

RADIUS Parameters
Server Authentication Port: 1812
Server Accounting Port: 1813
Retry Interval: 10 seconds
Server Secret Key: •••••••••••
Common Password:
ACL Netmask Convert: Standard
Microsoft CHAPv2 Capable: ☑

SDI Messages

### Configuring dACL

This can be accomplished by configuring an **RADIUS Policy**, and setting the **Access Policy** to **ACCEPT**, then setting **Cisco InBound ACL** for **Additional Attributes**.

In this example, we will use the **User-Name** attribute, and the Genians **User Group** feature to limit group members network access to a single server.

1. Go to **Policy** in the top panel.
2. Go to **Policy > RADIUS Policy** in the left panel.
3. Click **Tasks > Create**
4. For **General**, input **Name**, **Priority**, and activation **Status**.
5. For **Conditions**, select **Attribute**. For this example, select **User-Name**.
6. Set **Operator** and **Value** to **user is one of the User Group** and **[Your User Group]**
7. Click **Add** button.
8. For **Policy**, choose to **ACCEPT** Authentication Requests that match the attribute conditions, and select **Cisco InBound ACL** for **Additional Attributes**
9. For **Value**, enter a Cisco ACL, example:

```
Permit ip any host 192.168.55.200
deny ip any any
```

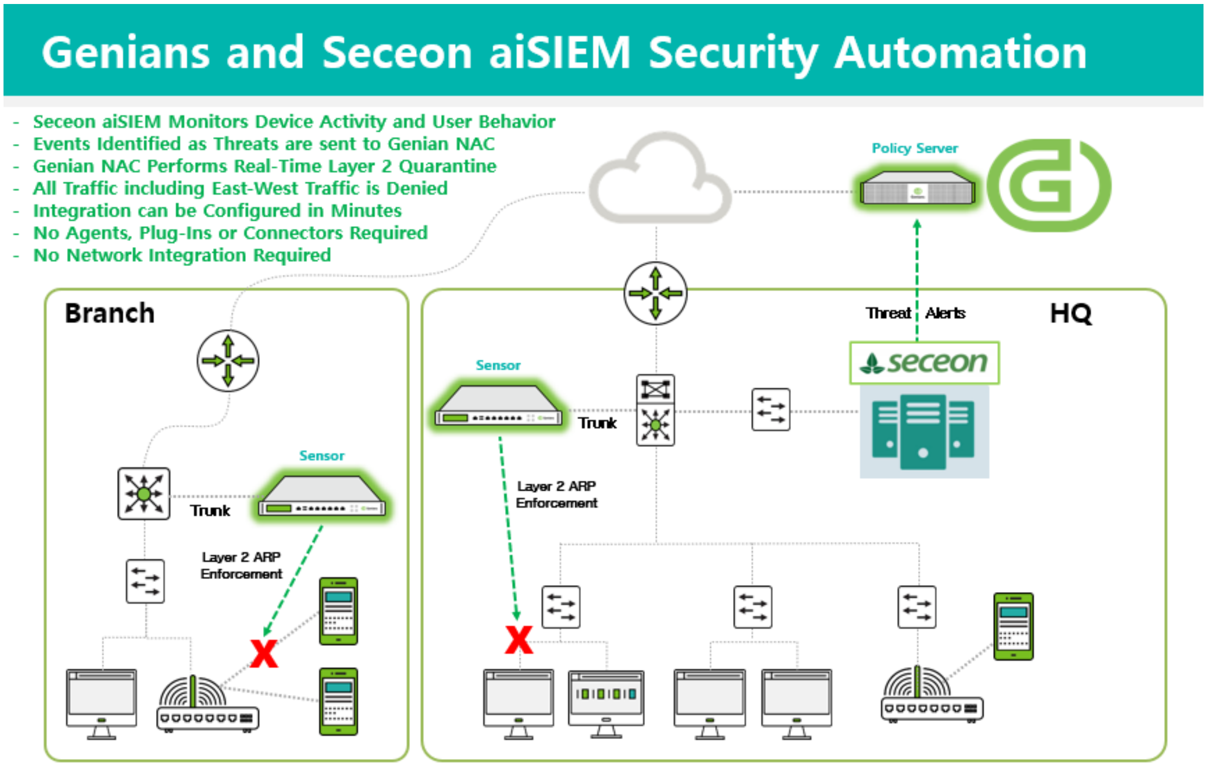
10. Click **Add** button.
11. Click **Create** button.

When an Authentication request is accepted from a member of the selected group, the access control list will be applied, thus limiting access to network resources.

For more info on on authorization through RADIUS Attributes, see: *Configuring Authorization*

### 11.10.5 Integrating Seceon aiSIEM

This document describes how to integrate Seceon aiSIEM with Genian ZTNA using syslog. This integration provides the ability to extend Seceon aiSIEM threat detection capabilities into the Enforcement capabilities of Genians ZTNA. A full video Webinar covering this integration along with a demo is available on the Genians website under **Resources > Videos.**


Genians and Seceon aiSIEM Security Automation
- Seceon aiSIEM Monitors Device Activity and User Behavior
- Events Identified as Threats are sent to Genian NAC
- Genian NAC Performs Real-Time Layer 2 Quarantine
- All Traffic including East-West Traffic is Denied
- Integration can be Configured in Minutes
- No Agents, Plug-Ins or Connectors Required
- No Network Integration Required
Policy Server
Branch
HQ
Threat Alerts
seceon
Sensor
Trunk
Layer 2 ARP Enforcement
Sensor
Trunk
Layer 2 ARP Enforcement

The main steps of this integration are as follows:

1. Configure a Remediator in the Seceon APE
2. Configure Genian ZTNA to interpret this syslog event sent by the APE Remediator and apply enforcement to the impacted node.

#### APE Remediator Configuration

Login to the Seceon APE UI:

1. Under **Administration > Remediator > Add**, select Genians ZTNA as the Device, Firewall as the Device Type and enter the IP of your Genian ZTNA Policy Server.
2. The User Name, Password and Confirm Password fields are mandatory but not required for the integration to function so can be populated with any data.

### Genian ZTNA Syslog Configuration

A Server Rule set must be added before receiving syslogs. We will configure a server rule based on the format of the Seceon aiSIEM message to extract information about the device to be blocked. In this integration, we will use the IP address to identify the device to be blocked.

1. Navigate to **General > Log** in the **Preferences** section.
2. Click the **Add** button to the right of the **Server Rules** label, and fill out the pop-up form.
3. Enter a name for the Rule.
4. For **Filter**,select a variable by which to evaluate incoming syslogs for allowance. Choose from **Program** , **Host**, **Match**, or **Netmask.** This option allows for syslogs from a given source location/ program, or a given message content to be allowed. In this case, select **Host**.
5. Define a **Filter Value.** If the **Filter** variable of the imported syslog matches the **Filter Value** , the syslog will be merged into the policy server logs. In this case, enter the **Seceon CCE IP**.
6. Define `src_ip:` as a prefix for IP values.
7. Define the character set which the syslogs will be imported in.
8. Click **Add** at the bottom of the pop-up window.
9. Click **Update** at the bottom of the Log Preferences page.

Now the message from the Infoblox system will be correlated with the nodes detected by Genian ZTNA.

### Genian ZTNA Tag and Policy Configuration

Under **Preferences > Properties > Tag**:

1. Create a tag called “Seceon-Threat-Detected” then click Save. This tag will be linked to a log filter and eventually to an Enforcement Policy in future steps.
2. Click on **Log and then Add filters.** Syslog alerts from Seceon aiSIEM include the key words “THREAT so performing”. Type these words into the Description field of the log filter and click Search. You can further narrow the search by using the IP of your Seceon system.
3. Give the log filter a name, description and add the previously created “Seceon-Threat-Detected” tag then click Save. In this example, we will apply the tag to the node (MAC+IP), though log filters can also apply tags to MACs, Users, or WLANs. Be sure to select **Node** in the **From** and **To** sections.

Under **Policy > Group**:

1. Click **Tasks > Create** to create a new Node Group.
2. Under General enter an ID and Description and set the Status to Enabled.
3. Under Condition, click Add to add the previously created “Seceon-Threat-Detected” tag.
4. Click **Save**.

Under **Policy > Enforcement Policy**:

1. Click **Tasks > Create** to create a new Enforcement Policy.
2. Follow the wizard and select the previously created “Seceon-Threat-Detected” Node Group.
3. Select the desired Permissions, enable Captive Portal and enter a message to be displayed to the end user.
4. Click **Save**.

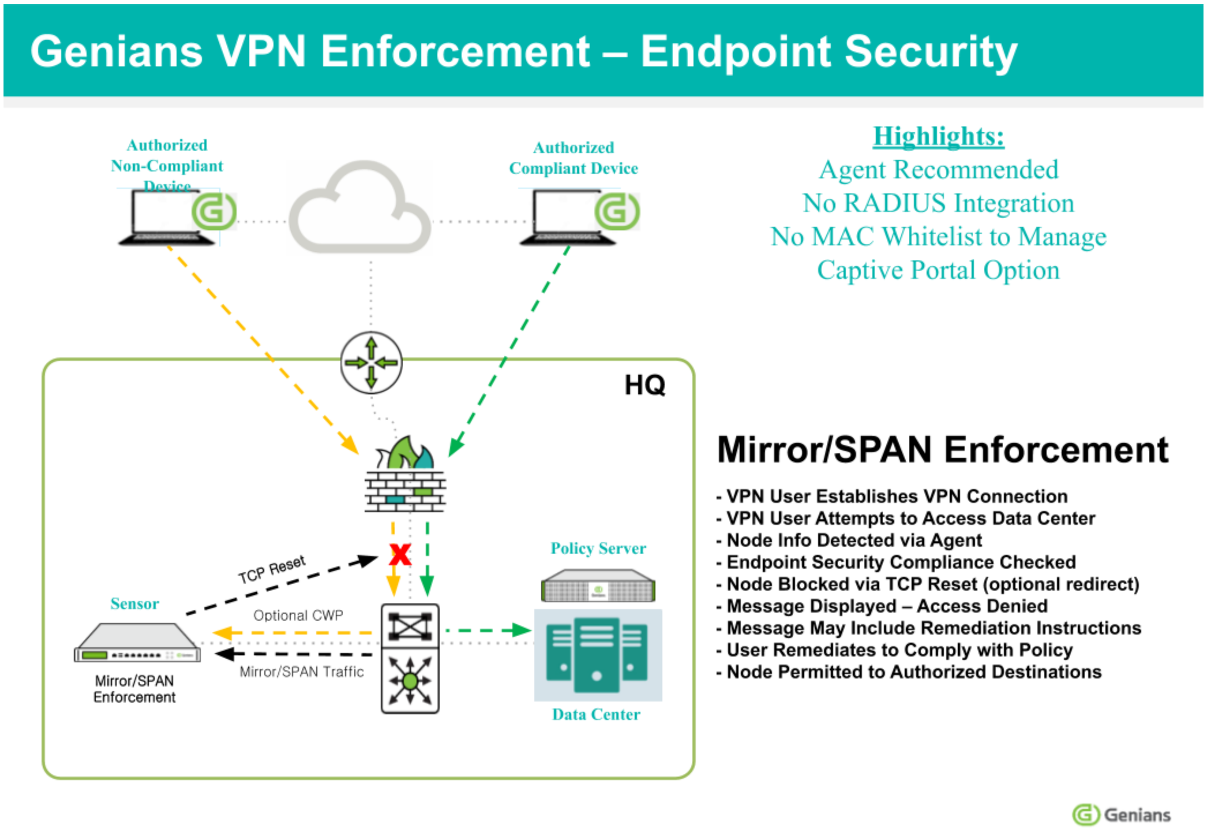
With all configurations now in place, the Genians Network Sensor must be switched from Monitoring to Enforcement mode to facilitate the Layer 2 quarantine of non-compliant nodes on the network. Navigate to **System > Sensor > Edit Sensor Settings** and set the Sensor Operating Mode to Enforcement then click Update at the bottom of the page.

### Testing and Validation

1. Select a test machine within a network that is managed by a sensor from your Seceon Integrated Genian ZTNA system.
2. Browse to a Seceon designated malware site with a test machine.
3. In roughly 1-3 minutes (time required for Seceon threat processing), Seceon will send a syslog alert to Genian ZTNA.
4. The test node should have Tag assigned once alert is received from Seceon.
5. The node will then be Layer 2 quarantined in real-time by Genian ZTNA. Pings will fail and if any new websites are accessed, a captive portal will be display indicating the device has been quarantined due to a Seceon detected threat.

## 11.11 Blocking Unauthorized or Non-Compliant VPN Devices

In some situations, correct user credentials may be supplied to log into a VPN, but the device itself is not approved for use on the network. This may be the result of stolen credentials,being used to access the network, or an authorized user signing into the network with an unapproved or non-compliant device. Genian ZTNA can block these unapproved devices at Layer 3 using a Network Sensor deployed in Mirror Mode.



Genians VPN Enforcement – Endpoint Security

**Highlights:**

Agent Recommended
No RADIUS Integration
No MAC Whitelist to Manage
Captive Portal Option

Mirror/SPAN Enforcement

- VPN User Establishes VPN Connection
- VPN User Attempts to Access Data Center
- Node Info Detected via Agent
- Endpoint Security Compliance Checked
- Node Blocked via TCP Reset (optional redirect)
- Message Displayed – Access Denied
- Message May Include Remediation Instructions
- User Remediates to Comply with Policy
- Node Permitted to Authorized Destinations

### 11.11.1 Cofigure Sensor

To configure a Sensor in Mirror Mode, see: *Configuring Mirror Mode*

### 11.11.2 Cofigure Groups and Enforcement Policies

Enforcing against VPN users with a mirror sensor uses the same configurations that are used for ARP Enforcement in a LAN environment.

Simply create Groups and Enforcement Policies to defined which nodes, devices, or users can access which network resources and at which times. It is also possible to redirect the non-compliant node to a captive portal, where they can be served with a message from the administer, or required to download an agent. You can create separate Groups and Policies for VPN users

The Mirror Sensor will use TCP Reset or ICMP unreachable replies to block any attempted access to prohibited resources. the VPN connection itself will remain unaltered.

To Create Groups and Enforcement Policies to allow or disallow access, see:

- *Managing Node Groups*
- *Creating and Viewing Enforcement Policy for Nodes*

**Note:** Traffic detected by a Mirror Sensor does not result in the creation of a node in the Web Console. Therefore traffic may be blocked without any logging occurring. Nodes with an Agent installed will be shown in the Web Console, and logging will occur when their policy status changes. Use of the Agent and is recommended for gathering endpoint information.

For more content relating to VPN users, see:

- *Authenticating VPN Users*
- *Integrating Cisco ASA - Applying Dynamic ACLs*

## 11.12 Controlling Access to Cloud Resources

The Genian ZTNA Gateway can be deployed in the Cloud to control access to Cloud Resources. Combined with the ZTNA Client feature embedded within the Genian ZTNA Agent, a secure connection is established between a remote endpoint and the ZTNA Cloud Gateway. After a user is successfully authenticated, only the access defined by the administrator will be available. Any other connection attempts will be discarded by the ZTNA Cloud Gateway.

### 11.12.1 Deploying the ZTNA Gateway in the AWS Cloud

**Note:** Presently the Genian ZTNA Gateway can only be deployed into AWS Cloud environments from the Genian ZTNA UI. To deploy a ZTNA Gateway in an environment other than AWS, See: Installing ZTNA Gateway

**Note:** Prior to following the steps below, be sure you have already added a Cloud Provider and Cloud Site. See: *Managing Nodes in the Cloud*

### 11.12.2 Enable ZTNA Client in Cloud Site

1. From the top menu, navigate to System > Site
2. Click on the desired Site Name
3. Under ZTNA Client, set Status to 'Enabled'
4. Leave the Network field blank for auto-assignment of an IP pool for remote endpoints connecting to the Cloud Gateway
5. Click Save

### 11.12.3 Add the ZTNA Connection Manager Agent Action to Node Policy

1. Select the applicable Node Policy (the Default Node Policy may be used unless you want to create a specific Node Policy)
2. From the top menu, navigate to Policy > Node Policy and click on the desired Node Policy
3. Under Authentication Policy, change Authentication Method from Password Authentication to Host Authentication
4. Scroll down to the Agent Action section and Click Assign
5. Select the 'ZTNA Connection Manager' by moving it from the Available window to the Selected window then click Update
6. Click on the name of the Node Policy
7. Scroll down and click on the ZTNA Connection Manager Agent Action
8. Under the Plugin section, click Assign to the right of the Site window
9. Select the desired site users will be connecting remotely to through the Cloud Sensor using the ZTNA Client
10. Click Update then click the blinking Apply in the upper right-hand corner

### 11.12.4 Deploy Cloud Sensor

1. From the top menu, navigate to System > Site
2. Check the box next to yoursite.genians.net
3. Click Tasks then select Add Cloud Sensor
4. Select the desired site where you will be deploying the Cloud Sensor
5. Select an Amazon Machine Image (AMI) (a recommended AMI will be displayed)
6. Select the desired EC2 Instance Type (t2.medium is recommended)
7. Select the desired Subnet ID for the subnet the Cloud Sensor will be deployed in
8. Select the desired keypair for remote CLI access to the Cloud Sensor EC2

**Note:** Typically, CLI access to the Cloud Sensor is not required, however, the key pair is mandatory for the AWS EC2 creation process. Any valid key pair created for the specified region may be used. Refer to AWS documentation for more information on how to create a keypair for remote EC2 access.

1. Click Check Init

2. A Terraform initialization test will be performed to confirm all the information selected will succeed in EC2 creation
3. If any errors are displayed during the Check Init process, address the issues in your AWS environment before proceeding

**Note:** At least one Elastic IP must be available in the region you deploy a Cloud Sensor to.

1. Click Create
2. When the Apply Complete message is displayed, this means the Cloud Sensor was successfully deployed
3. Click Close to close the window
4. The Cloud Sensor will now be displayed in the System list

**Note:** It may take up to 15 minutes for the Cloud Sensor to fully initialize and communicate with your Cloud Policy Server. To verify the status of the Cloud Sensor EC2, login to the AWS EC2 Console.

### 11.12.5 Set Cloud Sensor to Cloud Gateway Mode

1. From the top menu, navigate to System
2. Click on the Cloud Sensor IP
3. Click on the Sensor tab
4. For the eth0 interface, in the far-right Settings column, click on Sensor
5. Under Sensor Operation, change Sensor Mode from Host to Inline and change Mirror Operating Scope from Local to Global
6. Scroll down and click Update

### 11.12.6 Install Genian ZTNA Client and Verify Cloud Access

1. Create a test account for remote access under Management > User > Tasks > Add User
2. Browse to https://yoursite.genians.net/agent
3. Click the Download button and follow the prompts to install the Agent
4. Once installed, right click on the Agent icon, select Network Access and click Connect
5. Enter the username and password created in the step above
6. The ZTNA Client should pop up a message indicating you are now connected and provide your IP for the connection
7. All traffic from the endpoint will now be routed through the Cloud Gateway
8. The remote session information can be viewed under System > Site > ZTNA Client

# 11.13 Controlling Access to Customer Cloud or On-Prem Resources through a ZTNA Gateway

When a ZTNA Sensor is configured as ZTNA Gateway, it can be deployed in a Customer Cloud or On-Prem to control remote access to Cloud or On-Prem Resources. Combined with the ZTNA Client feature embedded within the Genian ZTNA Agent, a secure connection is established between a remote endpoint and the ZTNA Gateway. After a user is successfully authenticated, only the access defined by the administrator will be available. Any other connection attempts will be discarded by the ZTNA Gateway.

## 11.13.1 Deploying the ZTNA Sensor in a Customer Cloud or On-Premises

Skip this step if you have already installed a ZTNA Sensor in your Cloud or On-Prem. For instructions on how to install a ZTNA Sensor in a Customer Cloud or On-Prem:

See: /install/installing-genian-nac.

## 11.13.2 Create On-Prem Site

**Note:** On-Prem Infrastructure type is used for any non-AWS Cloud environment

1. From the top menu, navigate to System > Site
2. Click Tasks then Create
3. Enter a Name for the site (ex. 'Corp Hub')
4. For Infrastructure select On-Prem
5. For Type select Hub or Branch (typically Hub if this is the first Gateway you have deployed)
6. For Network Address enter the network address for the On-Prem or Cloud network (ex. 10.0.0.0/16 or 172.31.16.0/20)
7. Click Save

## 11.13.3 Enable ZTNA Client in On-Prem Site

1. From the top menu, navigate to System > Site
2. Click on the desired Site Name
3. Under ZTNA Client, set Status to 'Enabled'
4. Leave the Network field blank for auto-assignment of an IP pool for remote endpoints connecting to the ZTNA Gateway
5. Click Save

### 11.13.4 Add the ZTNA Connection Manager Agent Action to Node Policy

1. Select the applicable Node Policy (the Default Node Policy may be used unless you want to create a specific Node Policy)
2. From the top menu, navigate to Policy > Node Policy and click on the desired Node Policy
3. Under Authentication Policy, change Authentication Method from Password Authentication to Host Authentication
4. Scroll down to the Agent Action section and Click Assign
5. Select the 'ZTNA Connection Manager' by moving it from the Available window to the Selected window then click Update
6. Click on the name of the Node Policy
7. Scroll down and click on the ZTNA Connection Manager Agent Action
8. Under the Plugin section, click Assign to the right of the Site window
9. Select the desired site users will be connecting remotely to through the ZTNA Gateway using the ZTNA Client
10. Click Update then click the blinking Apply in the upper right-hand corner

### 11.13.5 Set ZTNA Sensor to Gateway (In-Line) Mode

1. From the top menu, navigate to System
2. Click on the Sensor IP
3. Click on the Sensor tab
4. For the eth0 interface, in the far-right Settings column, click on Sensor
5. Under Sensor Operation, change Sensor Mode from Host to Inline and change Mirror Operating Scope from Local to Global
6. Scroll down and click Update

### 11.13.6 Install Genian ZTNA Client and Verify Access

**Note:** The ZTNA Client will connect to the ZTNA Gateway over ports TCP 443,1194, and UDP 3870,3871 so these ports must be opened from the public IP of the end user's device to the public IP of the ZTNA Gateway. Be sure to update firewall rules and security groups accordingly.

1. Create a test account for remote access under Management > User > Tasks > Add User
2. Browse to https://yoursite.genians.net/agent
3. Click the Download button and follow the prompts to install the Agent
4. Once installed, right click on the Agent icon, select Network Access and click Connect
5. Enter the username and password created in the step above
6. The ZTNA Client should pop up a message indicating you are now connected and provide your IP for the connection
7. All traffic from the endpoint will now be routed through the ZTNA Gateway
8. The remote session information can be viewed under System > Site > ZTNA Client

CHAPTER

TWELVE

# MANAGING ON-BOARDING PROCESS

**Note:** This feature requires Professional or Enterprise Edition

You can customize the Captive Web Portal, and Guest Management in this On-boarding process section.

## 12.1 Configuring Captive Web Portal

A **Captive Web Portal** (**CWP**) is a 'landing' web page, often used for info or authentication. The portal intercepts observed packets until the user is authorized to launch browser sessions. The user is granted conditional Internet or Network access once Authentication, EULA Agreement, Payment, or other valid credentials have been completed.

### 12.1.1 Enable The Captive Web Portal

1. Go to **Policy** in the top panel
2. Go to **Enforcement Policy** in the left Policy panel
3. Select the desired **Enforcement Policy**
4. Under **General > Status** select **Enabled**
5. Under **Enforcement Options > Captive Web Portal** tab
6. Select **Default CWP Page** under **Redirecting to** section
7. Click **Update**
8. Click **Apply**

### 12.1.2 Configuring Proxy Server Exceptions

Captive portals may not be able to provide proper redirection if internal hosts on the network are configured to use a proxy server. By making the proper proxy exceptions on your proxy server, this will ensure captive portal redirection functions properly.

In the examples below, replace `x.x.x.x` with the IP of the Genian ZTNA Policy Server, and add to your existing proxy server configuration.

### .pac example

```
function FindProxyForURL(url, host) { if (isInNet(host, "x.x.x.x",
"255.255.255.255")) return "DIRECT"; else return
"PROXY proxy.company.com:8080"; }
```

### .dat example

```
function FindProxyForURL(url, host)
{
if (isPlainHostName(host) ||
isInNet(host, "x.x.x.x", "255.255.255.255"))
return "DIRECT";
else
return "PROXY proxy.company.com:8080";
};
```

## 12.1.3 Customizing Messages

Default messages can feel bland or uninformative. While they get straight to the point, a default message might not provide enough information as to why a user is blocked from the network. Other times, there may be scheduled maintenance that will cause downtime on the network, an important update that needs to be downloaded, or a new policy in place that people need to be informed about. Thus, a Custom Web Portal Message is the perfect solution.

### Add a Custom Web Portal Message

1. Go to **Policy** in the top panel
2. Go to **Policy > Enforcement Policy** in the left Policy panel
3. Click desired **Enforcement Policy** name
4. Find **Enforcement Options > Captive Web Portal** section
5. Select desired **Redirecting to** option
6. Enter **User Message** to be displayed on **CWP** (*This message is displayed when access is denied*)
7. Click **Update**

## 12.1.4 Managing Notice

Notices are bulletin style messages used for making employees or customers aware of important updates, events, or factors regarding the network. Notices are usually longer statements describing one or more topics, whereas messages are used for short, direct statements about why a user is blocked or what needs to be done to gain access to the network.

### Create a Notice

1. Go to **Preferences** in the top panel
2. Go to **Captive Web Portal > Notice** in the left Preferences panel
3. Click **Tasks > Create**
4. If a **Posting Period** is required, click on **Checkbox** and select a **date** and **time**
5. Enter **Subject**
6. Create **Content**
7. Select the **Type** (*HTML, Text, or Markdown*)
8. Click **Save**

### Delete a Notice

1. Go to **Preferences** in the top panel
2. Go to **Captive Web Portal > Notice** in the left Preferences panel
3. Click **Checkbox** of **Notice** to be deleted
4. Click **Tasks > Delete**
5. Click **Ok**

## 12.1.5 Managing Custom Buttons

You can create **Custom Buttons** that get inserted onto the **Captive Web Portal** page to redirect users to other web pages.

| Button type | Description |
|---|---|
| Hyperlink | The current tab will be redirected to a specific URL. |
| Pop-up window | Open a specific URL in a new window |
| Agent Try Menu | Open a specific URL in a new window once you click the Agent tray menu. |
| Webpage | Go to the information collection page. |
| Download | Download the uploaded file. |

### Create a Button

1. Go to **Preferences** in the top panel
2. Go to **Captive Web Portal > Custom Button** in the left Preferences panel
3. Click **Tasks > Create**
4. Add a **Name** and **Description** for the button
5. **Upload** a custom **Image** to use with the button (*Optional*)
6. Add a **Hyperlink** for the button
7. Click **Save**

### Delete a Button

1. Go to **Preferences** in the top panel
2. Go to **Captive Web Portal > Custom Button** in the left Preferences panel
3. Click **Checkbox** for **Button name** in Custom Button window
4. Click **Tasks > Delete**
5. Click **Ok**

### Reorder Buttons

1. Go to **Preferences** in the top panel
2. Go to **Captive Web Portal > Custom Button** in the left Preferences panel
3. Click **Tasks > Reorder**
4. Click to **highlight Buttons** to be reordered in Reorder window
5. Click **Save**

## 12.1.6 Creating Custom Pages

You can also create custom Captive Web Portal layouts for use in different situations.

### Customizing Captive Web Portal Design

Customizing the **Captive Web Portal** page allows you to edit the current Default page, create something completely new, or add logos from current companies web page. This gives you the ability to display the same look and feel as your current internal web pages for your end users. Under **Preferences > Captive Web Portal > Design Template** Four tabs will be displayed to allow you to customize your CWP page

- **Component Options**: Allows you to edit the page using the component.
- **Edit**: Allows you to customize your own CWP page.
- **CSS Style**: Allows you to add CSS Style.
- **Layout**: Allows you to edit page layout.
- **Image**: Alows you to upload custom images to make the CWP look and feel like your own.

### Component Options

1. Click the add or delete button for the required component
2. Page preview on Main page in the right side of the Web-console
3. Click **Update**

### Edit

1. CWP page display in html code form
2. Provide pages in html code format

- Modify the page by adding or removing the tag of the component to the code
- Can be modified using html code

3. Click **Update**
4. A Page preview will display on the Main page in the right side of the Web console.

### CSS Style

You can define CSS Style class and use it in EDIT Tab or Layout Tab.

1. Input the CSS style code in "CSS Style" tab.

```
.test {color:red;}
```

2. To use defined CSS style in "Edit" tab

```
<div class="test">
TEST
</div>
```

3. Click **Update**
4. A Page preview will display on the Main page in the right side of the Web console.

### Layout

You can modify the layout of the page using Html code.

```
<?xml version='1.0' encoding='UTF-8' ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/
↪xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"
   xmlns:ui="http://xmlns.jcp.org/jsf/facelets"ß
   xmlns:h="http://xmlns.jcp.org/jsf/html"
   xmlns:p="http://primefaces.org/ui"
   xmlns:gncomponent="http://xmlns.jcp.org/jsf/composite/gncomponent">
$HEAD
<body id="body1">
 $PAGEHEADER
 <div id="wrap" class="wrap">
     $CUSTOMPAGEHEADER
     <div id="content" class="content">
         <!-- Don't delete code -->
         $CONTENT
         <!-- Don't delete code -->
     </div>
     $CUSTOMPAGEFOOTER
 </div>
```

(continues on next page)

(continued from previous page)

```
</body>
</html>
```

### Image

Upload custom images to make CWP look and feel like your own.

**Note:** Only jpg/gif/png files with alphabetic character file names are supported.

### Apply the defined CWP template

1. Go to **Policy** in the top panel/li>
2. Go to **Node Policy** in the left Policy panel
3. Find and click **name of Node Policy**
4. Find **CWP Design Template** in the main **Management Policy**
5. Select a Design Template for a CWP page
6. Click **Update** and **apply** on the right top panel.

# 12.2 Configuring Security Policy Consent Page on Captive Web Portal

Genian ZTNA can notify users of internal network security policy terms and display a consent request page on the Captive Web portal. Devices/nodes status is updated based on if they have consented to the terms outlined in the captive portal. This can be used to group nodes/devices and apply ploicies to control devices.(Ex: Block network access until user consents to terms of usage)

## 12.2.1 Create Security Policy page

Administrator can custom Security Policy Consent pages.

Genian ZTNA Security policy pages have content fields and information collection fields. Administrator can display terms and conditions in Contents field and collect consenter information by Assigning User Input Fields.

1. Go to **Preferences** in the top panel
2. Go to **Captive Web Portal > Consent Page > Security Policy** in the left Policy panel
3. Find **Tasks** and click **Create**
4. Fill **Contents** and Assign **User Input Field**
5. Click `save`

### 12.2.2 Enable Security Policy Page on Captive Web Portal

Genian ZTNA displays the Security Policy Page to users by using the Captive Web Portal
To enable the security policy page, administrators need to create an *Enforcement Policy*

Typically,fist time users should be asked to consent to a security policy

This is most easily accomplished with an Enforcement Policy configured to redirect the user to the Security Policy page. When configuring a Node Group to use for this Enforcement Policy, the `Consent` criteria can be used as a condition so that devices that have not completed the consent process fall under the Enforcement Policy, and be redirected to the Security Policy page.

1. Go to **policy** in the top panel
2. Go to **Enforcement Policy** in the left Policy panel
3. Click **ID**
4. Go to **Enforcement Options > Captive Web Portal > Redirecting to** and Choose **Secirity Policy Page**
5. Configure **URL, Security Policy Result Message, User Message** and click `update`
6. Click `Apply` in top right corner

## 12.3 Configuring Guest Management

Genian ZTNA can create temporary Guest Accounts for authorized visitors and manage them. Administrators can Specify whether to disable or delete an expired Guest Account. Guest Accounts may be created by the Administrator or requested by the user.

This guide will help you to add or delete a Guest Account as an Administrator.

### 12.3.1 Add Guest Account as an Administrator

An Administrator can create new Guest Accounts and set the ID and Password for guest.

1. Go to **Management > User** in the top panel
2. Click **Tasks > Add User**
3. Go to **General > Purpose** and choose **Guest Account**
4. Click `Save`

### 12.3.2 How to Configure Expired Guest Account Options

An Administrator can Specify whether to disable or delete an expired User Account.

1. Go to **Preferences** in the top panel
2. Go to **Properties > Purpose > User** in the left Policy panel
3. Click a **GUEST** in the list
4. Go to **Options > Approval Options > Expired Account Options**

5. Choose **Disable Account** or **Delete Account**
6. Click `Update`

### 12.3.3 Remove Guest Account

1. Go to **Management > User** in the top panel
2. Find **User** and click **Checkbox**
3. Click **Tasks > Remove User**
4. Click **Ok**

### 12.3.4 Enable Approval for Guest request

#### Enable Approval for Guest request

Genian ZTNA can identify and manage visitors by creating Guest Accounts. Guest Accounts may be created by the Administrator or requested by the user.

This guide will help you to understand the process of Guest Account requests and approvals.

**Note:** User cannot login with the new account until Administrator or Sponsor approve the request.

#### How to submit Guest Account requests

Guest Users can submit a Guest Account request on the CWP (Captive Web Portal) page using the **Request User Account** feature.

#### Enable Request User Account Button On CWP

In order for Guest user to submit Guest Account requests on CWPpage, an Administrator must activate Request User Account Button.

**Note:** Make sure the Network Sensor is in enforcement mode and an Enforcement Policy is enabled to redirect unauthenticated users to the CWP.

1. Go to **Policy** in the top panel
2. Go to **Policy > Node Policy** in the left Policy panel
3. Find and click **Node Policy**
4. Find **Advanced > Authentication Policy > User Account Request** and choose **On** to configure features
5. Click **Update**

### CWP Address

```
http://(IP of Policy Server)/cwp
```

### How to approve Guest Account requests

Guest users can login with the new account after their request is approved. There are three ways for approving Guest Account request: Administrator Approval, Email Approval and Instant Approval.

### Case 1 : Administrator Approval

Administrator can approve Guest Accounts on through Web Console.

Administrator can still approve new requests on Request Management page, even if Administrator configured Email Approval.

**How to configure Administrator Approval**

1. Go to **Preferences** in the top panel
2. Go to **Properties > Purpose > User** in the left Policy panel
3. Click a **GUEST** in the list
4. Go to **Options > Approval Options > Email Approval for Guest** and choose **Off** to configure features
5. Go to **Instant Approval** and Choose **Off**
6. Click `Update`

**How to Accept / Reject Guest Requests as an Administrator**

1. Go to **Management > Request** in the top panel
2. Go to **User Account Request > Request** in the left Request Management panel
3. Find **Requests** in the list. Click **Checkbox** of desired request(s)
4. Click **Tasks > Accept All** or **Reject All**

### Case 2 : Email Approval

Administrators and Sponsors can approve Guest Accounts via email. If the Guest Account request is submitted, an Administrator or Sponsor will receive a clickable approval mail. You can configure email approvers as Administrator, Sponsors or Both.

**How to configure Administrator Approval**

1. Go to **Preferences** in the top panel
2. Go to **Properties > Purpose > User** in the left Policy panel
3. Click a **GUEST** in the list
4. Go to **Options > Approval Options > Email Approval for Guest** and choose **On** to configure features

5. For **Email Approver** and Choose **Administrator**, **Existing User(Sponsor)** or **Both**
6. Click **Update**

**How to Sponsor approve Guest Account request by email**

1. Open **'User Account Request'** E-mail in Sponsor's Inbox
2. Click `Approve` button on E-mail

**Warning:** If 'Failed to send Email' error occurs, please double check the Outbound Email Server configuration or Approver's Email address.

**Note:** In an environment where there is no network access to the Policy Server, Even if admins click the approve button in the mail, the approval is not processed.

### Case 3 : Instant Approval

When a Guest User submits the Request, the Request will be instantly approved.

**How to configure Administrator Approval**

1. Go to **Preferences** in the top panel
2. Go to **Properties > Purpose > User** in the left preferences panel
3. Click a **GUEST** in the list
4. Go to **Options > Approval Options > Email Approval for Guest** and choose **Off** to configure features
5. Go to **Instant Approval** and Choose **On**
6. Click `Update`

## How to view approval results

Guest Users can receive approval notification by CWP page View Results option and Email.

### Case 1 : View Approval results on CWP

**Enable Request View Results button On CWP**

1. Go to **Preferences** in the top panel
2. Go to **Captive Web Portal> Design Template** in the left preferences panel
3. Choose a Template name
4. Activate **[View Results] Button**
5. Click `Update`

#### Case 2 : Receiving Approval notification by Email

**How guest receive approval notification**

1. Go to **Preferences** in the top panel
2. Go to **Properties** > **Purpose** > **User** in the left Policy panel
3. Click a **GUEST** in the list
4. Go to **Request Field Options** and move **Email** to right
5. Click **Update**

**Note:** If the Guest Account request is approved by Administrator or Sponsor, the Email address in the request form will be notified.

#### Case 3: How to Check Approval results as an Administrator

Administrator can check Approval results in the Web Console.

1. Go to **Management>Request** in the top panel
2. Go to **User Account Request** > **Results** in the left Request Management panel
3. Check a results of approval

## 12.4 Redirecting to Custom URL

This is how to configure redirection to a specific page when the device's network access is blocked. Admins can specify a custom URL instead CWP, or configure users to be redirected to a custom URL when they click the OK button on the CWP.

### 12.4.1 Redirect to specific URL instead of CWP

when the device's network access is blocked, admins can configure redirection to specific url instead of the cwp. However, the new URL should provide instructions on how to remediate the reason for being blocked.

1. Go to **Policy** in the top panel.
2. Go to **Enforcement Policy** in the left panel.
3. Find and click the policy to change in the list.
4. Go to **Enforcement Options** > **Captive Web Portal** > **Redirecting to**
5. Change **Redirecting to** option to **Custom URL**
6. Type **URL** and **User Message**
7. Click **Update** button.

### 12.4.2 Redirect to a specific URL when a user clicks the OK button on the CWP

When the user clicks the OK button on the CWP. It will be redirected to specific url such as Google, Wikipedia or in-house website.

1. Go to **Policy** in the top panel.
2. Go to **Design Template** in the left panel.
3. Find and click the template to change in the list.
4. Find and click **OK** button in **Components**
5. Upload image file and type URL
6. Click **Update** button.
7. Click **Update** button one more time

## 12.5 Configuring AP Profile for Wlan Policy

AP Profile is for use with the Genians W10 Access point. For availability information, contact Genians or your regional Genians distribution partner. Configuring AP Profile can management entire/individual wireless networksensor's profile.

### 12.5.1 1. Creating AP Profile

AP Profile can select security Type from **Open, WEP, WPA2-Personal. WPA2-Enterprise**.

1. Go to **Policy** in the top panel
2. Go to **Policy > Wlan Policy > AP Profile** in the left Policy pannel
3. Select **Tasks > Create**
4. Enter the information of a trusted network
5. Click `Create`

### 12.5.2 2. Creating Wlan Policy for wireless network sensor

Wlan Policies are made up of AP Policy and Client Policy They can be used along with the endpoint agent to set preferences and restrictions for accessing wireless networks. Administrator can assign AP Profiles to AP Policy. It can Perform the action by without configuring Client Policy.

1. Go to **Policy** in the top panel
2. Go to **Policy > Wlan Policy** in the left Policy pannel
3. Select **Tasks > Create**
4. Select AP profiles to apply to the policy
5. Enter the information of a trusted network
6. Click `Save`

## 12.6 Configuring Client Profile for Wlan Policy

Administrator can use Wireless Connection Manager (WCM) to automatically register the Client Profile on window os user device. Administrator can automatically register and manage hidden wireless network and security setting without requiring the user to manual configure the settings. In order to distribute the client profile to the device, the administrator needs to create a Client Profile and configure the WLAN Policy. And after distributing client profile, WCM configuration is required to access the wireless LAN through the profile.

### 12.6.1 1. Creating Client Profile

Client Profile can select security Type from **Open, WEP, WPA2-Personal. WPA2-Enterprise, 802.1x**

1. Go to **Policy** in the top panel
2. Go to **Policy > Wlan Policy > Client Profile** in the left Policy pannel
3. Select **Tasks > Create**
4. Enter the information of a trusted network.
5. Click **Create**

### 12.6.2 2. Creating Wlan Policy for user device

Configure WLAN Policy to distribute Client Profile on user devices. Wlan Policies are made up of AP Policy and Client Policy. In order to distribute Client Profiles, the administrator only need to configure the Client Policy.

1. Go to **Policy** in the top panel
2. Go to **Policy > Wlan Policy** in the left Policy pannel
3. Select **Tasks > Create**
4. Select **Client profile** to apply to the policy.
5. Enter the information of a trusted network.
6. Click Save.

### 12.6.3 3. Configuring Wireless Connection Manager

For Configuring Wireless Connection Manager, please refer to *Configuring Wireless Connection Manager*

## 12.7 Managing Captive Web Portal Redirection Ports

Administrator changes HTTP/HTTPS(web service) to other port besides default port, Genian ZTNA CWPpage redirection feature became disable status. Administrator should add a new port for enable the CWP page Redirection feature.

### 12.7.1 How to configure HTTP/HTTPS port?

On Genian ZTNA, HTTP port is configured as 80,8080 by default and HTTPS port is configured by 443. Genian ZTNA use " **,** " mark for add a new port numbers.

1. Go to **Preferences** in the top panel
2. Go to **General > Node** in the left Preferences panel
3. Find **Redirection** and fill a **HTTP Port** , **HTTPS Port**
4. Click `update`

## 12.8 Troubleshooting

- *Blocked Nodes are not redirected to CWP page*

CHAPTER

THIRTEEN

# MANAGING USER AUTHENTICATION

**Note:** This feature requires Professional or Enterprise Edition

User Authentication means verifying the identity of someone (User) behind a device that wants to access the network. User Authentication also enables accountability, by using user ID and password which makes it possible to link access and actions to specific identities. Genians provides the ability to Authenticate Users in several ways.

You can create Users locally in Policy Server, or configure Policy Server to pull User Information from Active Directory, RADIUS, POP3, IMAP, SMTP, CSV, or other third-party user management systems.

**Locally** Users Authenticate against the local database created within the Genians Policy Server. Once credentials match, the user is then allowed to proceed onto the network.

**Externally** (*Active Directory, RADIUS, IMAP, POP3, SMTP, CSV*) Genians can integrate with External Authentication sources to permit user access upon successful login using proper credentials.

## 13.1 Enabling User Authentication

You can configure User Authentication using Captive Web Portal, Agent, 802.1x, AD, and RADIUS or ZTNA Connection Manager and Gateway

### 13.1.1 Authentication using Captive Web Portal

Genian ZTNA uses a **Captive Web Portal** (**CWP**) for Guest Access, Authentication, Information, and Instructions to become compliant with enforced policies. You can configure the Policy Server to redirect both users and guests to a **CWP login** page for **Authentication**. Users are then forced to enter Username and Password to authenticate against a database before being allowed access to the network. This allows you to identify users behind endpoint devices, and present them with information or login instructions.

Example configuration for authentication via CWP:

### Edit “User Not Authenticated” Node Group

1. Go to **Policy** in top panel
2. Go to **Group > Node** in the left Policy panel
3. Find and click on **User Not Authenticated** in the Node Group window
4. Find **General > Status** section and select **Enabled**
5. Click **Update**
6. Click **Apply** in top right corner

### Apply “User Not Authenticated” Node Group to “User Not Authenticated” Enforcement Policy

1. Go to **Policy** in the top panel
2. Go to **Enforcement Policy** in the left Policy panel
3. Find and click on **User Not Authenticated** Enforcement Policy
4. Find **General> Status** section and select **Enabled**
5. Find **Node Group** section and verify **User Not Authenticated** is added (*If not then click Assign and add it in*)
6. Click **Update**
7. Click **Apply** in top right corner

(*Navigate to /cwp and you should now see the Authentication Login icon on the page*)

## 13.1.2 Authentication using Agent

**Agent** not only assists in determining the posture of the endpoint device, but can also collect system information, access control, and authenticate users. You can configure the **Policy Server** to force users to authenticate using the **Agent** with the **Authenticate User Using Genian Agent** plugin. Once Users credentials have been Authenticated the **Agent** then communicates with the Policy Server every 2 minutes continually validating the User behind the endpoint device.

### Step 1. Create Node Group for Authentication by Agent

1. Go to **Policy** in top panel
2. Go to **Group > Node** in the left Policy panel
3. Click **Tasks > Create New Group for Policy**
4. Enter **ID** as **Agent Authentication**
5. Find **Condition** section in the Node Group window. Click **Add**
6. Enter the Following:
   - Criteria: **Agent**
   - Operator: **is**
   - Value: **Installed**
7. Click **Save**
8. Click **Apply** in the top right. Click Close

### Step 2. Create Node Policy for Agent Authentication

1. Go to **Policy** in top panel
2. Go to **Policy > Node Policy** in the left Policy panel
3. Click **Tasks > Create**. Complete steps in **Node Policy Wizard**
4. On **General** tab. Enter **ID** as **Agent Authentication**
5. On **Node Group** tab. Select **Agent Authentication** Node Group and move it to **Selected** column #. On **Preferences** tab. Enter in **desired Options** #. On **Agent Action** tab. Select **Authenticate User Using Genian Agent** and move to **Selected** column
6. On **Anomaly Definition** tab. (*Nothing required on this tab*)
7. Click **Finish**
8. Click **Apply** in the top right. Click Close

### Step 3. Configure User Authentication by Agent Plugin

1. Go to **Policy** in top panel
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel
3. Find and click **Authenticate User Using Genian Agent**
4. Add **desired Conditions** and **Agent Actions**
5. Click **Update**
6. Click **Apply** in the top right. Click **Close**

**Note:** Steps below are optional to use an existing Node Policy if you prefer not to create a new one

### Assign Agent Action to Node Policy

1. Go to **Policy** in top panel
2. Go to **Policy > Node Policy** in the left Policy panel
3. Find and click **Node Policy** name
4. Find **Agent Action** section. Click **Assign**
5. Locate **Authenticate User Using Genian Agent** and move to **Selected** column
6. Click **Add**
7. Click **Apply** in the top right. Click Close

### 13.1.3 Authentication using RADIUS (802.1x)

**Note:** This feature required Enterprise Edition

Genian ZTNA includes a built-in RADIUS server to support 802.1x port-based access control. In general, 802.1x is widely used to provide improved user authentication for devices that access wireless networks. In a wired network, a user authentication function can be provided for a device connected to the network through a switch supporting 802.1x.

First, you need to enable the RADIUS server. See, *Configuring RADIUS Enforcement*

For RADIUS authentication against external databases, authentication integrations must be configured. See: *Integrating User Directories*

The RADIUS accounting must be activated on the client or in Genian ZTNA in order for the node information to be updated. See *Single Sign-On*

#### Enable AD Account for RADIUS

1. Go to **Preferences** in the top panel
2. Go to **Service > RADIUS Server** in the left Preferences panel
3. Find **RADIUS Server: AD Account** section and select **On** in drop-down
4. Enter the following:
   - **Domain Name** (*e.g. genians.com*)
   - **Username** (*Default is Administrator. Account needs to have Admin Privileges*)
   - **Password** and retype
5. Click **Update**

#### Enable URL Account for RADIUS

1. Go to **Preferences** in the top panel
2. Go to **Service > RADIUS Server** in the left Preferences panel
3. Find **RADIUS Server: URL Account** section and select **On** in drop-down
4. Enter the following:
   - **URL** (*e.g. http://.com*)
   - **Methods** (*GET, POST*)
   - **Regex for Authentication** (*This regular expression will check for successful login*)
5. Click **Update**

### Enable Email Authentication for RADIUS

1. Go to **Preferences** in the top panel
2. Go to **Service > RADIUS Server** in the left Preferences panel
3. Find **RADIUS Server: Email Authentication** section and select **On** in
4. Click **Update**

### MAC Authentication Bypass

For endpoints not supporting 802.1x such as printers or IP phones, it may be necessary to authenticate using MAC address.

The MAC authentication feature is a mechanism by which incoming traffic originating from a specific MAC address is forwarded only if the source MAC address is successfully authenticated by a RADIUS server. The MAC address itself is used as the username and password for RADIUS authentication. The user does not need to provide a specific username and password to gain access to the network.

- If RADIUS authentication for the MAC address is successful, traffic from the MAC address is forwarded in hardware. - If the RADIUS server cannot validate the user's MAC address, then it is considered an authentication failure, and a specified authentication-failure action can be taken.

### Enabling MAC Authentication

See: *Configuring MAC Authentication (MAB)*

## 13.1.4 Single Sign-On

If user authentication through RADIUS is applied to the network, user authentication can be automatically performed through accounting packet provided by RADIUS client such as Access Point. Genian ZTNA receives external RADIUS accounting packets, saves them as audit records, and uses them as user authentication information.

When network access is granted to the user by the NAS, an Accounting Start (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "start") is sent by the NAS to the RADIUS server to signal the start of the user's network access. "Start" records typically contain the user's identification, network address, point of attachment and a unique session identifier. Periodically, Interim Update records (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "interim-update") may be sent by the NAS to the RADIUS server, to update it on the status of an active session. "Interim" records typically convey the current session duration and information on current data usage. Finally, when the user's network access is closed, the NAS issues a final Accounting Stop record (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "stop") to the RADIUS server, providing information on the final usage in terms of time, packets transferred, data transferred, reason for disconnect and other information related to the user's network access. Typically, the client sends Accounting-Request packets until it receives an Accounting-Response acknowledgement, using some retry interval.

### Via RADIUS Accounting

The RADIUS accounting server is responsible for receiving the accounting request and returning a response to the client indicating that it has successfully received the request. The RADIUS accounting server can act as a proxy client to other kinds of accounting servers.

To enable single sign on from external RADIUS Servers:

1. Go to **Preferences** in top panel
2. Go to **Service > RADIUS Server** in the left Preferences panel

Under **Accounting Server**

1. For **Single Sign-On**, select **On**.
2. For **Acct-Status-Type**, select events to update authentication status from the following: **Start, Stop, Interim-Update**.
3. For **Shared Secret Key**, enter the pre-shared secret key for RADIUS client authentication.
4. For **Attribute to Match**, select **MAC and IP** when RADIUS accounting packet contains **Calling-Station-Id** and **Framed-IP-Address**. If accounting packet doesn't have **Framed-IP-Address** attribute or generated by **Generating Accounting** option on Authentication Server setting, select **MAC**.
5. For **Node Status**, choose **All Nodes** or **Up Nodes** for authentication eligibility.
6. Click **Update**

### Via AD Domain Login

Genian ZTNA can read Active Directory domain logon user information and register the user as authenticated on that node. This may be accomplished with, or without an endpoint agent.

To use any method of AD Single Sign-On, you must enable it under the Node Policy you wish to apply it to:

**Apply SSO to Node Policies:**

1. Navigate to **Policy** in the top panel.
2. Go to **Node Policy** and select a policy to allow AD SSO.

Under **Authentication Policy:**

1. For **Single Sign-On Method**, select **Active Directory**.
2. For **Domain Name**, enter your domain name as FQDN.
3. Click **Update**.

### Enable Agent Based AD SSO

1. Install the agent as shown in *Installing Agent*.
   - The agent execution/installation account must be set as Domain account. If the agent is installed to a local account, SSO cannot function.

### Enable Agentless AD SSO

This feature performs agentless SSO through WMI query to the Domain Controller (Supports all nodes that have authenticated to the domain). ZTNA Network sensor perform SSO authentication by comparing AD server domain logon event logs with the network sensor detected device host/domain name through netbios. Therefore, the network sensor must communicate with device netnios, remote wmi.

1. Navigate to **Preferences** in the top panel, then select **Authentication Integration > AD Single Sign-On** on the left panel.

   Under **AD Single Sign-On:**

   - For **Connect to AD Server from**, Specify the sensor to connect to the AD server. If you do not select any, connect from Policy Server.
   - For **Server Address**, Specify a server address / domain for AD(Active Directory) Single Sign-On. Automatically authenticate users if the node is joined to a domain.
   - For **User ID**, Specify the User ID for monitoring the server's event log.
   - For **Password**, Specify the Password for monitoring the server's event log.
   - For **Secondary AD**, Specify whether to use a secondary AD.
   - Click **Update** button.

2. Choose **AD connection Settings**:

   - By default this query is performed by the Policy Server.
   - To perform the query from a Network Sensor, navigate to **Preferences > Beta Features** and select a Sensor from the **Connect to AD SSO Server from** drop down list.

**Domain Controller Configuration:**

1. Be sure the Bind DN account user is part of the following groups:

   Administrative account status is not required for these privileges.

   - Distributed COM Users
   - Event Log Readers
   - Server Operators

2. Run 'wmimgmt.msc' on the command prompt
3. From the Security tab on WMI Control Properties:
4. Select the CIMV2 folder
5. Click Security, Click Add and then select the Bind DN Account.
6. Check both Allow for **Enable Account** and **Remote Enable**
7. Apply changes

**How to check whether device is joined to AD domain :**

1. **How to check on the AD server:**

   - Go to **Control Panel > Active Directory Users and Computers**
   - Click **Domain> Computers** and check a joined computer list.

2. **How to check on the Client computer:**

   - Open the **Command Prompt**

  - Type `ping [AD domain]` and check the connection.

### Setting preferences for collecting remote WMI information

Windows Management Instrumentation (WMI) is a Microsoft tool for web-based enterprise management. The WMI can be used to check your device and collect information from your device.

### Basic Requirements

To use WMI on a Windows endpoint, verify the following settings: Remote WMI is only available when joined to an AD domain

- Port 135/TCP must be available for WMI communication.
- **The following services should be running:**
  - Server
  - Windows Management Instrumentation (WMI)
- WMI communication must be enabled in network firewalls.

### Additional Configuration/Troubleshooting Options

Verify/implement the following configuration settings to work with WMI.

1. **Configure the following Active Directory settings. You can configure some of these settings on endpoints using a Group Policy.**
   - Member of Domain Administrators or Local Administrators group
   - **Member of the following domain groups:**
     - Performance Log Users
     - Distributed COM Users
   - **Member of a group with the following permissions:**
     - Act as part of Operating System
     - Log on as a batch job
     - Log on as a service
     - Replace a process
2. **Run the dcomcnfg utility and configure the following endpoint permissions:**
   - Access Permissions: Enable all
   - Launch and Activation Permissions: Enable all
3. **Run the wmimgmt.msc utility and configure WMI namespace security settings. Assign permissions to the following namespaces:**
   - rootCIMv2
   - rootDefault
   - rootSecurityCenter
   - rootSecurityCenter2

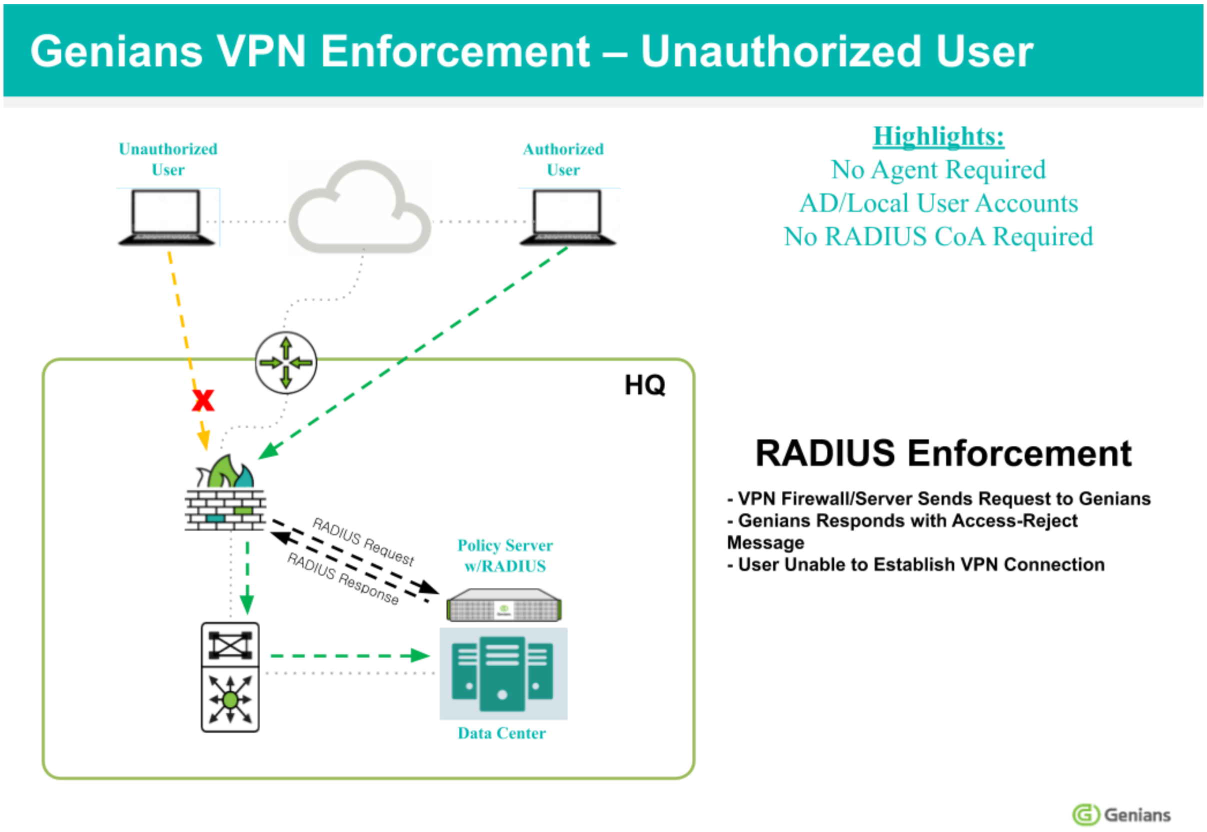
Assign the following permissions to each of the namespaces:

  - Execute Methods
  - Enable Account
  - Remote Enable
  - Read Security

- Please check Agentless Q&A on *Frequently Asked Questions* page.

### 13.1.5 Authenticating VPN Users

Genians RADIUS Server can be used as the Authentication Server for your VPN environment. You can also limit which users can authenticate with the RADIUS Server.



Genians VPN Enforcement – Unauthorized User

**Highlights:**
No Agent Required
AD/Local User Accounts
No RADIUS CoA Required

**RADIUS Enforcement**

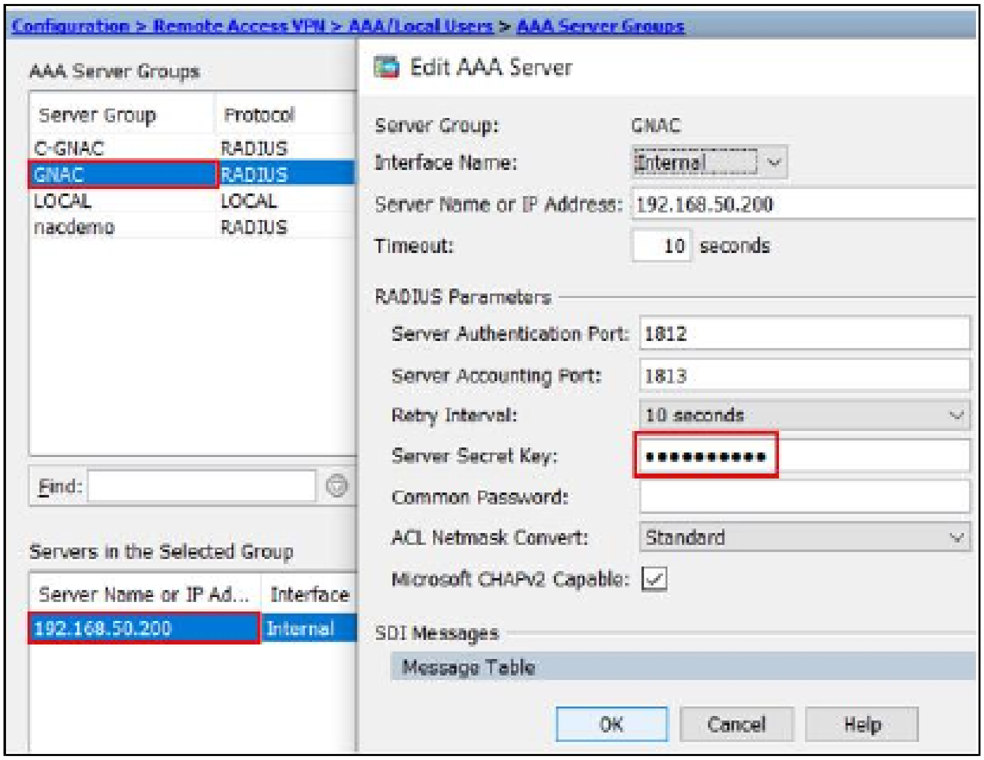
- VPN Firewall/Server Sends Request to Genians
- Genians Responds with Access-Reject Message
- User Unable to Establish VPN Connection

#### Integrating the Radius Server

First, ensure that the RADIUS Server is properly configured, and that your settings are compatible with your VPN environment.

See: *Configuring RADIUS Enforcement*

Next, configure Genian ZTNA as an Authentication Server in your VPN settings, by entering the **Shared Secret**, **Server Address**, **Authentication Port**, **Accounting Port**, and other info, as shown in the example below:



Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

AAA Server Groups

| Server Group | Protocol |
|---|---|
| C-GNAC | RADIUS |
| GNAC | RADIUS |
| LOCAL | LOCAL |
| nacdemo | RADIUS |

Servers in the Selected Group

| Server Name or IP Ad... | Interface |
|---|---|
| 192.168.50.200 | Internal |

Edit AAA Server

Server Group: GNAC
Interface Name: Internal
Server Name or IP Address: 192.168.50.200
Timeout: 10 seconds

RADIUS Parameters
Server Authentication Port: 1812
Server Accounting Port: 1813
Retry Interval: 10 seconds
Server Secret Key: ●●●●●●●●●●●
Common Password:
ACL Netmask Convert: Standard
Microsoft CHAPv2 Capable: ☑

SDI Messages

### Configuring Authentication Restrictions

In some situations, you may wish to place restrictions on who can authenticate using the RADIUS Server. This can be accomplished by configuring an **RADIUS Policy**, and setting the **Access Policy** to **REJECT**.

1. Go to **Policy** in the top panel.
2. Go to **Policy > RADIUS Policy** in the left panel.
3. Click **Tasks > Create**
4. For **General**, input **Name**, **Priority**, and activation **Status**.
5. For **Conditions**, select **Attribute**.
6. Select **Operator** and **Value**.
7. Click **Add** button.
8. For **Policy**, choose to **REJECT** Authentication Requests that match the attribute conditions.
9. Click **Add** button.
10. Click **Create** button.

When an Authentication request meets the conditions defined, it will be rejected, unless it also meets the conditions of a policy with a higher priority.

### 13.1.6 Enabling Multi-Factor Authentication for ZTNA Connection Manager (MFA, 2FA, 2-Step)

With the ZTNA Connection Manager installed on an endpoint, and a ZTNA Gateway is Deployed, admins can configure MFA to use SMS, Google OTP or Passkeys. The Passkeys setting includes options such as Windows Hello PIN, Fingerprint and Face.

Regardless of which MFA method is chosen, they are all configured through a RADIUS Policy. The RADIUS Policy defines conditions, access policies, attributes and MFA options.

Click on the appropriate link below depending on which MFA option you would like to enable.

#### Configuring MFA with SMS

SMS can be used to verify identity by prompting to enter a code only known to the person possessing the registered mobile phone number.

In order to enable MFA using SMS, you will need to create a new Radius Policy.

#### Step 1 - Create a new Radius Policy

1. Navigate to Policy in the top panel
2. In the left window, click on Radius Policy
3. Click on Tasks and select Create
4. Enter Name for Radius Policy
5. Under the Conditions section, select the criteria to match on
6. Click Add
7. Scroll down to the Policy Section
8. Set Access Policy to 'Continue' (this allows for the MFA challenge)
9. Set 2-Step Authentication to 'Text Message'
10. Click Create

**Note:** Status can be left in 'Disabled' mode until you are ready to test.

**Note:** In order for MFA using SMS to function, ensure the user account has a mobile number entered under Management > User > userid > User Information > Mobile Phone.

### Step 2 - Test / Validate

1. Connect using the Genian ZTNA Connection manager
2. Right-click on the tray icon
3. Select Network Access and then site name to connect
4. Sign in with user ID/password
5. An 'Authentication Code' window should display
6. This code will be sent via SMS to the number list in the user profile
7. Enter code into the 'Authentication Code' window
8. If code is correct, ZTNA Connection Manager should update that you are now connected

### Configuring MFA with OTP

One Time Passcode can be used to verify identity by prompting to enter a code only known to the person possessing the registered Authenticator App.

In order to enable MFA using OTP App, you will need to create a new Radius Policy.

### Step 1 - Create a new Radius Policy

1. Navigate to Policy in the top panel
2. In the left window, click on Radius Policy
3. Click on Tasks and select Create
4. Enter Name for Radius Policy
5. Under the Conditions section, select the criteria to match on
6. Click Add
7. Scroll down to the Policy Section
8. Set Access Policy to 'Continue' (this allows for the MFA challenge)
9. Set 2-Step Authentication to 'OTP'
10. Click Create

**Note:** Status can be left in 'Disabled' mode until you are ready to test.

**Note:** In order for MFA using OTP to function, ensure the OTP App is installed on your mobile device.

### Step 2 - Test / Validate

1. Connect using the Genian ZTNA Connection manager
2. Right-click on the tray icon
3. Select Network Access and then site name to connect
4. Sign in with user ID/password
5. A 'OTP' window should display
6. Click 'Confirm' to begin the process to issue a new security key
7. On the next page, select the 'QR-Code' option and click 'Generate Security Key'
8. On your mobile device, open the Authenticator App and click the + sign
9. Scan the QR Code that was generated in the previous step
10. On the next page, enter the 6-digit code displayed in the Authenticator App
11. If code is correct, ZTNA Connection Manager should update that you are now connected

### Configuring MFA with Passkeys

Passkeys can be used to verify identity by prompting to enter biometric information such as a fingerprint, face scan or a PIN only known to the person possessing the registered endpoint.

In order to enable MFA with Passkeys, you will need to create a new Radius Policy.

### Step 1 - Create a new Radius Policy

1. Navigate to Policy in the top panel
2. In the left window, click on Radius Policy
3. Click on Tasks and select Create
4. Enter Name for Radius Policy
5. Under the Conditions section, select the criteria to match on
6. Click Add
7. Scroll down to the Policy Section
8. Set Access Policy to 'Continue' (this allows for the MFA challenge)
9. Set 2-Step Authentication to 'Passkeys'
10. Click Create

**Note:** Status can be left in 'Disabled' mode until you are ready to test.

**Note:** In order for MFA using Passkeys to function, ensure the Windows Hello options are configured on your PC (PIN, Fingerprint, Face, etc).

### Step 2 - Test / Validate

1. Connect using the Genian ZTNA Connection manager
2. Right-click on the tray icon
3. Select Network Access and then site name to connect
4. Sign in with user ID/password
5. A Windows Hello window should display
6. Enter the appropriate method to verify your identity (PIN, Fingerprint, Face)

**Note:** If you are not presented with an option to choose from, this may be due to limitations of the endpoint you are connecting with. Check Windows Hello and/or Sign On options as applicable to confirm the capabilities of your specific endpoint/OS.

1. You will be prompted to register once and then prompted a second time to verify
2. Once verified, ZTNA Connection Manager should update that you are now connected

## 13.2 Managing Users and Groups

You can manage users by adding information such as departments and job titles to create, assign, and group users.

### 13.2.1 Managing Users

Provides instructions for creating, grouping, and tagging users.

#### Add a User

1. Go to **Management > User** in the top panel
2. Click `Tasks` **> Add User**
3. Click `Save`

#### Remove User

1. Go to **Management > User** in the top panel
2. Find **User** and click **Checkbox**
3. Click `Tasks` **> Remove User**
4. Click `Ok`

### Assign Tag User

1. Go to **Management > User** in the top panel
2. Find **User** and click **Checkbox**
3. Click `Tasks` **> Assign User Tag**
4. Click `Save`

### Assigning user departments

1. Go to **Management > User** in the top panel
2. Click User ID
3. In the User Information topic, click the `Search` button to assign a department.
4. Click `Update`

**Note:** Department assignment is not possible for users added through information synchronization.

### Configuring User Account Options

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > User Account** in the left Preferences panel

### Configure User Account Inactivity Options

1. Enter the following options:
   - **Disabling Inactive User** - Select an Inactivity period after which to disable an account, and select if the rule should be applied to Admin accounts.
   - **Deleting Inactive User** - Select an Inactivity period after which to delete an account, and select if the rule should be applied to Admin accounts.
2. Click `Update`

## 13.2.2 Managing User Groups

You can manage groups of users that uniquely identify them by Department, Job title, or by the machine type they use. This gives you more control over your users on the network.

### Create a User Group

1. Go to **Policy** in the top panel
2. Go to **Group > User** in the left Policy panel
3. Click **Tasks > Create**
4. Click `Save`

### Assign a User Group

1. Go to **Management > User** in the top panel
2. Find **User** and click **Checkbox**
3. Click `Tasks` **> Assign User Group**
4. Click `Save`\`

### Delete a User Group

1. Go to **Policy** in the top panel
2. Go to **Group > User** in the left Policy panel
3. Find **User Group** and click **Checkbox**
4. Click `Tasks` **> Delete**
5. Click `Ok`

## 13.2.3 User Account Password Policy

To configure a password policy that applies to end users

For password policies, this is a common policy that sets administrator accounts in addition to end-user accounts equally.

### Configure Password Policy

To configure Password Policy for end users:

1. Enter the following options:
   - **Minimum Length** - Must be at least 9 Characters.
   - **Maximum Length** - Is 30 characters.
   - **Start with Alphabet** - To force password to start with a letter.
   - **Uppercase/Lowercase** - To force a mixture of Uppercase and Lowercase letters.
   - **Repeated Characters** - To specify whether or not they are allowed to have repeated characters in a row. i.e. “000, aaa”
   - **Numerical or Alphabetical Order** - To allow or not allow a numerical or alphabetical order.
   - **Regular Expression** - To use to validate a password. Enter in Expression and Error message.
   - **Username Password Restriction** - Passwords will not be able to use usernames.

- **Password Blacklist** - Block weak or easily guessed passwords. This will require you to upload a Blacklist file in .txt format.

2. Click `Update`

### 13.2.4 User Department Management

You can manage departments by adding or deleting department information that is available for your account

#### Adding departments

1. Go to **Management > User** in the top panel
2. Go to Departments in the left panel
3. Click `Tasks` **> Create**
4. Enter the following:
   - Department Code,This is the code for the department
   - Department,The name of the department
   - Parent Department,Select a higher department.(You must select this item to display it as a tree structure.)
   - Node Group(option),Select whether to include as a node group condition
5. Click the `Save` botton

#### Import Department CSV File

Create departments based on predefined files in the form of external CSV files

1. Go to **Management > User** in the top panel
2. Go to **Departments** in the left panel
3. Click `Tasks` **> Import**
4. Click `Select File` to select the CSV file to import
5. Click `Run`

**Note:** The CSV file is download through the download icon on the left side of the TASK button, and is used by following the form.

#### Deleting Departments

1. Go to **Management > User** in the top panel
2. Go to **Departments** in the left panel
3. Check the check box on the left side of the department you want to delete.
4. Click `Tasks` **> Delete**

**Note:** To delete a department, you must either release the department from the account assigned to it or there must be no sub-department entries associated with it

### To specify a department node group

To use an IP request system on a department-based basis, you must specify a node group containing departmental assignable IP bands

1. Go to **Management > User** in the top panel
2. Go to **Departments** in the left panel
3. Select the check box for the department you want to assign a node group to
4. Click `Tasks` **> Add to Node Group**
5. Click `Save`

### Undepartmentalize node groups

1. Go to **Management > User** in the top panel
2. Go to **Departments** in the left panel
3. Select the check box for the department you want to assign a node group to
4. Click `Tasks` **> Remove from Node Group**
5. Click `Save`

## 13.2.5 Manage job titles

You can manage titles by adding or deleting available titles to your account.

You can define user groups using user titles, and create node groups based on the user groups defined.

Based on the node group created, you can specify a policy as the target for enforcement in the Genian ZTNA.

### Adding Job Titles

1. Go to **Management > User** in the top panel
2. Go to **Job Titles** in the left panel
3. Click `Tasks` **> Create**
4. Enter the following:
   - Job Title Code
   - Job Title
5. Click `Save`

### Deleting Jot Titles

1. Go to **Management > User** in the top panel
2. Go to **Job Titles** in the left panel
3. Check the check box on the left side of the Job Title you want to delete.
4. Click `Tasks` **> Delete**

### Import Job Titles CSV File

When creating a user job title, create job titles based on a predefined file in the form of an external CSV file.

1. Go to **Management > User** in the top panel
2. Go to **Job Titles** in the left panel
3. Click `Tasks` **> Import**
4. Click `Select File` to select the CSV file to import
5. Click `Run`

**Note:** The CSV file is downloaded through the download icon on the left side of the TASK button, and is used by following the form.

## 13.2.6 Using the User Registration Page

You can use the User Registration feature to receive a request from the user to create an account for the Genian ZTNA itself.

1. Go to **Policy** in the top panel
2. Click the node **policy name** to which you want to receive the account creation request.
3. Enable the User Account Request option for the Authentication Policy entry.
4. Click the `Update` button at the bottom.
5. Click the upper right `apply` button.

## 13.2.7 Passkeys Authentication

Passkeys (FIDO2 WebAuthn) are a standards-based, passwordless authentication method that allows secure authentication without manually entering a password.

Passkeys can be used with platform authenticators or external authenticators and typically rely on device-local biometric or PIN verification combined with cryptographic keys stored on the authenticator.

This document describes how Genian ZTNA supports Passkeys for various authentication flows (admin, user (CWP/Agent), ZTNA-Client) and how to configure them.

### Supported flows and integration

- Admin console authentication
- User CWP authentication
- Agent authentication
- ZTNA-Client authentication

### Configuration overview

The Passkeys feature can be configured per authentication target (admin, user (CWP/Agent), ZTNA-Client). Detailed pages describe settings and registration flows.

### Admin Passkeys Authentication

Passkeys (FIDO2) can be configured as primary (1st) or secondary (2nd) authentication methods for admin accounts in the Web Console (MC2).

### Prerequisites

- Modern browsers (Chrome/Edge/Safari/Firefox)
- Platform authenticators such as Windows Hello or external FIDO2 authenticators (USB/NFC/BLE)
- HTTPS and proper server configuration

**Note:** Passkeys are bound to a specific admin account and device. If a user cannot use Passkeys, you can configure alternative authentication methods (password, OTP, SMS, etc.) for that account.

### Authentication modes

### Passkeys Only

- Shows an input field for the identifier on the login screen.
- After identifier input, the system prompts for the Passkey authentication associated with that account.
- If a platform authenticator is available, authentication is performed using Passkeys.
- If no Passkey is registered, you can allow password authentication first, then register Passkeys after successful login.

### Password or Passkeys

- Shows an identifier input field on the login screen.
- If the account's current authentication method is Password, the password input field is shown.
- If the account has no authentication method configured, users can register Passkeys as primary.
- If an account already has Passkeys registered, login will be possible via Passkeys.
- If no Passkey is registered, allow password authentication then register Passkeys post-login.
- If Passkeys were previously registered or disabled, the account can still be protected using Password.

### Configuration steps

### 1. Single-factor (1st) authentication setup

- Path: Preferences > General > Console > 2-Step Authentication Set Method > Select Authentication Method
- Option: Passkeys or Password or Passkeys - Passkeys: Use Passkeys as the single-factor authentication method. - Password or Passkeys: Allow selecting Passkeys or Password per admin account.

### 2. Two-factor (2nd) authentication setup (selection)

- You can add secondary authentication such as SMS/OTP/Email when required.
- Option: Either custom settings or policy-based enforcement - Custom settings: Configure 2nd factor options per admin account. - Policy enforcement: Enforce 2nd factor for all or specific admin accounts.

**Note:** If the 2nd factor configuration in Preferences > General > Console > 2-Step Authentication Set Method is set to "Individual settings", and the current authentication user has not configured MFA, the UI will show that the permission is limited.

### 3. Passkeys registration

- Path: Management > Administrators > Select Admin Accounts
- Registration: General > User passkey authentication information > Create a Passkey > complete the registration following the on-screen instructions.

### Related documents

- *Passkeys Authentication*
- *2-Step Authentication*

### User CWP Passkeys Authentication

On the User CWP login page, Passkeys (FIDO2 WebAuthn) can be configured as primary (1st) or secondary (2nd) authentication.

#### Prerequisites

- Modern browsers (Chrome/Edge/Safari/Firefox)
- Platform authenticators such as Windows Hello or external FIDO2 authenticators (USB/NFC/BLE); Android devices may support Bluetooth or built-in authenticators
- HTTPS and proper server configuration

#### Authentication modes

#### Passkeys Only

- Shows an identifier input field on the login page.
- After identifier input, the system prompts for the Passkey authentication associated with that account.
- If a platform authenticator is available, authentication is performed using Passkeys.
- If platform authentication is not available, the system may offer alternative device registration methods.

**Note:** Some Android devices require additional setup steps (Bluetooth permission or QR code enrollment) for platform authenticators.

#### Password or Passkeys

- Shows an identifier input field on the login page.
- After identifier input, users may be presented with either Password or Passkeys depending on the account configuration.
- If no platform authenticator is available, a fallback to password is supported.

#### Configuration steps

#### Related documents

- *Passkeys Authentication*
- *2-Step Authentication*

### User Agent Passkeys Authentication

Windows Agent login supports Passkeys (FIDO2) as a second-factor authentication.

#### Prerequisites

- Using an agent that supports Passkeys
- Platform authenticators such as Windows Hello or external FIDO2 authenticators (USB/NFC/BLE)
- HTTPS and proper server configuration

#### Authentication modes

#### 1st factor Password and 2nd factor Passkeys

- After completing the agent login with the 1st factor (password or other primary auth), the agent can use Passkeys as the 2nd factor.
- If Passkeys are already registered, agent login can be performed using Passkeys.
- If Passkeys are not registered, the agent may present a registration prompt after successful primary authentication.

**Note:** Agent-based Passkeys 2-factor authentication requires the agent to be configured under Preferences > Authentication > Agent Authentication > Authentication Method.

#### Configuration

#### 1. Single-factor (1st) authentication setup

- Path: Policy > Node Policy > Authentication Policy > Authentication Method > Select 2-Step Authentication Method option
- Option: Passkeys - Passkeys: Use Passkeys as the 2nd factor for agent authentication.

**Note:** If agent authentication is configured to use Passkeys only, adjust the Preferences > User Authentication > User Account > "1-Step User Authentication Set Method" accordingly to avoid leaving accounts inaccessible.

#### 2. Passkeys registration

- Agent login flow: Log in with user ID/PW, then perform local authentication and register device information; complete registration when prompted.

### Related documents

- *Passkeys Authentication*
- *2-Step Authentication*

### ZTNA-Client Passkeys Authentication

ZTNA connection agents (or OpenVPN-compatible clients) can use Passkeys (FIDO2) as a second-factor authentication when connecting via RADIUS.

### Prerequisites

- Genian agent or OpenVPN-compatible client
- Platform authenticators such as Windows Hello or external FIDO2 authenticators (USB/NFC/BLE)
- HTTPS and proper server configuration
- ZTNA-Client configuration (see: *ZTNA-Client*)

### Authentication modes

### 1st factor Password and 2nd factor Passkeys

- When connecting the ZTNA client, complete the 1st factor authentication (password or primary authentication) then use Passkeys as the 2nd factor.
- If Passkeys are already registered, connection can use Passkeys for the 2nd factor.
- If not registered, the system may request Passkeys registration during the connection flow.

**Note:** ZTNA-Client using Passkeys requires RADIUS server configuration that accepts Passkeys as a 2nd factor.

### Configuration

1. Go to Policy > RADIUS Policy > Task > Create
2. Configure the condition (user group etc.) to match the users and set detailed RADIUS options: - attribute: User-Name - condition: user is one of the User Group - value: USER-ALL
3. In the policy Preferences, set the 2nd factor to Passkeys and configure RADIUS to accept Passkeys.

### Related documents

- *Passkeys Authentication*
- *ZTNA-Client*
- *2-Step Authentication*

## 13.3 Integrating User Directories

You can configure the Policy Server to authenticate to external authentication systems using LDAP, RADIUS, IMAP, POP3, SMTP, or other third-party systems.

### 13.3.1 RADIUS

Remote Authentication and Dial-in User Service (RADIUS) is a broadly supported client-server protocol that provides centralized authentication, authorization, and accounting functions.

You can configure Policy Server to integrate with existing external RADIUS Server for User Authentication. When a user is authenticated through a captive web portal or an agent, the user password is authenticated through a RADIUS server.

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Authentication Integration** in the left Preferences panel
3. Find **RADIUS Server** section in the main window
4. For **Server Address**, enter the RADIUS server's IP Address or FQDN.
5. For **Server Port**, enter the RADIUS server's port (Default is 1812)
6. For **Shared Secret Key**, enter the pre-shared secret key for RADIUS authentication.
7. Click **Update**

### 13.3.2 LDAP (Active Directory)

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain data that may include departments, people, groups of people, passwords, email addresses, and much more. Genian ZTNA can be integrated with LDAP to collect User Information and validate User Credentials.

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Authentication Integration** in the left Preferences panel
3. Find **LDAP Server** section in the main window
4. Enter the following:
   - **Server Address**:
   - **Server Port**: (*LDAP=389, LDAPS=636*)
   - **Base DN**: (*e.g. CN=Users,DC=company,DC=com*)
   - **Bind DN**: (*Should be FQDN: e.g. Administrator@company.com*) (*Bind Account should have Administrator Privileges*)
   - **Bind Password**:

   - **User Naming Attribute**: (*e.g. sAMAccountName*)
   - **SSL Connection**: (*Turn on if using LDAPS*)

5. Click **Update**
6. Click **Test** to test configuration settings (*Test account can be any User Account found within the Base DN*)

**Note:** Known Issues

LDAP Server connection failed. URI=ldaps://[IP]:[PORT]/, ERRMSG='-1:Can't contact LDAP server, TLSv1.0=-1:Can't contact LDAP server'

Possible Fix: Update AD(LDAP) Server Operating System to latest patches. Known issues authenticating against Active directory over Secure LDAP on un-patched servers due to encryption incompatibility.

EMAIL is the service provided by most organizations, making it an easy choice to provide the user directory. You can check the user's username and password using **SMTP**, **POP3**, and **IMAP**.

### 13.3.3 IMAP

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Authentication Integration** in the left Preferences panel
3. Find **IMAP Server** section in main window
4. Enter in **Server Address**, **Server Port**, and **Domain Name**
5. Click **Update**
6. Click **Test** to test configuration settings

**Examples**

| Service Name | Server Name | Port | Domain |
|---|---|---|---|
| Google G Suites | imap.gmail.com | 993 | Your Domain |
| Exchange Online (Office 365) | outlook.office365.com | 993 | Your Domain |

### 13.3.4 POP3

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Authentication Integration** in the left Preferences panel
3. Find **POP3 Server** section in main window
4. Enter in **Server Address**, **Server Port**, and **Domain Name**
5. Click **Update**
6. Click **Test** to test configuration settings

**Examples**

| Service Name | Server Name | Port | Domain |
|---|---|---|---|
| Google G Suites | pop.gmail.com | 995 | Your Domain |
| Exchange Online (Office 365) | outlook.office365.com | 995 | Your Domain |

### 13.3.5 SMTP

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Authentication Integration** in the left Preferences panel
3. Find **SMTP Server** section in main window
4. Enter in **Server Address**, **Server Port**, **Connection Security** and **Domain Name**
5. Click **Update**
6. Click **Test** to test configuration settings

**Examples**

| Service Name | Server Name | Port | Connection Security | Domain |
|---|---|---|---|---|
| Google G Suites | smtp.gmail.com | 465 | SMTPS | Your Domain |
| Office 365 | smtp.office365.com | 587 | MSA/STARTTLS | Your Domain |

**Note:** Known Issues

**Gmail Error: "Authentication failed.Authentication failed.SMTP(535-5.7.8:Username and Password not accepted. Learn more at https://support.google.com/mail/?p=BadCredentialsy32sm41405227qt)"**

Fix: Turn on Less secure app access in Google account settings / security or use SAML integration

### 13.3.6 SAML 2.0

Security Assertion Markup Language (SAML) is an open standard that allows exchanging authentication and authorization data between parties. SAML consists of an End User and a Service Provider (SP) that requires authentication, and an Identity Provider (IdP) that provides authentication services. If Genian ZTNA is integrated with Google through SAML, Genian ZTNA becomes SP and Google becomes IdP.

The following are the basic configuration steps for SAML integration.

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Authentication Integration** in the left Preferences panel
3. Find **SAML2** section in main window
4. Copy the **SP Entity ID** and **SP ACS URL** values
5. Input these values into the *IdP server* during Genian ZTNA SAML configuration.
6. For **IdP Entity ID** and **IdP SSO URL** , enter the values obtained from the IdP server.
7. For **x509 Certificate**, Paste the certificate issued by the IdP server.
8. Click **Update**
9. Click **Test** to test configuration settings

### okta (SAML2.0) - CWP

This guide details authentication between Genian ZTNA (Service Provider), and okta (Identity Provider).

This enables user authentication through okta without having to manage users in Genian ZTNA.

SSO is achieved by invoking okta authentication using the SAML2.0 protocol on the Genian ZTNA CWP(Captive Web Portal) page and checking okta for user authentication.

#### Recommended Version

| Product | Version |
|---|---|
| Genian ZTNA PolicyServer | V6.0 |
| okta APP | SAML2.0 |

#### Supported features

The okta SAML integration currently supports the following features:

- SP-initiated SSO
- IdP-initiated SSO
- JIT (Just-In-Time) provisioning
- Single Logout (SLO)
- Signed Requests

For more information on the listed features, visit the https://help.okta.com/okta_help.htm?type=oie&id=ext_glossary

#### Configuration steps

The following steps provide only a basic integration, which will be automatically applied after the first setup.

#### Step 1: Register an okta account (If needed)

1. Go to https://www.okta.com/free-trial/ and apply for a trial account.
   - Select your information and country and enter the domain you want to use for authentication.
2. Check the authentication mail received at the email address you requested.
   - An account information confirmation mail will be sent to the requested email address under the title 'Activate your okta account'.
3. Click the **Activate okta Accout** button for activating your account.
   - When you log in, you will see a screen that sets the initial password change, security image, and security questions.
   - okta console connection requires OTP 2factor authentication and requires iPhone, Android OTP app installation and OTP registration.
   - Once you have completed OTP registration and login, SAML APP setup for interworking will now begin.

### Step 2: Add and set up SAML APP for authentication integration

1. In the menu, navigate to **Applications > Applications**.
2. From the **Browse App Catalog** menu, search for the Genians ZTNA application and select application.
3. Click the "Add Integration".
4. Enter an application label.
5. In the **Base URL** field, enter the URL of the ZTNA policy server, as shown in the example below.
    - e.g. https://test.genians.net/cwp2
6. Select the Sign On tab.
7. Click the **Sign on methods > SAML 2.0 > More details** button in the middle of the screen to view IdP information.
8. Copy and paste the following details into the Genian ZTNA **Web Console > Preferences > User Authentication > Authentication Integration > SAML2**.
    - **IdP SSO URL** - the Identity Provider **Sign on URL** from okta.
    - **IdP Entity ID** - the Identity Provider **Issuer** from okta.
    - **x509 Certificate** - download the **Signing Certificate** from okta and copy and paste the contents of the file.
9. To enable JIT provisioning, you need to set up 'On' **JIT provisioning** in ZTNA
    - In the ZTNA UI, **JIT provisioning > Additional columns** , click the Add button to set the Username and Email for the user account. The Username attribute will be used to populate the first and last name of the Genian ZTNA account that is provisioned. The Email attribute will be used to populate both the username and email for the account.
        - For User Name, enter: **{firstName} {lastName}**.
            - Brackets are required for multiple attributes
        - For email, enter: **email**.
            - The above attributes are already defined on okta and will be used during account provisioning..
            - Attributes other than the predefined ones can be added using the **Attributes (Optional)** menu.
10. To enable Single Logout(SLO), you need to set up 'On' **Single Logout(SLO)** in ZTNA
    - In okta, go to Sign on > Settings and check **Enable Single Logout**.
    - Download the SP X.509 certificate and upload it to Signature Certificate in okta. You need the SP's certificate to use the SLO feature.
    - **IdP SLO URL** - the Identity Provider **Single Logout URL** from okta.
        - If the **Single Logout URL** is not visible on the okta screen, please ensure that the **Enable Single Logout** setting is checked and then click the **Save** button.
        - Return to the Sign On tab and verify the **Single Logout URL**.
11. To enable Signed Requests, you need to set up 'On' **Signed Requests** in ZTNA
    - For Signed Requests, you need to set up SAML through okta's **Applications > Create App Integration** to enable the feature.

- Download the SP X.509 certificate and upload it to Signature Certificate in okta. You need the SP's certificate to use the Signed Requests feature.
- Set up the Signed Requests entry in okta's SAML Settings.

12. In **Sign in button text**, enter the text that will appear on the SAML authentication button in the ZTNA Web Console Authentication page.
13. Click the **Update** button at the bottom of the Genian ZTNA Web Console Settings screen.

---

**Note:** Make sure that you entered the correct value in the Base URL field under the Sign on tab. Using the wrong value will prevent you from authenticating via SAML to ZTNA. e.g. https://test.genians.net/cwp2

---

### Step 3: Adding and assigning accounts for okta Authentication Integration

If you are already registered, go to number 5

1. Go to the okta Console screen menu **Directory > Groups**.
2. Click the **Add Group** button in the middle of the screen to create a group.
3. Go to the okta Console Screen Menu **Directory > People**
4. Click the **Add Person** button in the middle of the screen to add users.

---

**Note:** The Password entry selects whether the administrator should specify a password to create or change it at the user's initial login.

---

5. Go to the okta Console screen menu **Application > Application**.
6. Click the triangle icon on the right side of the APP that you registered above and click **Assign to Users**
7. On the pop-up screen, click the **Assign** button on the right side of the account to be used for authentication integration through the APP to assign it to the APP.

### Authentication Integration Test

**How to test on okta My Apps (IdP-initiated SSO)**

1. Connect to the okta My Apps and click the ZTNA SAML App.

**How to use App Embed Link (IdP-initiated SSO)**

1. Moving to the bottom of the General tab screen in okta provides an **App Embed Link**.
2. You can sign into ZTNA through that link.

**How to test on Genian ZTNA Web Console (SP-initiated SSO)**

1. Connect to the Web Console and click the **Test** button in the topic **Preferences > User Authentication > Authentication Integration > Authentication Test**.
2. In the pop-up window, select **SAML2** for the repository.
3. A new pop-up window displays the okta authentication page and authenticates by entering your username and password.
4. On the authentication screen, click the login button.

**How to test on the Genian ZTNA CWP page (SP-initiated SSO)**

1. Prepare the device (node) to which the Genian ZTNA Node Policy is assigned the Authentication Method password policy.
2. Access the Genian ZTNA CWP page.
3. Click the **Login** button on the CWP page.
4. On the authentication screen, click the login button.
5. A new pop-up window displays the okta authentication page and authenticates by entering your username and password.
6. If the message 'Authentication succeeded' is displayed, the authentication link has been successful.

**How to test Single Logout (SLO)**

1. Enable the SLO feature.
2. Authenticate using the SSO functionality.
3. Log out using the logout button at the top of the CWP page.
4. If you're prompted to enter your okta account information when you try SAML authentication again, the SLO worked correctly.

---

**Note:** After setting up the authentication link, you must add the okta IdP domain to the enforcement policy permissions to display the authentication link window even in the blocked state.

---

```
1. To add permissions
2. Go to Policy > Object > Network
3. Click Task > Create
4. Enter general information
5. Condition > FQDN > Enter IdP Domain (e.g. genians.okta.com)
6. Click Create
7. Go to Permission
8. Create permissions using network objects that you create
9. Assign permissions that you create in a enforcement policy
```

### Okta (SAML2.0) - Web Console

This guide details authentication between Genian ZTNA (Service Provider), and Okta (Identity Provider).

SSO is achieved by invoking Okta authentication using the SAML2.0 protocol on the Genian ZTNA web console page and checking Okta for administrator authentication.

#### Recommended Version

| Product | Version |
|---|---|
| Genian ZTNA PolicyServer | V6.0 |
| Okta APP | SAML2.0 |

### Prerequisites

### Supported features

The Okta SAML integration currently supports the following features:

- SP-initiated SSO
- IdP-initiated SSO
- JIT (Just-In-Time) provisioning
- Single Logout (SLO)
- Signed Requests

For more information on the listed features, visit the https://help.okta.com/okta_help.htm?type=oie&id=ext_glossary

### Configuration steps

The following steps provide only a basic integration, which will be automatically applied after the first setup.

#### Step 1: Register an Okta account (If needed)

1. Go to https://www.Okta.com/free-trial/ and apply for a trial account.
   - Select your information and country you want to use for authentication.
2. Check the authentication mail received at the email address you requested.
   - An account information confirmation mail will be sent to the requested email address under the title 'Activate your Okta account'.
3. Click the **Activate Okta Accout** button for activating your account.
   - When you log in, you will see a screen that sets the initial password change, security image, and security questions.
   - Okta console connection requires OTP 2factor authentication and requires iPhone, Android OTP app installation and OTP registration.
   - Once you have completed OTP registration and login, SAML APP setup for interworking will now begin.

#### Step 2: Add and set up SAML APP for authentication integration

1. In the menu, navigate to **Applications > Applications**.
2. From the **Browse App Catalog** menu, search for the Genians ZTNA application and select application.
3. Click the "Add Integration".
4. Enter an application label.
5. In the **Base URL** field, enter the URL of the ZTNA policy server, as shown in the example below.
   - e.g. https://test.genians.net/mc2
6. Select the Sign On tab
7. Click the **Settings > Sign on methods > SAML 2.0 > More details** button to view IdP information.

8. Copy and paste the following details into the Genian ZTNA **Web Console > Preferences > General > Console > SAML2 Authentication > Identity Provider (IdP)**.
   - **IdP SSO URL** - the Identity Provider **Sign on URL** from Okta.
   - **IdP Entity ID** - the Identity Provider **Issuer** from Okta.
   - **x509 Certificate** - download the **Signing Certificate** from Okta and copy and paste the contents of the file.
9. To enable JIT provisioning, you need to set up 'On' **JIT provisioning** in ZTNA
   - In the ZTNA UI, **JIT provisioning > Additional columns** , click the Add button to set the Username and Email for the user account. The Username attribute will be used to populate the first and last name of the Genian ZTNA account that is provisioned. The Email attribute will be used to populate both the username and email for the account.
     - For User Name, enter: **{firstName} {lastName}**.
       - Brackets are required for multiple attributes
     - For Email, enter: **email**.
       - The above attributes are already defined on okta and will be used during account provisioning..
       - Attributes other than the predefined ones can be added using the **Attributes (Optional)** menu.
   - In the ZTNA UI, **JIT provisioning > Administrator Roles**, Click the Add button to add an administrative role.
     - Please enter the name **_ADMINROLE_superAdmin**, which is set in the **Configured SAML Attributes** section of okta.
     - To add other administrative roles, you'll need to set up other role groups through **Group Attribute Statements** by clicking **Attributes (Optional)** in okta.
     - To enable JIT provisioning, you need to set up Group Attributes.
       - You must specify this by prefixing the name with _ADMINROLE_, as shown in the example below.
       - The name after _ADMINROLE_ must be the same (case sensitive) as the Administrator Role ID created in ZTNA (e.g. superAdmin, auditor).
       - The Configured SAML Attributes entry has _ADMINROLE_superAdmin set. You can do this by setting up a Group that roles as superAdmin.

| Name | Filter |
|---|---|
| _ADMINROLE_superAdmin | Equals superAdmin |

       - Please refer to the Step 3 **Add Group** description below for the group name.
10. To enable Single Logout(SLO), you need to set up 'On' **Single Logout(SLO)** in ZTNA
    - In okta, go to Sign on > Settings and check **Enable Single Logout**.
    - Download the SP X.509 certificate and upload it to Signature Certificate in okta. You need the SP's certificate to use the SLO feature.
    - **IdP SLO URL** - the Identity Provider **Single Logout URL** from Okta.

- If the **Single Logout URL** is not visible on the okta screen, please ensure that the **Enable Single Logout** setting is checked and then click the **Save** button.
- Return to the Sign On tab and verify the **Single Logout URL**.

11. To enable Signed Requests, you need to set up 'On' **Signed Requests** in ZTNA
    - For Signed Requests, you need to set up SAML through okta's **Applications > Create App Integration** to enable the feature.
    - Download the SP X.509 certificate and upload it to Signature Certificate in okta. You need the SP's certificate to use the Signed Requests feature.
    - Set up the Signed Requests entry in okta's SAML Settings.
12. In **Sign in button text**, enter the text that will appear on the SAML authentication button in the ZTNA Web Console Authentication page.
13. Click the **Update** button at the bottom of the Genian ZTNA Web Console Settings screen.

**Note:** Make sure that you entered the correct value in the Base URL field under the Sign On tab. Using the wrong value will prevent you from authenticating via SAML to ZTNA. e.g. https://test.genians.net/mc2

### Step 3: Adding and assigning accounts for Okta Authentication Integration

If you are already registered, go to number 5

1. Go to the Okta Console screen menu **Directory > Groups**.
2. Click the **Add Group** button in the middle of the screen to create a group.
    - For JIT provisioning functionality, you need to create an Administrator Role Group. (e.g. superAdmin)

| ID | description |
|---|---|
| superAdmin | Super administrator |
| auditor | Audit administrator |

You can see all the administrative roles offered by ZTNA in Preferences > User Authentication > Administrator Role.

3. Go to the Okta Console Screen Menu **Directory > People**
4. Click the **Add Person** button in the middle of the screen to add users.
    - For users who require JIT provisioning, you should select the Group created in step 2.

**Note:** The Password entry selects whether the administrator should specify a password to create or change it at the user's initial login.

5. Go to the Okta Console screen menu **Application > Application**.
6. Click the triangle icon on the right side of the APP that you registered above and click **Assign to Users**
7. On the pop-up screen, click the **Assign** button on the right side of the account to be used for authentication integration through the APP to assign it to the APP.

### Authentication Integration Test

**How to test on Okta My Apps (IdP-initiated SSO)**

1. Connect to the Okta My Apps and click the ZTNA SAML App.

**How to use App Embed Link (IdP-initiated SSO)**

1. Moving to the bottom of the General tab screen in okta provides an **App Embed Link**.
2. You can sign into ZTNA through that link.

**How to test on the Genian ZTNA Admin Web Console page (SP-initiated SSO)**

1. Connect to the Genian ZTNA Admin Web Console sign in page.
2. Click the **SAML Login** button on the sign in page.
3. A new pop-up window displays the Okta authentication page and authenticates by entering your username and password.

**How to test Single Logout (SLO)**

1. Enable the SLO feature.
2. Authenticate using the SSO functionality.
3. Log out using the logout button at the top of the web console.
4. If you're prompted to enter your Okta account information when you try SAML authentication again, the SLO worked correctly.

**Note:** After setting up the authentication link, you must add the OKTA IdP domain to the enforcement policy permissions to display the authentication link window even in the blocked state.

```
1. To add permissions
2. Go to Policy > Object > Network
3. Click Task > Create
4. Enter general information
5. Condition > FQDN > Enter IdP Domain (e.g. genians.okta.com)
6. Click Create
7. Go to Permission
8. Create permissions using network objects that you create
9. Assign permissions that you create in a enforcement policy
```

### Microsoft Entra ID (SAML2.0) - CWP

This guide provides configuration instructions for integrating Microsoft Entra ID with Genian ZTNA, a network access control system, for authentication functionality.

### Overview

Through integration with Microsoft Entra ID solution, Genian ZTNA can perform user authentication via Microsoft Entra ID without the need to manage a separate ZTNA user database.

For user authentication, the Genian ZTNA CWP page calls Microsoft Entra ID authentication using the SAML2.0 protocol, Microsoft Entra ID verifies user authentication status, and proper SSO is achieved.

### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2022.05 |
| Microsoft Entra ID | SAML2.0 | Integratable as of 2025.10 |

### Prerequisites

- Microsoft Entra ID (formerly Azure AD) tenant
- Microsoft Entra ID administrator privileges (Global Administrator or Application Administrator)
- Genian ZTNA Web Console administrator privileges
- Network connection (communication between Genian ZTNA ↔ Microsoft Entra ID)

### Purpose of Integration

Genian ZTNA and Microsoft Entra ID integration provides the following benefits:

- No need to manage separate user databases for ZTNA and Microsoft Entra ID authentication.
- Users can authenticate to ZTNA using SSO with their Microsoft Entra ID accounts.

### Supported Features

Microsoft Entra ID SAML integration supports the following features:

- SP-initiated SSO
- IdP-initiated SSO
- JIT (Just-In-Time) Provisioning
- Single Logout (SLO)
- Signed Requests

For more detailed information about these features, please visit https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/add-application-portal-setup-sso.

### Integration Setup Method

The Genian ZTNA and Microsoft Entra ID configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

### Step 1: Create Microsoft Entra ID Enterprise Application

1. Access https://portal.azure.com and log in with your Microsoft account.
2. Navigate to the **Microsoft Entra ID** service.
3. Click **Enterprise applications** in the left menu.
4. Click the **New application** button at the top of the screen.
5. Click the **Create your own application** button.
6. Enter app creation information.
   - **What's the name of your app?**: Enter "Genian ZTNA CWP" (or your preferred name)
   - **What are you looking to do with your application?**: Select "Integrate any other application you don't find in the gallery (Non-gallery)"
   - Click the **Create** button.

### Step 2: Configure SAML Single Sign-On

1. On the **Overview** page of the created Enterprise Application, click the **Single sign-on** menu.
2. Select the **SAML** method.
3. Click the **Edit** button in the **Basic SAML Configuration** section.
4. Enter the following information:
   - **Identifier (Entity ID)**: Enter the CWP Base URL of the ZTNA Policy Server.
     - ex) https://test.genians.net/cwp2/faces/saml2/saml2Metadata.xhtml
   - **Reply URL (Assertion Consumer Service URL)**: Enter the automatically generated ACS URL for the ZTNA Policy Server CWP Base URL.
     - You can find this value in the **SP ACS URL** field on the Genian ZTNA **Web Console > Preferences > User Authentication > Authentication Integration > SAML2 Authentication Integration** screen.
     - ex) https://test.genians.net/cwp2/faces/saml2/saml2Acs.xhtml
   - **Sign on URL**: Enter the CWP Base URL of the ZTNA Policy Server. (Optional)
     - ex) https://test.genians.net/cwp2
5. Click the **Save** button.

### Step 3: Configure Attributes & Claims

1. Click the **Edit** button in the **Attributes & Claims** section.
2. Verify the default Claims provided:
   - **Unique User Identifier (Name ID)**: user.userprincipalname
   - **givenname**: user.givenname
   - **surname**: user.surname
   - **emailaddress**: user.mail
   - **name**: user.userprincipalname
3. If using JIT provisioning functionality, verify that the above default Claims are configured to be included in the SAML Response.

---

**Note:** SAML Attributes (givenname, surname, emailaddress) items are already predefined in Microsoft Entra ID. Additional attributes beyond the predefined ones can be added using the **Attributes & Claims** menu.

---

### Step 4: Verify SAML Signing Certificate and IdP Information

1. Download the **Certificate (Base64)** from the **SAML Certificate** section.
2. Open the downloaded certificate file in a text editor and copy its contents.
3. Verify the following IdP information in the **Set up Genian ZTNA CWP** section:
   - **Login URL** (used as IdP SSO URL)
   - **Microsoft Entra Identifier** (used as IdP Entity ID)
   - **Logout URL** (used as IdP SLO URL when using Single Logout)
4. In Genian ZTNA **Web Console > Preferences > User Authentication > Authentication Integration > SAML2 Authentication Integration**, copy and enter the following values from Microsoft Entra ID:
   - **IdP SSO URL** - Microsoft Entra ID's **Login URL**.
   - **IdP Entity ID** - Microsoft Entra ID's **Microsoft Entra Identifier**.
   - **x509 Certificate** - Copy and paste the contents of the downloaded **Certificate (Base64)** file.
   - SAML Certificates section, download **Federation Metadata XML** file and upload using IdP Metadata upload feature.
5. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.
   - In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the user account's name and email.
     - For the Name column, enter the IdP attribute value **{http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname} {http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname}**.
     - For the Email column, enter the IdP attribute value **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress**.

      - Microsoft Entra ID does not create a Claim if the Source attribute value is empty. Verify that the **Mail**, **First name**, and **Last name** values in the user profile are filled, or change the Source attribute to an existing attribute.
      - IdP attribute values must specify Claims names. The default is in namespace format (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname).
      - The namespace can be removed to use the value set in Name.

6. To use Single Logout (SLO), turn **Single Logout(SLO)** setting to 'On' in ZTNA.
   - You must download ZTNA's **SP X.509 certificate** and upload it to Microsoft Entra ID. The SP's certificate is required to use the SLO functionality.
   - Click the **Edit** button in **Verification certificates (optional)** of the **SAML Signing Certificate** section in Microsoft Entra ID.
   - Check **Require verification certificates** and upload ZTNA's SP X.509 certificate.
   - In ZTNA's **IdP SLO URL** - Copy and paste Microsoft Entra ID's **Logout URL**.
7. To use Signed Requests, turn **Signed Requests** setting to 'On'.
   - Download ZTNA's **SP X.509 certificate** and upload it to the **SAML Signing Certificate** section in Microsoft Entra ID. The SP's certificate is required to use the Signed Requests functionality.
   - Click the **Edit** button in **Verification certificates (optional)** of the **SAML Signing Certificate** section in Microsoft Entra ID.
   - Check **Require verification certificates** and upload ZTNA's SP X.509 certificate.
8. Enter the text to display on the Microsoft Entra ID authentication button in **Login Button Text** that will be shown on the Genian ZTNA CWP authentication screen.
9. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

**Note:** Please ensure that the Identifier and Reply URL fields in Basic SAML Configuration are correctly entered. Incorrect values will prevent authentication to ZTNA via SAML. ex) Identifier: https://test.genians.net/cwp2/faces/saml2/saml2Metadata.xhtml ex) Reply URL: https://test.genians.net/cwp2/faces/saml2/saml2Acs.xhtml

### Step 5: Add and Assign Accounts for Microsoft Entra ID Authentication Integration

If users are already registered, skip to step 5

1. Navigate to **Groups** in the Microsoft Entra ID console menu.
2. Click the **New group** button at the top of the screen to create a group.
   - **Group type**: Select "Security"
   - **Group name**: Enter a group name (e.g., "ZTNA CWP Users")
   - **Group description**: Enter group description
   - **Members**: Select users to add
   - Click the **Create** button
3. Navigate to **Users** in the Microsoft Entra ID console menu.
4. Click the **New user** button at the top of the screen to add a user.

- Select **Create new user**
- **User principal name**: Enter user account
- **Display name**: Enter user name
- **Password**: Set initial password
- **Groups**: Select the Group created in step 2
- Click the **Create** button

> **Note:** The Password option allows you to choose whether the administrator should set the password during creation or require the user to change it on first login.

5. Navigate to **Enterprise applications** in the Microsoft Entra ID console menu.
6. Click the "Genian ZTNA CWP" Application registered above.
7. Click **Users and groups** in the left menu.
8. Click the **Add user/group** button at the top of the screen.
9. Select **Users** or **Groups** to assign accounts or groups to be used for authentication integration through the APP.
10. Click the **Assign** button to complete the assignment.

## Authentication Integration Testing Method

**Using Application URL (IdP-initiated SSO)**

1. Check the **User access URL** in the **Properties** menu of the Enterprise Application.
2. You can log in to ZTNA CWP through that link.

**Testing from Genian ZTNA Web Console (SP-initiated SSO)**

1. Access the Web Console and click the **Test** button in **Preferences > User Authentication > Authentication Integration > Authentication Test**.
2. Select **SAML2** as the authentication repository in the popup window.
3. A Microsoft Entra ID authentication page will be displayed in a new popup window, enter username and password to authenticate.
4. Complete additional authentication if Multi-Factor Authentication (MFA) is configured.
5. If the message 'Authentication successful.' is displayed, the authentication integration is working properly.

**Testing from Genian ZTNA CWP Page (SP-initiated SSO)**

1. Prepare a device (node) that has been assigned the Genian ZTNA node policy password policy.
2. Access the Genian ZTNA CWP page.
3. Click the **Authenticate** button on the CWP page.
4. Click the authentication button configured in Step 4 above on the authentication screen.
5. A Microsoft Entra ID authentication page will be displayed in a new popup window, enter username and password to authenticate.

6. Complete additional authentication if Multi-Factor Authentication (MFA) is configured.

**Testing Single Logout (SLO)**

1. Configure SLO functionality to be enabled.
2. Authenticate using SSO functionality.
3. Log out using the logout button at the top of the CWP page.
4. If you are prompted to enter your Microsoft Entra ID account information when attempting SAML authentication again, SLO is working properly.

**Note:** After setting up authentication integration, you must add the Microsoft Entra ID IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
5. Network Address > Select FQDN > Enter IdP domain (e.g. login.microsoftonline.com)
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
9. Assign the created permission to the control policy that controls device network
```

### Microsoft Entra ID (SAML2.0) - Web Console

This guide provides configuration instructions for integrating Microsoft Entra ID with Genian ZTNA, a network access control system, for authentication functionality.

For administrator authentication, the Genian ZTNA Web Console page calls Microsoft Entra ID authentication using the SAML2.0 protocol, Microsoft Entra ID verifies user authentication status, and proper SSO is achieved.

#### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2022.05 |
| Microsoft Entra ID | SAML2.0 | Integratable as of 2025.10 |

#### Prerequisites

- Microsoft Entra ID (formerly Azure AD) tenant
- Microsoft Entra ID administrator privileges (Global Administrator or Application Administrator)
- Genian ZTNA Web Console administrator privileges
- Network connection (communication between Genian ZTNA ↔ Microsoft Entra ID)

### Purpose of Integration

Genian ZTNA and Microsoft Entra ID integration provides the following benefits:

- No need to manage separate user databases for ZTNA and Microsoft Entra ID authentication.
- Administrators can authenticate to ZTNA using SSO with their Microsoft Entra ID accounts.

### Supported Features

Microsoft Entra ID SAML integration supports the following features:

- SP-initiated SSO
- IdP-initiated SSO
- JIT (Just-In-Time) Provisioning
- Signed Requests

For more detailed information about these features, please visit https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/add-application-portal-setup-sso.

### Integration Setup Method

The Genian ZTNA and Microsoft Entra ID configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

### Step 1: Create Microsoft Entra ID Enterprise Application

1. Access https://portal.azure.com and log in with your Microsoft account.
2. Navigate to the **Microsoft Entra ID** service.
3. Click **Enterprise applications** in the left menu.
4. Click the **New application** button at the top of the screen.
5. Click the **Create your own application** button.
6. Enter app creation information.
    - **What's the name of your app?**: Enter "Genian ZTNA" (or your preferred name)
    - **What are you looking to do with your application?**: Select "Integrate any other application you don't find in the gallery (Non-gallery)"
    - Click the **Create** button.

### Step 2: Configure SAML Single Sign-On

1. On the **Overview** page of the created Enterprise Application, click the **Single sign-on** menu.
2. Select the **SAML** method.
3. Click the **Edit** button in the **Basic SAML Configuration** section.
4. Enter the following information:
    - **Identifier (Entity ID)**: Enter the Base URL of the ZTNA Policy Server.
        - ex) https://test.genians.net/mc2/faces/saml2/saml2Metadata.xhtml
    - **Reply URL (Assertion Consumer Service URL)**: Enter the automatically generated ACS URL for the ZTNA Policy Server Base URL.
        - You can find this value in the **SP ACS URL** field on the Genian ZTNA **Web Console > Preferences > Environment Settings > Admin Console > SAML2 Authentication** screen.
        - ex) https://test.genians.net/mc2/faces/saml2/saml2Acs.xhtml
    - **Sign on URL**: Enter the Base URL of the ZTNA Policy Server. (Optional)
        - ex) https://test.genians.net/mc2
5. Click the **Save** button.

### Step 3: Configure Attributes & Claims

1. Click the **Edit** button in the **Attributes & Claims** section.
2. Verify the default Claims provided:
    - **Unique User Identifier (Name ID)**: user.userprincipalname
    - **givenname**: user.givenname
    - **surname**: user.surname
    - **emailaddress**: user.mail
    - **name**: user.userprincipalname
3. If using JIT provisioning functionality, configure Group Claims additionally:
    - Click the **Add a group claim** button.
    - In **Which groups associated with the user should be returned in the claim?**, select **Security groups** or **Groups assigned to the application**.
    - **Source attribute**: Select "Group ID"
    - In **Advanced options**, select **Filter groups** to filter groups (group name set in Step 8) that the user belongs to.
    - In **Advanced options**, check **Customize the name of the group claim**
    - **Name**: Enter the IdP attribute value to map with ZTNA's management role, e.g. _ADMIN-ROLE_superAdmin
    - Click the **Save** button.

**Note:** Group Claims names use the "_ADMINROLE_" prefix to map with ZTNA's management roles (superAdmin, auditor, etc.). Detailed settings are provided in Step 5.

### Step 4: Verify SAML Signing Certificate and IdP Information

1. Download the **Certificate (Base64)** from the **SAML Certificate** section.
2. Open the downloaded certificate file in a text editor and copy its contents.
3. Verify the following IdP information in the **Set up Genian ZTNA** section:
   - **Login URL** (used as IdP SSO URL)
   - **Microsoft Entra Identifier** (used as IdP Entity ID)
   - **Logout URL** (used as IdP SLO URL when using Single Logout)
4. In Genian ZTNA **Web Console > Preferences > Environment Settings > Admin Console > SAML2 Authentication > IdP**, copy and enter the following values from Microsoft Entra ID:
   - **IdP SSO URL** - Microsoft Entra ID's **Login URL**.
   - **IdP Entity ID** - Microsoft Entra ID's **Microsoft Entra Identifier**.
   - **x509 Certificate** - Copy and paste the contents of the downloaded **Certificate (Base64)** file.
   - SAML Certificates section, download **Federation Metadata XML** file and upload using IdP Metadata upload feature.

### Step 5: Configure Genian ZTNA JIT Provisioning (Optional)

1. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.
   - In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the administrator account's name and email.
     - For the Name column, enter the IdP attribute value **{http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname} {http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname}**.
     - For the Email column, enter the IdP attribute value **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddre**
       - SAML Attributes (givenname, surname, emailaddress) items are already predefined in Microsoft Entra ID.
       - Additional attributes beyond the predefined ones can be added using the **Attributes & Claims** menu.
       - Microsoft Entra ID does not create a Claim if the Source attribute value is empty. Verify that the **Mail**, **First name**, and **Last name** values in the user profile are filled, or change the Source attribute to an existing attribute.
       - IdP attribute values must specify Claims names. The default is in namespace format (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname).
         - The namespace can be removed to use the value set in Name.
   - In ZTNA UI's **JIT provisioning > Administrator Management Role**, click the add button to add management roles.
     - Enter the IdP attribute value in the format **_ADMINROLE_{role id}** (e.g., _ADMINROLE_superAdmin).

- To add other management roles, you must create additional Groups in Microsoft Entra ID and include them in the SAML Response through Group Claims settings.
- Group Claims must be configured to use JIT provisioning functionality.
  - Configure Group Claims as described in Step 3.

| Management Role ID | IdP Attribute Value |
|---|---|
| superAdmin | _ADMINROLE_superAdmin |
| auditor | _ADMINROLE_auditor |

  - You can check all management roles provided by ZTNA in Preferences > User Authentication > Management Roles.

### Step 6: Configure Single Logout (SLO) (Optional)

1. To use Single Logout (SLO), turn **Single Logout(SLO)** setting to 'On' in ZTNA.
   - You must download ZTNA's **SP X.509 certificate** and upload it to Microsoft Entra ID. The SP's certificate is required to use the SLO functionality.
   - Click the **Edit** button in **Verification certificates (optional)** of the **SAML Signing Certificate** section in Microsoft Entra ID.
   - Check **Require verification certificates** and upload ZTNA's SP X.509 certificate.
   - In ZTNA's **IdP SLO URL** - Copy and paste Microsoft Entra ID's **Logout URL**.

### Step 7: Configure Signed Requests (Optional)

1. To use Signed Requests, turn **Signed Requests** setting to 'On'.
   - Download ZTNA's **SP X.509 certificate** and upload it to the **SAML Signing Certificate** section in Microsoft Entra ID. The SP's certificate is required to use the Signed Requests functionality.
   - Click the **Edit** button in **Verification certificates (optional)** of the **SAML Signing Certificate** section in Microsoft Entra ID.
   - Check **Require verification certificates** and upload ZTNA's SP X.509 certificate.
2. Enter the text to display on the Microsoft Entra ID authentication button in **Login Button Text** that will be shown on the Genian ZTNA Web Console authentication screen.
3. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

### Step 8: Add and Assign Accounts for Microsoft Entra ID Authentication Integration

If users are already registered, skip to step 5

1. Navigate to **Groups** in the Microsoft Entra ID console menu.
2. Click the **New group** button at the top of the screen to create a group.
   - Administrator Role Groups must be created for JIT provisioning functionality.
   - **Group type**: Select "Security"

- **Group name**: Enter a name representing the management role (e.g., "ZTNA Super Admin Group")
- **Group description**: Enter group description
- **Members**: Select administrator users to add
- Click the **Create** button

  You can check all management roles provided by ZTNA in Preferences > User Authentication > Management Roles.

3. Navigate to **Users** in the Microsoft Entra ID console menu.
4. Click the **New user** button at the top of the screen to add a user.
   - Select **Create new user**
   - **User principal name**: Enter user account
   - **Display name**: Enter user name
   - **Password**: Set initial password
   - **Groups**: Select the Group created in step 2
   - Click the **Create** button

   **Note:** The Password option allows you to choose whether the administrator should set the password during creation or require the user to change it on first login.

5. Navigate to **Enterprise applications** in the Microsoft Entra ID console menu.
6. Click the "Genian ZTNA" Application registered above.
7. Click **Users and groups** in the left menu.
8. Click the **Add user/group** button at the top of the screen.
9. Select **Users** or **Groups** to assign accounts or groups to be used for authentication integration through the APP.
10. Click the **Assign** button to complete the assignment.

## Authentication Integration Testing Method

**Using Application URL (IdP-initiated SSO)**

1. Check the **User access URL** in the **Properties** menu of the Enterprise Application.
2. You can log in to ZTNA through that link.

**Testing from Genian ZTNA Web Console Page (SP-initiated SSO)**

1. Access the Genian ZTNA Web Console page.
2. Click the **SAML Login** button.
3. Click the authentication button configured in Step 7 above on the authentication screen.
4. A Microsoft Entra ID authentication page will be displayed in a new popup window, enter username and password to authenticate.
5. Complete additional authentication if Multi-Factor Authentication (MFA) is configured.

**Testing Single Logout (SLO)**

1. Configure SLO functionality to be enabled.
2. Authenticate using SSO functionality.
3. Log out using the logout button at the top of the Web Console.
4. If you are prompted to enter your Microsoft Entra ID account information when attempting SAML authentication again, SLO is working properly.

**Note:** After setting up authentication integration, you must add the Microsoft Entra ID IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
5. Network Address > Select FQDN > Enter IdP domain (e.g. login.microsoftonline.com)
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
9. Assign the created permission to the control policy that controls device network
```

### 13.3.7 OIDC (OpenID Connect)

OIDC (OpenID Connect) is an open standard authentication layer built on top of OAuth 2.0. Through OIDC, clients can verify the identity of end users based on the authentication of an Authorization Server and obtain basic profile information. When Genian ZTNA is integrated with an external Identity Provider through OIDC, Genian ZTNA becomes the Relying Party (RP) and the external system becomes the OpenID Provider (OP).

The following OIDC Providers are supported:

#### Google (OIDC) - CWP

This guide provides configuration instructions for integrating Genian ZTNA, a network access control system, with Google's authentication functionality.

#### Overview

Through OIDC APP integration between Genian ZTNA and Google solutions, user authentication can be performed via Google without the need to manage a separate Genian ZTNA user database.

For user authentication, the Genian ZTNA CWP page calls Google authentication using the OIDC (OpenID Connect) protocol, Google verifies user authentication status, and proper SSO is achieved.

### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2025.10 |
| Google OAuth 2.0 | OIDC 1.0 | Integratable as of 2025.10 |

### Purpose of Integration

Genian ZTNA and Google integration provides the following benefits:

- No need to manage separate user databases for ZTNA and Google authentication.
- Users can authenticate to ZTNA using SSO with their Google accounts.
- Provides secure user authentication through the OIDC standard protocol.
- Utilizes Google Workspace users and permissions.

### Supported Features

Google OIDC integration supports the following features:

- Authorization Code Flow (standard OIDC authentication flow)
- PKCE (Proof Key for Code Exchange) security enhancement
- JIT (Just-In-Time) Provisioning
- Access Token and ID Token validation
- User information retrieval through UserInfo Endpoint
- Google Workspace Groups integration (for organizational accounts)

### Integration Setup Method

The Genian ZTNA and Google configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

### Step 1: Google Cloud Console Project Creation and Setup

1. Access https://console.cloud.google.com/ and log in with your Google account.
2. Create a new project or select an existing project.
   - Click the **Create Project** button.
   - **Project Name**: Enter "Genian ZTNA CWP"
   - **Organization or Folder**: Select the appropriate organization (optional)
   - Click the **Create** button.
3. After selecting the project, go to **APIs & Services > Library**.
4. Search for and enable **Google+ API** (for user profile information retrieval).

- Click **Google+ API** from the search results.
- Click the **Enable** button.

### Step 2: OAuth 2.0 Client ID Creation

1. Go to **APIs & Services > Credentials**.
2. Click **Create Credentials** button and select **OAuth client ID**.
3. If the OAuth consent screen is not set up, you need to configure the consent screen first.
   - Select **External** or **Internal** user type. (Internal recommended when using Google Workspace)
   - **Application Name**: Enter "Genian ZTNA CWP"
   - **User Support Email**: Enter administrator email
   - **Developer Contact Information**: Enter administrator email
   - Click **Save and Continue** button.
4. In the **Scopes** step, add the following scopes:
   - **../auth/userinfo.email**: Email address verification
   - **../auth/userinfo.profile**: Basic profile information verification
   - **openid**: OpenID Connect authentication
5. Continue creating the OAuth client ID:
   - **Application Type**: Select **Web application**
   - **Name**: Enter "Genian ZTNA CWP"
   - **Authorized JavaScript origins**: Enter ZTNA server domain
     - e.g., https://test.genians.net
   - **Authorized redirect URIs**: Enter ZTNA CWP's OIDC callback URL
     - e.g., https://test.genians.net/cwp2/faces/oidc/oidcCallback.xhtml
6. Click the **Create** button.
7. Copy and save the generated **Client ID** and **Client secret** in a secure location.
   - **Client ID** example: 123456789012-abcdef.apps.googleusercontent.com
   - **Client secret** example: GOCSPX-abcdef123456

### Step 3: Genian ZTNA OIDC Configuration

1. In Genian ZTNA **Web Console > Preferences > User Authentication > Authentication Integration > OIDC Authentication Integration**, copy and enter the following values from Google:
   - **Provider Name** - Enter "Google"
   - **Issuer** - https://accounts.google.com
   - **Client ID** - Google's **Client ID**.
   - **Client Secret** - Google's **Client secret**.
   - **Use Discovery** - Select "Off" (automatic endpoint discovery does not work)

```
{
    "issuer": "https://accounts.google.com",
    "authorization_endpoint": "https://accounts.google.com/o/oauth2/v2/
↪auth",
    "token_endpoint": "https://oauth2.googleapis.com/token",
    "userinfo_endpoint": "https://openidconnect.googleapis.com/v1/
↪userinfo",
    "jwks_uri": "https://www.googleapis.com/oauth2/v3/certs"
}
```

- **Scope** - Enter "openid profile email"
- **Additional Parameters** (Optional) - You can enter Google-specific parameters in JSON format.

```
{
    "access_type": "offline",
    "prompt": "consent"
}
```

**Note:** **Additional Parameters** configures custom parameters to be included in the OIDC Authorization Request.

**Google Recommended Parameters:**

- `access_type: "offline"` - Request Refresh Token (long-term authentication)
- `prompt: "consent"` - Display consent screen every time
- `prompt: "select_account"` - Display account selection screen
- `hd: "example.com"` - G Suite domain restriction
- `include_granted_scopes: "true"` - Include previous permissions

**OIDC Standard Parameters:**

- `ui_locales: "ko-KR"` - UI language setting
- `login_hint: "user@example.com"` - User email hint
- `max_age: "3600"` - Maximum authentication validity time (seconds)

For more details, refer to https://developers.google.com/identity/protocols/oauth2/openid-connect#authenticationuriparameters.

2. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.
   - In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the user account's name and email.
     - Enter **{family_name}{given_name}** for the name.
     - Enter **email** for the email.
       - OIDC Claims (given_name, family_name, email) items are already defined as standard in Google.
3. Enter the text to display on the Google authentication button in **Login Button Text** that will be shown on the Genian ZTNA CWP authentication screen.
   - Example: "Sign in with Google", "Google Login"

4. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

**Note:** Please ensure that the Client ID and Client secret are entered correctly. Using incorrect values will prevent authentication to ZTNA CWP through OIDC.

### Authentication Integration Testing Method

**Testing from Genian ZTNA Web Console (SP-initiated SSO)**

1. Access the Web Console and click the **Test** button in **Preferences > User Authentication > Authentication Integration > Authentication Test**.
2. In the popup window, select **OIDC** as the authentication information store.
3. In the Provider selection screen, select the configured "Google" Provider.
4. A Google authentication page will be displayed in a new popup window.
5. Select a Google account or enter username and password to authenticate.
6. When Google displays the permission consent screen, click **Allow**.
7. If the 'Authentication successful' message is displayed, the authentication integration was successful.

**Testing from Genian ZTNA CWP Page (SP-initiated SSO)**

1. Set the authentication method of the node policy's authentication policy to **OIDC**.
2. Access the Genian ZTNA CWP page.
3. Click the **Authentication** button on the CWP page.
4. On the authentication screen, click the authentication button ("Sign in with Google") configured in Step 3 above.
5. A Google authentication page will be displayed in a new popup window.
6. Select a Google account or enter username and password to authenticate.
7. When Google displays the permission consent screen, click **Allow**.
8. Upon successful authentication, JWT ID Token and Access Token are received, user information is extracted, and you are logged into ZTNA CWP.

**Note:** After setting up authentication integration, you must add the Google IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
5. Network Address > Select FQDN > Enter IdP domain
   - accounts.google.com
   - apis.google.com
   - www.googleapis.com
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
```

(continues on next page)

(continued from previous page)

```
9. Assign the created permission to the control policy that controls␣
↪endpoint networks
```

### Google (OIDC) - Web Console

This guide provides configuration instructions for integrating Genian ZTNA, a network access control system, with Google's authentication functionality.

For administrator authentication, the Genian ZTNA Web Console page calls Google authentication using the OIDC (OpenID Connect) protocol, Google verifies user authentication status, and proper SSO is achieved.

#### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2025.10 |
| Google OAuth 2.0 | OIDC 1.0 | Integratable as of 2025.10 |

#### Prerequisites

- Google Cloud Console project (Google Cloud Platform account required)
- Domain administrator privileges (when using Google Workspace)
- Genian ZTNA server in HTTPS environment

#### Purpose of Integration

Genian ZTNA and Google integration provides the following benefits:

- No need to manage separate user databases for ZTNA and Google authentication.
- Users can authenticate to ZTNA using SSO with their Google accounts.
- Provides secure authentication through the OIDC standard protocol.
- Utilizes Google Workspace users and permissions.

#### Supported Features

Google OIDC integration supports the following features:

- Authorization Code Flow (standard OIDC authentication flow)
- PKCE (Proof Key for Code Exchange) security enhancement
- Access Token and ID Token validation
- User information retrieval through UserInfo Endpoint

For more information on the above features, please refer to https://developers.google.com/identity/protocols/oauth2/openid-connect.

### Integration Setup Method

The Genian ZTNA and Google configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

### Step 1: Google Cloud Console Project Creation and Setup

1. Access https://console.cloud.google.com/ and log in with your Google account.
2. Create a new project or select an existing project.
   - Click the **Create Project** button.
   - **Project Name**: Enter "Genian ZTNA"
   - **Organization or Folder**: Select the appropriate organization (optional)
   - Click the **Create** button.
3. After selecting the project, go to **APIs & Services > Library**.
4. Search for and enable **Google+ API** (for user profile information retrieval).
   - Click **Google+ API** from the search results.
   - Click the **Enable** button.

### Step 2: OAuth 2.0 Client ID Creation

1. Go to **APIs & Services > Credentials**.
2. Click **Create Credentials** button and select **OAuth client ID**.
3. If the OAuth consent screen is not set up, you need to configure the consent screen first.
   - Select **External** or **Internal** user type. (Internal recommended when using Google Workspace)
   - **App Name**: Enter "Genian ZTNA"
   - **User Support Email**: Enter administrator email
   - **Developer Contact Information**: Enter administrator email
   - Click **Save and Continue** button.
4. In the **Scopes** step, add the following scopes:
   - **../auth/userinfo.email**: Email address verification
   - **../auth/userinfo.profile**: Basic profile information verification
   - **openid**: OpenID Connect authentication
5. Continue creating the OAuth client ID:
   - **Application Type**: Select **Web application**
   - **Name**: Enter "Genian ZTNA Web Console"
   - **Authorized JavaScript origins**: Enter ZTNA server domain
     - e.g., https://test.genians.net
   - **Authorized redirect URIs**: Enter ZTNA Admin Console's OIDC callback URL

- e.g., https://test.genians.net/mc2/faces/oidc/oidcCallback.xhtml

6. Click the **Create** button.
7. Copy and save the generated **Client ID** and **Client secret** in a secure location.
   - **Client ID** example: 123456789012-abcdef.apps.googleusercontent.com
   - **Client secret** example: GOCSPX-abcdef123456

### Step 3: Genian ZTNA OIDC Configuration

1. In Genian ZTNA **Web Console > Preferences > Environment Settings > Admin Console > OIDC Authentication > Identity Provider (IdP)**, copy and enter the following values from Google:
   - **Provider Name** - Enter "Google"
   - **Issuer** - https://accounts.google.com
   - **Client ID** - Google's **Client ID**.
   - **Client Secret** - Google's **Client secret**.
   - **Use Discovery** - Select "Off"

```
{
    "issuer": "https://accounts.google.com",
    "authorization_endpoint": "https://accounts.google.com/o/oauth2/v2/
↪auth",
    "token_endpoint": "https://oauth2.googleapis.com/token",
    "userinfo_endpoint": "https://openidconnect.googleapis.com/v1/
↪userinfo",
    "jwks_uri": "https://www.googleapis.com/oauth2/v3/certs"
}
```

   - **Scope** - Enter "openid profile email"
   - **Additional Parameters** (Optional) - You can enter Google-specific parameters in JSON format.

```
{
    "access_type": "offline",
    "prompt": "consent"
}
```

**Note: Additional Parameters** configures custom parameters to be included in the OIDC Authorization Request.

**Google Recommended Parameters:**

- `access_type: "offline"` - Request Refresh Token (long-term authentication)
- `prompt: "consent"` - Display consent screen every time
- `prompt: "select_account"` - Display account selection screen
- `hd: "example.com"` - G Suite domain restriction
- `include_granted_scopes: "true"` - Include previous permissions

**OIDC Standard Parameters:**

- `ui_locales: "ko-KR"` - UI language setting

    - `login_hint: "user@example.com"` - User email hint
    - `max_age: "3600"` - Maximum authentication validity time (seconds)

  For more details, refer to https://developers.google.com/identity/protocols/oauth2/openid-connect#authenticationuriparameters.

2. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.
   - In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the user account's name and email.
     - Enter **{family_name}{given_name}** for the name.
     - Enter **email** for the email.
       - OIDC Claims (given_name, family_name, email) items are already defined as standard in Google.
3. Enter the text to display on the Google authentication button in **Login Button Text** that will be shown on the Genian ZTNA Web Console authentication screen.
   - Example: "Sign in with Google", "Google Login"
4. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

**Note:** Please ensure that the Client ID and Client secret are entered correctly. Using incorrect values will prevent authentication to ZTNA through OIDC.

### Authentication Integration Testing Method

**Testing from Genian ZTNA Web Console Page (SP-initiated SSO)**

1. Access the Genian ZTNA Web Console page.
2. Click the **OIDC Login** button.
3. On the authentication screen, click the authentication button ("Sign in with Google") configured in Step 3 above.
4. A Google authentication page will be displayed in a new popup window.
5. Select a Google account or enter username and password to authenticate.
6. When Google displays the permission consent screen, click **Allow**.
7. Upon successful authentication, JWT ID Token and Access Token are received, user information is extracted, and you are logged into ZTNA.

**Note:** After setting up authentication integration, you must add the Google IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
5. Network Address > Select FQDN > Enter IdP domain
```

(continues on next page)

(continued from previous page)

```
   - accounts.google.com
   - apis.google.com
   - www.googleapis.com
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
9. Assign the created permission to the control policy that controls␣
↪endpoint networks
```

### Keycloak (OIDC) - CWP

This guide provides configuration instructions for integrating Keycloak with Genian ZTNA, a network access control system, for authentication functionality.

#### Overview

Through OIDC APP integration between Genian ZTNA and Keycloak solutions, user authentication can be performed via Keycloak without the need to manage a separate Genian ZTNA user database.

For user authentication, the Genian ZTNA CWP page calls Keycloak authentication using the OIDC (OpenID Connect) protocol, Keycloak verifies user authentication status, and proper SSO is achieved.

#### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2025.10 |
| Keycloak | 20.0 or higher | Integratable as of 2025.10 |

#### Purpose of Integration

Genian ZTNA and Keycloak integration provides the following benefits:

- No need to manage separate user databases for ZTNA and Keycloak authentication.
- Users can authenticate to ZTNA using SSO with their Keycloak accounts.
- Provides secure user authentication through the OIDC standard protocol.
- Utilizes Keycloak's powerful authentication/authorization management features.
- Enables integrated user management through multi-Realm and Federation features.

### Supported Features

Keycloak OIDC integration supports the following features:

- Authorization Code Flow (standard OIDC authentication flow)
- PKCE (Proof Key for Code Exchange) security enhancement
- JIT (Just-In-Time) Provisioning
- Access Token and ID Token validation
- User information retrieval through UserInfo Endpoint
- Keycloak Groups/Roles integration

### Integration Setup Method

The Genian ZTNA and Keycloak configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

### Step 1: Keycloak Realm Creation and Setup

1. Access the Keycloak Admin Console (http://localhost:8080/admin) and log in with the administrator account.
2. Click the **Realm selection** dropdown in the left menu and select **Create realm**.
3. Enter Realm creation information.
   - **Realm name**: Enter "genian-ztna-users"
   - **Enabled**: Keep checked
   - Click the **Create** button.
4. With the created Realm selected, click **Realm settings** in the left menu.
5. In the **General** tab, verify the Realm basic settings.
   - **Require SSL**: Select "External requests" or "All requests" (HTTPS environment recommended)
   - **User registration**: Configure as needed (activate when allowing CWP user registration)

### Step 2: Keycloak Client Creation (for CWP)

1. Click **Clients** in the left menu.
2. Click the **Create client** button.
3. In **General settings**, enter the following:
   - **Client type**: Select "OpenID Connect"
   - **Client ID**: Enter "genian-ztna-cwp"
   - **Name**: Enter "Genian ZTNA CWP"
   - **Description**: Enter "Genian ZTNA User Portal OIDC Integration"
   - Click the **Next** button.
4. In **Capability config**, set the following:

- **Client authentication**: Check 'On' (Confidential client)
- **Authorization**: 'Off' (generally unnecessary)
- **Standard flow**: Check 'On' (Authorization Code Flow)
- **Direct access grants**: 'Off' (recommended for security)
- Click the **Next** button.

5. In **Login settings**, enter the following:
   - **Root URL**: https://test.genians.net (ZTNA server domain)
   - **Home URL**: /cwp2/
   - **Valid redirect URIs**:
     - https://test.genians.net/cwp2/faces/oidc/oidcCallback.xhtml
   - **Web origins**: https://test.genians.net
   - Click the **Save** button.
6. Copy the **Client secret** from the **Credentials** tab of the created Client.
   - **Client secret** example: xyz987uvw654rst321opq098mno765lk

### Step 3: Keycloak User and Group Setup

1. Click **Groups** in the left menu.
2. Click the **Create group** button.
3. Enter user group information.
   - **Name**: Enter "ztna-users"
   - **Description**: Enter "ZTNA general user group"
   - Click the **Create** button.
4. Create an additional privilege group. (optional)
   - **Name**: Enter "ztna-vip-users"
   - **Description**: Enter "ZTNA VIP user group"
   - Click the **Create** button.
5. Click **Users** in the left menu.
6. Click the **Create new user** button.
7. Enter test user account information.
   - **Username**: Enter "testuser"
   - **Email**: Enter "testuser@company.com"
   - **First name**: Enter "Test"
   - **Last name**: Enter "User"
   - **Email verified**: Check 'On'
   - **Enabled**: Check 'On'
   - Click the **Create** button.

8. Go to the **Credentials** tab of the created user.
   - Click **Set password**.
   - **Password**: Enter temporary password
   - **Password confirmation**: Re-enter the same password
   - **Temporary**: 'Off' (so users don't need to change it themselves)
   - Click the **Save** button.

### Step 4: Genian ZTNA OIDC Configuration

1. In Genian ZTNA **Web Console > Preferences > User Authentication > Authentication Integration > OIDC Authentication Integration**, copy and enter the following values from Keycloak:
   - **Provider Name** - Enter "Keycloak"
   - **Issuer** - https://{keycloak-server}/realms/{realm name}
   - **Client ID** - "genian-ztna-cwp"
   - **Client Secret** - Keycloak's **Client secret**
   - **Scope** - Enter "openid profile email"
   - **Use Discovery** - Select "Off" (automatic endpoint discovery does not work)
     - You can check related Endpoint information by clicking Endpoints in the General tab of Realm settings.
     - You can check related Endpoint information by accessing the following URL:

       https://{keycloak-server}/realms/{Realm name}/.well-known/openid-configuration
   - **Additional Parameters** (Optional) - You can enter Keycloak-specific parameters in JSON format.

```
{
    "kc_idp_hint": "saml",
    "kc_locale": "ko",
    "prompt": "login"
}
```

**Note: Additional Parameters** configures custom parameters to be included in the OIDC Authorization Request.

**Keycloak Recommended Parameters:**

- `kc_idp_hint: "saml"` - Redirect to specific Identity Provider (when using Identity Brokering)
- `kc_locale: "ko"` - Keycloak UI language setting (ko, en, ja, etc.)
- `kc_action: "UPDATE_PASSWORD"` - Require specific action (password change, etc.)
- `prompt: "login"` - Force re-authentication
- `prompt: "consent"` - Display consent screen every time

**OIDC Standard Parameters:**

- `ui_locales: "ko-KR"` - UI language setting (OIDC standard)

    - `login_hint: "user@example.com"` - User email hint
    - `max_age: "3600"` - Maximum authentication validity time (seconds)
    - `acr_values: "gold"` - Authentication Context Class Reference

  For more details, refer to https://www.keycloak.org/docs/latest/securing_apps/index.html#parameters-forwarding.

2. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.
   - In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the user account's name and email.
     - Enter **{given_name} {family_name}** for the name.
     - Enter **email** for the email.
       - OIDC Claims (given_name, family_name, email) items are already defined as standard in Keycloak.
3. Enter the text to display on the Keycloak authentication button in **Login Button Text** that will be shown on the Genian ZTNA CWP authentication screen.
   - Example: "Sign in with Keycloak", "Keycloak Login"
4. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

**Note:** Please ensure that the Client ID and Client Secret are entered correctly. Also verify that the Keycloak server's Issuer URL is accessible from ZTNA.

### Step 5: Keycloak Client Mappers Configuration (Group Information Mapping)

Add Groups claim configuration for CWP user permission mapping.

1. Select the created Client ("genian-ztna-cwp") in Keycloak Admin Console.
2. Go to the **Client scopes** tab.
3. Click **genian-ztna-cwp-dedicated**.
4. In the **Mappers** tab, click **Add mapper** > **By configuration**.
5. Select **Group Membership** to add group information.
   - **Name**: Enter "group membership"
   - **Token Claim Name**: Enter "groups"
   - **Full group path**: 'Off' (include only group names)
   - **Add to ID token**: Check 'On'
   - **Add to access token**: Check 'On'
   - **Add to userinfo**: Check 'On'
   - Click the **Save** button.

### Authentication Integration Testing Method

**Testing from Genian ZTNA Web Console (SP-initiated SSO)**

1. Access the Web Console and click the **Test** button in **Preferences > User Authentication > Authentication Integration > Authentication Test**.
2. In the popup window, select **OIDC** as the authentication information store.
3. In the Provider selection screen, select the configured "Keycloak" Provider.
4. A Keycloak authentication page will be displayed in a new popup window.
5. Enter Keycloak username and password to authenticate.
6. If the 'Authentication successful' message is displayed, the authentication integration was successful.

**Testing from Genian ZTNA CWP Page (SP-initiated SSO)**

1. Set the authentication method of the node policy's authentication policy to **OIDC**.
2. Access the Genian ZTNA CWP page.
3. Click the **Authentication** button on the CWP page.
4. On the authentication screen, click the authentication button ("Sign in with Keycloak") configured in Step 4 above.
5. A Keycloak authentication page will be displayed in a new popup window.
6. Enter Keycloak username and password to authenticate.
7. Upon successful authentication, JWT ID Token and Access Token are received, user information is extracted, and you are logged into ZTNA CWP.

**Note:** After setting up authentication integration, you must add the Keycloak IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
5. Network Address > Select FQDN > Enter IdP domain
   - keycloak-server (internal domain)
   - your-keycloak.company.com (external domain)
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
9. Assign the created permission to the control policy that controls endpoint networks
```

### Keycloak (OIDC) - Web Console

This guide provides configuration instructions for integrating Keycloak with Genian ZTNA, a network access control system, for authentication functionality.

For administrator authentication, the Genian ZTNA Web Console page calls Keycloak authentication using the OIDC (OpenID Connect) protocol, Keycloak verifies user authentication status, and proper SSO is achieved.

#### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2025.10 |
| Keycloak | 20.0 or higher | Integratable as of 2025.10 |

#### Prerequisites

- Keycloak server installation and operation (version 20.0 or higher)
- Keycloak Admin Console access permissions
- Genian ZTNA Web Console administrator privileges
- Network connection (communication between Genian ZTNA ↔ Keycloak server)

#### Purpose of Integration

Genian ZTNA and Keycloak integration provides the following benefits:

- No need to manage separate administrator databases for ZTNA and Keycloak authentication.
- Administrators can authenticate to ZTNA Web Console using SSO with their Keycloak accounts.
- Provides secure administrator authentication through the OIDC standard protocol.
- Utilizes Keycloak's powerful authentication/authorization management features.
- Enables integrated management through multi-Realm and Federation features.

#### Supported Features

Keycloak OIDC integration supports the following features:

- Authorization Code Flow (standard OIDC authentication flow)
- PKCE (Proof Key for Code Exchange) security enhancement
- JIT (Just-In-Time) Provisioning
- Access Token and ID Token validation
- Administrator information retrieval through UserInfo Endpoint
- Keycloak Groups integration

### Integration Setup Method

The Genian ZTNA and Keycloak configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

### Step 1: Keycloak Realm Creation and Setup

1. Access the Keycloak Admin Console and log in with the administrator account.
2. Click the **Realm selection** dropdown in the left menu and select **Create realm**.
3. Enter Realm creation information.
   - **Realm name**: Enter "genian-ztna"
   - **Enabled**: Keep checked
   - Click the **Create** button.
4. With the created Realm selected, click **Realm settings** in the left menu.
5. In the **General** tab, verify the Realm basic settings.
   - **Require SSL**: Select "External requests" or "All requests" (HTTPS environment recommended)
   - **User registration**: Configure as needed (generally disabled)

### Step 2: Keycloak Client Creation

1. Click **Clients** in the left menu.
2. Click the **Create client** button.
3. In **General settings**, enter the following:
   - **Client type**: Select "OpenID Connect"
   - **Client ID**: Enter "genian-ztna-adminconsole"
   - **Name**: Enter "Genian ZTNA Admin Console"
   - **Description**: Enter "Genian ZTNA Admin Console OIDC Integration"
   - Click the **Next** button.
4. In **Capability config**, set the following:
   - **Client authentication**: Check 'On' (Confidential client)
   - **Authorization**: 'Off' (generally unnecessary)
   - **Standard flow**: Check 'On' (Authorization Code Flow)
   - **Direct access grants**: 'Off' (recommended for security)
   - Click the **Next** button.
5. In **Login settings**, enter the following:
   - **Root URL**: https://test.genians.net (ZTNA server domain)
   - **Home URL**: /mc2/
   - **Valid redirect URIs**:

    - https://test.genians.net/mc2/faces/oidc/oidcCallback.xhtml
  - **Web origins**: https://test.genians.net
  - Click the **Save** button.
6. Copy the **Client secret** from the **Credentials** tab of the created Client.
   - **Client secret** example: abc123def456ghi789jkl012mno345pq

### Step 3: Keycloak Users

1. Click **Users** in the left menu.
2. Click the **Create new user** button.
3. Enter administrator account information.
   - **Username**: Enter "admin"
   - **Email**: Enter "admin@company.com"
   - **First name**: Enter "Admin"
   - **Last name**: Enter "User"
   - **Email verified**: Check 'On' (optional)
   - Click the **Create** button.
4. Go to the **Credentials** tab of the created user.
   - Click **Set password**.
   - **Password**: Enter temporary password
   - **Password confirmation**: Re-enter the same password
   - **Temporary**: 'Off' (so users don't need to change it themselves)
   - Click the **Save** button.

### Step 4: Keycloak Groups Creation

1. Click **Groups** in the left menu.
2. Click the **Create group** button.
   - **Name**: Must include the _ADMINROLE_ prefix and roleId (superAdmin) like "_ADMINROLE_superAdmin_ZTNA".
   - Click the **Save** button.
3. In the **Members** tab of the created group, click **Add member**.
   - Assign users to apply to the **_ADMINROLE_superAdmin_ZTNA** group.

### Step 5: Genian ZTNA OIDC Configuration

1. In Genian ZTNA **Web Console > Preferences > Environment Settings > Admin Console > OIDC Authentication**, copy and enter the following values from Keycloak:

   - **Provider Name** - Enter "Keycloak"
   - **Issuer** - https://{keycloak-server}/realms/{realm name}
   - **Client ID** - "genian-ztna-adminconsole"
   - **Client Secret** - Keycloak's **Client secret**
   - **Use Discovery** - Select "Off" (automatic endpoint discovery does not work)
     - You can check related Endpoint information by clicking Endpoints in the General tab of Realm settings.
     - You can check related Endpoint information by accessing the following URL:

       https://{keycloak-server}/realms/{Realm name}/.well-known/openid-configuration
   - **Scope** - Enter "openid profile email"
   - **Additional Parameters** (Optional) - You can enter Keycloak-specific parameters in JSON format.

   ```
   {
       "kc_idp_hint": "saml",
       "kc_locale": "en",
       "prompt": "login"
   }
   ```

   **Note: Additional Parameters** configures custom parameters to be included in the OIDC Authorization Request.

   **Keycloak Recommended Parameters:**

   - `kc_idp_hint: "saml"` - Redirect to specific Identity Provider (when using Identity Brokering)
   - `kc_locale: "en"` - Keycloak UI language setting (en, ko, ja, etc.)
   - `kc_action: "UPDATE_PASSWORD"` - Require specific action (password change, etc.)
   - `prompt: "login"` - Force re-authentication
   - `prompt: "consent"` - Display consent screen every time

   **OIDC Standard Parameters:**

   - `ui_locales: "en-US"` - UI language setting (OIDC standard)
   - `login_hint: "user@example.com"` - User email hint
   - `max_age: "3600"` - Maximum authentication validity time (seconds)
   - `acr_values: "gold"` - Authentication context class reference

   For more details, refer to https://www.keycloak.org/docs/latest/securing_apps/index.html#parameters-forwarding.

2. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.

- In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the administrator account's name and email.
  - Enter **{given_name} {family_name}** for the name.
  - Enter **email** for the email.
    - OIDC Claims (given_name, family_name, email) items are already defined as standard in Keycloak.
- Set the basic permissions for administrators created through JIT provisioning.
  - In ZTNA UI's **JIT provisioning > Administrator Management Role**, select the management role to assign to new administrators.
  - You can set different permissions per administrator through Keycloak Groups.
  - The group name to assign administrators must include the _ADMINROLE_ prefix and roleId (superAdmin) like _ADMINROLE_superAdmin_ZTNA.

| Management Role | Value |
|---|---|
| superAdmin | _ADMINROLE_superAdmin_ZTNA |

3. Enter the text to display on the Keycloak authentication button in **Login Button Text** that will be shown on the Genian ZTNA Admin Console login screen.
   - Example: "Sign in with Keycloak", "Keycloak Login"
4. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

**Note:** Please ensure that the Client ID and Client Secret are entered correctly. Also verify that the Keycloak server's Issuer URL is accessible from ZTNA.

### Step 5: Keycloak Client Mappers Configuration (Advanced)

You can configure additional group information mapping for JIT Provisioning.

1. Select the created Client in Keycloak Admin Console.
2. Go to the **Client scopes** tab.
3. Click **genian-ztna-adminconsole-dedicated**.
4. In the **Mappers** tab, click **Add mapper** > **By configuration**.
5. Select **Group Membership** to add group information.
   - Set an appropriate name in Name.
   - Enter "groups" in Token Claim Name.
   - Turn off Full group path and save.
   - Click the **Save** button.

### Authentication Integration Testing Method

**Testing from Genian ZTNA Admin Console Page (SP-initiated SSO)**

1. Access the Genian ZTNA Admin Console login page.
2. Click the authentication button ("Sign in with Keycloak") configured in Step 4 above on the login screen.
3. A Keycloak authentication page will be displayed in a new popup window.
4. Enter Keycloak username and password to authenticate.
5. Upon successful authentication, JWT ID Token and Access Token are received, administrator information is extracted, and you are logged into the ZTNA Admin Console.

**Note:** After setting up authentication integration, you must add the Keycloak IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
5. Network Address > Select FQDN > Enter IdP domain
   - keycloak-server (internal domain)
   - your-keycloak.company.com (external domain)
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
9. Assign the created permission to the control policy that controls the admin console
```

## Microsoft Entra ID (OIDC) - CWP

This guide provides configuration instructions for integrating Microsoft Entra ID (formerly Azure AD) with Genian ZTNA, a network access control system, for authentication functionality.

### Overview

Through OIDC APP integration between Genian ZTNA and Microsoft Entra ID solutions, user authentication can be performed via Microsoft Entra ID without the need to manage a separate Genian ZTNA user database.

For user authentication, the Genian ZTNA CWP page calls Microsoft Entra ID authentication using the OIDC (OpenID Connect) protocol, Microsoft Entra ID verifies user authentication status, and proper SSO is achieved.

### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2025.10 |
| Microsoft Entra ID | v2.0 Endpoint | Integratable as of 2025.10 |

### Prerequisites

- Microsoft Entra ID (formerly Azure AD) tenant
- Microsoft Entra ID app registration permissions (Application Administrator or Global Administrator)
- Genian ZTNA Web Console administrator privileges
- Network connection (communication between Genian ZTNA ↔ Microsoft Entra ID)

### Purpose of Integration

Genian ZTNA and Microsoft Entra ID integration provides the following benefits:

- No need to manage separate user databases for ZTNA and Microsoft Entra ID authentication.
- Users can authenticate to ZTNA using SSO with their Microsoft Entra ID accounts.
- Provides secure user authentication through the OIDC standard protocol.
- Provides integrated authentication environment with Microsoft 365 users.
- Enables application of advanced security policies through Conditional Access.

### Supported Features

Microsoft Entra ID OIDC integration supports the following features:

- Authorization Code Flow (standard OIDC authentication flow)
- PKCE (Proof Key for Code Exchange) security enhancement
- JIT (Just-In-Time) Provisioning
- Access Token and ID Token validation
- User information retrieval through Microsoft Graph API

### Integration Setup Method

The Genian ZTNA and Microsoft Entra ID configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

### Step 1: Microsoft Entra ID App Registration (for CWP)

1. Access https://portal.azure.com and log in with your Microsoft account.
2. Navigate to **Microsoft Entra ID** (formerly Azure Active Directory) service.
3. Click **App registrations** in the left menu.
4. Click the **New registration** button.
5. Enter app registration information.
    - **Name**: Enter "Genian ZTNA CWP"
    - **Supported account types**: Select "Accounts in this organizational directory only" (Single tenant)
    - **Redirect URI**: Select "Web" and enter the following URL
        - https://test.genians.net/cwp2/faces/oidc/oidcCallback.xhtml
    - Click the **Register** button.
6. Copy the following information from the **Overview** page of the registered app:
    - **Application (client) ID** example: 98765432-4321-4321-4321-210987654321
    - **Directory (tenant) ID** example: 87654321-4321-4321-4321-210987654321
        - Used when constructing Endpoint URLs.

### Step 2: Microsoft Entra ID App Authentication Settings (for CWP)

1. Click **Authentication** in the left menu of the registered app.
2. Verify that the **Web** platform is added in **Platform configurations**.
3. Verify that the following is correctly entered in **Redirect URIs**:
    - https://test.genians.net/cwp2/faces/oidc/oidcCallback.xhtml
4. Add the following to **Logout URL**. (optional)
    - https://test.genians.net/cwp2/faces/login.xhtml
5. Check the following in **Implicit grant and hybrid flows**:
    - **Access tokens** (optional)
    - **ID tokens** Check (required)
6. In **Advanced settings**, configure the following:
    - **Treat client as public client** : "No" (default)
    - **Allow family and school accounts** : Configure as needed
7. Click the **Save** button.

### Step 3: Microsoft Entra ID Client Secret Generation (for CWP)

1. Click **Certificates & secrets** in the left menu of the app.
2. Click **New client secret** in the **Client secrets** tab.
3. Enter client secret information.
   - **Description**: Enter "ZTNA CWP Secret"
   - **Expires**: Select "24 months" (recommended)
   - Click the **Add** button.
4. Copy and save the **Value** of the generated **client secret** in a secure location.
   - **Client secret** example: 9z8Y7x6W5v4U3t2S1r0Q~p9O8n7M6l5K4j3I2h1G0f

**Note:** The client secret value can only be viewed immediately after creation. It cannot be viewed again once you leave the page, so be sure to save it.

### Step 4: Microsoft Entra ID API Permissions Settings (for CWP)

1. Click **API permissions** in the left menu of the app.
2. Click the **Add a permission** button.
3. Select **Microsoft Graph**.
4. Select **Delegated permissions**.
5. Add the following permissions:
   - **openid** (default, required for OpenID connection)
   - **profile** (default, user profile information)
   - **email** (default, email address)
   - **User.Read** (user basic information retrieval)
   - **Directory.Read.All** (optional, for group information retrieval)
6. Click the **Add permissions** button.
7. Click the **Grant admin consent for {tenant name}** button. (Global Administrator permission required)
8. Click **Yes** in the admin consent confirmation dialog.

### Step 5: Microsoft Entra ID User and Group Settings (for CWP)

1. Click **Users** in the left menu of Microsoft Entra ID.
2. Verify users who will be granted CWP access.
3. In the **Groups** menu, click **New group** to create a user group. (optional)
   - **Group type**: Select "Security"
   - **Group name**: Enter "ZTNA-Users"
   - **Group description**: Enter "ZTNA general user group"

   - **Members**: Add users
   - Click the **Create** button.

4. Create an additional VIP user group. (optional)
   - **Group name**: Enter "ZTNA-VIP-Users"
   - **Group description**: Enter "ZTNA VIP user group"
5. Navigate to **Enterprise applications**.
6. Search for and select the created "Genian ZTNA CWP" app.
7. In the **Users and groups** menu, click **Add user/group**.
   - Assign users or the ZTNA-Users group.

### Step 6: Genian ZTNA OIDC Configuration

1. In Genian ZTNA **Web Console > Preferences > User Authentication > Authentication Integration > OIDC Authentication Integration**, copy and enter the following values from Microsoft Entra ID:
   - **Provider Name** - Enter "Microsoft Entra ID"
   - **Issuer** - https://login.microsoftonline.com/{Directory(tenant) ID}/v2.0
   - **Client ID** - Microsoft Entra ID's **Application (client) ID**
   - **Client Secret** - Microsoft Entra ID's **Client secret value**
   - **Scope** - Enter "openid profile email User.Read"
   - **Use Discovery** - Select "Off" (automatic endpoint discovery does not work)
     - You can check related Endpoint information by clicking Endpoints on the registered App screen.
     - You can check related Endpoint information by accessing the following URL:

       https://login.microsoftonline.com/{Directory(tenant) ID}/v2.0/.well-known/openid-configuration

```
{
    "issuer": "https://login.microsoftonline.com/{Directory(tenant) ID}/
↪v2.0",
    "authorization_endpoint": "https://login.microsoftonline.com/
↪{Directory(tenant) ID}/oauth2/v2.0/authorize",
    "token_endpoint": "https://login.microsoftonline.com/
↪{Directory(tenant) ID}/oauth2/v2.0/token",
    "userinfo_endpoint": "https://graph.microsoft.com/oidc/userinfo",
    "jwks_uri": "https://login.microsoftonline.com/{Directory(tenant) ID}
↪/discovery/v2.0/keys"
}
```

   - **Additional Parameters** (Optional) - You can enter Microsoft-specific parameters in JSON format.

```
{
    "domain_hint": "example.com",
    "prompt": "select_account"
}
```

**Note: Additional Parameters** configures custom parameters to be included in the OIDC Authorization Request.

**Microsoft Recommended Parameters:**

- `domain_hint: "example.com"` - Guide login to specific tenant
- `login_hint: "user@example.com"` - User email hint
- `prompt: "select_account"` - Display account selection screen
- `prompt: "login"` - Always display login screen
- `prompt: "consent"` - Display consent screen

**OIDC Standard Parameters:**

- `ui_locales: "ko-KR"` - UI language setting
- `max_age: "3600"` - Maximum authentication validity time (seconds)

For more details, refer to https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-auth-code-flow.

2. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.
   - In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the user account's name and email.
     - Enter **name** for the name.
     - Enter **email** for the email.
       - OIDC Claims (name, email) items are already defined as standard in Microsoft Entra ID.
3. Enter the text to display on the Microsoft Entra ID authentication button in **Login Button Text** that will be shown on the Genian ZTNA CWP authentication screen.
   - Example: "Sign in with Microsoft", "Microsoft Login"
4. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

**Note:** Please ensure that the Application ID and Client secret are entered correctly. Also verify that the Tenant ID is correctly included in the Issuer URL.

## Authentication Integration Testing Method

### Testing from Genian ZTNA Web Console (SP-initiated SSO)

1. Access the Web Console and click the **Test** button in **Preferences > User Authentication > Authentication Integration > Authentication Test**.
2. In the popup window, select **OIDC** as the authentication information store.
3. In the Provider selection screen, select the configured "Microsoft Entra ID" Provider.
4. A Microsoft authentication page will be displayed in a new popup window.
5. Enter Microsoft account username and password to authenticate.
6. Complete two-factor authentication (MFA) if required.

7. If the 'Authentication successful' message is displayed, the authentication integration was successful.

**Testing from Genian ZTNA CWP Page (SP-initiated SSO)**

1. Set the authentication method of the node policy's authentication policy to **OIDC**.
2. Access the Genian ZTNA CWP page.
3. Click the **Authentication** button on the CWP page.
4. On the authentication screen, click the authentication button ("Sign in with Microsoft") configured in Step 6 above.
5. A Microsoft authentication page will be displayed in a new popup window.
6. Enter Microsoft account username and password to authenticate.
7. Complete two-factor authentication (MFA) if required.
8. Upon successful authentication, JWT ID Token and Access Token are received, user information is extracted, and you are logged into ZTNA CWP.

**Note:** After setting up authentication integration, you must add the Microsoft IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
5. Network Address > Select FQDN > Enter IdP domain
   - login.microsoftonline.com
   - graph.microsoft.com (Microsoft Graph API)
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
9. Assign the created permission to the control policy that controls endpoint networks
```

### Microsoft Entra ID (OIDC) - Web Console

This guide provides configuration instructions for integrating Microsoft Entra ID (formerly Azure AD) with Genian ZTNA, a network access control system, for authentication functionality.

For administrator authentication, the Genian ZTNA Web Console page calls Microsoft Entra ID authentication using the OIDC (OpenID Connect) protocol, Microsoft Entra ID verifies user authentication status, and proper SSO is achieved.

### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2025.10 |
| Microsoft Entra ID | v2.0 Endpoint | Integratable as of 2025.10 |

### Prerequisites

- Microsoft Entra ID (formerly Azure AD) tenant
- Microsoft Entra ID app registration permissions (Application Administrator or Global Administrator)
- Genian ZTNA Web Console administrator privileges
- Network connection (communication between Genian ZTNA ↔ Microsoft Entra ID)

### Purpose of Integration

Genian ZTNA and Microsoft Entra ID integration provides the following benefits:

- No need to manage separate administrator databases for ZTNA and Microsoft Entra ID authentication.
- Administrators can authenticate to ZTNA Web Console using SSO with their Microsoft Entra ID accounts.
- Provides secure administrator authentication through the OIDC standard protocol.

### Supported Features

Microsoft Entra ID OIDC integration supports the following features:

- Authorization Code Flow (standard OIDC authentication flow)
- PKCE (Proof Key for Code Exchange) security enhancement
- JIT (Just-In-Time) Provisioning
- Access Token and ID Token validation
- Administrator information retrieval through Microsoft Graph API

### Integration Setup Method

The Genian ZTNA and Microsoft Entra ID configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

### Step 1: Microsoft Entra ID App Registration

1. Access https://portal.azure.com and log in with your Microsoft account.
2. Navigate to **Microsoft Entra ID** (formerly Azure Active Directory) service.
3. Click **App registrations** in the left menu.
4. Click the **New registration** button.
5. Enter app registration information.
    - **Name**: Enter "Genian ZTNA Admin Console"
    - **Supported account types**: Select "Accounts in this organizational directory only" (Single tenant)
    - **Redirect URI**: Select "Web" and enter the following URL
        - https://test.genians.net/mc2/faces/oidc/oidcCallback.xhtml

- Click the **Register** button.

6. Copy the following information from the **Overview** page of the registered app:
    - **Application (client) ID** example: 12345678-1234-1234-1234-123456789012
    - **Directory (tenant) ID** example: 87654321-4321-4321-4321-210987654321
        - Used when constructing Endpoint URLs.

### Step 2: Microsoft Entra ID App Authentication Settings

1. Click **Authentication** in the left menu of the registered app.
2. Verify that the **Web** platform is added in **Platform configurations**.
3. Verify that the following is correctly entered in **Redirect URIs**:
    - https://test.genians.net/mc2/faces/oidc/oidcCallback.xhtml
4. Check the following in **Implicit grant and hybrid flows**:
    - **Access tokens** (optional)
    - **ID tokens** Check (required)
5. In **Advanced settings**, configure the following:
    - **Treat client as public client** : "No" (default)
6. Click the **Save** button.

### Step 3: Microsoft Entra ID Client Secret Generation

1. Click **Certificates & secrets** in the left menu of the app.
2. Click **New client secret** in the **Client secrets** tab.
3. Enter client secret information.
    - **Description**: Enter "ZTNA Admin Console Secret"
    - **Expires**: Select "24 months" (recommended)
    - Click the **Add** button.
4. Copy and save the **Value** of the generated **client secret** in a secure location.
    - **Client secret** example: 1a2B3c4D5e6F7g8H9i0J~k1L2m3N4o5P6q7R8s9T0u

**Note:** The client secret value can only be viewed immediately after creation. It cannot be viewed again once you leave the page, so be sure to save it.

### Step 4: Microsoft Entra ID API Permissions Settings

1. Click **API permissions** in the left menu of the app.
2. Click the **Add a permission** button.
3. Select **Microsoft Graph**.
4. Select **Delegated permissions**.
5. Add the following permissions:
   - **openid** (default, required for OpenID connection)
   - **profile** (default, user profile information)
   - **email** (default, email address)
   - **User.Read** (user basic information retrieval)
   - **Directory.Read.All** (optional, for group information retrieval)
6. Click the **Add permissions** button.
7. Click the **Grant admin consent for {tenant name}** button. (Global Administrator permission required)
8. Click **Yes** in the admin consent confirmation dialog.

### Step 5: Microsoft Entra ID User and Role Settings

1. Click **Users** in the left menu of Microsoft Entra ID.
2. Verify users who will be granted administrator privileges.
3. In the **Groups** menu, click **New group** to create an administrator group. (optional)
   - **Group type**: Select "Security"
   - **Group name**: Enter "_ADMINROLE_roleId" example: _ADMINROLE_superAdmin
   - **Group description**: Enter "ZTNA administrator group"
   - **Members**: Add administrator users
   - Click the **Create** button.
4. Navigate to **Enterprise applications**.
5. Search for and select the created "Genian ZTNA Admin Console" app.
6. In the **Users and groups** menu, click **Add user/group**.
   - Assign administrator users or the _ADMINROLE_superAdmin group.

### Step 6: Genian ZTNA OIDC Configuration

1. In Genian ZTNA **Web Console > Preferences > Environment Settings > Admin Console > OIDC Authentication**, copy and enter the following values from Microsoft Entra ID:

   - **Provider Name** - Enter "Microsoft Entra ID"
   - **Issuer** - https://login.microsoftonline.com/{Directory(tenant) ID}/v2.0
   - **Client ID** - Microsoft Entra ID's **Application (client) ID**
   - **Client Secret** - Microsoft Entra ID's **Client secret value**
   - **Scope** - Enter "openid profile email Group.Read.All"
   - **Use Discovery** - Select "Off" (automatic endpoint discovery does not work)
     - You can check related Endpoint information by clicking Endpoints on the registered App screen.
     - You can check related Endpoint information by accessing the following URL:

       https://login.microsoftonline.com/{Directory(tenant) ID}/v2.0/.well-known/openid-configuration

```
{
    "issuer": "https://login.microsoftonline.com/{Directory(tenant) ID}/v2.0",
    "authorization_endpoint": "https://login.microsoftonline.com/{Directory(tenant) ID}/oauth2/v2.0/authorize",
    "token_endpoint": "https://login.microsoftonline.com/{Directory(tenant) ID}/oauth2/v2.0/token",
    "userinfo_endpoint": "https://graph.microsoft.com/oidc/userinfo",
    "jwks_uri": "https://login.microsoftonline.com/{Directory(tenant) ID}/discovery/v2.0/keys"
}
```

   - **Additional Parameters** (Optional) - You can enter Microsoft Entra ID-specific parameters in JSON format.

```
{
    "domain_hint": "example.com",
    "login_hint": "user@example.com",
    "prompt": "select_account"
}
```

**Note: Additional Parameters** configures custom parameters to be included in the OIDC Authorization Request.

**Microsoft Entra ID Recommended Parameters:**

- `domain_hint: "example.com"` - Azure AD tenant domain hint (simplifies authentication)
- `login_hint: "user@example.com"` - Pre-fills user email
- `prompt: "login"` - Forces re-authentication
- `prompt: "select_account"` - Displays account selection screen
- `prompt: "consent"` - Displays consent screen every time

**OIDC Standard Parameters:**

- `ui_locales: "en-US"` - UI language setting
- `max_age: "3600"` - Maximum authentication validity time (seconds)
- `acr_values: "urn:mace:incommon:iap:silver"` - Authentication context class reference

For more details, refer to https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-auth-code-flow.

2. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.
   - In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the administrator account's name and email.
     - Enter **name** for the name.
     - Enter **email** for the email.
       - OIDC Claims (name, email) items are already defined as standard in Microsoft Entra ID.
   - Set the basic permissions for administrators created through JIT provisioning.
     - In ZTNA UI's **JIT provisioning > Administrator Management Role**, select the management role to assign to new administrators.
     - You can set different permissions per administrator through Microsoft Entra ID Groups.
     - The group name to assign administrators must include the _ADMINROLE_ prefix and roleId (superAdmin) like _ADMINROLE_superAdmin_ZTNA.

| Management Role | Value |
|---|---|
| superAdmin | _ADMINROLE_superAdmin_ZTNA |

3. Enter the text to display on the Microsoft Entra ID authentication button in **Login Button Text** that will be shown on the Genian ZTNA Admin Console login screen.
   - Example: "Sign in with Microsoft", "Microsoft Login"
4. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

**Note:** Please ensure that the Application ID and Client secret are entered correctly. Also verify that the Tenant ID is correctly included in the Issuer URL.

## Authentication Integration Testing Method

### Testing from Genian ZTNA Admin Console Page (SP-initiated SSO)

1. Access the Genian ZTNA Admin Console login page.
2. Click the authentication button ("Sign in with Microsoft") configured in Step 6 above on the login screen.
3. A Microsoft authentication page will be displayed in a new popup window.
4. Enter Microsoft account username and password to authenticate.
5. Complete two-factor authentication (MFA) if required.

6. Upon successful authentication, JWT ID Token and Access Token are received, administrator information is extracted, and you are logged into the ZTNA Admin Console.

**Note:** After setting up authentication integration, you must add the Microsoft IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
5. Network Address > Select FQDN > Enter IdP domain
   - login.microsoftonline.com
   - graph.microsoft.com (Microsoft Graph API)
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
9. Assign the created permission to the control policy that controls the admin console
```

### Okta (OIDC) - CWP

This guide provides configuration instructions for integrating Okta with Genian ZTNA, a network access control system, for authentication functionality.

#### Overview

Through OIDC APP integration between Genian ZTNA and Okta solutions, user authentication can be performed via Okta without the need to manage a separate Genian ZTNA user database.

For user authentication, the Genian ZTNA CWP page calls Okta authentication using the OIDC (OpenID Connect) protocol, Okta verifies user authentication status, and proper SSO is achieved.

#### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2025.10 |
| Okta APP | OIDC 2.0 | Integratable as of 2025.10 |

#### Purpose of Integration

Genian ZTNA and Okta integration provides the following benefits:

- No need to manage separate user databases for ZTNA and Okta authentication.
- Users can authenticate to ZTNA using SSO with their Okta accounts.
- Provides secure user authentication through the OIDC standard protocol.

### Supported Features

Okta OIDC App integration supports the following features:

- Authorization Code Flow (standard OIDC authentication flow)
- PKCE (Proof Key for Code Exchange) security enhancement
- JIT (Just-In-Time) Provisioning
- Access Token and ID Token validation
- User information retrieval through UserInfo Endpoint

### Integration Setup Method

The Genian ZTNA and Okta configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

### Step 1: Okta Account Registration for Integration

1. Access https://www.okta.com/free-trial/ to apply for a trial account.
   - Select user information and country.
2. Check the authentication confirmation email received at the applied email address.
   - An account information confirmation email with the subject 'Activate your Okta account' will be sent to the applied email address.
3. Click the 'Activate Okta Account' button in the email to activate the account.
   - Perform initial password change for authentication and configure two-factor authentication.
   - Okta console access requires OTP 2-factor authentication and requires iPhone/Android OTP app installation and OTP registration.
   - Once OTP registration and login are complete, OIDC APP configuration for integration begins.

### Step 2: Adding and Configuring OIDC APP for Authentication Integration

1. Go to **Applications > Applications** in the menu.
2. Click the **Create App Integration** button.
3. Select **OIDC - OpenID Connect** in **Sign-in method**.
4. Select **Web Application** in **Application type**.
5. Click the **Next** button.
6. Enter "Genian ZTNA CWP" in **App integration name**.
7. Verify that **Authorization Code** is selected in **Grant type**.
8. Enter the ZTNA Policy Server's CWP OIDC callback URL in **Sign-in redirect URIs** as shown in the example below:
   - e.g., https://test.genians.net/cwp2/faces/oidc/oidcCallback.xhtml
9. Enter the ZTNA Policy Server's CWP main page URL in **Sign-out redirect URIs**:

  - e.g., https://test.genians.net/cwp2

10. Select an appropriate assignment method in **Controlled access** section:
    - Select **Allow everyone in your organization to access** or specify specific groups.
11. Click the **Save** button to create the app.
12. Check and note the **Client ID** and **Client secret** from the **General** tab of the created app.
    - **Client ID** example: 0oa1a2b3c4d5e6f7g8h9
    - **Client secret** can be viewed by clicking the eye icon next to **Client secret**.
13. In Genian ZTNA **Web Console > Preferences > User Authentication > Authentication Integration > OIDC Authentication Integration**, copy and enter the following values from Okta:
    - **Provider Name** - Enter "Okta"
    - **Issuer** - Okta's **Org URL** (e.g., https://your-domain.okta.com).
    - **Client ID** - Okta's **Client ID**.
    - **Client Secret** - Okta's **Client secret**.
    - **Use Discovery** - Select "Off" (automatic endpoint discovery does not work)

```
{
    "provider_name": "Okta",
    "issuer": "https://your-domain.okta.com",
    "redirect_uri_mc": "https://test.genians.net/mc2/faces/oidc/
↪oidcCallback.xhtml",
    "redirect_uri_cwp": "https://test.genians.net/cwp2/faces/oidc/
↪oidcCallback.xhtml",
    "scopes": "openid,profile,email",
    "authorization_endpoint": "https://your-domain.okta.com/oauth2/v1/
↪authorize",
    "token_endpoint": "https://your-domain.okta.com/oauth2/v1/token",
    "userinfo_endpoint": "https://your-domain.okta.com/oauth2/v1/userinfo
↪",
    "jwks_uri": "https://your-domain.okta.com/oauth2/v1/keys",
    "end_session_endpoint": "https://your-domain.okta.com/oauth2/v1/
↪logout"
}
```

    - **Additional Parameters** (Optional) - You can enter Okta-specific parameters in JSON format.

```
{
    "idp": "0oa1a2b3c4d5e6f7g8h9",
    "sessionToken": "...",
    "prompt": "login"
}
```

**Note:** **Additional Parameters** configures custom parameters to be included in the OIDC Authorization Request.

**Okta Recommended Parameters:**

- `idp: "0oa1a2b3c4d5e6f7g8h9"` - Redirect to specific Identity Provider (when using Okta Federation)
- `sessionToken: "..."` - Authentication using session token (when using Okta Authentication API)

- `prompt: "login"` - Force re-authentication
- `prompt: "none"` - Attempt authentication without user interaction (SSO)
- `login_hint: "user@example.com"` - User email hint

**OIDC Standard Parameters:**

- `ui_locales: "ko-KR"` - UI language setting
- `max_age: "3600"` - Maximum authentication validity time (seconds)
- `acr_values: "urn:okta:loa:2fa:any"` - Authentication Context Class Reference (require MFA)

For more details, refer to https://developer.okta.com/docs/reference/api/oidc/#authorize.

---

14. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.
    - In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the user account's name and email.
      - Enter **{given_name} {family_name}** for the name.
      - Enter **email** for the email.
        - OIDC Claims (given_name, family_name, email) items are already defined as standard in Okta.
        - Attributes other than standard claims can also be added using the **Custom Claims** menu.
    - Set the basic permissions for users created through JIT provisioning.
      - In ZTNA UI's **JIT provisioning > Permission Settings**, select the basic permissions to assign to new users.
      - Different permissions per user can also be set through Okta Groups.
15. Enter the text to display on the Okta authentication button in **Login Button Text** that will be shown on the Genian ZTNA CWP authentication screen.
16. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

---

**Note:** Please ensure that the Client ID and Client Secret are entered correctly. Using incorrect values will prevent authentication to ZTNA CWP through OIDC.

---

### Step 3: OIDC Discovery and Advanced Configuration (Optional)

1. **PKCE (Proof Key for Code Exchange)** security configuration is enabled by default.
   - This is a security feature that prevents Authorization Code hijacking.
   - Okta supports PKCE by default, so no additional configuration is required.

### Step 4: Adding and Assigning Accounts for Okta Authentication Integration

1. Go to **Directory > People** in the Okta console menu.
2. Click the **Add Person** button in the middle of the screen to add a user.

**Note:** The Password field allows you to choose whether the administrator specifies the password during creation or whether the user changes it during their first login.

1. Go to **Application > Application** in the Okta console menu.
2. Click the gear icon to the right of the "Genian ZTNA CWP" APP registered above and click **Assign to Users**.
3. In the popup screen, click the **Assign** button to the right of the account to be used for authentication integration through the APP to assign it to the APP.

### Authentication Integration Testing Method

**Testing from Genian ZTNA Web Console (SP-initiated SSO)**

1. Access the Web Console and click the **Test** button in **Preferences > User Authentication > Authentication Integration > Authentication Test**.
2. In the popup window, select **OIDC** as the authentication information store.
3. Select "Okta" Provider.
4. An Okta authentication page will be displayed in a new popup window where you enter username and password to authenticate.
5. If the 'Authentication successful' message is displayed, the authentication integration was successful.

**Testing from Genian ZTNA CWP Page (SP-initiated SSO)**

1. Set the authentication method of the node policy's authentication policy to **OIDC**.
2. Access the Genian ZTNA CWP page.
3. Click the **Authentication** button on the CWP page.
4. On the authentication screen, click the authentication button ("Sign in with Okta") configured in Step 2 above.
5. An Okta authentication page will be displayed in a new popup window where you enter username and password to authenticate.
6. Upon successful authentication, JWT ID Token and Access Token are received, user information is extracted, and you are logged into ZTNA CWP.

**Note:** After setting up authentication integration, you must add the Okta IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
```

(continues on next page)

(continued from previous page)

```
5. Network Address > Select FQDN > Enter IdP domain (e.g. your-domain.okta.com)
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
9. Assign the created permission to the control policy that controls endpoint networks
```

## Okta (OIDC) - Web Console

This guide provides configuration instructions for integrating Okta with Genian ZTNA, a network access control system, for authentication functionality.

For administrator authentication, the Genian ZTNA Web Console page calls Okta authentication using the OIDC (OpenID Connect) protocol, Okta verifies user authentication status, and proper SSO is achieved.

### Recommended Versions

| Product Name (Component) | Version | Notes |
|---|---|---|
| Genian ZTNA (Policy Server) | V6.0 or higher | Release version after 2025.10 |
| Okta APP | OIDC 2.0 | Integratable as of 2025.10 |

### Prerequisites

### Purpose of Integration

Genian ZTNA and Okta integration provides the following benefits:

- No need to manage separate user databases for ZTNA and Okta authentication.
- Users can authenticate to ZTNA using SSO with their Okta accounts.
- Provides secure authentication through the OIDC standard protocol.

### Supported Features

Okta OIDC App integration supports the following features:

- Authorization Code Flow (standard OIDC authentication flow)
- PKCE (Proof Key for Code Exchange) security enhancement
- JIT (Just-In-Time) Provisioning
- Access Token and ID Token validation
- User information retrieval through UserInfo Endpoint

### Integration Setup Method

The Genian ZTNA and Okta configuration method covered in this guide provides only the essential items for integration. It is automatically applied after the initial one-time setup.

#### Step 1: Okta Account Registration for Integration

1. Access https://www.okta.com/free-trial/ to apply for a trial account.
   - Select user information and country.
2. Check the authentication confirmation email received at the applied email address.
   - An account information confirmation email with the subject 'Activate your Okta account' will be sent to the applied email address.
3. Click the 'Activate Okta Account' button in the email to activate the account.
   - Perform initial password change for authentication and configure two-factor authentication.
   - Okta console access requires OTP 2-factor authentication and requires iPhone/Android OTP app installation and OTP registration.
   - Once OTP registration and login are complete, OIDC APP configuration for integration begins.

#### Step 2: Adding and Configuring OIDC APP for Authentication Integration

1. Go to **Applications > Applications** in the menu.
2. Click the **Create App Integration** button.
3. Select **OIDC - OpenID Connect** in **Sign-in method**.
4. Select **Web Application** in **Application type**.
5. Click the **Next** button.
6. Enter "Genian ZTNA" in **App integration name**.
7. Verify that **Authorization Code** is selected in **Grant type**.
8. Enter the ZTNA Policy Server's OIDC callback URL in **Sign-in redirect URIs** as shown in the example below:
   - e.g., https://test.genians.net/mc2/faces/oidc/oidcCallback.xhtml
9. Enter the ZTNA Policy Server's main page URL in **Sign-out redirect URIs**:
   - e.g., https://test.genians.net/mc2
10. Select an appropriate assignment method in **Controlled access** section:
    - It is recommended to select **Limit access to selected groups** and specify ZTNA administrator groups.
11. Click the **Save** button to create the app.
12. Check and note the **Client ID** and **Client secret** from the **General** tab of the created app.
    - **Client ID** example: 0oa1a2b3c4d5e6f7g8h9
    - **Client secret** can be viewed by clicking the eye icon next to **Client secret**.

13. In Genian ZTNA **Web Console > Preferences > Environment Settings > Admin Console > OIDC Authentication > Identity Provider (IdP)**, copy and enter the following values from Okta:

    - **Provider Name** - Enter "Okta"
    - **Issuer** - Okta's **Org URL**.
    - **Client ID** - Okta's **Client ID**.
    - **Client Secret** - Okta's **Client secret**.
    - **Use Discovery** - Select "Off" (automatic endpoint discovery does not work)

    ```
    {
        "provider_name": "Okta",
        "issuer": "https://your-domain.okta.com",
        "redirect_uri_mc": "https://test.genians.net/mc2/faces/oidc/
    ↪oidcCallback.xhtml",
        "scopes": "openid,profile,email,groups",
        "authorization_endpoint": "https://your-domain.okta.com/oauth2/v1/
    ↪authorize",
        "token_endpoint": "https://your-domain.okta.com/oauth2/v1/token",
        "userinfo_endpoint": "https://your-domain.okta.com/oauth2/v1/userinfo
    ↪",
        "jwks_uri": "https://your-domain.okta.com/oauth2/v1/keys",
        "end_session_endpoint": "https://your-domain.okta.com/oauth2/v1/
    ↪logout",
    }
    ```

    - **Additional Parameters** (Optional) - You can enter Okta-specific parameters in JSON format.

      ```
      {
          "idp": "0oa1a2b3c4d5e6f7g8h9",
          "sessionToken": "...",
          "prompt": "login"
      }
      ```

      **Note: Additional Parameters** configures custom parameters to be included in the OIDC Authorization Request.

      **Okta Recommended Parameters:**

      - `idp: "0oa1a2b3c4d5e6f7g8h9"` - Redirect to specific Identity Provider (when using Okta Federation)
      - `sessionToken: "..."` - Authenticate using session token (when using Okta Authentication API)
      - `prompt: "login"` - Force re-authentication
      - `prompt: "none"` - Attempt authentication without user interaction (SSO)
      - `login_hint: "user@example.com"` - User email hint

      **OIDC Standard Parameters:**

      - `ui_locales: "en-US"` - UI language setting
      - `max_age: "3600"` - Maximum authentication validity time (seconds)
      - `acr_values: "urn:okta:loa:2fa:any"` - Authentication context class reference (require MFA)

For more details, refer to https://developer.okta.com/docs/reference/api/oidc/#authorize.

14. To use JIT provisioning functionality, change **JIT provisioning** to 'On' in ZTNA.
    - In ZTNA UI's **JIT provisioning > Additional Information**, click the add button to set the user account's name and email.
        - Enter **{given_name} {family_name}** for the name.
        - Enter **email** for the email.
            - OIDC Claims (given_name, family_name, email) items are already defined as standard in Okta.
            - Attributes other than standard claims can also be added using the **Custom Claims** menu.
    - In ZTNA UI's **JIT provisioning > Administrator Management Role**, click the add button to add a management role.
        - Please enter the name **_ADMINROLE_superAdmin** set in Okta's Groups Claims items.
        - To add other management roles, you need to create groups in Okta's **Directory > Groups** and set other role Groups through **Custom Claims**.
        - To use JIT provisioning functionality, you need to configure Group Claims.
            - The group name to assign administrators must include the _ADMINROLE_ prefix and roleId (superAdmin) like _ADMINROLE_superAdmin_ZTNA.

| Management Role | Value |
|---|---|
| superAdmin | _ADMINROLE_superAdmin_ZTNA |

15. Enter the text to display on the Okta authentication button in **Login Button Text** that will be shown on the Genian ZTNA Web Console authentication screen.
16. Click the **Update** button at the bottom of the Genian ZTNA Web Console configuration screen.

**Note:** Please ensure that the Client ID and Client Secret are entered correctly. Using incorrect values will prevent authentication to ZTNA through OIDC.

### Step 3: Adding and Assigning Accounts for Okta Authentication Integration

Skip to step 5 if users are already registered.

1. Go to **Directory > Groups** in the Okta console menu.
2. Click the **Add Group** button in the middle of the screen to create a group.
    - For JIT provisioning functionality, you need to create administrator Role Groups. (e.g., _ADMINROLE_superAdmin)

| ID | Description |
|---|---|
| _ADMINROLE_superAdmin | Super Administrator |
| _ADMINROLE_auditor | Audit Administrator |

You can check all management roles provided by ZTNA in Preferences > User Authentication > Management Roles.

3. Go to **Directory > People** in the Okta console menu.
4. Click the **Add Person** button in the middle of the screen to add a user.
    - For users who need JIT provisioning, you need to select the Group created in step 2.

**Note:** The Password field allows you to choose whether the administrator specifies the password during creation or whether the user changes it during their first login.

5. Go to **Application > Application** in the Okta console menu.
6. Click the gear icon to the right of the "Genian ZTNA" APP registered above and click **Assign to Users**.
7. In the popup screen, click the **Assign** button to the right of the account to be used for authentication integration through the APP to assign it to the APP.

### Step 4: OIDC Discovery and Advanced Configuration (Optional)

1. **PKCE (Proof Key for Code Exchange)** security configuration is enabled by default.
    - This is a security feature that prevents Authorization Code hijacking.
    - Okta supports PKCE by default, so no additional configuration is required.
2. **Custom Claims** configuration (if needed)
    - For JIT provisioning functionality, you need to configure administrator Role Groups.
    - Go to the **Sign On** tab of the Okta App.
    - Click **Edit** in the **OpenID Connect ID Token** section.
    - Set **Groups claim type** to "Filter".
    - Enter "groups" in **Groups claim name**.
    - Enter the following in **Groups claim filter**: **_ADMINROLE_superAdmin**

### Authentication Integration Testing Method

**Testing from Genian ZTNA Web Console Page (SP-initiated SSO)**

1. Access the Genian ZTNA Web Console page.
2. Click the **OIDC Login** button.
3. On the authentication screen, click the authentication button ("Sign in with Okta") configured in Step 2 above.
4. An Okta authentication page will be displayed in a new popup window where you enter username and password to authenticate.
5. Upon successful authentication, JWT ID Token and Access Token are received, user information is extracted, and you are logged into ZTNA.

**Note:** After setting up authentication integration, you must add the Okta IdP domain to the control policy permissions so that the authentication integration window is displayed even in a blocked state.

```
1. How to add permissions
2. Policy > Objects > Network
3. Select Action > Create
4. Enter basic information
5. Network Address > Select FQDN > Enter IdP domain (e.g. your-domain.okta.com)
6. Click Create
7. Go to Permissions menu
8. Create permission using the created network object
9. Assign the created permission to the control policy that controls endpoint networks
```

### 13.3.8 SAML ZTNA Client 인증

ZTNA Client VPN 인증시 SAML 인증을 사용하여 VPN 연결을 지원합니다.

#### SAML ZTNA Client VPN Authentication

#### Overview

VPN user authentication can be performed through SAML integration with the Genian ZTNA Client.

#### Prerequisites for Integration

- SAML 2.0 Configuration
- For SAML 2.0 configuration details, please refer to the document intergrate-external-saml.

#### Integration Setup Procedure

1. Navigate to **Settings** in the top menu.
2. In the left-hand settings panel, go to **service > RADIUS server** 으로 이동합니다.
3. Locate **SAML Authentication** in the main window.
4. Set **SAML Authentication** to **ON**.
5. Click **Modify** button.

#### Testing Procedure

Initiate a VPN connection using the Genian ZTNA Client, check for the SAML authentication button, and start the SAML authentication process.

### 13.3.9 Testing Integration

You can test the integration configurations of **RADIUS**, **LDAP**, **IMAP**, **POP3**, **SMTP**, or **SAML** to verify successful connections.

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Authentication Integration** in the left Preferences panel
3. Find **Authentication Test** section at the bottom of main window
4. Click **Update** if you made any configuration changes
5. Click **Test** to test configuration settings

### 13.3.10 Troubleshooting

- *LDAP Search Failed - Operations Error*

## 13.4 Synchronizing User Directories

Additional information such as department, job title, email, and group is required if policy is to be established using the usage information. If the user is not created locally but exists externally, this information should be retrieved via synchronization. Additional information can be used to create user groups or use them as node group conditions. Genian ZTNA can source this info from various sources.

**Note:** This feature required Enterprise Edition

### 13.4.1 RDBMS

**Note:** This feature required Enterprise Edition

You can synchronize user directories with a Relational Database Management System(RDBMS). A Relational Database Management System (RDBMS) is a database engine/system based on a relational model. Most modern commercial and open-source database applications are relational in nature

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Data Synchronization** in the left Preferences panel
3. Click **Tasks > Create**
4. Find **General** section in main window
5. For **ID**, Enter name here
6. For **Update Interval**, Select the specified time or periodic interval for synchronization.
7. For **Policy Apply**, After synchronization, select `Enabled` to reflect the changes. If you have multiple sync settings, you can set it to `Disabled` and enable only the last sync.

8. For **Environment**, Input is not required for basic synchronization tasks. However, it is used when defining variable values to be commonly referenced within a separate custom shell script executed for integration with external systems.

   > **Warning:** **Configuration Caution**: Incorrect environment variable declarations can lead to malfunctions in the integration script or system errors. Before configuration, please ensure that the variables are correctly processed within the script.

   Usage Scenario: Log Level Control Used when you want to control simple operation options such as Log Level or Retry Count during external script execution.

   ```
   export LOG_LEVEL='ERROR'
   ```

9. For **Query**, Enter the SQL query to be executed immediately after information synchronization is complete. This is used when secondary processing is required based on specific conditions using the synchronized information.

   > **Warning:** **Risk of Data Loss**: This feature directly affects the database. In particular, the use of `UPDATE` or `DELETE` statements may result in **irreversible data loss**.

   Usage Scenario: Account Lock Processing based on Employment Status Used when you want to automatically disable the NAC account of resigned (or on-leave) employees according to the 'Employment Status' code after information synchronization.

   Prerequisites 1. Create a field to manage employment status (e.g., USER_CUSTOM08) in [Settings] > [Property Management] > [Custom Fields] > [User Custom Fields]. 2. Assign the user custom field created in step 1 to [Additional Info] under [User Information] in [Information Synchronization].

   Writing Example If the value of USER_CUSTOM08 is '001' (Resigned/On-leave, etc.), update USER_STATUS to '0' (Disabled).

   ```
   UPDATE USER
   SET USER_STATUS = 0
   WHERE USER_CUSTOM08 = '001';
   ```

10. Find **Advanced > External DB** section in main window. Select **RDBMS**
11. Find **Advanced** > **User, Department, Job Title, Node, and LifeCycle Information** sections in main window. Add in information as needed.
12. Click **Tasks > Synchronize Now**

## 13.4.2 Synchronizing User Directories

**Note:** This feature required Enterprise Edition

Genian ZTNA can use an LDAP directory as a source of user and organizational information. LDAP synchronization allows user accounts to be created locally and used for administration or policies. LDAP synchronization is commonly used with Microsoft Active Directory (AD) systems.

### Creating Synchronization with AD

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Data Synchronization** in the left Preferences panel
3. Click **Tasks > Create**

Under **General**

1. For **ID**, type unique name.
2. For **Update Interval**, select the specified time or periodic interval for this Synchronization.
3. For **Applying Policy**, select `Enabled` for applying change after Synchronization. If there are several synchronization settings, you can set it to Disabled and enable only the last one.
4. For **Environment**, Input is not required for basic synchronization tasks. However, it is used when defining variable values to be commonly referenced within a separate custom shell script executed for integration with external systems.

   > **Warning: Configuration Caution**: Incorrect environment variable declarations can lead to malfunctions in the integration script or system errors. Before configuration, please ensure that the variables are correctly processed within the script.

   Usage Scenario: Log Level Control Used when you want to control simple operation options such as Log Level or Retry Count during external script execution.

   ```
   export LOG_LEVEL='ERROR'
   ```

5. For **Query**, Enter the SQL query to be executed immediately after information synchronization is complete. This is used when secondary processing is required based on specific conditions using the synchronized information.

   > **Warning: Risk of Data Loss**: This feature directly affects the database. In particular, the use of `UPDATE` or `DELETE` statements may result in **irreversible data loss**.

   Usage Scenario: Account Lock Processing based on Employment Status Used when you want to automatically disable the NAC account of resigned (or on-leave) employees according to the 'Employment Status' code after information synchronization.

   Prerequisites 1. Create a field to manage employment status (e.g., USER_CUSTOM08) in [Settings] > [Property Management] > [Custom Fields] > [User Custom Fields]. 2. Assign the user custom field created in step 1 to [Additional Info] under [User Information] in [Information Synchronization].

   Writing Example If the value of USER_CUSTOM08 is '001' (Resigned/On-leave, etc.), update USER_STATUS to '0' (Disabled).

   ```
   UPDATE USER
   SET USER_STATUS = 0
   WHERE USER_CUSTOM08 = '001';
   ```

Under **Database**

1. For **Type**, section `LDAP`
2. For **Server Address**, type IP Address or FQDN of Active Directory server

3. For **Server Port**, type AD LDAP service port. by default LDAP port is `389`. if you use LDAPS (LDAP over SSL) default port is `636`.
4. For **SSL Connection**, select `On` if you use LDAPS.
5. For **DB Username**, type Bind DN of Active Directory. Normally, you can use email format like `administrator@company.com`
6. For **DB Password**, type Bind DN user's password

Under **User Information**

1. For **Table Name**, type base distinguished name (DN) of users. For example: `CN=Users,DC=company,DC=com`
2. For **Where Clause for DB**, type `(&(objectClass=user)(objectCategory=person))` for filtering person object.
3. For **Column Name for Username**, type `sAMAccountName`
4. For **Column Name for Full Name**, type `displayName`
5. For **Column Name for Department**, type `$distinguishedName, IF(LOCATE('OU=',$)>0, SUBSTRING($,LOCATE(',',$)+1),'')`
6. For **Column Name for Memberships**, type `memberOf`
7. For any other extra information, you can use LDAP attribute name for each column name.

Under **Department Information**

1. For **Table Name**, type base distinguished name (DN) of organizationUnit (OU). For example: `DC=company,DC=com`
2. For **Where Clause for DB**, type `objectClass=organizationalUnit` for filtering OU object.
3. For **Sort Criteria**, type `@NAMEPATH` for ordering based on department name.
4. For **Column Name for Department ID**, type `distinguishedName`
5. For **Column Name for Department**, type `name`
6. For **Column Name for Parent Dept.**, type `$distinguishedName, SUBSTRING($,LOCATE(',',$)+1)`
7. Click **Save** at the bottom

**Attention:** Active Directory does not provide a userPassword attribute, so user passwords cannot be synchronized. Therefore, separate linkage should be set. check the *LDAP (Active Directory)*

### 13.4.3 CSV file or URL

**Note:** This feature required Enterprise Edition

You can add users to the Policy Server by importing end user information from a comma-separated value (CSV) file.

1. Go to **Preferences** in the top panel.
2. Navigate to **User Authentication> Authentication Synchronization** in the left panel.
3. Click **Tasks> Create**.

4. Find the **General** menu.
5. For **ID**, Enter name here
6. For **Update Interval**, Select the specified time or periodic interval for synchronization.
7. For **Policy Apply**, After synchronization, select `Enabled` to reflect the changes. If you have multiple sync settings, you can set it to `Disabled` and enable only the last sync.
8. For **Environment**, Input is not required for basic synchronization tasks. However, it is used when defining variable values to be commonly referenced within a separate custom shell script executed for integration with external systems.

   > **Warning: Configuration Caution**: Incorrect environment variable declarations can lead to malfunctions in the integration script or system errors. Before configuration, please ensure that the variables are correctly processed within the script.

   Usage Scenario: Log Level Control Used when you want to control simple operation options such as Log Level or Retry Count during external script execution.

   ```
   export LOG_LEVEL='ERROR'
   ```

9. For **Query**, Enter the SQL query to be executed immediately after information synchronization is complete. This is used when secondary processing is required based on specific conditions using the synchronized information.

   > **Warning: Risk of Data Loss**: This feature directly affects the database. In particular, the use of `UPDATE` or `DELETE` statements may result in **irreversible data loss**.

   Usage Scenario: Account Lock Processing based on Employment Status Used when you want to automatically disable the NAC account of resigned (or on-leave) employees according to the 'Employment Status' code after information synchronization.

   Prerequisites 1. Create a field to manage employment status (e.g., USER_CUSTOM08) in [Settings] > [Property Management] > [Custom Fields] > [User Custom Fields]. 2. Assign the user custom field created in step 1 to [Additional Info] under [User Information] in [Information Synchronization].

   Writing Example If the value of USER_CUSTOM08 is '001' (Resigned/On-leave, etc.), update USER_STATUS to '0' (Disabled).

   ```
   UPDATE USER
   SET USER_STATUS = 0
   WHERE USER_CUSTOM08 = '001';
   ```

10. Find **Advanced> DB Type** and select **CSV**.
11. In the **Data Synchronization** list, click the **checkbox** in the desired synchronization list.
12. Click **Tasks> Synchronize now**.

### 13.4.4 Google G Suite

**Note:** This feature required Enterprise Edition.

Genian ZTNA can use the G Suite directory as a source of user and organizational information. G Suite Sync lets you create user accounts locally and use them for management or policies.

Here's how to sync user and organization information based on G Suite.

#### Create sync settings

1. Move to **Preferences** in top panel.
2. Move to **User Authentication > Data Synchronization** in left panel.
3. Click **Tasks > Create**.

In **General** section

1. For **ID**, Enter name here
2. For **Update Interval**, Select the specified time or periodic interval for synchronization.
3. For **Policy Apply**, After synchronization, select `Enabled` to reflect the changes. If you have multiple sync settings, you can set it to `Disabled` and enable only the last sync.
4. For **Environment**, Input is not required for basic synchronization tasks. However, it is used when defining variable values to be commonly referenced within a separate custom shell script executed for integration with external systems.

   **Warning: Configuration Caution**: Incorrect environment variable declarations can lead to malfunctions in the integration script or system errors. Before configuration, please ensure that the variables are correctly processed within the script.

   Usage Scenario: Log Level Control Used when you want to control simple operation options such as Log Level or Retry Count during external script execution.

   ```
   export LOG_LEVEL='ERROR'
   ```

5. For **Query**, Enter the SQL query to be executed immediately after information synchronization is complete. This is used when secondary processing is required based on specific conditions using the synchronized information.

   **Warning: Risk of Data Loss**: This feature directly affects the database. In particular, the use of `UPDATE` or `DELETE` statements may result in **irreversible data loss**.

   Usage Scenario: Account Lock Processing based on Employment Status Used when you want to automatically disable the NAC account of resigned (or on-leave) employees according to the 'Employment Status' code after information synchronization.

   Prerequisites 1. Create a field to manage employment status (e.g., USER_CUSTOM08) in [Settings] > [Property Management] > [Custom Fields] > [User Custom Fields]. 2. Assign the user custom field created in step 1 to [Additional Info] under [User Information] in [Information Synchronization].

Writing Example If the value of USER_CUSTOM08 is '001' (Resigned/On-leave, etc.), update USER_STATUS to '0' (Disabled).

```
UPDATE USER
SET USER_STATUS = 0
WHERE USER_CUSTOM08 = '001';
```

In **Data Source** section

1. **DB Type** : `Google G Suite`
2. **Authorization Code**: Enter Authorization code. Click the `Generate Google Authorization Code` button at the top, and copy and enter the code that is output after clicking the `Allow` button on the account login.
3. **DOMAIN**: When you enter a domain, only the information from that domain is synchronized. If not entered, information about all domains to which the account belongs is synchronized.
4. **VIEW TYPE**: Select the data synchronization range according to authority. Typically, `admin_view` for an account with admin privileges, otherwise `domain_public`.

In **User information** section

1. For **Table Name**, Enter `users`.
2. For **Column Name for Username**, Enter `primaryEmail`.
3. For **Column Name for Full Name**, Enter `name/fullName`.
4. For **Column Name for Department ID**, Enter `orgUnitPath`.

In **Department Information** section

1. For **Table Name**, Enter `orgunits`.
2. For **Displaying Sorted Hierarchies**, Enter `@NAMEPATH` to show based on department name.
3. For **Column Name for Department Code**, Enter `orgUnitId`.
4. For **Column Name for Department Name**, Enter `name`.
5. For **Column Name for Parent Department**, Enter `parentOrgUnitId`.
6. Click **Create** button.

> **Attention:** G Suite does not provide a password attribute when using the API, so user passwords cannot be synchronized. Therefore, separate linkage should be set. See `SAML 2.0` in: doc: *../ integrate-external*.

## 13.4.5 REST API Server

Genian ZTNA can use REST API Server as a source of user and organization information.

REST API Server synchronization allows user accounts to be created locally and used for administration or policy.

REST API Server requests are called using the HTTP GET method, and the response data format must be in JSON Object format.

The following example describes how to synchronize user information with REST API, from the application Slack.

User information in slack can be fetched through the users.list API, from URL https://slack.com/api/users.list which supports GET and POST requests. Info on how to use can be found at https://api.slack.com/methods/users.list

In ZTNA, REST API information is provided through `Swagger`.

Select REST API Server as the DB type and enter https://slack.com as the server address. Enter `/api/users.list?token=<API Token>` for the user information source. For column name, enter the path to extract values from JSON Object. See the content below, or the previous users.list help link for more examples.

### Pre-Requisites (In Slack)

- Create a Slack app with a properly privileged Slack Workspace account. Use ** Add features and functionality > Permissions **
- Obtain an access token and give it a `user:read` OAuth Scope. In our example we will use a **Bot User OAuth Access Token**
- Once these steps are completed, install the app to your Workspace. The app must be reinstalled after every configuration.

### Test the connection

In order to perform a connection test, default values must be entered for:

| ITEM | set value | Description |
|---|---|---|
| REST API Server | Server Address | Enter the server IP to call the REST API. |
| | page parameter name | Page parameter name to process multiple outputs set |
| | Page start number | Set the page start number. |
| | Page Size Parameter Name | Enter the parameter name that specifies the number |
| | | of prints on one page set. |
| | page size | Set the number of prints per page. |
| | datasource cutoff | Set when using multiple synchronization servers. |

**Note:** If the connection test does not work properly, first check whether the communication between **Policy Server** and **Synchronization Server** is normal.

### Create sync settings

1. Go to **Preferences** In the top menu Bar
2. Go to **User Authentication > Data Synchronization** in the left side panel.
3. Select **Tasks > Create** and fill out the following forms.

### General

1. For **ID**, Enter name here
2. For **Update Interval**, Select the specified time or periodic interval for synchronization.
3. For **Policy Apply**, After synchronization, select `Enabled` to reflect the changes. If you have multiple sync settings, you can set it to `Disabled` and enable only the last sync.
4. For **Environment**, Input is not required for basic synchronization tasks. However, it is used when defining variable values to be commonly referenced within a separate custom shell script executed for integration with external systems.

**Warning: Configuration Caution**: Incorrect environment variable declarations can lead to malfunctions in the integration script or system errors. Before configuration, please ensure that the variables are correctly processed within the script.

Usage Scenario: Log Level Control Used when you want to control simple operation options such as Log Level or Retry Count during external script execution.

```
export LOG_LEVEL='ERROR'
```

5. For **Query**, Enter the SQL query to be executed immediately after information synchronization is complete. This is used when secondary processing is required based on specific conditions using the synchronized information.

**Warning: Risk of Data Loss**: This feature directly affects the database. In particular, the use of `UPDATE` or `DELETE` statements may result in **irreversible data loss**.

Usage Scenario: Account Lock Processing based on Employment Status Used when you want to automatically disable the NAC account of resigned (or on-leave) employees according to the 'Employment Status' code after information synchronization.

Prerequisites 1. Create a field to manage employment status (e.g., USER_CUSTOM08) in [Settings] > [Property Management] > [Custom Fields] > [User Custom Fields]. 2. Assign the user custom field created in step 1 to [Additional Info] under [User Information] in [Information Synchronization].

Writing Example If the value of USER_CUSTOM08 is '001' (Resigned/On-leave, etc.), update USER_STATUS to '0' (Disabled).

```
UPDATE USER
SET USER_STATUS = 0
WHERE USER_CUSTOM08 = '001';
```

### Data Source

- For DB type, select REST API Server and enter the server address being used.
- Ex) `https://slack.com` for slack, `https://(policy server IP):8443` for ZTNA

1. **DB Type** : `REST API Server`
2. **Server Address** : Enter the URL of the server.
3. **Parameter Name for Page Number** : Set the page number parameter name to be sent to the server during paging processing.
4. **Start Number for Page Number** : Set the page start number during paging processing.
5. **Parameter Name for Records Size Per Page** : Set the page size parameter name to be sent to the server during paging processing.
6. **Records Size Per Page** : Set number of records to fetch per page.
7. **Data Source Name** : Set a DSN to protect against accidental data deletion during synchs.

**Note:** Steps 3-6 can be left at their default values when synching from Slack

### User Info

When entering user information sources, enter `/api/users.list?token=<API Token>` if using API Key for mutual authentication or `/api/users.list` if using API service account. * Column name enters the path to extract values from JSON Object. path is separated by `.`

- Ex) ID in case of JSON Response [ { "id": "..", "name": ".." }, { "id": "..", "name": ".." } ] Enter `id` for the column ID and `name` for the column name.
- Ex) JSON Response { "users": { "members" : [ { "id": "..", "name": ".." }, { "id": "..", "name": In case of ".." } ] } }, enter `users.members.id` for the ID column name and `users.members.name` for the name column name.

1. **Data Source** : Enter the path to query. In our case we will add our access token to the path where the user list is stored at slack.com. `/api/users.list?token=xoxb-xxxxxxxxxx-xxxxxxxxxxxxx-xxxxxxxxxxxxxxxxxxxxxxxx`
2. **Where Clause for User** : Leave blank.
3. **Column Name for Username** : Enter the path of the desired user value in JSON Object. In this example we will use `members.name` to use the first name of the Slack user.
4. **Column Name for Full Name** : Enter the path of the desired user value in JSON Object. In this example we will use `members.real_name` to use the display name of the Slack user.
5. **Department ID column name** : Enter the path of the desired user value in JSON Object. In this example we will use `members.team_id` to use the team id of the Slack user.

**Note:**

- You may synch any variable returned with any info field that Genian ZTNA supports. Example: Email addresses as Usernames (may require different permissions in data source).
- You can repeat the process show under the **User Info** section for Department, Job Title, Node, and Device information.

## 13.4.6 Testing Synchronization

1. Go to **Preferences** in the top panel
2. Go to **User Authentication > Data Synchronization** in the left Preferences panel
3. Select checkbox of desired configuration.
4. Click **Tasks > Synchronize Now**
5. You can check result through **Logs** to verify.

**Note:** Some database types can be configured with a "Data Source Name", which can prevent accidental deletion of content.If a data source name is not configured, the information from the database will be fully overwritten during the sync.

### 13.4.7 Troubleshooting

- *LDAP Search Failed - Operations Error*

## 13.5 Configuring User Authentication Options

### 13.5.1 General Options

General options for authentication criteria, device ownership, logon recovery, and restrictions can be found under **Preferences > User Authentication > User Authentication**

#### Available Options

- **Authentication Criteria**
- Select **Node** or **Device** (Mac+IP or MAC).
- **Authorized IP**
- Specify whether to automatically set Authorized IP as IP address first authenticated from. This applies when the Authorized IP in the User Management settings is blank.
- **Authorized MAC**
- Specify whether to automatically set Authorized MAC as MAC address first authenticated from. This applies when the Authorized MAC in the User Management settings is blank.
- **Automatic Ownership**
- Specify whether to automatically assign User and Department ownerships to IP and/or MAC when a user is authenticated.
- **Regex for Username**
- Enter a regular expression to validate username.
- **Hiding Username**
- Hide username under asterisks during authentication/
- **Log Out Button**
- Specify whether to display Log Out button in CWP page.
- **Find Username / Reset Password**
- Enable or disable recovery for lost username/password.
- **Verification code valid time**
- Set the validity code valid time for sms 2 factor authentication ( 2fa / mfa )
- **Displaying Authentication Info**
- Specify whether to display User Authentication Information in Agent Tray Menu and CWP page.
- **User Info for Node Info**
- Specify whether to add User Information (Name and Description) into Node Information for User Account Request approval.

### 13.5.2 Configuring Authentication Options by Single node

1. Click a node **IP Address** and select **Policy tab**
2. Select one option under **User Authentication Policy**

#### Available Options

- **Comply with Authentication Policy under Node Policy**
- **Require User Authentication (Allow All Users)**
- **Require User Authentication (Allow Specified User(s))**

### 13.5.3 Configuring Authentication Options by Group

Node Authentication policies determine when and how nodes of a given group will be required to authenticate, as well as the conditions of the process.

To configure options for authentication methods, requirements, time restrictions and logon procedure, select a node policy under **Policy > Node Policy > [Policy Name]** and scroll down to **Advanced > Authentication** in the main panel.

#### Available Options

- **Authentication Method**
- Select **Host Authentication** (Allow by node identity) or **Password Authentication**.
- For **Password Authentication** specify allowed **Authentication Sources** and Enable/Disable **2 Factor Authentication.** ( 2fa / mfa )
- **Single Sign-On Method**
- Select **Active Directory**, **External API** or **Genian API** and enter required info.
- **Auth User Group**
- Select a user group to allow for authentication from the policy member nodes.
- **Auto-Logout**
- Enable to log out users after a set time period.
- **Auto-Logout For Down Node**
- Enable to log out users after a node link status is down for a set time period.
- **Reauthentication Interval**
- Specify how often to renew authentication.
- **Session Timeout Notification**
- Specify time prior to the login session expiration that you want to notify users.
- Agent required.
- **Custom User Login Page URL**
- Specify URL for a custom user login page which will be redirected when a user clicks a Login button in CWP page.
- **Authentication at Startup**

- Specify whether to require Authentication when the computer restarts or wakes.
- Agent required. Not compatible when Single Sign-On is enabled.
- **Display Name of Username**
- Specify a display Name of Username for use on Captive Portal and Agent Authentication prompt.
- **Display Name of Password**
- Specify a display Name of Password for use on Captive Portal and Agent Authentication prompt.

## 13.6 Instant Approval of User Account Request

Genian ZTNA provide Instant Approval, a method that is automatically approved without the administrator manually approving the user account.

You can increase ease of use for guest accounts by automatically granting approval for specific uses without administrator confirmation.

### 13.6.1 Create User Account Request Purpose

Create a purpose to automatically set the authorization method when creating an account to perform user authentication in Genian ZTNA.

1. Go to **Preferences** in the top panel.
2. Select **Purpose > User** from the **Properties** column on the left.
3. Select **Create** from the **Tasks** menu.
4. In the **Options** section, set the **Approval Options > Email Approval for Guest** setting to **OFF**.
5. Set the setting value to **ON** in the lower **Instant Approval** item.
6. Click the **Save** button.

### 13.6.2 Creating and Authenticating User Accounts for Purposes Set with Instant Approval

When applying for a user account, if you select the Instant Approval set user purpose and proceed with the application, the account will be activated when the request is completed.

1. Click the **Request User Account** button on the CWP page.
2. Select the **Purpose** item as **Instant Approval set user purpose**.
3. Enter **indicates a required field** in your user account request.
4. Click the **Submit** button.
5. After checking the **Results Page**, click the **Main Page** button.
6. Click the **Login** button to perform **authentication** using the account created.

## 13.7 Use the Collection consent page when requesting a user account

In Genian ZTNA, you can use CWP to display terms and conditions for collecting information about personal information that is entered upon user account request and obtain user consent.

## 13.8 Add User Consent Page

Set the contents of the consent page to display to the user. The Agree to Collect User Information page is divided into the terms and conditions to display to the user and the collection information items that set the information to collect to the user.

1. Go to **Prefrences** in the top panel
2. Go to **Captive Web Potal > Consent Page > Privacy Policy** in the left panel
3. Click `Tasks` **> Create**
4. Enter the following items:
   - Title,Consent Page Name
   - Description,Description of the consent page
   - Node Group Exception,Node group targets that do not want to display the Agree page
   - Priority,Display order of consent pages
   - Contents,Agree Page Content
   - Type,Content creation type(Choose from HTML, Markdown, or TEXT)
   - **User Input Field,Add buttons or fields to be filled in by the user.**
     (For field generation, see the following document: *Using custom fields to enter additional information to account*)

### 13.8.1 Setting up user consent pages

In order to get user consent from the CWP page, you must first activate the user registration button and then activate the consent page.

1. Go to **Prefrences** in the top panel
2. Click the node **policy name** to which the users are assigned to accept consent.
3. Enable the User Account Request option for the Authentication Policy entry.
4. Enable the Consent Page option as well.
5. Click the `Update` button at the bottom.
6. Click the upper right `apply` button.

## 13.9 Approve User Accounts via Email

In Genian ZTNA, the user account can be approved for use by a general account (where a user account exists), not an administrator, using email.

By using the method of approval via email, you can act as an administrator by granting permission for approval to general users, not administrators.

**Note:** Mail server configuration is required to use Email Approval. Email information is required for the general user account.

### 13.9.1 Create User Account Request Purpose

Approval method is emailed to user account request, and the purpose of giving Email Approver for request to Existing User is created

1. Go to **Preferences** in the top panel.
2. Select **Purpose > User** from the **Properties** column on the left.
3. Select **Create** from the **Tasks** menu.
4. In the **Options** section, set the **Approval Options > Email Approval for Guest** setting to **ON**.
5. In the **Email Approver** item, set the setting value to **Existing User(Sponsor)**.
6. Click the **Save** button.

### 13.9.2 Approve user account requests via email

When requesting a user account, you must specify the purpose for which email approval is possible.

1. Check the **approval request email** on the email server.
2. Click the **Approve** button in the email.

## 13.10 User Account Request period setting

When requesting a User Account from Genian ZTNA, you can enter the account usage period.

It can be used for the purpose of managing visitors and outsourced personnel by setting the period of use for the account.

### 13.10.1 Creating a User Account Purpose with a set period of use

Create a purpose to receive the period of use. If you use Email Approval or Instant Approval as the approval method, please refer to the following items.

*Instant Approval of User Account Request* , *Approve User Accounts via Email*

1. Go to **Preferences** in the top panel.
2. Select **Purpose > User** from the **Properties** column on the left.
3. Select **Create** from the **Tasks** menu.

4. Under **Request Field Options**, click **Assign**.
5. Add **Expiry** item in **Request Field** window.
6. Click the **OK** button.
7. Click the **Save** button.

### 13.10.2 Setting a limit on the period of use

You can limit the period of use by changing the period setting for the purpose. If the limit date is set to 3 days, the user can enter a period of use from a minimum of 1 day to a maximum of 3 days.

1. Go to **Preferences** in the top panel.
2. Select **Purpose > User** from the **Properties** column on the left.
3. Click **New Request** in the **Field Options** section to the right of the created use.
4. Click **Expiry** in the Field Name field.
5. In **Settings**, change the **Start Date Restrictions > Period Restrictions** item from **90 days** to **3 days**.
6. Change the setting value in **Required Field** to **ON**.
7. Click the **Update** button.

CHAPTER

FOURTEEN

# CONTROLLING ENDPOINTS WITH AGENT

**Note:** This feature required Professional or Enterprise Edition

An Endpoint device is an Internet-capable computer hardware device on a TCP/IP network. This can be anything from desktop computers, laptops, smartphones, tablets, thin clients, printers or other specialized hardware.

You can control Windows and macOS, Linux endpoint devices with the Genian ZTNA Agent. When installed onto the endpoint, it then runs in the background and communicates with the Policy Server when changes to the endpoint are made. The Agent takes action with policies to manage the endpoint system information, such as the operating system, updates, applications, registry entries, and services, that aids you in detecting and dealing with anomalies on the endpoint.

## 14.1 Configuring Agent Defaults

Agent default policies determine the basic installation and operation of the agent on endpoints. Additional node specific agent settings may also be configured. See: *Configuring Agent Settings by Node Policy*

To configure agent default options, select **Preferences** on the menu bar and **Agent** in the left panel.

### 14.1.1 Installation Path

- Defines the location the agent files will be installed to. Default: %ProgramFiles%GeniGenian (Windows Only)

### 14.1.2 User Confirmation before Installing

- Determines if the installer gives a consent prompt to install agent when the installer is executed. (Windows Only)
- Select: **On**,or **Off**

### 14.1.3 Displaying Installation Progress

- Displays progress of installation. (Windows Only)
- Select: **On**, or **Off**
- If **On**, select **On**, or **Off** for installation result message.

### 14.1.4 Registering Install Information

- Select: **On**, or **Off** for displaying agent under the Programs section in Control Panel. (Windows Only)

### 14.1.5 Agent Deletion Method

- Select: **Use Authorization Code**, **Without Authorization Code**,or **Not Allowed** to designate if and how an end user can remove the agent from their endpoint.

### 14.1.6 Automatic Update Target

- Select a Network Object to receive automatic agent updates.

### 14.1.7 Service Target Group

- Specify a network object to enable the agent running.

### 14.1.8 Automatic pop-up message

- Enable to display detailed message contents in a pop-up badge, rather than only a preview.

### 14.1.9 View My Status on Tray Menu

- Select: **On**, or **Off** for Tray/ Menu Bar Agent Icon info. (Windows and OSX only)

### 14.1.10 Web Browser Type

- Select: **Internet Explorer**, **Default Browser** or **Enter Path** to set the default browser for agent popups. (Windows only)
- Enter **Path** if applicable

#### For Internet Explorer

- Select: **Enable**, or **Disable** for **Hiding Address Bar / Toolbar**
- Select window size: **Normal**, or **Maximized**
- Select **On**, or **Off** for **Display Window in Front**

### 14.1.11 Agent Custom Icon

- Upload a custom image for the tray icon. (Windows only)

### 14.1.12 KeepAlive Interval

- Specify: **Second(s)**, or **Minute(s)** for communication interval to update Agent runtime log. 5 Missed communications will define the agent as not running.

### 14.1.13 Scheduling Agent Restart

- Specify: **Minutes Hours** past computer entering sleep mode for the agent to reboot. (Windows and OSX only)

### 14.1.14 SSL Certificate

- Select: **On**, or **Off** for installing SSL Certificate from the policy server. (Windows and OSX only)

### 14.1.15 Agent UI

After the agent is installed, the agent UI is available by clicking on the icon created. (Linux only)

The Agent UI supports the following functions.

- **Message**: You can check received notification messages.
- **Notice**: You can check the announcements you received.
- **Device information**: You can check the details of the USB connected to the device.
- **Delete Agent**: You can delete an agent.
- **About**: Detailed information such as agent version is available.

## 14.2 Supported Operating Systems and Plugins

### 14.2.1 Supported Windows Plugins

| Plugin Name | Description |
|---|---|
| TcpSessionControl | Collects TCP Connection Information periodically and disables a network interface that exceeds the configured c |
| ChangeHostName | Changes the computer name. |
| IESecurityControl | Changes the way the computer manages internet connections and browser settings for Internet Explorer. |

Table 1 – continued from previous page

| Plugin Name | Description |
|---|---|
| NetIfControl | Disables a network interface when an anomaly is detected. |
| CheckValidPwd | Checks password validation policies to let users to use stronger passwords. |
| WLanControl | Controls Wireless Connection Manager options and actions. |
| GetMonitorInfo | Collects information about all monitors currently connected to the computer. |
| GetPrinterInfo | Collects information about all printers currently installed on the computer. |
| WMIInfoCollect | Uses WMI to collect the system information. |
| ScreenSaverControl | Changes lock screen and wallpaper settings to control. |
| SharedFolderControl | Collects information about the shared folders over a network and controls its settings. |
| WinSecureControl | Controls Windows security settings for Firewall, Remote Desktop and Autorun. |
| InfoSW | Collects information about all installed software on the system. |
| InfoNet | Collects information about all network interfaces and the ports detected to display in Node information. |
| InfoWin | Collects information about OS installed on the computer. |
| WinUpdate | Checks for Windows updates and executes an action on a scheduled basis. |
| InfoHW | Collects hardware information such as motherboard, memory and disk space to display in Node Information. |
| Vaccine | Collects information about the Antivirus software installed on the computer and the virus mitigation logs in real t |
| GeniAuth | Uses Genian Agent Authentication and customizes the display options. |
| PowerCtrl | Conserves energy and controls the power options of the user's computer. |
| DeployCtrl | Deploys and executes files or copies files into a specific location. |
| FileCtrl | Runs, deletes, copies, moves and renames the files on the computer. |
| ProcessCtrl | Terminates a specific process defined in Condition Settings. |
| Blank | Checks Condition Settings configured in Agent Action. |
| DeviceCtrl | Controls external device settings to disables any external devices not allowed. |
| WConMgr | Controls Wireless Connection Manager options and actions. |
| ARPCtrl | Manages ARP table to prevent from ARP spoofing. |
| UserMsg | Changes slide-out notification settings to notify users. |
| AppRemove | Uninstalls a program registered in Control Panel. |
| DNSCtrl | Controls DNS settings. |
| LanProfile | Controls the wired authentication options and actions to provide authenticated network access for the Ethernet ac |
| TrafficCtrl | Collects network traffic Information periodically and disables a network interface that exceeds the configured lim |
| MalwareDetector | Collects information to detect Malware by integrating with Insights ECO. |
| CheckSoftware | Collects information about all installed software on the system. |
| NetCtrl | Controls Windows security settings for Firewall, Remote Desktop and Autorun. |
| ZTNAClient | Controls Zero trust network access Connection Manager options and actions. |

### 14.2.2 Supported Windows

| Microsoft Windows OS (32bit/64bit) | v6.0.x |
|---|---|
| Microsoft Windows 8 | 6.0.0~ |
| Microsoft Windows 8.1 | 6.0.0~ |
| Microsoft Windows 10 | 6.0.0 |
| Microsoft Windows 11 | 6.0.0~ |
| Microsoft Windows Server 2012 | 6.0.0~ |
| Microsoft Windows Server 2016 | 6.0.0~ |
| Microsoft Windows Server 2019 | 6.0.0~ |
| Microsoft Windows Server 2022 | 6.0.24~ |
| Microsoft Windows Server 2025 | 6.0.32~ |

### 14.2.3 Supported macOS Plugins

| Plugin Name | Description | Agent Version |
|---|---|---|
| InfoOS | Collects information about OS installed on the computer. | 6.0.0~ |
| InfoHW | Collects information about hardware of motherboard, memory and disk space. | 6.0.0~ |
| InfoSW | Collects information about all installed applications on the system to display Applications in Software of Node Management. | 6.0.0~ |
| InfoNet | Collects information about all network interfaces and the open ports detected to display in Node information. | 6.0.0~ |
| InfoVaccine | Collects information about Antivirus software installed on the system. | 6.0.0~ |
| MacUpdate | Checks for macOS updates and executes an action on a scheduled basis. | 6.0.0~ |
| ProcessCtrl | Terminates a specific process defined in Condition Settings. | 6.0.0~ |
| Blank | Checks Condition Settings configured in Agent Action. | 6.0.0~ |
| GeniAuth | Uses Genian Agent Authentication and customizes the display options. | 6.0.0~ |
| SaverCtrl | Collects information about the lock screen configured and controls the configuration settings. | 6.0.0~ |
| InfoPrinter | Collects information about all printers currently installed on the computer. | 6.0.0~ |
| InfoMonitor | Collects information about all monitors currently connected to the computer. | 6.0.0~ |
| PowerCtrl | Controls the power options of the system. | 6.0.0~ |
| CheckSoftware | Collects information about all installed applications on the system to display Applications in Software of Node Management. | 6.0.0~ |
| UserMsg | Changes slide-out notification settings to notify users. | 6.0.0~ |
| WirelessCtrl | Provides information about wireless APs detected on wireless network interfaces and restricts disallowed AP connections. | 6.0.0~ |
| ARPCtrl | Perform administrative tasks on ARP tables on your PC. | 6.0.0~ |
| DeployCtrlv2 | Run the file or download it to a specific location. | 6.0.16~ |
| HostNameCtrl | Change the host name of the computer. | 6.0.0~ |
| DeviceCtrl | Controls external device settings to disables any external devices not allowed. | 6.0.0~ |

### 14.2.4 Supported macOS

| OS X/macOS | Version | v6.0 ~ |
|---|---|---|
| macOS Big Sur | 11.0(including M1) | 6.0.0~ |
| macOS Monterey | 12.0(including M1) | 6.0.0~ |
| macOS Ventura | 13.0(including M1) | 6.0.4~ |
| macOS Sonoma | 14.0(including M1) | 6.0.16~ |
| macOS Sequoia | 15.0(including M1) | 6.0.23~ |
| macOS Tahoe | 26.0(including M1) | 6.0.36~ |

### 14.2.5 Supported Linux Plugins

| Plugin Name | Description | Agent Version |
|---|---|---|
| Blank | Checks Condition Settings configured in Agent Action. | 6.0.0~ |
| InfoHW | Collects hardware information such as motherboard, memory and disk space to display in Node Information. | 6.0.0~ |
| InfoSW | Collects information about all installed software on the system. | 6.0.0~ |
| InfoNet | Collects information about all network interfaces and the open ports detected to display in Node information. | 6.0.0~ |
| InfoOS | Collects information about OS installed on the computer. | 6.0.0~ |
| NetIfCtrl | Disables a network interface when an anomaly is detected. | 6.0.0~ |
| ZTNAConManager | Controls Zero trust network access Connection Manager options and actions. | 6.0.0~ |
| UpdateOS | Checks for linux updates and report. | 6.0.0~ |
| InfoAV | Collects information about Antivirus software installed on the system. | 6.0.0~ |
| ProcessCtrl | Terminates a specific process defined in the action. | 6.0.0~ |
| ARPCtrl | Manages ARP table to prevent from ARP spoofing. | 6.0.0~ |
| DeployCtrlv2 | Executes files or downloads files into a specific location. | 6.0.0~ |
| UserMsg | Changes slide-out notification settings to notify users. | 6.0.0~ |
| InfoMonitor | Collects information about all monitors currently connected to the computer. | 6.0.0~ |
| CheckValidPwd | Checks password validation policies to let users to use stronger passwords. | 6.0.0~ |
| DeviceCtrl | Controls external device settings to disables any external devices not allowed. | 6.0.0~ |
| SharedFolderCtrl | Collects information about the shared folders over a network and controls its settings. | 6.0.0~ |
| Uninstall Programs | Removes specific uninstallable programs among Debian packages and programs installed with Snap. | 6.0.0~ |
| Transferring agent information externally | Passes information that the agent has to external programs. | 6.0.0~ |

### 14.2.6 Supported Linux

| Linux OS | Version | v6.0 ~ |
|---|---|---|
| Ubuntu | 18 ~ 24 | 6.0.5 ~ |
| Gooroom | 2 ~ 4 | 6.0.5 ~ |
| HamoniKR | 3.0 ~ 4.0 | 6.0.0 ~ |
| Hancom Gooroom | 2 ~ 3 | 6.0.5 ~ |
| Tmax Gooroom | 2, 21 | 6.0.5 ~ |
| CentOS | 8 | 6.0.34 ~ |
| CentOS Stream | 9 ~ 10 | 6.0.34 ~ |
| Rocky Linux | 8 ~ 10 | 6.0.36 ~ |
| Red Hat Enterprise Linux | 8 ~ 10 | 6.0.39 ~ |
| Oracle Linux | 8 ~ 10 | 6.0.39 ~ |

## 14.3 Configuring Agent Settings by Node Policy

Agent policies can be configured on the basis of individual node policies, which are then applied to node groups. To configure, select a node policy under **Policy > Node Policy > [Policy Name]** and scroll down to **Advanced > Agent Policy** in the main panel to access the following options:

### 14.3.1 Agent

- Specify:
- **On**, **Off**, or **Delete** to toggle agent run status or remove the agent from the node(s).
- Deleting Agent Not Running:
- Define a time frame of **Hours**, **Days**, **Weeks** or **Months** upon which to Delete the agent, if it has not connected to the policy server. Input **0** to disable this function.

### 14.3.2 Dissolvable Agent

- The Windows Dissolvable Agent is a temporary executable that is pushed to a Windows system during a scan and automatically exits after collecting info from the endpoint. Control plugins are not fully supported by the dissolvable agent. Their control functions are inactive when the agent is in dissolvable mode, but they still may be used to collect endpoint information.
- Select **On**, or **Off**

### 14.3.3 Agent Fail-safe

- Deactivates the agent after a defined a time frame of **Minutes**, **Hours**, **Days**, **Weeks** or **Months** since the agent has not been connected to the policy server.
- Select **On**, or **Off**

### 14.3.4 Tray Icon

- Toggles the appearance of the Agent Icon in the OSX Menu- Status Bar or the Windows System Tray.
- Select **On**, or **Off**

### 14.3.5 Execution Account

- Select **Computer Logon Account**, **Privileged Account**,or **Local System Account** to run the agent. Ensure the account selected has the proper permissions to perform agent actions configured under enforcement policy. See: *Controlling Windows*, *Controlling macOS*.
- **Computer Logon Account** - Runs the agent from whatever account is logged in. Use this option if you plan to deploy the Agent through Active Directory GPO, SCCM or other software distribution mechanism.
- **Privileged Account** - Select this option for multiple non administrators within a domain to self install the Agent, and configure with domain administrator credentials.
- **Local System Account** - Select this account option for root level credentials on the local machine. Best used for node policies applied to a single device. The agent must be installed by the local account you wish to use.

### 14.3.6 Policy Update Interval

- Specify a time frame of **Hours** for the agent to check the policy server for updates.
- Select between 1-4 **Hours**

### 14.3.7 Deleting Outdated Information

- Define a time frame of **Hours**, **Days**, **Weeks** or **Months** upon which to Delete the agent information, if it has not connected been updated. Input **0** to disable this function.

## 14.4 Controlling Windows

The following Agent plugins are supported on Windows endpoints.

### 14.4.1 Agent Sensor

The Agent Sensor plug-in performs basic node detection on network segments without network sensors.

The agent sensor receives information contained in packets such as DHCP, NetBIOS, UPNP, and mDNS that occur periodically on the network, but does not perform active scanning or enforcement. It is ideally used for monitoring only, and installation in networks where full sensor deployment may be inconvenient.

The agent sensor receives information contained in packets such as DHCP, NetBIOS, UPNP, and mDNS that occur periodically on the node, so that it can gather information without affecting the node. Information gathering using nmap, snmp, etc. is collected by physical sensor equipment with registered agent sensors.

- Monitor nodes in network segments where network sensors are difficult to install
- Network segment that only wants to perform node monitoring without network control

### Technical Details:

- This plug-in does not require a separate setup.
- No enforcement actions are conducted by this plugin.
- The agent-based sensor plugin communicates directly to the Policy Server but is not registered as a full Network Sensor.
- The agent-based sensor can be operated regardless of Windows login (service)
- **Agent plugin Functions:**
  - **New Node Registration:** Registers nodes based off of recieved traffic.
  - **Subnet Scanner:** Detects new nodes based on the result of ARP Request transmission for the entire subnet (C class) every 6 hours
  - **Node Health Check:** Updates the node link status by sending a ping once every 10 seconds and checking the ARP table in Windows.
  - If a node is not identified in the ARP table for 3 minutes, it is shown as having a link status of Down.
  - If a node is not identified in the ARP table for 2 minutes, a ping is sent every 10 seconds.
  - The plugin will listen on port 3871 to see if a full Network Sensor is deployed in ther network.
    - If a Full Network Sensor is detected, the agent based sensor will go into standby.
    - When multiple window sensors are operating in the same band, transmission is performed to distinguish them.

### How to use the Agent Sensor

1. Set the agent sensor band on a physical network sensor so that the agent sensor can be added as a child of that network sensor.

- Go to **System** in the top panel.
- **Select a network sensor** from the list of equipment.
- Go to the **Appliance tab** and enter the network for the agent sensor in Other Settings Item > Agent Sensor Network.

2. Assign a sensor node action to the node policy in the band where you want to use the agent sensor.

- Go to **Policy** in the top panel.
- Go to **Node Policy** in the left Policy panel.
- Click the **Default Policy** or another Policy in Node Policy window.
- Find **Agent Action**. Click **Assign.**
- Find **Agent Sensor** in the **Available** section. Select and drag it into the **Selected** section.
- Click **Add.**
- Click **Update.**

**Note:** When the plug-in is installed and operational on the agent installed on the node, a virtual agent sensor is added to the policy server.

### 14.4.2 Changing Computer Name

You can control the name of the Windows device.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Change Computer Name** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions: **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Control Method**, specify a if you would like to change the Hostname to a **User Defined** value, or a value based on the **Hostname Rule of the Node Policy**
   - If **User Defined**: enter a hostname.
2. For **Restart Options**, specify whether to Prompt or Restart.
   - **Delaying Computer Restart**, specify time to postpone a restart. (*seconds - hours*)
3. For **Agent Execution Account**, specify an account that can change a computer name from drop-down.
4. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.
7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Change Computer Name** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

**Note:** The name cannot contain all special and blank characters except the minus sign (-), and must be less than 63 bytes.

### 14.4.3 Collecting Antivirus Software Information

Policy Server communicates with the Agent to collect antivirus software information that is installed on your Windows devices.

These antiviruses can also be detected via Agentless WMI query. See: *WMI Node Info Scan*

## List of Supported Antivirus

Check all Antivirus supported with Genian ZTNA by version.

| Vendor | Product | Genian Version |
|---|---|---|
| Ahnlab | AhnLab V3 Endpoint Security | 3.5.0 |
| Ahnlab | AhnLab V3 Internet Security | 3.5.0 |
| Ahnlab | AhnLab V3 Net for Windows Server | 3.5.0 |
| Avira | Avira Antivirus Pro V15 | 5.0.3 |
| Avira | Avira Endpoint Security V15 | 5.0.3 |
| Avira | Avira Free Antivirus V15 | 5.0.3 |
| BitDefender | Bitdefender Antivirus Plus | 5.0.14 |
| BitDefender | Bitdefender Internet Security | 5.0.14 |
| BitDefender | Bitdefender Total Security | 5.0.14 |
| CrowdStrike | CrowdStrike FALCON Sensor | 5.0.29 |
| Cylance | CylancePROTECT | 5.0.24 |
| ESET | ESET Endpoint Security | 5.0.3 |
| ESET | ESET Internet Security | 5.0.3 |
| ESET | ESET Smart Security | 5.0.3 |
| ESET | ESET NOD32 Antivirus | 5.0.3 |
| Estsecurity | Estsecurity AIYak V2 V3 | 3.5.0 |
| F-Secure | F-Secure Anti-Virus | 5.0.15 |
| Hauri | Hauri ViRobot VRIS 2011 | 3.5.0 |
| Hauri | Hauri ViRobot 5.5, 7.0 | 3.5.0 |
| INCA internet | Anti-Virus/Spyware 3.0 | 4.0.11/3.5.19 |
| McAfee | McAfee VirusScan Enterprise | 4.0.23/3.5.19 |
| McAfee | McAfee Total Procetion | 5.0.24 |
| McAfee | McAfee Endpoint Security | 5.0.24 |
| Microsoft | MS Forefront | 4.0.7/3.5.1 |
| Microsoft | MS Security Essentials | 5.0.3 |
| Microsoft | MS System Center | 5.0.3 |
| Microsoft | Windows Defender | 4.0.14 |
| Panda Security | Panda Endpoint Protection Plus | 5.0.30 |
| Sophos | Endpoint | 5.0.17 |
| Sophos | Home | 5.0.17 |
| Symantec | Symantec Endpoint Protection | 4.0.2/3.5.0 |
| Trend Micro | OfficeScan | 3.5.0 |
| Virus Chaser | Virus Chaser | 4.0.2/3.5.0 |
| SentinelOne | Sentinel Agent | 6.0.34 |

## Collect Antivirus Software Information

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Antivirus Software Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Action** section:

1. For **Boolean Operator**, leave as default **OR.**
2. For **Settings**, leave the default and click **Add** button to include others if they are not listed.
3. Click **Update.**
4. Go to Node **Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action** section, click **Assign.**
7. Find **Collect Antivirus Software Information** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

### 14.4.4 Collecting Computer OS Information

The Policy Server uses the Agent collects Operating System information from Windows endpoints.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Computer OS Information** in the Agent Action window. (*Notice there are two. One for Windows, and another for MacOS*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Collect Computer OS Information** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

### 14.4.5 Collecting Hardware Information

Policy Server communicates with the Agent to collect hardware information about Windows devices.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Hardware Information** in the Agent Action window. (*Notice there are three. One for Windows,one for MacOS and another for Linux*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Plugin Settings**, adjust **CPU, Memory, and Disk Space Utilization Thresholds** based off of your network requirements.
4. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.
7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Collect Hardware Information** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

### 14.4.6 Collecting Malware Info

When running, the Agent collects information about executable files on the endpoint, including but not limited to their source, file have, and signatures. The information collected may be provided to a vendor or third party for analysis.The information collected is not provided for any purpose other than malicious code detection and analysis.

- Detection results are provided in real time.
- Results may differ from similar solutions. User/ Administrator is responsible for actions taken in response to the results.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Malware Information** in the Agent Action window.
4. Enter in **CWP message**, **Conditions**, based off of your network requirements.

Under **Consent Agreement** section:

1. Select **I Agree** from the drop down to consent to sharing endpoint data for threat analysis.

Under **Collection Exceptions** section:

1. List directories to exempt from data collection. Commonly exempted sections include antivirus quarantine folders, or other directories where known malicious files may be stored.
2. Click **Update.**

To Apply this Agent Action to a Node Policy:

1. Go to **Node Policy** in the left Policy panel.
2. Click the **[Desired Node Policy]** in Node Policy window.
3. Find **Agent Action**. Click **Assign.**
4. Find **Collect Malware Information** in the **Available** section. Select and drag it into the **Selected** section.
5. Click **Add.**
6. Click **Update.**

### 14.4.7 Collecting Monitor Information

Policy Server communicates with the Agent to collect information about the monitor that is connected to your Windows.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Monitor Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Collect Monitor Information** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.4.8 Collecting Network Information

Policy Server communicates with the Agent to collect network information on the end users Windows devices.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Network Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings**:

1. For **Traffic Utilization Change Threshold**, change the percentage for bandwidth to trigger network traffic utilization.
2. For **Update Interval**, adjust Periodic Interval. (*Seconds - hours*)
3. For **Moving Average**, adjust the moving time to be greater then the Update Interval.
4. For **Collecting Open Port Information**, turn **On** to collect open port information.
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.
7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Collect Network Information** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

### 14.4.9 Collecting Printer Information

Policy Server communicates with the Agent to collect printer information on end users Windows devices.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Printer Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

3. For **Virtual Printer Exceptions**, turn **On** to ignore printer drivers which are not connected to physical devices.
4. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
5. Click **Update.**
6. Go to **Policy > Node Policy** in the left Policy panel.
7. Click the **desired Policy ID** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Collect Printer Information** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

### 14.4.10 Collecting Software Information

Policy Server communicates with the Agent to collect software information that is running on end users Windows devices.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Software Information** in the Agent Action window. (*Notice there are two. One for Windows, and another for MacOS*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Collect Software Information** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.4.11 Collecting Windows System Information using WMI

Policy Server communicates with the Agent which uses Windows Management Instrumentation (WMI) to obtain Windows system information on end users Windows devices.

System information for domain joined machines can also be collected through agentless WMI query. See: *WMI Node Info Scan*

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Click **Tasks > Create** to create new Agent Action.
4. For **Name**, type unique name. (*e.g. WMI Identify Internal Battery*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Plugin**, select **Collect System Information Using WMI** from drop-down.
4. For **Settings: Namespace**, select appropriate Namespace from drop-down or define Namespace in: **User Defined Namespace** (*e.g. rootCIMV2*)
5. For **Settings: WMI Query**, type in optional queries separated by semicolon. (*e.g. SELECT Caption FROM Win32_Battery*)
6. For **Execution Interval**, adjust Periodic Interval. (*seconds - months*)
7. Click **Update.**
8. Go to **Node Policy** in the left Policy panel.
9. Click the **Default Policy** in Node Policy window.
10. Find **Agent Action** section, click **Assign.**
11. Find and double click newly created **Agent Action.** (*e.g. WMI Identify Internal Battery*)
12. Click **Add.**
13. Click **Update.**

#### See WMI Results

You can wait for the Policy to run on the defined schedule or you can Run Actions Now to see results immediately.

1. Click **Policy** in the top panel.
2. Go to **Node Policy** in the left Policy panel.
3. Click **Checkbox** of Default Policy.
4. Click **Tasks > Run Actions Now.** (*Wait a few minutes for this Action to run*)
5. Go to **Management > Node**, find and click on **IP** of Windows Node with Agent Installed.
6. Find and click **System** tab.

7. Find **WMI Status** section to view WMI results.

### Creating Node Group for WMI Results

Create a Node Group based off of the WMI results from the **Agent Action** created from above. This Node Group then allows you to identify and enforce policies depending on your network requirements.

1. Click **Policy** in the top panel.
2. Go to **Group > Node** in the left Policy panel.
3. Click **Tasks > Create**

Under **General** section:

1. For **Category**, Choose default or Create New. (*This allows you to categorize your Node Groups*)
2. For **ID**, type unique name. (*e.g. WMI Internal Battery Group*)
3. For **Description:** (*Brief description of what this Node Group is for*)
4. For **Status:**, select **Enabled.**

Under **Condition** section:

1. For **Boolean**, select "**AND**" or “**OR**”. (”*AND*” *all conditions have to apply.* “*OR*” *any of the conditions have to apply*)
2. For **Settings**, click **Add.** (*These are the various conditions to be applied for proper grouping*)
3. For **Options**, select **WMI.**
4. For **Operator**, select appropriate option from drop-down. (*e.g. class/property value are equal to*)
5. For **Value**, type appropriate class/property value. (*e.g. Win32_Battery/Caption, Internal Battery*)
6. Click **Add.**
7. Click **Save.**

**WMI Query Examples:**

| WMI Name | Namespace | WMI Query |
|---|---|---|
| Battery Info | rootCIMV2 | SELECT Caption FROM Win32_Battery |
| HDD Vendor | rootCIMV2 | SELECT Caption FROM Win32_DiskDrive |
| HDD Size | rootCIMV2 | SELECT Size FROM Win32_DiskDrive |
| HDD Model | rootCIMV2 | SELECT Model FROM Win32_DiskDrive |
| HDD Serial | rootCIMV2 | SELECT SerialNumber FROM Win32_DiskDrive |
| Volume Serial | rootCIMV2 | SELECT VolumeSerialNumber FROM Win32_LogicalDisk |
| Graphics Card Info | rootCIMV2 | SELECT Caption, DriverVersion FROM Win32_DisplayConfiguration |
| Graphics Card Resolution | rootCIMV2 | SELECT CurrentHorizontalResolution, CurrentVerticalResolution FROM Win32_VideoController |
| HP Driver Version | rootCIMV2 | SELECT * FROM Win32_PnPSignedDriver WHERE Devicename LIKE 'HP%' |
| NDIS Driver Version | rootCIMV2 | SELECT * FROM Win32_PnPSignedDriver WHERE Devicename LIKE 'NDIS%' |
| Printer Info | rootCIMV2 | SELECT Drivername FROM Win32_Printer |
| DHCP service | rootCIMV2 | SELECT Description, DHCPEnabled, IPEnabled FROM Win32_NetworkAdapterConfiguration |
| NIC Traffic Info | rootCIMV2 | SELECT BytesSentPersec,BytesReceivedPersec FROM Win32_PerfRawData_Tcpip_NetworkInterface |

**WMI Node Group Examples:** (*Sample of the use of Operator: Equal to or Not Equal to, and Greater than or Less than*)

| Node Group | Options | Operator | Value |
|---|---|---|---|
| WMI Internal Battery | WMI | class/property, value are equal to | Win32_Battery/Caption, Internal Battery |
| WMI HDD Size | WMI | class/property, value are less then | Win32_DiskDrive/Size, 536870912000 |

## 14.4.12 Checking Password Validation

Policy Server communicates with the Agent to collect check the strength of a windows password

### Add the Agent Action to a Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign.**
5. Find **Checking Password Validation** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

### Checking Password Validation

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Checking Password Validation** in the Agent Action window.
4. Enter in **Conditions**, optional settings.

Under **Plugin Settings:**

1. Select **On** or **Off** for:
   - **Display Account with Strong Password**: Specify whether to display an account with a strong password.
   - **Immovable Dialog Box** - Specify whether to lock Dialog Box in the center of the screen.

- The settings below may be defined for both **Logged On Users** and **Logged Off Users**.

1. For **Password Check Options**, select **None**, **Protection** (check for password), or **Strength** (Checks password against password policy. See: *Managing Users and Groups*)
   - For **Action**, select **Force Password Change** (Which will mandate a password to be added, or mandate a password is made compliant, depending on the main password check option chosen), or **Check Password Strength** (Can be selected to check password strength without additional action, regardless of the main password check option. See: *Managing Users and Groups*) .
2. For **Maximum Password Age**, Specify the period of time (*hours - months*) that a password can be used before the system requires the user to change it Enter `0` to Disable.
   - For **Expiry Notification**, Specify the period of time that users are notified before password expiration (*minutes - months*).

3. For **Username Exceptions**, Enter Username(s) to be excluded from password validation check.
4. For **Execution Interval**, adjust Periodic Interval. (*seconds - months*)
5. Click **Update.**

## 14.4.13 Inspecting TCP Connections

Policy Server communicates with the Agent to collect TCP Connection Information periodically and disables a network interface that exceeds the configured connection limits.

### Add the Agent Action to a Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign.**
5. Find **Inspect TCP Connections** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

### Inspect TCP Connections

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Inspect TCP Connections** in the Agent Action window.
4. Enter in **Conditions**, optional settings.

Under **Update Interval:**

1. For **Update Interval**, Specify the time interval to update the TCP connection information. Enter: `0` for No Update.
2. For **Connections Change Threshold**, Specify the percentage change in bandwidth to trigger TCP connection information update. (excluding LISTENING)
3. For **Connections Threshold**, Specify the number of connections to be considered as TCP connection information.

Under **Interface Control:**

1. For **Interface Control**, Specify whether to disable an interface if the connections exceed the specified limit.

Under **Interface Disabled Event Notification:**

1. For **Interface Disabled Event Notification**, Specify how to notify a user for the event of disabling an interface if the connections exceed the specified limit.
2. Click **Update.**

### 14.4.14 Controlling Instant Messaging Application

Policy Server communicates with the Agent to collect instant messaging application information on end users Windows devices. (e.g. Aim, GoogleTalk, Yahoo, MSN and more)

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Instant Messaging Application Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Action** section:

1. For **Boolean Operator**, leave as default **AND.**
2. For **Settings**, leave the default and click **Add** button to include others if they are not listed.
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Control Instant Messaging Application** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.4.15 Collecting Peer-to-peer Application Information

Policy Server communicates with the Agent to collect peer-to-peer application information on end users Windows devices. (*e.g. Torrent, Ares, BearShare, Shareaza, and more*)

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Peer-to-peer Application Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Action** section:

1. For **Boolean Operator**, leave as default **AND.**
2. For **Settings**, leave the default and click **Add** button to include others if they are not listed.
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Click **Update**

5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Collect Peer-to-peer Application Information** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.4.16 Configuring Windows Security Settings

Policy Server communicates with the Agent to configure the Windows Security Settings on end users Windows devices. You can disable Guest Accounts, turn on Windows Firewall, block specific inbound ports (e.g. UDP/5355), turn off Remote Desktop, control Autorun settings, and setup sync with NTP.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Configure Windows Security Settings** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Firewall Control**, select **Turn On** to enable Windows Firewall, and enter inbound connection Protocols/Ports for blocking.
2. For **Remote Desktop**, select **Disable** to disable to use of Remote Desktop.
3. For **Recovery Console Auto Logon** select **Disable** or **Do Nothing**
4. For **Autorun**, select **Disable** to disable autorun on external devices. (*Media, External Device, Others*)
5. For **Internet Time Synchronization**, select **Turn On** to synchronize with NTP server. Enter **IP Address** and specify **Synch Interval.**
6. For **Scheduled Task for Windows XP**, select **Disable** to control scheduled tasks for Windows XP only.
7. For **Disabling Guest Account**, turn **On** to disable the use of Guest Accounts.
8. For **Require a password on wakeup**, select **Turn On** to enable a password to be required upon wakeup.
9. For **Screen**, select an inactivity period after which to turn off the screen.
10. For **Sleep**, select an inactivity period after which to put the machine to sleep.
11. For **Turn on fast startup**, choose to **Turn on**, **Turn off**, or to **Do Nothing** (For Windows 8 and later)
12. Click **Update.**
13. Go to **Node Policy** in the left Policy panel.

14. Click the **Default Policy** in Node Policy window.
15. Find **Agent Action**. Click **Assign.**
16. Find **Configure Windows Settings** in the **Available** section. Select and drag it into the **Selected** section.
17. Click **Add.**
18. Click **Update.**

## 14.4.17 Configuring Wireless Connection Manager

Wireless Connection Manager provides convenience for wireless connection configuration. - WCM makes it easier for users to use wireless LAN than the built-in wireless connection service offered by Windows - WCM provides 802.1x authentication

Policy Server communicates with the Agent to configure Wireless Connections with auto-connect, auto-reconnect, preferring specific networks, and much more. This Agent Action requires a configured Wlan Policy for use.

### Wlan Policy

**Wlan Policies** are made up of **AP Profiles** and **Client Profiles**

They can be used along with the endpoint agent to set preferences and restrictions for accessing wireless networks.

To configure a Wlan Policy follow the steps below:

#### Creating AP Profile

For Creating AP Profile, please refer to *Configuring AP Profile for Wlan Policy*

#### Creating Client Profile

For Creating AP Profile, please refer to *Configuring Client Profile for Wlan Policy*

#### Creating Wlan Policy

1. Navigate to **Policy > Wlan Policy**.
2. Select **Tasks > Create**.
3. Enter the SSID(s) to be authorized for use.
4. Under **RADIUS Policy**, select a User group to allow for authentication.
5. Select **Client** and **AP profiles** to apply to the policy.
6. Click **Save**.

### Plugin Configuration

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Wireless Connection Manager** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **WLAN Policy**, click **Assign** to assign a WLAN Policy.
2. For **Wireless Connection Manager**, turn **On** to enable Wireless Connection Manager.
   - **Enforcing Wireless Connection Manager**, turn **On** to force the Wireless Connection Manager to run.
   - **Hiding Wireless Connection Manager for Wired**, specify whether to hide Wireless Connection Manager when a wired network is connected.
   - **Auto-Reconnect**, specify whether to automatically reconnect to a wireless network allowed with the strongest signal.
   - **Password Expiry Notification**, adjust time to allow a user to change password. (*hours - months*)
   - **Preferred Wireless Network**, specify whether the user connects to preferred wireless or wireless with strongest signal.
   - **Display Username**, use this field to display Username.
   - **Display Password**, use this field to display Password.
   - **Enabling Save Username**, turn **On** to allow user to save Username.
   - **Enabling Save Password**, turn **On** to allow user to save Password.
   - **Enabling Auto-Connect**, turn **On** to allow the latest wireless network to be connected automatically.
   - **Window Image**, click **Upload** to load a BMP file for the dialog box.
   - **Window Color**, specify a color for the dialog box.
   - **Font Color**, specify a color for the text in the dialog box.
   - **Contents for Window**, type to enter contents in the dialog box.
   - **HTML**, turn **On** to use HTML for contents to be displayed in the dialog box.
   - **Program at Log On**, click **Add** to add a Program to launch when user logs in. Specify Path or CLI parameter.
3. If **Wireless Connection Manager** Option set **Off**, Installed Wireless Connection Manager application will be removed.
   - if **Wireless Connection Manager** Action Policy is Disabled or removed on the applied Node Policy, Installed Wireless Connection Manager application will be removed also.
4. Click **Update**

5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action** and Click **Assign**
8. Find **Wireless Connection Manager** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add**
10. Click **Update**

## 14.4.18 Configuring 802.1x Wired Authentication

802.1x is an IEEE Standard Switch-Port Authentication which provides assurance that a person behind an Endpoint Device is who they claim to be. In the wired environment, this is a physical port on a switch. In a wireless environment, it is an association with an Access Point(AP).In Port-Based Authentication, an Endpoint Device attempting to connect to a network (supplicant) will attempt to connect to an access point (authenticator)which will request authentication using EAP messages before communication with any other internal network devices can start. You can configure the Policy Server to authenticate users access through 802.1x.

### Step 1. Create Node Group for Authentication by 802.1x

1. Go to **Policy** in top panel.
2. Go to **Group > Node** in the left Policy panel.
3. Click **Tasks > Create New Group for Policy**
4. Enter **ID** as **802.1x Authentication.**
5. Find **Condition** section in the Node Group window. Click **Add.**
6. Enter in the Following:
   - Criteria: **IP**
   - Operator: **is one of subnet**
   - Value: **(Network Subnet)**
7. Click **Save.**
8. Click **Apply** in the top right. Click **Close**.

### Step 2. Create Node Policy for 802.1x Authentication

1. Go to **Policy** in top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click **Tasks > Create**. Complete steps in **Node Policy Wizard.**
4. On **General** tab. Enter **ID** as **802.1x Authentication.**
5. On **Node Group** tab. Select **802.1x Authentication** Node Group and move it to **Selected** column.
6. On **Policy Preferences** tab. Enter in **desired Options.**
7. On **Agent Action** tab. Select **Configuring 802.1X Wired Authentication** and move to **Selected** column.
8. On **Anomaly Definition** tab. (*Nothing required on this tab*)

9. Click **Finish.**
10. Click **Apply** in the top right. Click Close.

### Step 3. Configure 802.1X Wired Authentication Plugin

1. Go to **Policy** in top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Configuring 802.1X Wired Authentication.**
4. Add **Conditions** and **Agent Actions.**
5. Click **Update.**
6. Click **Apply** in the top right. Click Close.

(*Steps below are optional to use an existing Node Policy if you prefer not to create a new one*)

### Step 4. Assign Agent Action to Node Policy

1. Go to **Policy** in top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Find and click **Node Policy name.**
4. Find **Agent Action** section. Click **Assign.**
5. Locate **Configuring 802.1X Wired Authentication** and move to **Selected** column.
6. Click **Add.**
7. Click **Apply** in the top right. Click Close.

### Remove Agent Action from Node Policy

1. Go to **Policy** in top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Find and click **Node Policy name.**
4. Find **Agent Action** section. Locate **Configuring 802.1X Wired Authentication** and click **Delete** far right.
5. Click **Apply** in the top right. Click Close.

## 14.4.19 Authenticate User Using Genian Agent

Policy Server communicates with the Agent to authenticate users on windows devices.

### Node Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. The authentication method must be selected as 'User Authentication' before agent authentication can be used on the endpoint.
4. Select two-step authentication as needed.
   - See *2-Step Authentication*

### Add the Agent Action to a Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign**.
5. Find **Authenticate User Using Genian Agent** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

### Authenticate User Using Genian Agent

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Authenticate User Using Genian Agent** in the Agent Action window.
4. Enter in **Conditions**, optional settings.

Under **Agent Authentication Dialog Box Design:**

1. For **Window Image**, Specify an image for the Agent authentication dialog box.
2. For **Displaying Titlebar**, Specify whether to display a title bar on the Agent authentication dialog box.
3. For **Dialog Box Color**, Specify a dialog box background color.
4. For **Font Color**, Specify a font color.
5. For **Help Message**, Specify a Help Message.
6. For **URL Button**, Specify a link to embed in the authentication window, and a button caption.
7. For **Login Button Background Color**, Specify a Login button background color.
8. For **Login Button Font Color**, Specify a Login button font color.

Under **Miscellaneous:**

1. For **Authentication Enforcement**, Specify whether to enforce an authentication by disabling the close action for the Agent Authentication dialog box.
2. For **Program Run after Authentication**, Add a program that is run after a user is successfully authenticated.

<<<<<<< .working #. Click **Update.** ||||||| .merge-left.r141338

[ Settings ]

| Item Name | Setting Item | Description | Remarks |
|---|---|---|---|
| File Path | Enter target file path | Specify the file path to which information will be delivered | %SystemDrive% "Windows installation drive" Ex) "C:\\" |
| | | | %WinDir% "Windows installation folder" Ex) "C:\Windows" |
| | | | %SystemDir% "Windows system folder" Ex) "C:\Windows\System32" |
| | | | %ProgramFiles% "Windows program installation folder" Ex) "C:\Program Files" |
| | | | %UserDir% "Windows user folder" Ex) "C:\Documents and Settings\Administrator" |
| | | | %Temp% "Windows temporary folder" Ex) "C:\Documents and Settings\Administrator\Local Settings\Temp" |
| | | | %TempInternet% "Temporary internet files folder" Ex) "C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files" |
| Run Options | Enter file run options | Options to use when running the file | Option "{AUTH_ID}" will be replaced with input ID, " {AUTH_PWD}" with input password |
| Encryption Method | None | Encrypt the run options when executing the file | When using an encryption option other than BASE64, it will be additionally encoded as BASE64 |
| | Base64 | | |
| | AES | | |
| | Blowfish | | |
| | CAST | | |
| | SEED | | |
| Encryption Key | Enter key to use for encryption | Enter the encryption key if required by the encryption method | Use only the key length required by the encryption method |
| | | | If the entered key is short, the rest will be filled with 0 |
| | | | The initialization vector value is set to 0 |

1. Click the Add button under **File Path** to add the file information to be executed after authentication, then enter the file path.
2. Enter the **Run Options**.
3. Select the **Encryption Method**.
4. Enter **the Encryption Key**.
5. Select **the Encryption Target**.
6. Click the **Add** button.

- If there are additional files to be executed after authentication, click the **Add** button to add them.
- To modify the options for a file to be executed after authentication, click the **file path** of the corresponding item to edit it.
- Click the **Modify** button at the bottom to complete the action settings.

1. Go to **Policy > Node Policy** in the left Policy panel.
2. Click the **desired Policy ID** in Node Policy window.
3. Find Agent Action. Click Assign.
4. Find **Authenticate User Using Genian Agent** in the **Available** section. Select and drag it into the **Selected** section.

5. Click **Add.**
6. Click **Update.**=======

   [ Settings ]

| Item Name | Setting Item | Description | Remarks |
|---|---|---|---|
| File Path | Enter target file path | Specify the file path to which information will be delivered | File Path Macro Options |
| Run Options | Enter file run options | Options to use when running the file | Option "{AUTH_ID}" will be replaced with input ID, "{AUTH_PWD}" with input password |
| Encryption Method | None | Encrypt the run options when executing the file | When using an encryption option other than BASE64, it will be additionally encoded as BASE64 |
| | Base64 | | |
| | AES | | |
| | Blowfish | | |
| | CAST | | |
| | SEED | | |
| Encryption Key | Enter key to use for encryption | Enter the encryption key if required by the encryption method | Use only the key length required by the encryption method |
| | | | If the entered key is short, the rest will be filled with 0 |
| | | | The initialization vector value is set to 0 |

1. Click the Add button under **File Path** to add the file information to be executed after authentication, then enter the file path.
2. Enter the **Run Options**.
3. Select the **Encryption Method**.
4. Enter **the Encryption Key**.
5. Select **the Encryption Target**.
6. Click the **Add** button.

- If there are additional files to be executed after authentication, click the **Add** button to add them.
- To modify the options for a file to be executed after authentication, click the **file path** of the corresponding item to edit it.
- Click the **Modify** button at the bottom to complete the action settings.

1. Go to **Policy > Node Policy** in the left Policy panel.
2. Click the **desired Policy ID** in Node Policy window.
3. Find Agent Action. Click Assign.
4. Find **Authenticate User Using Genian Agent** in the **Available** section. Select and drag it into the **Selected** section.
5. Click **Add.**
6. Click **Update.**>>>>>>> .merge-right.r141339

### 14.4.20 Controlling Antivirus Software Settings

Policy Server communicates with the Agent to collect information on the Antivirus Software installed on end users Windows devices so you can control scans, and force updates.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Antivirus Software Settings** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value.**

Under **Plugin Settings** section:

1. For **Scheduled Antivirus Software Scan**, adjust frequency to collect information. (*Seconds - hours*)
2. For **Real-time Scan Off Events Exceptions**, specify the amount of times for Off Events to not be reported.
3. For **Antivirus Software Integration**, turn **On** to integrate with other Antivirus Software.
    - **Supported AV**
    - Ahnlab V3
    - Checkpoint Endpoint Security
    - ESTsoft Alyak
    - Hauri Virobot
    - INCA nProtect
    - Trend Micro APEX One
    - **Generating Mitigation Logs**, select **Generate Logs or Generate Error Logs** to generate mitigation logs.
    - **Period for Duplicate Logs Exception**, adjust time to exclude duplicate logs. (*Minutes - hours*)
    - **Real-time Scan Enforcement**, select **Off** to disable real-time scanning.
    - **Force Scan**, adjust how often to Force Scan. (*hours - months. Enter 0 to not enforce*)
    - **Scan Type**, select between **Full or Quick Scan.**
    - **Hiding Scanner**, turn **On** to hide the virus scan window from user.
    - **Force Update**, adjust how often to Force Update. (*hours - months*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Control Antivirus Software Settings** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**

10. Click **Update.**

### 14.4.21 Control Internet Explorer Security Settings

You can control the Security Settings of Internet Explorer on end users Windows devices. You can configure the options under General, Security, Content, and Connections tabs, as well as Add-Ons. Additionally, you can change browser settings using Add-on Controls.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Internet Explorer Security Settings** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value.**

Under **Plugin Settings** section:

1. For **Internet Options General:**
   - **Home Page**, specify a home page or leave blank to not control.
   - **Empty Temporary Internet Files Folder**, select **Enforce** to delete all the temporary internet files stored during the session.
2. For **Internet Options Security:**
   - **Downloading Unsigned ActiveX Controls**, select **Disable** to not download unsigned ActiveX controls.
   - **Automatic Prompting for ActiveX Controls**, select **Disable** to disable the automatic prompting notifications.
   - **Automatic Prompting for File Downloads**, select **Disable** to disable the automatic prompting for download attempts.
   - **Blocking Pop-up**, select **Enforce** to prevent most pop-up windows from appearing.
   - **Trusted Sites**, turn **On** to add or remove Trusted Sites. Also can **Enable** and **Disable Server Verifications.**
3. For **Internet Options Connections:**
   - **Proxy Server**, specify whether to use or how to use a proxy server for User LAN. (*These settings will not apply to dial-up or VPN*)
     - **Do Not Use**, does not utilize the **Proxy Server.**
     - **Use Proxy Server**, add Address Port, enable optional Bypassing Proxy Server, enter in exceptions.
     - **Configure Advanced Settings**, enter HTTP, Secure, FTP, Socks Ports. Enable optional Bypassing Proxy Server, enter in exceptions.
4. For **Internet Options Content:**
   - **AutoComplete for Forms**, select **Disable** to prevent auto completion of forms.
5. For **Add-on Controls:**

- **Deleting Unused ActiveX Control**, turn **On** to delete unused ActiveX Controls installed.
- **Removing Toolbar**, turn **On** to remove Toolbar.
- **Removing Browser Helper Object**, turn **On** to remove Browser Helper Object.
- **Exceptions**, type name of Add-ons to not be removed.

6. Click **Update.**
7. Go to **Node Policy** in the left Policy panel.
8. Click the **Default Policy** in Node Policy window.
9. Find **Agent Action**. Click **Assign.**
10. Find **Control Internet Explorer Security Settings** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**
12. Click **Update.**

## 14.4.22 Controlling Network Interface

Provides the functionality to disable interfaces when a risk event occurs. This feature is part of the various control methods offered by ZTNA, specifically the interface control functionality.

- Administrators can define various conditions as policies to control the network interfaces of endpoints.

You can configure endpoint users' Windows devices to disable wired, wireless, bridge, and promiscuous modes. Additionally, custom messages displayed in pop-ups can notify users of events where interfaces are disabled.

### Network Interface Control Options Configuration

1. **Block by Type**: Specify the type of network to disable (*Wired, Wireless, or All*).
2. **Default Device Exception**: When set to "On," network devices capable of communicating with the policy server are excluded from being blocked.
3. **Bridge Blocking**: When set to "On," forces bridge interfaces to be disabled, regardless of the Default Device Exception option.
4. **Promiscuous Blocking**: When set to "On," forces promiscuous interfaces to be disabled, regardless of the Default Device Exception option.
5. **Block Notifications**: Sends messages to users for interface block events via options such as (*Custom User Message or Agent Pop-Up*).
6. **Internet Connection Sharing**: Disables the Internet Connection Sharing property of the interface.
7. **IPv6**: Disables the IPv6 property of the interface.
8. **Wi-Fi Random Hardware Address**: Disables the randomized hardware address feature for wireless interfaces.
   - **Control Method**: Selecting 'Change Value Only' applies the value change, requiring a reboot. Selecting 'Apply Immediately' restarts the network interface, which may disconnect wireless network connections.
   - **Notification Options**: Specify the notification method based on the 'Control Method'. Choosing 'No Notification' under 'Apply Immediately' will restart the network interface immediately after configuration changes.
   - **Application Delay**: When 'User Notification' is selected under 'Apply Immediately,' you can configure the time to display the notification before immediate application.

### Configuring Network Interface Control Policies via Node Policies

1. Navigate to the **Policy** section in the top menu.
2. Go to **Policy > Node Policy > Node Action** in the left menu.
3. In the Node Action Management window, find and click **Interface Control**.
4. Configure the necessary options in the **Plugin Settings** section.
5. Navigate to **Policy > Node Policy** in the left menu.
6. Click the node policy to which you want to apply the interface control policy.
7. Find **Node Action Settings** and click **Assign**.
8. Drag **Interface Control** from **Available** to the **Selected** section.
9. Click the **Add** button.
10. Click the **Modify** button.
11. Click the **Apply Policy Changes** button in the top-right corner.

### Configuring Network Interface Control Policies via Control Policies

**Step 1. Create a Target Node Group**

1. Navigate to the **Policy** section in the top menu.
2. Go to **Group > Node** in the left menu.
3. Click **Select Action > Create**.
4. Click the **Add** button.
5. Set the conditions for the target and click **Add**.
6. Click the **Create** button.

**Step 2. Create a Control Action**

1. Go to **Policy > Control Policy > Control Action** in the left menu.
2. Click **Select Action > Create**.
3. Select the **Interface Control** plugin in the Plugin Selection section.
4. Configure the **Conditions** and options.
5. Click the **Create** button.

**Step 3. Create a Control Policy**

1. Go to **Policy > Control Policy > Control Policy** in the left menu.
2. Click **Select Action > Create**, and complete the **Control Policy Wizard**.
3. In the **Policy Default Settings** tab, enter the **Policy ID** to use.
4. In the **Node Group Settings** tab, select the **newly added node group** and move it to the **Selected** section.
5. Configure the desired options in the **Permission Assignment** and **Control Options** tabs.
6. In the **Control Action Settings** tab, find the **created control action** and move it to the **Selected** section.
7. Click the **Finish** button.
8. Click the **Apply Policy Changes** button in the top-right corner.

### 14.4.23 Controlling Network Traffic

Policy Server communicates with the Agent to collect TCP Connection Information periodically and disables a network interface that exceeds the configured connection limits.

#### Add the Agent Action to a Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign.**
5. Find **Controlling Network Traffic** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

#### Controlling Network Traffic

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Controlling Network Traffic** in the Agent Action window.
4. Enter in **Conditions**, optional settings.

Under **Network Traffic Control:**

1. For **Update Interval**, Specify the time interval to update the network traffic information.
2. For **Total Threshold**, Specify the total traffic for its limit.
3. For **Incoming Threshold**, Specify the Incoming traffic for its limit.
4. For **Outgoing Threshold**, Specify the Outgoing traffic for its limit.

Under **Notification:**

1. For **Interface Disabled Event Notification**, Specify how to notify a user for the event of disabling an interface if the connections exceed the specified limit.
2. Click **Update.**

### 14.4.24 Control Windows Firewall

When you use the **Enable automatic rule settings on plug-in assignment option.**
**Windows Firewall outbound rule is set** with the **permission object information of the enforcement policy** to which the node belongs.
Additional Windows Firewall restrictions can be configured in the Agent Plugin settings.

### Configure Network Control Options

1. **Notification** : Prompts the user for pop-up when setting up automatic rules.
2. **Message** : Enter the contents of the pop-up message when setting up the automatic rule.
3. **Custom Rule** : Set Windows Firewall rules yourself.
4. **Using FailSafe** : Stop the plug-in if it cannot connect to the Policy Server.

### Add Agent Action to a Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Windows Firewall** in the Agent Action Window.
4. Add **Conditions** and **Agent Actions**.
5. Go to **Policy > Node Policy** in the left Policy panel.
6. Find and Click the **Node policy** to configure the network blocking policy.
7. Find **Agent Action** section. Click **Assign**.
8. Locate **Control Windows Firewall** and move to **Selected** column.
9. Click **Add**.
10. Click **Apply** in the top right. Click Close.

### Configure Network Blocking Policies in Enforcement Policy

**Step 1. Create Agent Action For Enforcement Policy**

1. Go to **Policy** in the top panel.
2. Go to **Enforcement Policy > Agent Action** in the left panel.
3. Go to **Tasks > Create**.

Under **General**

1. For **ID**, type unique name.
2. For **Description**.(*Brief description of what this Node Group is for*).
3. Find **Agent Action** section and configure the following options:
   - **OS Type** (*Windows*)
   - **Condition** (*Set the operating conditions*)
   - **Plugin** (*Network Control*)
   - **Settings** (*Set user notifications and custom rules*)
   - **Language**
   - **OS Edition**
4. Click **Create**

5. Click **Apply** in top right corner.

**Note:** Using the agent action in enforcement policy is an optional usage of the agent action, and not actually required.

**Step 2. Create Enforcement Policy**

1. Go to **Policy** in the top panel.
2. Go to **Policy > Enforcement Policy** in the left Policy panel.
3. Click **Tasks > Create**.
4. **Action** tab click **Next**
5. **General** tab create an **ID** and enter brief **Description** to identify what the Policy does(*Prioity stays as default. Status should be Enabled*) Click **Next**.
6. **Node Group** tab select the **Node Group** that was created, move to **Selected** section and Click **Next**.
7. **Permission** tab select **Available Permission** and move to **Selected** and click **Next**
8. **Redirection Action** tab is optiuonal to set **CWP** and **Switch Block options**. Click **Next**.
9. **Agent Action** tab is **optional** to add **Agent Action**. Click **Finish**.

### Internet Kill Switch

This feature automatically blocks general internet traffic on the endpoint when the VPN tunnel is abnormal or disconnected, preventing data/IP leaks.

- Ensures forced VPN connection when used with the Always-On option of the ZTNA Connection Manager action.

For instructions on using the ZTNA Connection Manager, refer to the *ZTNA-Client* document.

### Configuration Method

Assign the minimum policy required to connect to the VPN. When the Internet Kill Switch setting is On, all internet traffic is blocked, and it operates in a WhiteList manner.

1. Go to **Policy** in the top menu.
2. Go to **Policy > Node Policy** in the left policy menu.
3. Click the Node Policy to which you want to apply the Internet Kill Switch.
4. In the **Agent Action** section, assign the **Control Windows Firewall** node action.
5. Enable the **Internet Kill Switch** option.

When using ZTNA-Client, assign the minimum policy as follows.

| Direction | Program | Local IP | Remote IP | Protocol |
|---|---|---|---|---|
| Outbound | Any | Any | ZTNA Gateway IP or Domain | TCP, Local Port: Any, Remote Port: 1194 |

## 14.4.25 Controlling WLAN

Policy Server communicates with the Agent to collect SSID information. You can control the WLAN by blocking unauthorized SSIDs, and message users with pop-up notifications.

### Wireless LAN management environment setting

You can set items to increase the accuracy of the collected data related to the wireless network.

1. Go to **Preferences > General** from the top panel.
2. Click **WLAN** in the left menu.

| Item | Explanation | Reference |
|---|---|---|
| AP Down Detection | Specify the period of time an AP is no longer detected to display as DOWN. | |
| AP Deletion | Specify the period of time an AP is no longer detected to delete the AP. | |
| Connection History Deletion | Specify the period of time an AP is no longer connected to delete the connection history. | |
| Internal AP detection | Set the method to detect the AP location. | |

### Plugin setting

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control WLAN** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **SSID Information Scope**, collects information about Detected SSIDs from a WLAN Interface and Connected SSIDs to a WLAN Interface.
2. For **Collecting Connections History**, turn **On** to collect information about the wireless connection history.
   - **Time Range for Daily Update**, specify the time range to update the wireless connection history. (*e.g. 0:00-23:59*)
   - **Attempts**, specify number of days to ry and collect connections history. (*If the info cannot be sent, it will update on startup*)
   - **Duration**, specify the time duration in hours for the collected connections history.
3. For **Disabling Wireless Connection**, specify whether to disable connections to non-approved SSID(s).

- **How to Define Allowed SSIDs**, select how to define SSIDs to be allowed. (*Selecting WLAN Group, Entering SSIDs, Using Regular Expression*)
- **Allowed WLAN Group**, select a WLAN Group to be allowed from drop-down.
- **Delay**, specify the time of how long to wait before disabling connection. (*seconds - minutes*)
- **Disabled Connection Notification and Resolution**, specify whether to notify a user and how to resolve the disabled connection from drop-down.
- **Auto-Connect to Allowed SSIDs**, specify whether to automatically connect to SSIDs allowed. (*Windows Vista or above required*)

4. For **Disabling AP Mode**, specify whether to disable AP mode such as SoftAP or Ad-hoc for wireless network interface.
   - **Interface Disabled Event Notification**, turn **On** to notify a user for the wireless AP mode disabled.
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.
7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Control WLAN** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

### 14.4.26 Controlling DNS

You can control DNS to obtain DNS automatically or assign DNS manually to point to a specific DNS server. You can also add and remove entries within the devices Host File.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control DNS** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **DNS Configuration**, select to obtain DNS automatically, to enter DNS manually, or Use management sensor's address.
   - Use management sensor's address - Uses the default DNS settings with sensor addresses.

   This requires the **Malicious Domain Blocking** in **System > System Management** to be active.
4. For **Editing Hosts File**, turn **On** to add or remove hosts in the Hosts file.
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.

7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Control DNS** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

### 14.4.27 Controlling External Device

- External devices are all devices that can be connected to the Windows system.
- You can find in Device Manager such as USB flash drives, USB disk drives, external USB hard drives, printers, keyboards, mice, and more.
- You can control an external device by disabling or removing the external device so that it can request approval for a set period of time.
- (*External device can be any device found in Device Manager that knows the class name and vendor name. For example, class name = "Universal Serial Bus Controller" / device name = "USB Mass Storage Device"*) )

#### Step 1. Create Device Group

- A device group is a function that defines a set of devices required for control. It can be used for blocking or exception on the policy.

1. Go to **Policy** in the top panel.
2. Go to **External Device Group** in the left Policy panel.
3. Click **Tasks > Create.**
4. Find **General** section enter unique **ID name.** (*e.g. "USB Storage Devices"*)
5. Find **Settings** section enter the following:
   - **Class Name**: "**Some-Name**" found in Device Manager. (*e.g. Universal Serial Bus controllers*)
   - **Device Name**: "**Some-Vendor-Name**" found in Device Manager Details. (*e.g. USB Mass Storage Device*)
   - **Device Description**: "**Description of device**" found in Device Manager Details.
   - **Removable Device**: Select option for device removable properties.
   - **USB Vendor**: Specify USB Vendor name.
   - **USB Model**: Specify USB Model name.
   - **USB Serial No.**: Specify USB Serial Number.

   **Note:** Conditions must be defined in accordance with the language settings of the endpoints operating system.

6. Click **Add.**
7. Click **Save.**

**Configuration Examples :**

| Device Type | Class Name | Name |
|---|---|---|
| External Storage | Universal Serial Bus controllers | USB Mass Storage Device |
| | Storage controllers | USB Attached SCSI (UAS) Mass Storage Device |
| | Portable Devices | * |
| Optical Device | DVD/CD-ROM drives | * |
| Printer | Printers | * |

## Step 2. Create External Device Policy

- Control External Device Policy defines the device groups to block or allow the target to perform device control.
- When the plugin is uploaded, the device policy for the basic output device is provided as a template. (Device Control Policy ID: Data Leakage Prevention)

1. Go to **Policy** in the top panel.
2. Go to **Policy > External Device Policy** in the left Policy panel.
3. Click **Tasks > Create**
4. Find **General** section enter unique **ID name.** (*e.g. "USB Storage Policy"*)
5. Find **Node Group** section click **Assign** and choose **Node Group**
6. Find **External Devices** section click **Assign** and choose **USB Storage Devices.** (You can select **Default Device Group** below.)
7. Click **Save.**
8. Click **Apply.**

**External Device Exceptions :**

| | |
|---|---|
| **Bluetooth** | • Devices in Bluetooth class |
| **CD/DVD/Floppy** | • Devices in CD-ROM, Floppy Disk Drive Class |
| **Local Printer** | • Printer connected directly to the local PC (removes devices belonging to printer class)<br>• Remove the device because the local printer can print out even if it is "disabled" in the device list. |
| **USB Disk** | • USB type storage device (a disk drive whose instance path starts with 'USBSTOR') |
| **USB Network Adapter** | • Network adapter connected via a USB port (network adapter whose instance path in the device properties starts with 'USB') |
| **USB Tethering** | • Network adapter connected via USB cable to the mobile device (network adapter with service property usbrndis or Netaapl)<br>• If you are connected via Android, the network adapter uses the usbrndis service, and the iPhone uses the Netaapl service. |
| **Wireless Network Adapter** | • Wireless Network Card Device |

1. If there is exception devices, you can create an exception group and assign it to **External Device Exceptions** like Step.1.
2. Click the **Create** button.

### Step 3. Configure Control External Device Plugin

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control External Device.**
4. Find **Agent Action > Control Methods** section and choose to **Disable** or **Uninstall.**
5. Click **Update.**

### Step 4. Enable Agent Action on Node Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign.**
5. Find **Control External Device** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

## 14.4.28 Update Windows

Genian ZTNA supports patching of Windows devices using the Agent Action "Update Windows". Policy Server pulls down the latest Windows Updates and Patches periodically to help keep your endpoint devices current. With the Agent installed on the endpoints, you can control whether they are getting updates and how often.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Update Windows** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value.**

Under **Plugin Settings** section:

1. For **Windows Update Settings**, select a Windows Update Setting from drop-down, Or click + to create an Update Setting.
2. For **Scheduled Check**, specify whether to check for updates on a scheduled basis.
   - **Periodic Interval**, adjust the time interval to check for updates. (*hours - months*)
3. For **Operation Mode**, specify whether to check for updates or install the updates.
4. For **Scheduled Installation**, specify whether to install the updates on a scheduled basis.
5. For **Restart Options**, specify whether to Do Nothing, Prompt or Restart.
6. For **Automatic Update**, specify timing, download and installation preferences for automatic updates.
7. Click **Update.**
8. Go to **Node Policy** in the left Policy panel.
9. Click the **Default Policy** in Node Policy window.
10. Find **Agent Action**. Click **Assign.**
11. Find **Update Windows** in the **Available** section. Select and drag it into the **Selected** section.

12. Specify a **Fail-Safe** setting for the Agent when it is disconnected from the Policy Server. Choose either the **Fail-Safe** settings from the endpoints **Node Policy** or create a unique setting for the Agent action.
13. Click **Add.**
14. Click **Update.**
15. Click **Apply** in top right corner.

### Create New Windows Updates For Specific OS or Patches

1. Go to **Policy** in top panel.
2. Go to **Node Policy > Agent Action > Windows Update** in the left Policy panel.
3. Click **Tasks > Create.**

Under **General** and **Automatic Approval Options.**

1. For **ID**, type in unique name.
2. For **Description**, type in brief description.
3. For **Products**, (*Select ones that apply, or All*)
4. For **Classifications**, (*Select ones that apply, or All*)
5. Click **Create.**
6. Click **Apply** in top right corner.

or

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Update Windows** in the Agent Action window.
4. Find **Agent Action: Windows Update Settings** section and click **Edit.**

Under **General** and **Automatic Approval Options.**

1. For **ID**, type in unique name.
2. For **Description**, type in brief description.
3. For **Products**, (*Select ones that apply, or All*)
4. For **Classifications**, (*Select ones that apply, or All*)
5. Click **Create.**
6. Click **Apply** in top right corner.

(*To delete Windows Updates that were created and no longer used go to Policy > Node Policy > Agent Action > Windows Update > click Checkbox of desired update > Tasks > Delete*)

### Configuring GenianSyncer Software

GenianSyncer Software is designed to get Microsoft Updates and Patches from Microsoft website and sync with a Policy Server that cannot access the internet. GenianSyncer Software gets installed on a Windows machine to be able to download Microsoft Updates and Patches from the Microsoft website and be used as an internal repository. You can then set up the Policy Server to periodically sync with the Windows Machine to proxy to endpoint devices using the "Update Windows" Agent Action.

### To Download and Install GenianSyncer Software

1. Contact **Genians** to get **GenianSyncer Software.**
2. **Download GenianSyncer.zip.**
3. **Unzip GenianSyncer.zip.**
4. **Run GenianSyncer.exe.** (*New dialog window will appear*)
5. Click **Get Started** in new GenianSyncer dialog window. (*New dialog window will appear*)
6. Enter **Policy Server Address.**
7. Update **Options.** (*You can specify Classifications and Products to narrow down the scope of the files you will download*)
8. **Specify a folder to Download to** by clicking the **three dotted icon.**
9. Click **Register License** to activate a GenianSyncer.
   - **Download.** (*e.g. C:#Program Files [x86]#Geni#GenianSyncer*)
   - Click **Upload License** File.
   - Select **License.**
   - Enter **Genian Data URL.** (*e.g. https://geniupdate.geninetworks.com/geniupdate/v###.php*)
     - **How To Find Genian URL?**
     - Login to **Policy Server CLI.**
     - **cat /disk/data/system/logs/centerd | grep geniupdate.geninetworks.com** (*e.g. https://geniupdate.geninetworks.com/geniupdate/v450.php*)
     - Copy this **URL** into **Genian Data URL.**
     - Exit **Policy Server CLI.**
   - Select **Speed** option. (*You can limit the upload or download speed by specifying the Maximum speed*)
   - Click **OK.** (*New dialog window will appear*)
10. Click **Download From Policy Server** to access the Policy Server.
11. Enter a **Policy Server IP Address** or **Hostname**. Then enter **Username** and **Password** and click **OK.**
12. Click on **Download From Internet** to download the files from Microsoft. (*This must be done upon the first time of setting this up*)
13. Click **Upload To Policy Server** to upload the updates and patch files to the Policy Server.
14. Enter a **Policy Server IP Address** or **Hostname**. Then enter **Username** and **Password** and click **OK.**
15. **No uploaded files found** (*If "No uploaded files found. Would you like to upload the GENIAN DATA?") Click **OK.**

16. Click **OK** when files have been uploaded to the Policy Server successfully.

#### To Verify Updates and Patches Uploaded Successfully

1. Go to **Policy** in the top panel.
2. Go to **Node Policy > Agent Action > Windows Update** in the left Policy panel.
3. Click the **desired Update name** in Windows Update Settings window.
4. Find and click **Update** tab. (*You will see the new Updates and Patches*)

#### To Configure Update Service Settings

(*This is instructing the Agent to look for the Updates and Patches from the Policy Server versus the internet*)

1. Go to **Preferences** in the top panel.
2. Go to **General > Agent > Update Service** in the left Preferences panel.
3. Find **Windows Update: Check for Updates** section. Select **Local Repository.**
4. Click **Update.**

#### To Configure Appliance Settings

(*This is instructing the Policy Server to Proxy Updates and Patches to Agents*)

1. Go to **System** in the top panel.
2. Go to **System, click Policy Server IP Address > Appliance** tab.
3. Find **Proxy for Windows Updates** section. Select **On to Proxy Services.**
4. Click **Update.**

### 14.4.29 Shut Down System

You can control the power options (e.g. Sleep, Restart, and Shutdown) and control how long the Windows device stays up and running after it wakes from sleep.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find and click **Control Power Options** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Power Control Action**, specify how to control the power of the device. (*Sleep, Restart, Shutdown*)
2. For **Disable abort-shutdown**, toggle **On** or **Off** to select if the endpoint user can abort the shutdown.
3. For **Waiting time**, adjust the time to delay applying the policy after user input. (*Seconds - hours*)
4. For **Uptime for Power Control**, specify how long after computer awakening to execute the power control action.
5. For **Show Title bar**, toggle **On** or **Off** to select if the message box title bar will be displayed.
6. For **Message Contents**, specify the message contents, text and height. You can use HTML formatting and macros to display information from Genians.
7. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
8. Click **Update.**

### 14.4.30 Controlling Network Folder Sharing

You can collect shared network folder information, control access, and specify permissions.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Network Folder Sharing** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Collecting Shared Folder Information**, select **Off** to not collect info about shared folders over the network.
2. For ** Stopping Folder sharing**, turn **On** to stop folder sharing.
   - **Delay Timeout**, specify the time when the shared folder access is revoked. (*seconds - months*)
   - **Read-only Folder Exception**, turn **On** to allow access to the folder with read-only permissions.
   - **Stopping Everyone Folder Only**, turn **On** to stop sharing the folder with everyone permissions.
   - **Administrative Shares Exception**, select **Off** to disable access to the Administrative Share.
3. For **Folder Sharing Expiry Notification**, select Custom Message or Default Message in Pop-up window.
4. Click **Update.**
5. Go to **Policy > Node Policy** in the left Policy panel.
6. Click the **desired Policy ID** in Node Policy window.
7. Find Agent Action. Click Assign.
8. Find **Control Network Folder Sharing** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**

10. Click **Update.**

### 14.4.31 Controlling Screen Lock

You can control the screen lock on your Windows devices which requires users to authenticate upon wake from sleep. You can also force to use specific wallpaper image. (*e.g. Library Nodes, or Store Front Nodes*)

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Screen Lock** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Lock Screen Scan**, select **Off** to disable the collection of info on the configured Screen Lock.
2. For **Re-authentication**, turn **On** to require User Authentication from Wake or Screen Lock.
3. For **File Integrity Check Interval**, adjust time interval to check Screen Lock integrity. (*minutes - hours*)
4. For **Lock Screen Enforcement**, turn **On** enforce a Screen Lock.
   - **Waiting Time**, specify the time before the Screen Lock starts. (*minutes - hours*)
   - **User Waiting Time**, this will not apply if this time is longer than Waiting Time.
   - **Displaying Logon Screen**, displays logon screen upon Resume.
   - **Genian Lock Screen Message**, type message to display on Screen Lock.
   - **File**, upload a file to be used for Screen Lock.
   - **File Name**, define a name for the Screen Lock File.
   - **User-configured Lock Screen**, select **Off** to not allow a User to configure Screen Lock.
5. For **Wallpaper Image Enforcement**, turn **On** to enforce a Desktop Wallpaper:
   - **File**, upload a file to be used for Wallpaper.
   - **File Name**, define a name for the Wallpaper File.
   - **Position**, specify the position of the Wallpaper File. (*Center, Tile, Stretch*)
6. Click **Update.**
7. Go to **Node Policy** in the left Policy panel.
8. Click the **Default Policy** in Node Policy window.
9. Find **Agent Action**. Click **Assign.**
10. Find **Control Screen Lock** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**

12. Click **Update.**

### Add Authentication Code to Unlock Screen Lock

You can enable a Authentication Code for when users are unable to authenticate and unlock their screens from Screen Lock. Users can sometimes be offline and will need to authenticate to unlock their screens. The option below provides a button to generate a Agent Code to give to the Administrator to then get a Authentication Code to enter into the Screen Lock.

**Note:** **Control Screen Lock** must already be configured and enabled in the Node Policy. (*Default Policy*)

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign.**
5. Find **Authenticate User Using Genian Agent** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**
8. Go to **Policy > Node Policy > Agent Action**, click on **Authenticate User Using Genian Agent.**

Under **Agent Action: Miscellaneous:**

1. For **Authentication Enforcement**, turn **On** Screen Lock Authentication.
2. For **Page Background Color**, optional setting to change the background color.
3. For **Displaying Unlock Screen**, turn **On** to display a **Unlock Screen Button.**
4. Click **Update.**

**Note:** User clicks "Unlock Screen Button" to generate "Agent Code" and gives to Administrator. Administrator then uses this to get "Authentication Code" for user to enter in and "Unlock Screen Lock."

## 14.4.32 Manage ARP Table

You can manage the ARP Table on the devices by Deleting Static ARP Entries, or preventing ARP conflicts.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Manage ARP Table** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.

2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Deleting Static ARP Entries**, turn **On** to delete static ARP entries.
2. For **Static ARP for IP Conflict-prevention**, turn **On** to use Static ARP Entries for IP Conflict-prevention to prevent from ARP Spoofing.
   - **Node Group**, Optional setting to apply **Static ARP for IP Conflict-prevention** to specific Node Groups.
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Manage ARP Table** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

**Note:** Go to Management > Node > IPAM Tab > IP Policy to configure Conflict-prevention Settings.

### 14.4.33 Notify User

You can notify users with informational messages or warnings. The message may be displayed using a slide-out notification, HTML, or redirection to a URL.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Notify User** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Contents for Slide-out Box Notification**, type in contents to display in slide-out box notification.
2. For **CWP Page Redirection**, turn **On** to redirect to CWP page when a user clicks a slide-out notification.
   - **CWP Page Redirection URL**, click **Use Template** or specify a URL for CWP redirection when a user clicks a slide-out notification.
3. For **Enforcing Notification**, specify whether to disable to force closing a notification.
   - **Notification Message Type**, specify a message type for a user notification. (*Informational, Warning*)
   - **Generating Log for User Read Notification**, specify whether to generate a log when a user reads a notification.

4. For **Automatic pop-up**, Enable to display detailed message contents in a pop-up badge, rather than only a preview.
5. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
6. Enter in **CWP Message**, **Conditions**, and adjust **Agent Actions** based off of your network requirements.
7. Click **Update.**
8. Go to **Node Policy** in the left Policy panel.
9. Click the **Default Policy** in Node Policy window.
10. Find **Agent Action**. Click **Assign.**
11. Find **Notify User** in the **Available** section. Select and drag it into the **Selected** section.
12. Click **Add.**
13. Click **Update.**

### 14.4.34 Uninstall Programs

You can control software on your Windows devices by removing programs that you do not allow.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Uninstall Programs** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Program**, specify programs to be uninstalled on the endpoint, using the name listed in the Windows Control Panel.
2. For **Notification Before Uninstalling**, specify whether to notify a user before uninstalling a program.
   - **Contents**, add contents to notify user.
3. For **Account Options**, specify a account to uninstall a program from drop-down.
4. For **Restart Options**, specify whether to Notify User or Auto-Restart.
5. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
6. Click **Update.**
7. Go to **Node Policy** in the left Policy panel.
8. Click the **Default Policy** in Node Policy window.
9. Find **Agent Action**. Click **Assign.**
10. Find **Uninstall Programs** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**

12. Click **Update.**

### 14.4.35 Scan Condition Settings

You can scan Windows condition settings to include processes, files, system, and authenticated users.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Scan Condition Settings** in the Agent Action window.

Under **General** section:

#. For **CWP Message**, add message to be displayed in accordance with the Policy. #. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section: (*Must have Conditions added for this plugin to work*)

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Enter in **Conditions**, and adjust **Execution Interval.**
5. For **Periodic Interval**, choose from seconds, minutes, hours, days weeks, or months. (*Default is 12 hours*)
6. Click **Update.**
7. Go to **Node Policy** in the left Policy panel.
8. Click the **Default Policy** in Node Policy window.
9. Find **Agent Action**. Click **Assign.**
10. Find **Scan Condition Settings** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**
12. Click **Update.**

### 14.4.36 Terminate Process

You can kill specific processes that are running on the end users Windows devices and schedule the frequency to verify that they continue to not run.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Terminate Process** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Process Terminated Event Notification**, turn **On** to notify a user when a process is terminated.
    - **Contents**, type to enter contents to terminate a specific process.
2. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Terminate Process** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

## 14.4.37 Check Required Application Installation

The Check Required Application Installation Plugin provides basic options to inspecting the Antivirus, Disk Encryption, and Patch Management. Condition values will continue to be added.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Check Required Application Installation** in the Agent Action window.

Under **General** section:

1. For **Applications**, select that you want Antivirus, Disk encryption, and Patch Management.
2. For **Products**, select that you want the detailed product.

Under **Plugin Settings** section:

1. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
2. Click **Update.**
3. Go to **Node Policy** in the left Policy panel.
4. Click the **Default Policy** in Node Policy window.
5. Find **Agent Action**. Click **Assign.**
6. Find **Check Required Application Installation** in the **Available** section. Select and drag it into the **Selected** section.
7. Click **Add.**
8. Click **Update.**

### Supported Anti-Virus Products

| Vendor | Product Name | Product Version |
|---|---|---|
| Avira GmbH | Avira Antivirus Pro | 15.x |
| Avira GmbH | Avira Free Antivirus | 15.x |
| Avira GmbH | Avira Endpoint Security | 15.x |
| ESET | ESET Endpoint Security | 12.x |
| ESET | ESET Internet Security | 12.x |
| ESET | ESET Smart Security | 12.x |
| ESET | ESET NOD32 Antivirus | 12.x |
| Bitdefender | Bitdefender Antivirus Plus | 23.x |
| Bitdefender | Bitdefender Internet Security | 23.x |
| Bitdefender | Bitdefender Total Security | 23.x |
| Bitdefender | Bitdefender Antivirus Free Edition | 1.x |
| AhnLab, Inc. | AhnLab V3 Lite | 3.x |
| AhnLab, Inc. | AhnLab V3 Lite | 4.x |
| AhnLab, Inc. | AhnLab V3 Net for Windows Server | 9.x |
| AhnLab, Inc. | AhnLab V3 Endpoint Security | 9.x |
| AhnLab, Inc. | AhnLab V3 Internet Security | 9.x |
| AVG Technologies CZ, s.r.o. | AVG Business | 18.x |
| AVG Technologies CZ, s.r.o. | AVG Internet Security Business Edition | 18.x |
| AVG Technologies CZ, s.r.o. | AVG AntiVirus Business Edition | 18.x |
| AVG Technologies CZ, s.r.o. | AVG AntiVirus Free | 18.x |
| AVG Technologies CZ, s.r.o. | AVG Internet Security | 18.x |
| G Data Software AG | G Data Security Client | 14.x |
| G Data Software AG | G Data TotalSecurity | 25.x |
| G Data Software AG | G Data AntiVirus | 25.x |
| G Data Software AG | G Data Internet Security | 25.x |
| Malwarebytes Corporation | Malwarebytes Free | 3.x |
| McAfee, Inc. | McAfee All Access | 16.x |
| BullGuard Ltd. | BullGuard Antivirus | 10.x |
| BullGuard Ltd. | BullGuard Premium Protection | 10.x |
| BullGuard Ltd. | BullGuard Internet Security | 10.x |
| ESTSecurity Corp. | ALYac(For Public Use) | 2.x |
| ESTSecurity Corp. | ALYac | 3.x |
| ESTSecurity Corp. | ALYac | 4.x |
| Hauri, Inc. | ViRobot 7.0 | 10.x |
| K7 Computing Pvt Ltd | K7 AntiVirus Premium | 10.x |
| K7 Computing Pvt Ltd | K7 Total Security | 10.x |
| K7 Computing Pvt Ltd | K7 Ultimate Security | 10.x |
| F-Secure Corporation | F-Secure PSB Workstation Security | 10.x |

### Supported Data-Protection Products

| Vendor | Product Name | Product Version |
|---|---|---|
| Jetico, Inc. | BestCrypt Volume Encryption | 4.x |
| Jetico, Inc. | BestCrypt | 9.x |
| Jetico, Inc. | BCArchive | 2.x |
| Bitdefender | Bitdefender Internet Security | 23.x |
| Bitdefender | Bitdefender Total Security | 23.x |
| G Data Software AG | G Data TotalSecurity | 25.x |
| AVG Technologies CZ, s.r.o. | AVG AntiVirus Business Edition | 18.x |
| AVG Technologies CZ, s.r.o. | AVG Business | 18.x |
| AVG Technologies CZ, s.r.o. | AVG Internet Security | 18.x |
| McAfee, Inc. | McAfee All Access | 16.x |

### Supported Patch-Management Products

| Vendor | Product Name | Product Version |
|---|---|---|
| F-Secure Corporation | F-Secure PSB Workstation Security | 12.x |

## 14.4.38 Deploy Files v2

The file distribution plugin executes files or downloads them to a specific location. The Policy Server communicates with the agent to distribute, execute, and install files on endpoints.

- Distribute necessary files to endpoints
- Install uninstalled software on endpoints

File Distribution v2 plugin has been added, focusing on strengthening security from the existing file distribution plugin.

File Distribution v2 plugin provides file integrity verification and distributor identity confirmation for secure file distribution.

- Performs 3-step integrity verification
- Distributor identification and approval by end-user

The File Distribution v2 plugin mandatorily requires digital signatures for files being distributed and uses the Sigstore Signing method, designed for supply chain security, for digital signatures and signature verification. The File Distribution v2 plugin can selectively use two methods of Sigstore Signing: Sigstore Keyless Signing and Public Key Signing.

### Tools and Services for Digital Signature and Digital Signature Verification (Sigstore)

### Sigstore Overview

**`Sigstore`_** is an open, distributed infrastructure designed for software supply chain security.

Sigstore provides tools and services for signing software, verifying signatures, and tracing signatures.
It also provides tools and services for implementing SLSA (Software Supply Chain Levels of Assurance), a framework designed to improve software supply chain security.

Sigstore provides the following features to improve software supply chain security:

- Guarantees software integrity by signing software.
- Verifies signatures to ensure software has not been tampered with.
- Traces signatures to track software origin and distribution.
- Improves software supply chain security by implementing SLSA.

Sigstore is an open, distributed infrastructure designed to improve software supply chain security, and can help enhance the security of the software supply chain.

### Sigstore in Genian NAC

For enhanced security, Genian NAC's File Distribution Plugin v2 uses **tools provided by Sigstore for software integrity assurance**.

It uses **cosign**, a tool provided by Sigstore for digital signing and signature verification of files to be distributed, and additionally verifies digital signature information from an immutable ledger-based service for verification.

The cosign tool has been added to the Policy Server and plugins for digital signature verification.

| Verification Method | Sigstore Keyless Signing (Keyless) | Public Key Signing (self-managed-key) |
|---|---|---|
| Verification Content | • Performs digital signature on distribution files with identity information by authenticating with OIDC (OpenID Connect) from Google/Github/MS<br>• Endpoints receiving the file verify that it is a Sigstore-signed file using User ID (e.g., Google ID) and OIDC (Google Account) information | • Performs digital signature on distribution files using self-owned private/public keys<br>• Certificates (public keys) for verification are distributed upon Node Action reception |
| Environment Setup | • Usable only in environments with Internet access | • Usable in both Internet and isolated network environments |
| Key Management | • Requires only security for administrator accounts, as no separate keys are used | • Requires secure storage of separate private keys |
| Preparations | • Cosign binary file required for digital signing of distribution files (Download cosign-windows-amd64.exe from **Assets** at Sigstore GitHub Release v2.1.1 download)<br>• External internet communication required for digital signing/signature verification of distribution files (Signing PC, Policy Server, User Endpoint)<br>• OIDC (Google, Git, MS) accounts required for digital signing of distribution files | • Cosign binary file required for digital signing of distribution files<br>• Keys required for digital signing of distribution files, can be generated using cosign or prepared separately |
| Constraints | • Cannot change from the initially registered distributor to another distributor | • Cannot change from the initially registered distributor to another distributor<br>• Key files used for digital signing of distribution files must be managed separately (e.g., USB) |

### Sigstore Keyless Signing Method

Sigstore generates **short-lived certificates using OpenID Connect (OIDC)**.
**These certificates are used to sign software**, and the signed software can be publicly verified via cosign.

OIDC is an extension of OAuth 2.0, a framework that uses login authentication to provide users access to resources. Because OIDC can generate certificates without requiring user passwords, it is used by Sigstore to generate short-lived certificates.

**How to Use Sigstore Keyless Signing**

**Step1. Digital Signature of Distribution File**

1. Download cosign and save it to the directory to be used for digital signing of the distribution file.
2. Change the file name to cosign.exe.
3. Copy the file to be digitally signed to the directory.
4. Go to the directory where cosign.exe is located by entering cmd in Start > Run and executing it.
5. Perform digital signing by entering the command below:

```
> cosign.exe sign-blob {Distribution_File_Name} --output-certificate
↪{Generated_Cert_File_Name.cert} --output-signature {Generated_Signature_
↪File_Name.sig}
```

6. Copy the URL information displayed in the cmd window and access the web page using a browser.
7. Confirm that the 8-character value displayed in the cmd window is the same as the 8-character value displayed in the cmd window and click the `Submit` button.
8. Select one of the three OIDCs: `Git, Google, Microsoft` and perform authentication.
9. After a moment, enter `y` in the cmd window to agree to the terms of service.
10. Confirm that `Cert, Sig` files have been successfully generated in the directory.

**Step2. Verify Digital Signature**

1. In the Start window, enter the command below:

```
> cosign.exe verify-blob {Distribution_File_Name} --certificate
↪{Generated_Cert_File_Name.cert} --signature {Generated_Signature_File_
↪Name.sig} --certificate-identity={ID_Used_for_Auth} --certificate-oidc-
↪issuer={OIDC_Issuer}
Example> cosign.exe verify-blob agent.zip --certificate agent.cert --
↪signature agent.sig --certificate-identity=genian@genians.com --
↪certificate-oidc-issuer=https://accounts.google.com
```

2. If the digital signature is performed successfully, **Verified OK** will be displayed.

**Step3. Create Node Action**

1. Access the Policy Server Web Console and go to **Policy** in the top menu.
2. Go to **Node Policy > Node Action** in the left menu.
3. Click **Select Tasks > Create** in the top menu.

Below are **General**.

4. For **Action Name**, use the format "(Purpose)Action Name" according to its purpose for easy distinction of node actions during future operation.
5. **Description** can be used to distinguish the purpose of the node action if it is used differently depending on the purpose.
6. Adding a **Label** allows you to classify the plugin with a custom label displayed in the "Description" input field.

Configure the **Action Execution Settings** below.

7. For **OS Type**, select the appropriate OS among macOS, Linux, and Windows targets.
8. **Condition Settings** are generally used to distribute files to users meeting specific conditions.

```
Example: If you distribute using the condition "if c:\%ProgramFiles%\abc.
↪exe does not exist", distribution is only possible to endpoints where␣
↪abc.exe does not exist.
```

9. In **Plugin Selection**, select **File Distribution V2**.
10. For **Distribution File**, click the `Upload` button to select the file.
11. For **Distribution File Verification Method**, select Sigstore Keyless Signing.
12. For **Trusted OIDC Issuer**, select the OIDC (Github, Google, Microsoft) used for authentication during digital signing.
13. For **Trusted ID**, enter the ID (email address format) used for authentication during digital signing.
14. For **Certificate**, click the `Read File` button on the right to add the **cert** file generated during digital signing.
15. For **Signature**, click the `Read File` button on the right to add the **sig** file generated during digital signing.
16. For **Distribution Options**, configure the distribution method.

- **Execute File**: If it's a compressed file, configure the file to execute in "File Path", and set "Execution Options" and "Execution Account" to execute the file. Set reboot preference after file execution via "Reboot Option".
- **Download**: Specify the file and folder path on the endpoint where the distribution file will be copied.

17. Click the **Update** button.
18. Go to **Node Policy** in the left Policy menu, then click **Default Policy**.
19. Find **Node Action Settings** and click the **Assign** button.
20. In the **Available** items, find **File Distribution** and drag it to the **Selected** items.
21. Click the **Update** button, then click the **Update** button again.

**Note:**

For Sigstore Keyless Signing method, external communication is essential for digital signing/signature verification, and communication to the domains below must be allowed.

(Source: Policy Server, Agent), (Service Port: TCP/443)

rekor.sigstore.dev : Ledger recording system

oauth2.sigstore.dev : Sigstore oauth flow provisioning server

accounts.google.com : OIDC provider (If it's another OIDC, use that OIDC domain)

fulcio.sigstore.dev : sigstore CA server

tuf-repo-cdn.sigstore.dev : SLSA verification

### Public Key Signing Method

Sigstore cosign also provides a self-managed key digital signing method.

The Public Key Signing method involves directly generating a key for digital signing or using a separately created key that is already in use.

#### How to Use Public Key Signing

**Step1. Digital Signature of Distribution File**

1. Perform steps 1-4 of Step 1 in Sigstore Keyless Signing method, then proceed.
2. If you do not have a separate key for digital signing, enter the command below to generate a private key and public key for digital signing.

```
> cosign.exe generate-key-pair
> Enter private key password
> Confirm private key password
> Enter dir to confirm that private key (key) file and public key (pub)␣
↪file have been generated.
```

3. If you have generated a key, perform digital signing on the distribution file using the generated key as follows:

```
> cosign.exe sign-blob {Distribution_File_Name} --key cosign.key --tlog-
↪upload=false --output-signature {Generated_Signature_File_Name.sig}
Example> cosign.exe sign-blob agent.zip --key cosign.key --tlog-
↪upload=false --output-signature agent.sig
```

**Step2. Verify Digital Signature**

1. In the CMD window, enter the command below:

```
> cosign.exe verify-blob {Distribution_File_Name} --key {Public_Key_File_
↪Name.pub} --signature {Generated_Signature_File_Name.sig} --insecure-
↪ignore-tlog=true --insecure-ignore-sct=true
Example> cosign.exe verify-blob agent.zip --key cosign.pub --signature␣
↪agent.sig --insecure-ignore-tlog=true --insecure-ignore-sct=true
```

2. If the digital signature is performed successfully, **Verified OK** will be displayed.

**Step3. Create Node Action**

1. Perform steps 1-10 of Step 3 in Sigstore Keyless Signing method, then proceed.
2. For **Distribution File Verification Method**, select Public Key Signing.
3. For **Trusted Public Key**, click the `Read File` button on the right to add the **pub** file that was generated during key creation.
4. For **Signature**, click the `Read File` button on the right to add the **sig** file that was generated during digital signing.
5. Perform steps 16-21 of Step 3 in Sigstore Keyless Signing method.

> **Danger:**
>
> **It is impossible to change the initially set distribution method and distributor**, so the Private key used during the initial node action creation must be **kept securely to prevent loss**.

Registered distributor information can be confirmed in Web Console Settings > Preferences > Agent > Distribution Options section.

### Yubikey Personal Key Management Method

While managing private keys with the Public Key method, there are many cases of key loss due to formatting of the managed PC, etc. Furthermore, storing private keys on external tokens provides physical separation, protecting them from hacking or malicious software. For these reasons, it is recommended to securely manage private keys using an external token (YubiKey).

The `cosign piv-tool` command provides utilities for managing hardware tokens.

#### Step1. Yubikey Initialization

Model used in this introduction : yubikey 5 nfc

```
> cosign piv-tool reset
```

**Danger:**

This command initializes the hardware token, so if there are any existing certificates stored on the Yubikey, they will be deleted.

#### Step2. PIN Configuration

- After initialization, the default PIN is 123456
- Below is an example where the PIN is defined as ‘111222’.

```
> cosign piv-tool set-pin --new-pin=111222
? pin. This will overwrite the previous pin.: y
Setting new pin. This will overwrite the previous pin.: y
```

- To change the PIN when it is already defined, execute the command as follows:

```
> cosign piv-tool set-pin --old-pin=111222 --new-pin=232323
? pin. This will overwrite the previous pin.: y
Setting new pin. This will overwrite the previous pin.: y323
```

- The PIN changes from ‘111222’ to ‘232323’.

#### Step3. Certificate Generation

- Generate a certificate on the Yubikey.

```
> cosign piv-tool generate-key --random-management-key
```

#### Step4. Verify Registered Key

- Outputs the certificate information stored on the Yubikey.

```
> cosign piv-tool attestation
```

#### Step5. Extract Public Key

- As explained above, `target file`, `public key`, and `signature` are required for digital signature verification.

- You can export the Yubikey public key to a file using the following command. A publickey.pub file will be generated.

```
> cosign.exe public-key —sk > publickey.pub
```

**Step6. Code Signing (Signature Generation)**

- This is similar to the `cosign.exe sign-blob` command in **Public Key Signing Method - Step1. Digital Signature of Distribution File**, but with the difference of using a smart card token.
- Since piv is connected, in this command, the `--key` option is omitted, and code signing is attempted.

```
> cosign.exe sign-blob {Distribution_File_Name} --tlog-upload=false --
↪output-signature {Generated_Signature_File_Name.sig}
Example> cosign.exe sign-blob agent.zip --tlog-upload=false --output-
↪signature agent.sig
> Enter registered PIN
> Perform physical touch on Yubikey
```

**Step7. Integrity Verification**

- Perform identically to Public Key Signing Method - Step2. Verify Digital Signature.

## 14.4.39 ZTNA Connection Manager

Controls Zero trust network access Connection Manager options and actions.

### Plugin setting

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click ZTNA Connection Manager in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. **Site**: Allocate any added items from **System > Site**
2. **Authentication Method**: After connecting to the network, choose whether to perform user authentication according to the authentication method of the node policy.
3. **Always Connected**: Use the last connection information to stay connected to the ZTNA network at all times.
4. **Browser Auto Login**: The browser extension automatically shares authentication tokens to synchronize user authentication with the portal.
5. **Program Run after Network Access**: Add a program that runs after the network connection is complete.
6. Click **Update.**
7. Go to **Node Policy** in the left Policy panel.

8. Click the **Default Policy** in Node Policy window.
9. Find **Agent Action**. Click **Assign.**
10. Find ZTNA Connection Manager in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**
12. Click **Update.**

### 14.4.40 Transferring Agent Information Externally

**Note:**

- Transferring agent information externally is available from Genian NAC version 6.0.18 or higher. For versions below 6.0.18, please use the Deploy Files V2 plugin.

- Agent information external transmission is used when you want to integrate the agent's authentication information with external third-party applications.
- When a node performs authentication and the agent's authentication status becomes either Authenticated or Deauthenticated, the authentication information is transmitted to an external third-party application. This is used to perform authentication across multiple solutions with a single authentication process.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Transferring agent information externally** in the Agent Action window.
4. For **CWP Message**, add message to be displayed in accordance with the Policy.
5. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

[ Settings ]

| Item Name | Setting Item | Description | Notes |
|---|---|---|---|
| Path | Enter the target file path directly | Specify the file path of the target to which the information will be delivered. | File Path Macro Options |
| Transfer information | Login/Logout Credentials | Transmit both login and logout events | When using periodic logout via node policy, it is also possible to transmit only login authentication information. |
| | Login credentials | Transmit only login authentication information | |
| UserID conversion method | NONE | Used when converting the user ID before transmitting the received authentication information. | |
| | Regular expression | | |
| | Convert to uppercase | | |
| | Convert to lowercase | | |
| Interval | When information changes | Select the interval at which the agent's authentication information will be transmitted. | When information changes |
| | At Operating System Startup | | When information changes + At Operating System Startup |
| | In Periodic Interval | | When information changes + In Periodic Interval |
| Encryption Algorithm | None | Used when authentication information needs to be encrypted during transmission. | When using encryption options other than BASE64, the data is additionally encoded with BASE64 before transmission. |
| | Base64 | | |
| | AES-128 | | |
| | AES-256 | | |
| | Blowfish | | |
| | CAST | | |
| | SEED | | |

1. Click the Add button in the **External Transfer List** to add the file for transmitting authentication information (third-party integration process file).
2. Select the items to **Transfer information**.
3. Choose whether to perform **UserID conversion method**.
4. Select the **Interval**.
5. Choose the **Encryption Algorithm**.
6. Click the **Add** button.

- If there are additional targets for external transmission, click the Add button to include them.

1. Click **Update.**
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find Agent Action. Click Assign.
5. Find **Transferring Agent Information Externally** in the **Available** section. Select and drag it into the **Selected** section.

6. Click **Add.**
7. Click **Update.**

## 14.5 Controlling macOS

You can control macOS devices with the Agent installed using these plugins:

### 14.5.1 Authenticate User Using Genian Agent

Policy Server communicates with the Agent to authenticate users on Mac OS devices.

#### Node Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. The authentication method must be selected as 'User Authentication' before agent authentication can be used on the endpoint.
4. Select two-step authentication as needed.
   - See *2-Step Authentication*

#### Add the Agent Action to a Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign**.
5. Find **Authenticate User Using Genian Agent** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

#### Authenticate User Using Genian Agent

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Authenticate User Using Genian Agent** in the Agent Action window.
4. Enter in **Conditions**, optional settings.

Under **Appearance:**

1. For **Image**, Specify an image for the Agent authentication dialog box.
2. For **Displaying Titlebar**, Specify whether to display a title bar on the Agent authentication dialog box.

3. For **Dialog Box Color**, Specify a dialog box color.
4. For **Font Color**, Specify a font color.
5. For **Help Message**, Specify a Help Message, and if to display with HTML .
6. Click **Update.**

### 14.5.2 Check Required Application Installation

Checks if the required software is installed on the user's PC. You can check if an application is installed on your PC by selecting a specific product name.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Check Required Application Installation** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, Select the **Applications** and **Product**
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action** section, click **Assign.**
7. Find **Check Required Application Installation** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

### 14.5.3 Change Hostname

You can control the name of a macOS device.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Change Hostname** in the Agent Action window(select the macOS version).

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.

2. For **Settings**, click **Add** and select your optional conditions: **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Control Method**, specify a if you would like to change the Hostname to a **User Defined** value, or a value based on the **Hostname Rule of the Node Policy**
   - If **User Defined**: enter a hostname.
2. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Policy** you wish to edit in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Change Hostname** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

**Note:** The name cannot contain all special and blank characters except the minus sign (-), and must be less than 63 bytes.

### 14.5.4 Collecting Computer OS Information

The Policy Server collects Operating System information from end users macOS devices using the Agent.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Computer OS Information** in the Agent Action window (*Notice there are three. One for Windows, one for MacOS and another for Linux*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Collect Computer OS Information** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

### 14.5.5 Collecting Hardware Information

Policy Server communicates with the Agent to collect hardware information that is installed on end users macOS devices.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Hardware Information** in the Agent Action window. (*Notice there are two. One for Windows, and another for MacOS*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Plugin Settings**, adjust **CPU, Memory, and Disk Space Utilization Thresholds** based off of your network requirements.
4. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.
7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Collect Hardware Information** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

### 14.5.6 Collecting Monitor Information

Policy Server communicates with the Agent to collect information about the monitor that is connected to your Mac OS device.

#### Add Agent Action to a Policy

1. Go to **Node Policy** in the left Policy panel.
2. Click the **Default Policy** in Node Policy window.
3. Find **Agent Action**. Click **Assign.**
4. Find **Collect Monitor Information** in the **Available** section. Select and drag it into the **Selected** section.
5. Click **Add.**
6. Click **Update.**

### Collect Monitor Information

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Monitor Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds* - *months*)
4. Click **Update.**

## 14.5.7 ZTNA Connection Manager

Controls Zero trust network access Connection Manager options and actions.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click ZTNA Connection Manager in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. For **Connection Manager**, specify the type of connection manager.
    - **Site**: Set "Site Settings Information" in Connection Manager.
2. For **Execution Interval**, adjust Periodic Interval. (*Seconds* - *hours*)
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find ZTNA Connection Manager in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

Users can use it through the **Network Access** button on the tray icon.

1. Click the **Network Access** button on the tray icon.
2. Click the site you want to connect to.
3. Proceed with the connection through the **Agent Authentication window** that appears on the screen.
4. Select **two-step authentication** as needed.
   - See *2-Step Authentication*

### 14.5.8 Collecting Network Information

Policy Server communicates with the Agent to collect network information on end users macOS devices.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Network Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. For **Update Interval**, adjust Periodic Interval. (*Seconds - hours*)
2. For **Collecting Open Port Information**, turn **On** to collect open port information.
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Collect Network Information** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

### 14.5.9 Collecting Printer Information

Policy Server communicates with the Agent to collect printer information on end users Mac OS devices.

### Add the Agent Action to a Policy

1. Go to **Policy > Node Policy** in the left Policy panel.
2. Click the **desired Policy ID** in Node Policy window.
3. Find **Agent Action**. Click **Assign.**
4. Find **Collect Printer Information** in the **Available** section. Select and drag it into the **Selected** section.
5. Click **Add.**
6. Click **Update.**

### Collect Printer Information

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Printer Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Click **Update.**

## 14.5.10 Collecting Software Information

Policy Server communicates with the Agent to collect software information that is running on end users macOS devices.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Software Information** in the Agent Action window. (*Notice there are two. One for Windows, and another for MacOS*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.

6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Collect Software Information** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.5.11 Collecting Antivirus Software Information

Policy Server communicates with the Agent to collect antivirus software information that is installed on your macOS devices.

#### List of Supported Antivirus by Version

Check all Antivirus supported with Genian ZTNA.

| Vendor | Product | Genian Version |
|---|---|---|
| AhnLab | AhnLab V3 for Mac | 5.0.13 |
| Avast | Avast Mac Security | 5.0.9 |
| AVG | AVG Antivirus | 5.0.9 |
| BitDefender | Bitdefender Antivirus for Mac | 5.0.9 |
| ESET | ESET Cyber Security | 5.0.9 |
| ESET | ESET Endpoint Antivirus | 5.0.13 |
| Sophos | Sophos Endpoint | 5.0.17 |
| Sophos | Sophos Home | 5.0.17 |
| Symantec | Norton Antivirus | 5.0.9 |
| TrenMicro | Apex One | 5.0.63 |

#### Collect Antivirus Software Information

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Antivirus Software Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Action** section:

1. For **Boolean Operator**, leave as default: **OR**
2. For **Settings**, leave the default and click **Add** button to include others if they are not listed.
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action** section, click **Assign.**

7. Find **Collect Antivirus Software Information** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

### 14.5.12 Deploy Files v2

**Note:** Deploy File Plugin is not a feature in the CC evaluation, so it cannot be used by public institutions that require CC authentication.

The Deploy Files Plugin runs a file or downloads it to a specific location. The policy server can communicate with the agent to deploy, run and install files to the device.

- Deploying files for your device
- Installing software on the device

Deploy Files v2 Plugin is added with a focus on security enhancement in the existing Deploy Files Plugin.

Deploy Files v2 Plugin provides file integrity verification and distributor identification for secure file distribution.

- Perform three steps of integrity verification
- Identifying and approving end-user distributors

Deploy Files v2 Plugin requires an digital signature for the file you deploy, and it uses the Sigstore Signing method designed for supply chain security for digital signatures and signature verification. Deploy Files v2 Plugin uses Sigstore Signing to selectively use two methods: Sigstore Keyless Signing and Public Key Signing

| Verification Method | Sigstore Keyless Signing (Keyless) | Public Key Signing (self-managed-key) |
|---|---|---|
| Verification Contents | - Authenticate OIDC(OpenID Connect) in Google/Github/MS and electronically sign the distribution file with identity information<br>- The Certificate(Public Key) for verification is distributed when the node action is received | • Digital signature to distribution files using thier own secret/public keys |
| Environment Configuration | • Only available in Internet enabled environment | • Available in both Internet/closed network environment |
| Key Management | • Requires only security for administrator accounts in a way that does not use a separate key | • Requires secure storage of separate secret key |
| Preparations | - Requires cosign binary file for digital signature of distribution file (Sigstore Github Release v2.2.3 - Assets - cosign-darwin-* Download)<br>- External Internet communication used for digital signature/signature verification of distribution files is required (Digital signature PC, Policy Server, User Device), *Domain Information*<br>- Requires an OIDC (Google, Git, MS) account used for digital signatures of distribution files | - Cosign binary file is required for the digital signature of the distribution file<br>- Requires a key to be used for digital signatures of the distribution file and generates using cosign or prepares a separate key |
| Restrictions | - Cannot change from first registered distributor to another distributor | - Cannot change from first registered distributor to another distributor<br>- Key files used for digital signatures of distribution files need to be managed separately (USB, etc.) |

### Sigstore Keyless Signing Method

Sigstore uses **OpenID Connect(OIDC)** to generate a **short expiration certificate**.
**This certificate will be used to sign software**, and the signed software can be publicly verified through cosign.

OIDC is an extension of OAuth 2.0, a framework that uses login authentication to provide users with access to resources. OIDC can generate certificates without requiring a user's password, it is used by Sigstore to generate certificates with a short expiration date.

**How to use Sigstore Keyless Signing**

**Step1. Digital signature of distribution file**

1. Download the cosign and store it in the directory that you want to use for the digital signature of the distribution file.
2. Change the file name to cosign.
3. Copy the file to be digitally signed to the directory.
4. From the termianl, navigate to the directory where the cosign file is located.
5. Enter the following command to perform the digital signature.

```
> cosign sign-blob {FILE_NAME} --output-certificate {CERT_FILE_NAME.cert} --
↪output-signature {SIG_FILE_NAME.sig}
```

6. After a while, in ther terminal, enter `y` in Acceptance of the Terms of Service.
7. When the URL for authentication opens in the browser, select one of the three OIDCs: `Git, Google, Microsoft` and perform authentication.
8. Check that the file `Cert, Sig` is successfully created within the directory.

**Step2. Verifying digital signature**

1. Enter the following command in the terminal:

```
> cosign verify-blob {FILE_NAME} --certificate {CERT_FILE_NAME.cert} --
↪signature {SIG_FILE_NAME.sig} --certificate-identity={AUTH_USER_ID} --
↪certificate-oidc-issuer={OIDC 발행자}
Example> cosign verify-blob agent.zip --certificate agent.cert --signature␣
↪agent.sig --certificate-identity=genian@genians.com --certificate-oidc-
↪issuer=https://accounts.google.com
```

2. If the digital signature is valid, it will display **Verified OK**.

**Step3. Creating Node Actions**

1. Access the Policy Server Web Console and navigate to **Policy** at the top.
2. Go to **Node Policy > Agent Actions** from the left menu.
3. Click on **Actions Selection > Create** at the top.

Below are the **Basic Settings**.

4. For **Action Name**, use the format "(Purpose) Action Name" to easily differentiate node actions during operation.
5. **Description** can be used to differentiate node actions based on their purpose.
6. Adding **Labels** allows custom labels to be displayed in the Description input field, facilitating plugin categorization.

Configure the **Action Execution Settings** below.

7. Choose the appropriate OS type for macOS, Linux, or Windows targets under **OS Type**.
8. **Condition Settings** are typically used to deploy to specific users based on certain conditions during deployment.

```
Example: "c:\%ProgramFiles%\abc.exe 가 존재하지 않는 경우" 라는 조건을 사용하여␣
↪배포하게 되면 abc.exe 가 존재하지 않는 단말에만 배포가 가능합니다.
```

9. Select File Deployment V2 in **Plugin Selection**.
10. Click the `Upload` button under **Deployment File** to select the file.
11. Choose **Sigstore Keyless Signing** for **Deployment File Verification Method**.
12. Select the OIDC (Github, Google, Microsoft) used for authentication during digital signing in **Trusted OIDC Issuer**.
13. Enter the ID (in email address format) used for authentication during digital signing in **Trusted ID**.
14. Click the `Read File` button on the right side of **Certificate** to add the **cert** file generated during digital signing.
15. Click the `Read File` button on the right side of **Signature** to add the **sig** file generated during digital signing.
16. In **Deployment Options**, configure the deployment method:

- **Run App**: Execute macOS app file(.app).
- **Execute File**: If it's a compressed file, set the "File Path" to the file to execute, configure "Execution Options," and specify the "Execution Account" to run the file. Set the "Reboot Option" to specify whether to reboot after executing the file. (File Path Macro Options)
- **Download**: Specify the file and folder path where the deployment file will be copied. (File Path Macro Options)
- **Install Package**: Install macOS package file (.pkg).
- **Open File**: Open the uploaded file.
- **Run Script**: Runs the uploaded script file.

17. Click the **Edit** button.
18. Navigate from the left policy menu to **Node Policy**, then click on **Target Policy ID**.
19. Find **Agent Action Settings**, click the **Assign** button.
20. In the **Available** section, locate File Deployment, drag it to the **Selected** section.
21. Click the **Edit** button, then click **Update**.

**Note:**

For Sigstore Keyless Signing, communication with the following domains is essential for electronic signature/signature verification.

(Source: Policy Server, Agent), (Service Port: TCP/443)

rekor.sigstore.dev: Ledger Record System

oauth2.sigstore.dev: Sigstore OAuth Flow Provider

accounts.google.com: OIDC Provider (for other OIDCs, use the respective OIDC domain)

fulcio.sigstore.dev: Sigstore CA Server

tuf-repo-cdn.sigstore.dev: SLSA Verification

## Public Key Signing Method

Sigstore cosign also provides a self-managed key digital signature method.
Public Key Signing involves creating a key directly for digital signature or using an existing key for digital signature.

**Usage of Public Key Signing**

**Step 1. Digital Signature of Deployment File**

1. Perform Steps 1 to 4 of Sigstore Keyless Signing Method, then proceed with the following.
2. If you don't have a separate digital signing key, generate an digital signing private key and public key using the following command:

```
> cosign generate-key-pair
> Enter passphrase for key
> Confirm passphrase for key
> Type ls to verify that the private key (key) and public key (pub) files are created.
```

3. If the keys are generated, sign the deployment file using the generated key as follows:

```
> cosign sign-blob {FILE_NAME} --key cosign.key --tlog-upload=false --output-signature {SIG_FILE_NAME.sig}
Example> cosign sign-blob agent.zip --key cosign.key --tlog-upload=false --output-signature agent.sig
```

**Step 2. Verifying Digital Signature**

1. Enter the following command in the termianl:

```
> cosign verify-blob {FILE_NAME} --key {PUB_FILE_NAME.pub} --signature {SIG_FILE_NAME.sig} --insecure-ignore-tlog=true --insecure-ignore-sct=true
Example> cosign verify-blob agent.zip --key cosign.pub --signature agent.sig --insecure-ignore-tlog=true --insecure-ignore-sct=true
```

2. If the digital signature is valid, it will display **Verified OK**.

**Step 3. Creating Node Actions**

1. Perform Steps 1 to 10 of Sigstore Keyless Signing Method, then proceed with the following.
2. Select Public Key Signing for **Deployment File Verification Method**.
3. Click the `Read File` button on the right side of **Trusted Public Key** to add the **pub** file generated during key creation.
4. Click the `Read File` button on the right side of **Signature** to add the **sig** file generated during electronic signature.
5. Perform steps 16 to 21 of Sigstore Keyless Signing Method in Step 3.

**Danger:**

**Changing the initially configured deployment method and deployer is not possible**, so the private key used during the initial node action creation must be **safely stored to prevent loss**.
Registered deployer information can be found in Web Console Preferences > General > Agent > Deploy options section.

## 14.5.13 Controlling Screen Lock

You can control the screen lock on your Mac OS devices which requires users to authenticate upon wake from sleep.

### Add the Agent Action to a Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign**.
5. Find **Control Screen Lock** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

### Control Screen Lock

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Screen Lock** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Lock Screen Scan**, select **Off** to disable the collection of info on the configured Screen Lock.
2. For **Screen Lock Enforcement**, turn **On** enforce a Screen Lock.
   - **Waiting Time**, specify the time before the Screen Lock starts. (*minutes* - *hours*)
   - **User Waiting Time**, this will not apply if this time is longer than Waiting Time.
3. Click **Update.**

### 14.5.14 Controlling WLAN

Policy Server communicates with the Agent to collect SSID information. In macOS Sonoma 14.5 or later, location services permission is required to retrieve SSID information for wireless networks. Without this permission, the app cannot collect network information or perform network management functions.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control WLAN** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **SSID Information Scope**, choose to collect information about all **Detected** SSID or only those that are **Connected**.
    - For **Detected SSIDs** define a time value for:
        - **Update Interval** - Specify the time interval to update the SSID information.
        - **SSID Time-based Threshold** - Specify the minimum time duration to start collecting SSID information.
2. For **Disabling Wireless Connection**, choose **On** or **Off** to prohibit connection to certain SSIDs.
    - For **On** choose how allowed SSIDs will be defined, and configure enforcement options:
        - **How to Define Allowed SSID(s)** - Choose From **WLAN Group**, **SSID Name**, or **regular expression**, and fill in the prompt or menu.
        - **Control Cycle** - Enter a number of **seconds**, or **minutes** to specify the cycle for Checking whether the connected AP is an allowed AP.
        - **Delay Enforcement Policy** - Enter a number of **seconds**, or **minutes** to wait before disconnecting a prohibited connection.
        - **Disabled Connection Notification and Resolution** - Choose From **No Notifications**, **Slide-Out Notification**, or **Allow connection using an agent Authentication Code**
            - For **Agent Authentication Code**, enter a **Connection Time Limit**, and a Custom **HTML Message** to the end-user.
3. For **Private Wi-Fi Address Control**, the private Wi-Fi address option is disabled in macOS Sequoia or later, ensuring that the device's MAC address remains unchanged during network connections.
    - **Operation Mode** - Selecting 'Set Value Only' will only update the settings, and a reboot is required for the changes to take effect. Selecting 'Apply Immediately' will restart the network interface, which may disconnect the wireless network temporarily.
    - **Notify Option** - Specify the notification behavior according to the selected 'Operation Mode.' When 'Apply Immediately' is chosen and 'None' is selected, the network interface will restart immediately after the setting is changed.

- **Notify Time** - When 'User Notification' is selected with the 'Apply Immediately' option, you can configure the delay time to display a notification before applying the changes.

4. For **Location Services Permission Prompt Message**, enter the notification message to be displayed when requesting location services permission from the user.
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.
7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Control WLAN** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

### 14.5.15 Manage ARP Table

The ARP protocol thus makes network traffic communications a relatively simple and straightforward affair. However, ARP is also inherently vulnerable from a security perspective. ARP requires no authentication whatsoever of the addressing information it receives from any network peer. All ARP replies are cached in the ARP table as described above; existing table entries are automatically overwritten by the most recent information received. This lack of authentication makes ARP an easy target for cyber-security exploitation.

In particular, ARP is highly vulnerable to attacks such as “ARP Spoofing” and “ARP Poisoning.” The point of such attacks, the nature of which will be discussed further below, and which can be initiated from some compromised network device or from the hacker themselves if they have acquired physical access to the network in question, is to compromise the integrity of a local network’s ARP table by associating an attacker’s MAC address with the IP address of a particular target host. In this way, network traffic intended for a particular destination will instead be forwarded on to the attacker’s host location. That traffic can them be modified, stolen, or simply observed in order to support some additional cyberattack purpose in an on-demand fashion. ARP-related security breaches are very difficult to detect and defend against precisely because the ARP information is maintained and transmitted only within the L2 broadcast domain. Vigilant network administrators cannot tell, simply by looking at an ARP table, whether it’s been compromised or not, unless they have established some manual system to keep track of the expected IP-to-MAC address relationships.

ZTNA provides a plugin to manage ARP tables to solve these problems. Delete static ARP to prevent vulnerabilities bypassing ZTNA.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Manage ARP Table** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Deleting Static ARP Entries**, To remove static ARP set by the user of the Node that Agent is installed. (Except static ARP added by AAS)
2. For **Anti ARP Spoofing (AAS)**, To add Conflict Prevention Nodes to ARP table as Static.
    - **Node Group** : To apply specific Node Group (If not selected, it applies to all Nodes to which Agent Action is assigned)
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Manage ARP Table** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

## 14.5.16 Notify User

You can notify users with informational messages or warnings. The message may be displayed using a slide-out notification, HTML, or redirection to a URL.

### Notify User configuration

1. For **Contents for Slide-out Box Notification**, add message to be displayed on notification title.
2. For **CWP Page Redirection**, if you turn **On**, reditected to CWP page when user click notification.
    - **CWP Page Redirection URL** Click **Use Template** the button to use a template or enter the URL manually
3. For **Enforcing Notification** whether to show agent notifications again when they are closed. (*On / Off*)
    - **Notification Message Type** : Choose message type (*Normal, Warning*)
    - **Generating Log for User Read Notification** : Generating audit log When user checked message (*On / Off*)

### Configure Notify User through Node Policy

1. Go to **Node Policy** in the left Policy panel.
2. Click the **Default Policy** in Node Policy window.
3. Find Agent Action section, click **Assign**.
4. Find and double click newly created **Agent Action**. (e.g. Notfiy User)
5. Click **Add**.
6. Click **Update**.

### Configure Notify User through Enforcement Policy

**1. Create Group for Enforcement Policy**

1. Go to **Policy** in the top panel.
2. Go to **Groups> Nodes** in the left
3. Click **Tasks > Create**
4. Click the **Add** button
5. After setting the condition of the target, click the **Add** button.
6. Click the **Create** button.

**2. Create Action for Enforcement Policy**

1. Go to **Policy > Enforcement Policy > Agent Action**
2. Click **Tasks > Create**
3. Select **Notify User** plguin on the list.
4. Click **Create** button.

**3. Create Enforcement Policy**

1. Go to **Policy > Enforcement Policy**
2. Click **Tasks > Create**, Follow **Enforcement Policy Wizard**
3. For **General** tab, Please input **ID** and click **Next** button.
4. For **Node Group** tab, Please move Node Group you created to **Selected**
5. Click **Finish** button.
6. Click **Apply** button on the top right.

## 14.5.17 Scan Condition Settings

You can scan macOS condition settings to include processes, files, system, and authenticated users.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Scan Condition Settings** in the Agent Action window.

Under **General** section:

#. For **CWP Message**, add message to be displayed in accordance with the Policy. #. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section: (*Must have Conditions added for this plugin to work*)

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Enter in **Conditions**, and adjust **Execution Interval.**
5. For **Periodic Interval**, choose from seconds, minutes, hours, days weeks, or months. (*Default is 12 hours*)
6. Click **Update.**

7. Go to **Node Policy** in the left Policy panel.
8. Click the **Default Policy** in Node Policy window.
9. Find **Agent Action**. Click **Assign.**
10. Find **Scan Condition Settings** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**
12. Click **Update.**

## 14.5.18 Shut Down System

You can control the power options (e.g. Sleep, Restart, and Shutdown) and control how long the Mac OS device stays up and running after it wakes from sleep.

### Add the Agent Action to a Policy

1. Go to **Node Policy** in the left Policy panel.
2. Click the **Default Policy** in Node Policy window.
3. Find **Agent Action**. Click **Assign.**
4. Find **Control Power Options** in the **Available** section. Select and drag it into the **Selected** section.
5. Click **Add.**
6. Click **Update.**

### Control Power Options

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Click the desired **Policy ID** in Node Policy window.
4. Find and click **Control Power Options** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Power Control Action**, specify how to control the power of the device. (*Sleep, Restart, Shutdown*)
2. For **Disable abort-shutdown**, toggle **On** or **Off** to select if the endpoint user can abort the shutdown.
3. For **Waiting time**, adjust the time to delay applying the policy after user input. (*Seconds - hours*)
4. For **Uptime for Power Control**, specify how long after computer awakening to execute the power control action.
5. For **Show Title bar**, toggle **On** or **Off** to select if the message box title bar will be displayed.

6. For **Message Contents**, specify the message contents, text and height. You can use HTML formatting and macros to display information from Genians.
7. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
8. Click **Update.**

## 14.5.19 Terminate Process

You can configure the agent to automatically terminate a process when it is detected as running.

### Add Agent Action to a Policy

1. Go to **Policy** in the top panel.
2. Go to **Node Policy** in the left Policy panel.
3. Click the **Default Policy** in Node Policy window.
4. Find **Agent Action**. Click **Assign.**
5. Find **Terminate Process** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

### Configure Plugin

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Find and click **Terminate Process** in the Agent Action window.

Under **Conditions** section:

1. Click **Add**, add message to be displayed in accordance with the Policy.
2. For **Criteria** select **Process**, then configure the **Operator**, **Value**, and **Description**.

Under **Settings**:

1. Select **On**.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Execution Interval**:

1. Adjust Periodic Interval.(Seconds - Months)
2. Click **Update**

### 14.5.20 Update macOS

With this agent action, you can control if the macOS device gets updates and how often. You can also determine the whether to install updates automatically, or just download updates to allow the user to install on their own.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Update macOS** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Execution Interval**, specify the time interval to execute an action on a scheduled basis. (*hours - months*)
2. For **Scheduled Check**, turn **On** to check for updates on a scheduled basis.
3. For **Operation Mode**, specify whether to **check for updates** or to **install the updates.**
   - **Scheduled Installation**, specify whether to install the updates on a scheduled basis.
4. For **Restart Options**, specify whether to **Prompt** or **Restart.**
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.
7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find Update macOS in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

### 14.5.21 Controlling External Device

- External devices are all devices that can be connected to the macOS system.
- You can control an external device by disabling or removing the external device so that it can request approval for a set period of time.

### Step 1. Create Device Group

- A device group is a function that defines a set of devices required for control. It can be used for blocking or exception on the policy.

1. Go to **Policy** in the top panel.
2. Go to **External Device Group** in the left Policy panel.
3. Click **Tasks > Create.**
4. Find **General** section enter unique **ID name.** (*e.g. "USB Storage Devices"*)
5. Select **OS Type > macOS** in Device Group Setting section.
6. Click *Conditions > Add** and select **Device Name** to control.
7. Find **Settings** section enter the following:
8. If the deivce type is USB Disk, you can specify following information in **Conditions**.
   - **Vendor**: Specify USB Vendor name.
   - **Model**: Specify USB Model name.
   - **Serial No.**: Specify USB Serial Number.
9. If the deivce type is a CD/DVD, Printer, USB Tethering or USB LanAdapter, you can specify following information in **Conditions**.
   - **Model**: Specify the Model name.

   **Note:** Conditions must be defined in accordance with the language settings of the endpoints operating system.

10. Click **Add.**
11. Click **Save.**

### Step 2. Create External Device Policy

- Control External Device Policy defines the device groups to block or allow the target to perform device control.
- When the plugin is uploaded, the device policy for the basic output device is provided as a template. (Device Control Policy ID: Data Prevention)

1. Go to **Policy** in the top panel.
2. Go to **Policy > External Device Policy** in the left Policy panel.
3. Click **Tasks > Create**
4. Find **General** section enter unique **ID name.** (*e.g. "USB Storage Policy"*)
5. Find **Node Group** section click **Assign** and choose **Node Group**
6. Find **External Devices** section click **Assign** and choose **USB Storage Devices.** (You can select **Default Device Group** below.)
7. Click **Save.**
8. Click **Apply.**

**External Device Exceptions :**

| | |
|---|---|
| **Bluetooth Tethering** | • Network adapters that connects Android or iPhone via Bluetooth |
| **CD/DVD** | • Devices in CD-ROM Drive Class |
| **Local Printer** | • Printer connected directly to local PC |
| **USB Disk** | • USB type storage device (system profiler's SPUSBDataType information) |
| **USB Network Adapter** | • Network adapter connected via a USB port |
| **USB Tethering** | • Network adapter connected via USB cable to the mobile device (network's hardward port is iPhone USB)<br>• Android cannot connect to macOS via USB Tethering |

1. Click the **Create** button.

### Step 3. Configure Control External Device Plugin

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control External Device.**
4. Find **Agent Action > Control Methods** section and choose to **Disable** or **Uninstall.**
5. Click **Update.**

### Step 4. Enable Agent Action on Node Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign.**
5. Find **Control External Device** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

### 14.5.22 Controlling Network Folder Sharing

You can collect shared network folder information, control access, and specify permissions.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Network Folder Sharing** in the Agent Action window.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Collecting Shared Folder Information**, select **Off** to not collect info about shared folders over the network.
2. For ** Stopping Folder sharing**, turn **On** to stop folder sharing.
   - **Delay Timeout**, specify the time when the shared folder access is revoked. (*seconds* - *months*)
   - **Read-only Folder Exception**, turn **On** to allow access to the folder with read-only permissions. (Read smb_read_only value)
   - **Stopping Everyone Folder Only**, turn **On** to stop sharing the folder with everyone permissions. (Read smb_guest_access value)
3. For **Folder Sharing Expiry Notification**, select Custom Message or Default Message in Pop-up window.
4. Click **Update.**
5. Go to **Policy > Node Policy** in the left Policy panel.
6. Click the **desired Policy ID** in Node Policy window.
7. Find Agent Action. Click Assign.
8. Find **Control Network Folder Sharing** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.5.23 Checking Password Validation

Policy Server communicates with the Agent to collect check the strength of a macOS password

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Checking Password Validation** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. Select **On** or **Off** for:
    - **Display Account with Strong Password**: Specify whether to display an account with a strong password.
    - **Immovable Dialog Box** - Specify whether to lock Dialog Box in the center of the screen.

- The settings below may be defined for both **Logged On Users** and **Logged Off Users**.

1. For **Password Check Options**, select **None**, **Protection** (check for password), or **Strength** (Checks password against password policy. See: *Managing Users and Groups*)
    - For **Action**, select **Force Password Change** (Which will mandate a password to be added, or mandate a password is made compliant, depending on the main password check option chosen), or **Check Password Strength** (Can be selected to check password strength without additional action, regardless of the main password check option. See: *Managing Users and Groups*) .
2. For **Maximum Password Age**, Specify the period of time (*days - months*) that a password can be used before the system requires the user to change it Enter `0` to Disable.
    - For **Expiry Notification**, Specify the period of time that users are notified before password expiration (*days - months*).
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Checking Password Validation** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.5.24 Transferring agent information externally

**Note:**

- Transferring agent information externally is available from Genian NAC version 6.0.23 or higher. For versions below 6.0.23, please use the Deploy Files V2 plugin.

- Agent information external transmission is used when you want to integrate the agent's authentication information with external third-party applications.
- When a node performs authentication and the agent's authentication status becomes either Authenticated or Deauthenticated, the authentication information is transmitted to an external third-party application. This is used to perform authentication across multiple solutions with a single authentication process.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Transferring agent information externally** in the Agent Action window.
4. For **CWP Message**, add message to be displayed in accordance with the Policy.
5. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

[ Settings ]

| Item Name | Setting Item | Description | Notes |
|---|---|---|---|
| Path | Enter the target file path directly | Specify the file path of the target to which the information will be delivered. | File Path Macro Options |
| Transfer information | Login/Logout Credentials | Transmit both login and logout events | When using periodic logout via node policy, it is also possible to transmit only login authentication information. |
| | Login credentials | Transmit only login authentication information | |
| Execution Account | Root Account | Perform information transmission tasks as the root account | '.app' files can only be executed by the logged-in user account. |
| | Logon Account | Perform information transmission tasks as the logged-in user account | |
| UserID conversion method | NONE | Used when converting the user ID before transmitting the received authentication information. | |
| | Regular expression | | |
| | Convert to uppercase | | |
| | Convert to lowercase | | |
| Interval | When information changes | Select the interval at which the agent's authentication information will be transmitted. | When information changes |
| | At Operating System Startup | | When information changes + At Operating System Startup |
| | In Periodic Interval | | When information changes + In Periodic Interval |
| Encryption Algorithm | None | Used when authentication information needs to be encrypted during transmission. | When using encryption options other than BASE64, the data is additionally encoded with BASE64 before transmission. |
| | Base64 | | |
| | AES-128 | | |
| | AES-256 | | |
| | Blowfish | | |
| | CAST | | |
| | SEED | | |

1. Click the Add button in the **External Transfer List** to add the file for transmitting authentication information (third-party integration process file).
2. Select the items to **Transfer information**.
3. Choose whether to perform **UserID conversion method**.
4. Select the **Interval**.
5. Choose the **Encryption Algorithm**.

6. Click the **Add** button.

- If there are additional targets for external transmission, click the Add button to include them.

1. Click **Update.**
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find Agent Action. Click Assign.
5. Find **Transferring Agent Information Externally** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

## 14.5.25 Control macOS Firewall

- Allow or block traffic based on rules.
- Control network traffic using rules such as App BundleID, App Path, protocol, port, remote IP, etc.

### Configure macOS Firewall Control Options

1. **Rule Selection**: You can select a general rule and an Internet Kill Switch rule.
2. **General Rule**: Allows all Internet except for the connection blocking rule. It operates in BlackList mode.
3. **Internet Kill Switch**: Blocks all Internet except for the connection allowance rule. It operates in WhiteList mode.
4. **Connection Allow/Block Rule**: Select the conditions of the rule you want to control using direction, app path, app bundle ID, protocol, remote IP, port, etc.
5. **Notification Message**: Displays a pop-up message to the user when traffic is blocked due to a rule.
6. **Prevent Duplicate Message Notification**: Does not display duplicate notification messages when multiple traffics occur at short intervals.
7. **Prevent Duplicate Message Notification Time**: Does not display duplicate notification messages for a specified period of time.

### Internet Kill Switch

This feature automatically blocks general internet traffic on the endpoint when the VPN tunnel is abnormal or disconnected, preventing data/IP leaks.

- Ensures forced VPN connection when used with the Always-On option of the ZTNA Connection Manager action.

For instructions on using the ZTNA Connection Manager, refer to the *ZTNA-Client* document.

### Configuration Method

Assign the minimum policy required to connect to the VPN. When the Internet Kill Switch setting is On, all internet traffic is blocked, and it operates in a WhiteList manner.

1. Go to **Policy** in the top menu.
2. Go to **Policy > Node Policy** in the left policy menu.
3. Click the Node Policy to which you want to apply the Internet Kill Switch.
4. In the **Agent Action** section, assign the **Control macOS Firewall** node action.
5. Enable the **Internet Kill Switch** option.

When using ZTNA-Client, assign the minimum policy as follows.

# 14.6 Controlling Linux

You can control Linux devices with the Agent installed using these plugins:

## 14.6.1 Manage ARP Table

You can manage the ARP Table on the devices by Deleting Static ARP Entries, or preventing ARP conflicts.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Manage ARP Table** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Deleting Static ARP Entries**, turn **On** to delete static ARP entries.
2. For **Static ARP for IP Conflict-prevention**, turn **On** to use Static ARP Entries for IP Conflict-prevention to prevent from ARP Spoofing.
   - **Node Group**, Optional setting to apply **Static ARP for IP Conflict-prevention** to specific Node Groups.
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Manage ARP Table** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**

9. Click **Update.**

**Note:** Go to Management > Node > IPAM Tab > IP Policy to configure Conflict-prevention Settings.

### 14.6.2 Genian Login PAM

Perform VPN connection and program launch along with OS login.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Genian Login PAM** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. For **OS Account Single Sign-On**, Specifies whether to automatically authenticate users with OS logon accounts.
2. For **Execute program integration**, Add a program to run during OS authentication or after authentication is complete.
    - **Path**: Specify a path for a file that will be run after a user is successfully authenticated. (File Path Macro Options)
    - **Command Line Parameter**: Specify a command line parameter.
    - **Encryption Algorithm**: Specify how to encrypt an Execution Option.
    - **Encryption Key**: The key must be as long as the encryption algorithm in use allows.
    - **Run point**: Specify a program run point.
    - **Execution Account**: Specify an account to execute a file.
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Genian Login PAM** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.6.3 Update Linux

Checks for linux updates and report.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Update Linux** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
2. Click **Update.**
3. Go to **Node Policy** in the left Policy panel.
4. Click the **Default Policy** in Node Policy window.
5. Find **Agent Action**. Click **Assign.**
6. Find **Update Linux** in the **Available** section. Select and drag it into the **Selected** section.
7. Click **Add.**
8. Click **Update.**

### 14.6.4 ZTNA Connection Manager

Controls Zero trust network access Connection Manager options and actions.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click ZTNA Connection Manager in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. For **Connection Manager**, specify the type of connection manager.
   - **Site**: Set "Site Settings Information" in Connection Manager.

2. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find ZTNA Connection Manager in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

Users can use it through the **Network Access** button on the tray icon.

1. Click the **Network Access** button on the tray icon.
2. Click the site you want to connect to.
3. Proceed with the connection through the **Agent Authentication window** that appears on the screen.
4. Select **two-step authentication** as needed.
   - See *2-Step Authentication*

### 14.6.5 Collecting Network Information

Policy Server communicates with the Agent to collect Ipv4 and Ipv6 network information on end users Linux devices.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Network Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
2. Click **Update.**
3. Go to **Node Policy** in the left Policy panel.
4. Click the **Default Policy** in Node Policy window.
5. Find **Agent Action**. Click **Assign.**
6. Find **Collect Network Information** in the **Available** section. Select and drag it into the **Selected** section.
7. Click **Add.**
8. Click **Update.**

### 14.6.6 Collecting Monitor Information

Policy Server communicates with the Agent to collect information about the monitor that is connected to your Windows.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Monitor Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Collect Monitor Information** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.6.7 Control Personalization

You can control the screen lock on your Windows devices which requires users to authenticate upon wake from sleep.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Personalization** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. For **Lock Screen Scan**, select **Off** to disable the collection of info on the configured Screen Lock.
2. For **Screen Saver Enforcement**, turn **On** enforce a Screen Lock.
   - **Waiting Time**: Set the waiting time before switching to the screen saver. (*minutes - hours*)

- **User Waiting Time**: Change the waiting time even if it is longer than the waiting time used by the PC.

3. For **Reauthentication**, turn **On** to require User Authentication from Wake or Screen Lock.
4. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.
7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Control Personalization** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

## 14.6.8 Collecting Antivirus Software Information

Policy Server communicates with the Agent to collect antivirus software information that is installed on your Linux devices.

### List of Supported Antivirus

Check all Antivirus supported with Genian ZTNA by version.

| Vendor | Product | Genian Version |
|---|---|---|
| Cisco Systems | ClamAV | 5.0.46 |
| Sophos | Sophos server protection | 5.0.48 |

### Collect Antivirus Software Information

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Antivirus Software Information** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
2. Click **Update.**
3. Go to **Node Policy** in the left Policy panel.
4. Click the **Default Policy** in Node Policy window.

5. Find **Agent Action**. Click **Assign.**
6. Find **Collect Antivirus Software Information** in the **Available** section. Select and drag it into the **Selected** section.
7. Click **Add.**
8. Click **Update.**

### 14.6.9 Notify User

You can notify users with informational messages or warnings. The message may be displayed using a slide-out notification or redirection to a URL.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Notify User** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Contents for Slide-out Box Notification**, type in contents to display in slide-out box notification.
2. For **CWP Page Redirection**, turn **On** to redirect to CWP page when a user clicks a slide-out notification.
   - **CWP Page Redirection URL**, click **Use Template** or specify a URL for CWP redirection when a user clicks a slide-out notification.
3. For **Enforcing Notification**, specify whether to disable to force closing a notification.
   - **Notification Message Type**, specify a message type for a user notification. (*Informational, Warning*)
   - **Generating Log for User Read Notification**, specify whether to generate a log when a user reads a notification.
4. For **Automatic pop-up**, Enable to display detailed message contents in a pop-up badge, rather than only a preview.
5. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
6. Click **Update.**
7. Go to **Node Policy** in the left Policy panel.
8. Click the **Default Policy** in Node Policy window.
9. Find **Agent Action**. Click **Assign.**
10. Find **Notify User** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**
12. Click **Update.**

### 14.6.10 Collecting Software Information

Policy Server communicates with the Agent to collect software information that is running on end users Linux devices and displays it on The [Software Information - Software] List tab of the node information.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Software Information** in the Agent Action window. window (*Notice there are three, one for Windows, one for MacOS and another for Linux*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Collect Software Information** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.6.11 Scan Condition Settings

You can scan Linux condition settings to include processes, files, system, and authenticated users.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Scan Condition Settings** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section: (*Must have Conditions added for this plugin to work*)

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
4. Enter in **Conditions**, and adjust **Execution Interval.**
5. For **Periodic Interval**, choose from seconds, minutes, hours, days weeks, or months. (*Default is 12 hours*)

6. Click **Update.**
7. Go to **Node Policy** in the left Policy panel.
8. Click the **Default Policy** in Node Policy window.
9. Find **Agent Action**. Click **Assign.**
10. Find **Scan Condition Settings** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**
12. Click **Update.**

### 14.6.12 Collecting Computer OS Information

The Policy Server collects Operating System information from end users Linux devices using the Agent.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Computer OS Information** in the Agent Action window (*Notice there are three, one for Windows, one for MacOS and another for Linux*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
4. Set **Time Object**, **Retry Interval** and **Retry Attempts**
5. Click **Update.**
6. Go to **Node Policy** in the left Policy panel.
7. Click the **Default Policy** in Node Policy window.
8. Find **Agent Action**. Click **Assign.**
9. Find **Collect Computer OS Information** in the **Available** section. Select and drag it into the **Selected** section.
10. Click **Add.**
11. Click **Update.**

### 14.6.13 Controlling Network Interface

You can control wired and wireless network interfaces on end users linux devices by disabling wired, wireless mode.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Network Interface** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. For **Network Type**, specify the Network type to be disabled. (*Wired, Wireless, or both*)
2. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Control Network Interface** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

### 14.6.14 Terminate Process

You can kill specific processes that are running on the end users Linux devices and schedule the frequency to verify that they continue to not run.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Terminate Process** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Terminate Process**, set up a process that should not be used on the device through that option.

2. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
3. Click **Update.**
4. Go to **Node Policy** in the left Policy panel.
5. Click the **Default Policy** in Node Policy window.
6. Find **Agent Action**. Click **Assign.**
7. Find **Terminate Process** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

### 14.6.15 Collecting Hardware Information

Policy Server communicates with the Agent to collect hardware information about Linux devices.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Collect Hardware Information** in the Agent Action window. (*Notice there are three. One for Windows,one for MacOS and another for Linux*)

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**
3. For **Plugin Settings**, adjust **CPU, Memory, and Disk Space Utilization** Thresholds based off of your network requirements. **Motherboard info** is also collected.
4. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
5. Set **Time Object**, **Retry Interval** and **Retry Attempts**
6. Click **Update.**
7. Go to **Node Policy** in the left Policy panel.
8. Click the **Default Policy** in Node Policy window.
9. Find **Agent Action**. Click **Assign.**
10. Find **Collect Hardware Information** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**
12. Click **Update.**

### 14.6.16 Checking Password Validation

Policy Server communicates with the Agent to collect check the strength of a Linux password

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Checking Password Validation** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings:**

1. Select **On** or **Off** for:
   - **Display Account with Strong Password**: Specify whether to display an account with a strong password.
   - **Immovable Dialog Box** - Specify whether to lock Dialog Box in the center of the screen.

- The settings below may be defined for both **Logged On Users** and **Logged Off Users**.

1. For **Password Check Options**, select **None**, **Protection** (check for password), or **Strength** (Checks password against password policy. See: *Managing Users and Groups*)
   - For **Action**, select **Force Password Change** (Which will mandate a password to be added, or mandate a password is made compliant, depending on the main password check option chosen), or **Check Password Strength** (Can be selected to check password strength without additional action, regardless of the main password check option. See: *Managing Users and Groups*) .
2. For **Maximum Password Age**, Specify the period of time (*days - months*) that a password can be used before the system requires the user to change it Enter `0` to Disable.
   - For **Expiry Notification**, Specify the period of time that users are notified before password expiration (*days - months*).
3. For **Execution Interval**, adjust Periodic Interval. (*Seconds - hours*)
4. Click **Update.**
5. Go to **Node Policy** in the left Policy panel.
6. Click the **Default Policy** in Node Policy window.
7. Find **Agent Action**. Click **Assign.**
8. Find **Checking Password Validation** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

### 14.6.17 Controlling External Device

- External devices are all devices that can be connected to the Linux system.
- You can control an external device by disabling or removing the external device so that it can request approval for a set period of time.

#### Step 1. Create Device Group

- A device group is a function that defines a set of devices required for control. It can be used for blocking or exception on the policy.

1. Go to **Policy** in the top panel.
2. Go to **External Device Group** in the left Policy panel.
3. Click **Tasks > Create.**
4. Find **General** section enter unique **ID name.** (*e.g. "USB Storage Devices"*)
5. Select **OS Type > Linux** in Device Group Setting section.
6. Click *Conditions* > *Add** and select **Device Name** to control.
7. Find **Settings** section enter the following:
8. If the deivce type is USB Disk, you can specify following information.
   - **USB Vendor**: Specify USB Vendor name.
   - **USB Model**: Specify USB Model name.
   - **USB Serial No.**: Specify USB Serial Number.

   **Note:** Conditions must be defined in accordance with the language settings of the endpoints operating system.

9. Click **Add.**
10. Click **Save.**

#### Step 2. Create External Device Policy

- Control External Device Policy defines the device groups to block or allow the target to perform device control.
- When the plugin is uploaded, the device policy for the basic output device is provided as a template. (Device Control Policy ID: Data Prevention)

1. Go to **Policy** in the top panel.
2. Go to **Policy > External Device Policy** in the left Policy panel.
3. Click **Tasks > Create**
4. Find **General** section enter unique **ID name.** (*e.g. "USB Storage Policy"*)
5. Find **Node Group** section click **Assign** and choose **Node Group**
6. Find **External Devices** section click **Assign** and choose **USB Storage Devices.** (You can select **Default Device Group** below.)
7. Click **Save.**

8. Click **Apply.**

**External Device Exceptions :**

| | |
|---|---|
| **USB Disk** | • Storage devices of USB type. |
| **CD/DVD** | • Devices in CD-ROM Drive Class |
| **USB Network** | • Network connected to USB port. |
| **Local Printer** | • Printer connected directly to local PC. |
| **Bluetooth** | • All devices in bluetooth class. |
| **Camera** | • All devices in camera class. |
| **Mouse** | • All devices in mouse class. |
| **Keyboard** | • All devices in keyboard class. |
| **Sound** | • All devices in sound class. |
| **Microphone** | • All devices in microphone class. |

1. Click the **Create** button.

### Step 3. Configure Control External Device Plugin

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control External Device.**
4. Find **Agent Action > Control Methods** section and choose to **Disable** or **Uninstall.**
5. Click **Update.**

### Step 4. Enable Agent Action on Node Policy

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find **Agent Action**. Click **Assign.**
5. Find **Control External Device** in the **Available** section. Select and drag it into the **Selected** section.

6. Click **Add.**
7. Click **Update.**

### 14.6.18 Controlling Network Folder Sharing

You can collect shared network folder information, control access, and specify permissions.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Control Network Folder Sharing** in the Agent Action window.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Collecting Shared Folder Information**, select **Off** to not collect info about shared folders over the network.
2. For **Stopping Folder sharing**, turn **On** to stop folder sharing.
   - **Delay Timeout** : Specify the time when the shared folder access is revoked. (*seconds - months*)
   - **Read-only Folder Exception** : Allow to access the folder with read-only permission.
   - **Owner Exception** : The owner of the folder allows write permission.
   - **Restrict Guest Access** : If this option is set to On, only folders with Guest Access enabled will have sharing disabled.
   - **Folder Sharing Expiry Notification** : select Custom Message or Default Message in Pop-up window.
3. Click **Update.**
4. Go to **Policy > Node Policy** in the left Policy panel.
5. Click the **desired Policy ID** in Node Policy window.
6. Find Agent Action. Click Assign.
7. Find **Control Network Folder Sharing** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

### 14.6.19 Uninstall Programs

Removes specific uninstallable programs among Debian packages and programs installed with Snap.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Uninstall Programs** in the Agent Action linux.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Program**, Set the name of the program to be removed among Debian packages and programs installed with Snap.
2. For **Force removal**, When deleting a program, problems such as dependencies are ignored and forcibly removed.
3. For **Notification Before Uninstalling**, specify whether to notify a user before uninstalling a program.
   - **Contents**, add contents to notify user.
4. For **Restart Options**, specify whether to Notify User or Auto-Restart.
5. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
6. Click **Update.**
7. Go to **Node Policy** in the left Policy panel.
8. Click the **Default Policy** in Node Policy linux.
9. Find **Agent Action**. Click **Assign.**
10. Find **Uninstall Programs** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**
12. Click **Update.**

### 14.6.20 Transferring Agent Information Externally

**Note:**

- Transferring agent information externally is available from Genian NAC version 6.0.35 or higher. For versions below 6.0.35, please use the Deploy Files V2 plugin.

- Agent information external transmission is used when you want to integrate the agent's authentication information with external third-party applications.
- When a node performs authentication and the agent's authentication status becomes either Authenticated or Deauthenticated, the authentication information is transmitted to an external third-party application. This is used to perform authentication across multiple solutions with a single authentication process.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Find and click **Transferring agent information externally** in the Agent Action window.
4. For **CWP Message**, add message to be displayed in accordance with the Policy.
5. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Settings**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

[ Settings ]

| Item Name | Setting Item | Description | Notes |
|---|---|---|---|
| Path | Enter the target file path directly | Specify the file path of the target to which the information will be delivered. | File Path Macro Options |
| Transfer information | Login/Logout Credentials | Transmit both login and logout events | When using periodic logout via node policy, it is also possible to transmit only login authentication information. |
| | Login credentials | Transmit only login authentication information | |
| UserID conversion method | NONE | Used when converting the user ID before transmitting the received authentication information. | |
| | Regular expression | | |
| | Convert to uppercase | | |
| | Convert to lowercase | | |
| Interval | When information changes | Select the interval at which the agent's authentication information will be transmitted. | When information changes |
| | At Operating System Startup | | When information changes + At Operating System Startup |
| | In Periodic Interval | | When information changes + In Periodic Interval |
| Encryption Algorithm | None | Used when authentication information needs to be encrypted during transmission. | When using encryption options other than BASE64, the data is additionally encoded with BASE64 before transmission. |
| | Base64 | | |
| | AES-128 | | |
| | AES-256 | | |
| | Blowfish | | |
| | CAST | | |
| | SEED | | |

1. Click the Add button in the **External Transfer List** to add the file for transmitting authentication information (third-party integration process file).
2. Select the items to **Transfer information**.
3. Choose whether to perform **UserID conversion method**.
4. Select the **Interval**.
5. Choose the **Encryption Algorithm**.
6. Click the **Add** button.

- If there are additional targets for external transmission, click the Add button to include them.

1. Click **Update.**
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Click the **desired Policy ID** in Node Policy window.
4. Find Agent Action. Click Assign.

5. Find **Transferring Agent Information Externally** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

### 14.6.21 Shut Down System

You can control the power options (e.g. Sleep, Restart, and Shutdown) and control how long the Linux device stays up and running after it wakes from sleep.

#### Add the Agent Action to a Policy

1. Go to **Node Policy** in the left Policy panel.
2. Click the **Default Policy** in Node Policy window.
3. Find **Agent Action**. Click **Assign.**
4. Find **Control Power Options** in the **Available** section. Select and drag it into the **Selected** section.
5. Click **Add.**
6. Click **Update.**

#### Control Power Options

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Agent Action** in the left Policy panel.
3. Click the desired **Policy ID** in Node Policy window.
4. Find and click **Control Power Options** in the Agent Action window.

Under **General** section:

1. For **CWP Message**, add message to be displayed in accordance with the Policy.
2. For **Label**, add labels to help categorize your plugins with custom labels that appear in the "Description" field.

Under **Agent Actions** section:

1. For **Boolean Operator**, choose **AND** or **OR** to add optional conditions.
2. For **Condition**, click **Add** and select your optional conditions. **Criteria/Operator/Value**

Under **Plugin Settings** section:

1. For **Shutdown Type**, specify how to control the power of the device. (*Sleep, Restart, Shutdown*)
2. For **Disable abort-shutdown**, toggle **On** or **Off** to select if the endpoint user can abort the shutdown.
3. For **Wait Time Setting**, Power control is performed only after the set time has elapsed.
   - **Uptime for Power Control**, Specify the uptime more than the specified to control the power.
   - **No input waiting time**, Control is performed when there is no input for a set period of time.
4. For **Waiting time**, adjust the time to delay applying the policy after user input. (*Seconds - hours*)
5. For **Show Title bar**, toggle **On** or **Off** to select if the message box title bar will be displayed.

6. For **Method for Displaying Message**, Specify how to display the message.
   - For **Message Contents**, Please input messages you would like to show on the message box.
   - For **Image**, Upload a bitmap image file (.bmp).
7. For **Execution Interval**, adjust Periodic Interval. (*Seconds - months*)
8. Click **Update.**

## 14.6.22 Control Linux Firewall

### Internet Kill Switch

This feature automatically blocks general internet traffic on the endpoint when the VPN tunnel is abnormal or disconnected, preventing data/IP leaks.

- Ensures forced VPN connection when used with the Always-On option of the ZTNA Connection Manager action.

For instructions on using the ZTNA Connection Manager, refer to the *ZTNA-Client* document.

### Configuration Method

Assign the minimum policy required to connect to the VPN. When the Internet Kill Switch setting is On, all internet traffic is blocked, and it operates in a WhiteList manner.

1. Go to **Policy** in the top menu.
2. Go to **Policy > Node Policy** in the left policy menu.
3. Click the Node Policy to which you want to apply the Internet Kill Switch.
4. In the **Node Action** section, assign the **Control Linux Firewall** node action.
5. Enable the **Internet Kill Switch** option.

When using ZTNA-Client, assign the minimum policy as follows.

| Direction | Remote IP | Local IP | Protocol |
|---|---|---|---|
| Outbound | All | ZTNA Gateway IP or Domain | TCP, Local Port: All, Remote Port: 1194 |

## 14.6.23 Deploy Files v2

**Note:** The file distribution plugin is not included in the CC evaluation items, so public institutions requiring CC certification cannot use this plugin.

The file distribution plugin executes files or downloads them to a specific location. The Policy Server communicates with the agent to distribute, execute, and install files on endpoints.

- Distribute necessary files to endpoints
- Install uninstalled software on endpoints

Deploy Files v2 plugin has been added, focusing on strengthening security from the existing file distribution plugin.

Deploy Files v2 plugin provides file integrity verification and distributor identity confirmation for secure file distribution.

- Performs 3-step integrity verification
- Distributor identification and approval by end-user

The Deploy Files v2 plugin mandatorily requires digital signatures for files being distributed and uses the Sigstore Signing method, designed for supply chain security, for digital signatures and signature verification. Deploy Files v2 plugin can selectively use two methods of Sigstore Signing: Sigstore Keyless Signing and Public Key Signing.

| Verification Method | Sigstore Keyless Signing (Keyless) | Public Key Signing (self-managed-key) |
|---|---|---|
| Verification Content | • Performs digital signature on distribution files with identity information by authenticating with OIDC (OpenID Connect) from Google/Github/MS<br>• Endpoints receiving the file verify that it is a Sigstore-signed file using User ID (e.g., Google ID) and OIDC (Google Account) information | • Performs digital signature on distribution files using self-owned private/public keys<br>• Certificates (public keys) for verification are distributed upon Node Action reception |
| Environment Setup | • Usable only in environments with Internet access | • Usable in both Internet and isolated network environments |
| Key Management | • Requires only security for administrator accounts, as no separate keys are used | • Requires secure storage of separate private keys |
| Preparations | • Cosign binary file required for digital signing of distribution files (Download cosign-windows-amd64.exe from **Assets** at Sigstore GitHub Release v2.1.1 download)<br>• External internet communication required for digital signing/signature verification of distribution files (Signing PC, Policy Server, User Endpoint)<br>• OIDC (Google, Git, MS) accounts required for digital signing of distribution files | • Cosign binary file required for digital signing of distribution files<br>• Keys required for digital signing of distribution files, can be generated using cosign or prepared separately |
| Constraints | • Cannot change from the initially registered distributor to another distributor | • Cannot change from the initially registered distributor to another distributor<br>• Key files used for digital signing of distribution files must be managed separately (e.g., USB) |

### Sigstore Keyless Signing Method

Sigstore generates **short-lived certificates using OpenID Connect (OIDC)**.
**These certificates are used to sign software**, and the signed software can be publicly verified via cosign.

OIDC is an extension of OAuth 2.0, a framework that uses login authentication to provide users access to resources. Because OIDC can generate certificates without requiring user passwords, it is used by Sigstore to generate short-lived certificates.

**How to Use Sigstore Keyless Signing**

**Step1. Digital Signature of Distribution File**

1. Download cosign and save it to the directory to be used for digital signing of the distribution file.
2. Change the file name to cosign.
3. Copy the file to be digitally signed to the directory.
4. Open a terminal and go to the directory where the cosign file is located.
5. Perform digital signing by entering the command below:

```
> cosign sign-blob {Distribution_File_Name} --output-certificate
↪{Generated_Cert_File_Name.cert} --output-signature {Generated_Signature_
↪File_Name.sig}
```

6. Copy the URL information displayed in the terminal and access the web page using a browser.
7. Confirm that the 8-character value displayed in the terminal is the same as the 8-character value displayed in the terminal and click the `Submit` button.
8. Select one of the three OIDCs: `Git, Google, Microsoft` and perform authentication.
9. After a moment, enter `y` in the terminal to agree to the terms of service.
10. Confirm that `Cert, Sig` files have been successfully generated in the directory.

**Step2. Verify Digital Signature**

1. In the terminal, enter the command below:

```
> cosign verify-blob {Distribution_File_Name} --certificate {Generated_
↪Cert_File_Name.cert} --signature {Generated_Signature_File_Name.sig} --
↪certificate-identity={ID_Used_for_Auth} --certificate-oidc-issuer={OIDC_
↪Issuer}
Example> cosign verify-blob agent.zip --certificate agent.cert --
↪signature agent.sig --certificate-identity=genian@genians.com --
↪certificate-oidc-issuer=https://accounts.google.com
```

2. If the digital signature is performed successfully, **Verified OK** will be displayed.

**Step3. Create Node Action**

1. Access the Policy Server Web Console and go to **Policy** in the top menu.
2. Go to **Node Policy > Node Action** in the left menu.
3. Click **Select Action > Create** in the top menu.

Below are **Basic Settings**.

4. For **Action Name**, use the format "(Purpose)Action Name" according to its purpose for easy distinction of node actions during future operation.
5. **Description** can be used to distinguish the purpose of the node action if it is used differently depending on the purpose.
6. Adding a **Label** allows you to classify the plugin with a custom label displayed in the "Description" input field.

Configure the **Action Execution Settings** below.

7. For **OS Type**, select the appropriate OS among macOS, Linux, and Windows targets.
8. **Condition Settings** are generally used to distribute files to users meeting specific conditions.

   ```
   Example: "if c:\%ProgramFiles%\abc.exe does not exist" condition means␣
   ↪distribution is only possible to endpoints where abc.exe does not exist.
   ```

9. In **Plugin Selection**, select **Deploy Files V2**.
10. For **Distribution File**, click the `Upload` button to select the file.
11. For **Distribution File Verification Method**, select Sigstore Keyless Signing.
12. For **Trusted OIDC Issuer**, select the OIDC (Github, Google, Microsoft) used for authentication during digital signing.
13. For **Trusted ID**, enter the ID (email address format) used for authentication during digital signing.
14. For **Certificate**, click the `Read File` button on the right to add the **cert** file generated during digital signing.
15. For **Signature**, click the `Read File` button on the right to add the **sig** file generated during digital signing.
16. For **Distribution Options**, configure the distribution method.

    - **Execute File**: If it's a compressed file, configure the file to execute in "File Path", and set "Execution Options" and "Execution Account" to execute the file. Set reboot preference after file execution via "Reboot Option".
    - **Download**: Specify the file and folder path on the endpoint where the distribution file will be copied.

17. Click the **Modify** button.
18. Go to **Node Policy** in the left Policy menu, then click **Default Policy**.
19. Find **Node Action Settings** and click the **Assign** button.
20. In the **Available** items, find **Deploy Files** and drag it to the **Selected** items.
21. Click the **Modify** button, then click the **Modify** button again.

**Note:**

For Sigstore Keyless Signing method, external communication is essential for digital signing/signature verification, and communication to the domains below must be allowed.

(Source: Policy Server, Agent), (Service Port: TCP/443)

rekor.sigstore.dev : Ledger recording system

oauth2.sigstore.dev : Sigstore oauth flow provisioning server

accounts.google.com : OIDC provider (If it's another OIDC, use that OIDC domain)

fulcio.sigstore.dev : sigstore CA server

tuf-repo-cdn.sigstore.dev : SLSA verification

### Public Key Signing Method

Sigstore cosign also provides a self-managed key digital signing method.

The Public Key Signing method involves directly generating a key for digital signing or using a separately created key that is already in use.

#### How to Use Public Key Signing

#### Step1. Digital Signature of Distribution File

1. Perform steps 1-4 of Step 1 in Sigstore Keyless Signing method, then proceed.
2. If you do not have a separate key for digital signing, enter the command below to generate a private key and public key for digital signing.

   ```
   > cosign generate-key-pair
   > Enter private key password
   > Confirm private key password
   > Enter ls to confirm that private key (key) file and public key (pub)␣
   ↪file have been generated.
   ```

3. If you have generated a key, perform digital signing on the distribution file using the generated key as follows:

   ```
   > cosign sign-blob {Distribution_File_Name} --key cosign.key --tlog-
   ↪upload=false --output-signature {Generated_Signature_File_Name.sig}
   Example> cosign sign-blob agent.zip --key cosign.key --tlog-upload=false -
   ↪-output-signature agent.sig
   ```

#### Step2. Verify Digital Signature

1. In the terminal, enter the command below:

   ```
   > cosign verify-blob {Distribution_File_Name} --key {Public_Key_File_Name.
   ↪pub} --signature {Generated_Signature_File_Name.sig} --insecure-ignore-
   ↪tlog=true --insecure-ignore-sct=true
   Example> cosign verify-blob agent.zip --key cosign.pub --signature agent.
   ↪sig --insecure-ignore-tlog=true --insecure-ignore-sct=true
   ```

2. If the digital signature is performed successfully, **Verified OK** will be displayed.

#### Step3. Create Node Action

1. Perform steps 1-10 of Step 3 in Sigstore Keyless Signing method, then proceed.
2. For **Distribution File Verification Method**, select Public Key Signing.
3. For **Trusted Public Key**, click the `Read File` button on the right to add the **pub** file that was generated during key creation.
4. For **Signature**, click the `Read File` button on the right to add the **sig** file that was generated during digital signing.
5. Perform steps 16-21 of Step 3 in Sigstore Keyless Signing method.

> **Danger:**
>
> **It is impossible to change the initially set distribution method and distributor**, so the Private key used during the initial node action creation must be **kept securely to prevent loss**.

Registered distributor information can be confirmed in Web Console Settings > Preferences > Agent > Distribution Options section.

CHAPTER

FIFTEEN

# DETECTING ANOMALIES

**Note:** This feature required Professional or Enterprise Edition

An **Anomaly** is a signature of abnormal activity that may indicate a security breach, or an outside entity searching for network or device vulnerabilities.

A **Vulnerability** is an opening that can be exploited to cause damage to a device, or to network security.

Genian ZTNA inspects network traffic to identify abnormalities in the network and marks endpoint devices that have Anomalies. You can configure custom **Anomaly Definitions** or use the seven pre-defined definitions provided by default to detect endpoint devices that are exposed to major Anomalies such as **Ad hoc Networks, ARP Bombing, ARP Spoofing, MAC+IP Clones, Port Scanning** and more.

## 15.1 Understanding Anomaly Detection

**Network Sensor** listens for abnormalities in network traffic and identifies endpoints with **Anomaly** and blocks them based on your access policies. You can configure Anomaly Definitions to detect abnormal network traffic such as **Ad hoc Network, ARP Bomb, Spoofed ARP, MAC+IP Clones,** and more.

For an anomaly to be detected, anomalies definitions must be assigned to node policies.

### 15.1.1 ARP Bomb

While the network sensor is monitoring ARP, it detects a device that generates excessive ARP packets and designates it as a critical Node. It detects abnormal ARP behavior and prevents attempts to disable network access or disable network access control. An attacker Node continually keeps sending request packets to the target Node, thereby causing its cache to fill up quickly. Soon the target Node will spend more of its resources to maintain its cache, which may lead to buffer overflow. And real mapping would never be entered in the cache.

### 15.1.2 MAC+IP Clones

The IP protocol uses IP and MAC addresses to identify the destination of the communication. Since there is no verification procedure at this time, it is easy to steal. If you have cloned the MAC / IP of the malicious device on the network, it is very difficult to check the normal system and the stolen system at the packet level.

However, Genian ZTNA can detect MAC / IP theft in a variety of ways. The network sensor periodically sends an ARP request to check the operation status of the device. If two replies are received at the same time, suspend the MAC / IP clone and designate the Node as a critical Node. In addition, if the user changes the MAC on the endpoint where the Agent is installed and the MAC is already being used by another device, the device is designated as a critical Node.

In addition, Genian ZTNA provides industry-leading platform detection to detect when a Node is changing to another platform, allowing administrators to see when changes are made, and to block devices when unauthorized platform changes are detected.

### 15.1.3 Multi-Homed / Ad hoc Network

Detects direct client-to-client communication (*Agent required*)

### 15.1.4 Port Scanning

Detects any device trying to scan TCP or UDP ports. Genian ZTNA uses a honeypot IP for detecting scanning devices.

### 15.1.5 Rogue DHCP Server Detection

The DNS value assigned by the DHCP server with IP can be compared to the DNS set on the sensor to detect an unusual DHCP server.

### 15.1.6 Rogue Gateway

Detects a Node having a rogue gateway configured (*Agent required*)

### 15.1.7 Sensor MAC Clones

Detects whether a Sensor MAC address is cloned (*No configuration settings required*)

### 15.1.8 Spoofed ARP

While ARP Enforcement is a technology used to block communication of network devices, ARP Spoofing is mainly used in malicious codes and is used for eavesdropping communication of other parties. Genian ZTNA can detect ARP packets through a network sensor to detect devices attempting to be spoofed.

In addition, it provides a function to block devices that attempted spoofing and to return to normal MAC through ARP cache detox.

### 15.1.9 Unauthorized Service Request

Detects the service that are not authorized but requested.

### 15.1.10 SNMP Disabled

Genian ZTNA allows SNMP Trap interworking with external systems to receive network control and de-control requests and designate the device as a dangerous node. In addition, the tag assignment feature allows SNMP Trap to perform control over the received device.

Please refer to *Tagging Assets Using Event* for tag assignment function.

## 15.2 Pre-Requisites for Anomaly Detection

To detect Anomalies, Administrators need to preconfigure components such as the Network sensor or Agent.

### 15.2.1 Anomaly Detection Mechanism

Anomalies are detected by Sensor or Agent.

To Detect Anomalies, both Sensor and Agent must be pre configured.

If Anomalies are detected by **Agent**, Administrators should assign the appropriate Agent action under the Node Policy.

| Anomalies ID | Detection Mechanism | Required Configuration |
|---|---|---|
| Multi-Homed / Ad hoc Network | Agent | Collect Network Information Agent plugin |
| ARP Bomb | Network Sensor | Add Virtual IP to Sensor Interface |
| Spoofed ARP | Network Sensor | Add Virtual IP to Sensor Interface |
| MAC+IP Clone | Network Sensor / Agent(ARP Spoofing) | Enable Network Sensor MAC + IP Clone Detection |
| Malware Detection | Agent | Collect Malware Information Agent plugin |
| Port Scanning | Network Sensor | Add Virtual IP to Sensor Interface |
| SNMP Disabled | Policy Server | SNMP Trap Options |
| Rogue DHCP Server Detection | Network Sensor | Network Sensor DHCP Server Scan |
| Sensor MAC Clones | Network Sensor | Network Sensor MAC + IP Clone Detection |
| Unauthorized Service Request | Network Sensor | Add Virtual IP to Sensor Interface |
| Rogue Gateway | Agent | Collect Network Information Agent plugin |

### 15.2.2 Configuration Details

#### Add Virtual IP to Sensor Interface

- Refer to: Add Virtual IP to Sensor Interface

#### Configuring Network Sensor DHCP Server Scan

1. Go to **System** in the top panel
2. Go to **System > Sensor** in the left Policy panel
3. Find **Sensor** and Click **Checkbox**
4. Click **Tasks > Edit Network Sensor Settings**
5. Go to **Sensor Settings > Network Scan > DHCP Server Scan** and choose **On** to the configure features
6. Click `save`

#### Configuring Policy Server SNMP Trap Options

1. Go to **Preferences** in the top panel
2. Go to **General > Log** in the left Policy panel
3. Go to **Log > SNMP Trap Options > SNMP Trap** and choose **On** to the configure features
4. Enter **Community String**
5. Click `Update`

#### Configuring Network Sensor MAC + IP Clone Detection

1. Go to **System** in the top panel
2. Go to **System > Sensor** in the left Policy panel
3. Find **Sensor** and Click **Checkbox**
4. Click **Tasks > Edit Network Sensor Settings**
5. Go to **Sensor Settings > Node Status Scan > MAC+IP Clone Detection** and choose **On** to the configure features
6. Click `save`

## 15.3 Creating Anomaly Definition

You can create custom Anomaly definitions to apply to Node Groups.

By default, there are eight pre-defined **Anomaly Definitions** that are frequently used. With the steps provided below, you can create your own Anomaly Definitions.

### 15.3.1 To Create an Anomaly Definition

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Anomaly Definition** in the left Policy panel.
3. Click **Tasks > Create.**

Under **General:**

1. For **ID**, type unique name.
2. For **CWP Message**, enter message to be presented to user.
3. For **User-defined Severity**, choose **Low, Medium,** or **High** for Anomaly severity.
4. For **Status**, must be **Enabled** to be active.
5. For **Node Group Exception**, optional setting to choose group to be an exception to this Anomaly.

Under **Anomaly Event:**

1. For **Event**, choose which Anomaly Definition to use.
2. For **Options**, customize the options as needed based on selected **Event.**
3. Click **Create.**

### 15.3.2 To Delete an Anomaly Definition

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Anomaly Definition** in the left Policy panel.
3. Click **Checkbox** of desired **Anomaly Definition.**
4. Click **Tasks > Delete.**
5. Click **OK.**
6. Click **Apply.**

## 15.4 Detecting Anomalies

Once the configured **Anomaly Definition** is assigned to the **Node Policy** you would like to apply, any anomaly will be almost immediately detected either by a **Network Sensor** or by an **Agent**. You may see the results in a variety of ways.

- Find **Anomaly** column in **Node Management.**
- Edit Node View for **Anomaly View.**
- Trace **Anomaly Logs.**
- Glance **Dashabord Widget** for **Anomaly** tab.
- Filter **Status & Filters.**

Furthermore, you can be notified about any pre-defined anomalies that are detected.

For notifying a user about the anomalies detected, see: *Sending Events*

### 15.4.1 Assign Pre-Configured Anomaly Definitions to existing Node Policy

By default, Node Policies are not detecting anomalies. For creating anomaly definitions see: *Creating Anomaly Definition*

To add Anomaly Definitions to a Node Policy and actively detect anomalies:

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Find and click on ** [Policy Name] ** in the main Node Policy window.
4. Find **Anomaly** section. Click **Assign.**
5. Select **Anomaly** from **Available** column, and move to **Selected** column.
6. Click **Add.**
7. Click **Update.**

### 15.4.2 See Detected Anomalies

Detected Anomalies can be viewed by the following methods:

#### Anomaly Column in Node Management

1. Go to **Management > Node** in top panel.
2. Find **Anomaly** column and see an icon. (*You might be able to see its details by clicking on the icon displayed*)

#### Anomaly View in Node Management

1. Go to **Management > Node** in top panel.
2. Find **Menu (3 dots and lines)** button that places next to Tasks button and click on that.
3. Find **Views** and select **Anomaly View.**
4. **Threat Detected** and **Threat Definition** columns will appear. (*A column may be configurable by clicking* **Edit Columns**)

#### Anomaly Logs

1. Go to **Log > Log** in the top panel.
2. Go to **Logs > Anomaly Logs** in the left Log panel.

#### Anomaly Tab in Dashboard

1. Go to **Dashboard** in the top panel.
2. Go to **Anomaly** tab.

#### Status & Filters

1. Go to **Management > Node** in the top panel.
2. Go to **Status & Filters > Anomaly Detection** or **Node with Anomaly** in the bottom left panel.

### 15.4.3 Clear Anomaly Detection Records

1. Go to **Management > Node** in top panel.
2. Find and click **Checkbox** of desired Nodes.
3. Click **Tasks > Node and Device > Clear Anomaly Records.**
4. Click **OK.**

## 15.5 Blocking Anomalies

### 15.5.1 Identify Nodes through Node Group and Block them through New Enforcement Policy

You may create a dedicated Node Group and an Enforcement Policy accordingly.

#### Create Anomaly Node Group

This will group together all Nodes that will be identified by the default Policy using enabled Anomaly Definitions.

1. Go to **Policy** in the top panel.
2. Go to **Policy > Group > Node** in the left Policy panel.
3. Click on **Tasks > Create**
4. For **ID:** Unique Name. (*e.g. Anomaly Group*)
5. For **Status:** Enabled.
6. For **Boolean Operator** select **OR.**
7. Find and click on **Add** in **Condition** section.
8. For each **Anomaly** you want to add, use the followings:
    - **Options:** Anomaly
    - **Operator:** Detected is one of
    - **Value:** (*One of the listed Anomalies*)
9. Click **Add.**
10. Keep adding **Conditions** as needed.

11. Click **Save.**

### Create Enforcement Policy To Block Anomalies

This will block all Anomalies identified within the Node Policy and are listed in the Anomaly Group from Step 1.

1. Go to **Policy** in the top panel.
2. Go to **Enforcement Policy** in the left Policy panel.
3. Click on **Tasks > Create.**
4. **Action** tab, click **Next.**
5. Under **General** tab:
   - **ID:** Unique Name. (*e.g. Anomaly Enforcement Policy*)
   - **Description:** Anomaly Policy to block all Nodes detected as Anomalies.
   - **Status:** Enabled.
   - Click **Next.**
6. **Node Group** tab, find and double click ** Group** (*e.g. Anomaly Group*)
7. **Permission** tab, double click on **PERM-DNS**. Click **Next.**
8. **Redirection** tab, click **Next.**
9. **Agent Action** tab, click **Finish.**
10. Click **Apply.**

## 15.6 ARP Bomb

Genian ZTNA can detect high volumes of ARP request packets sent in a variety of ways. The Network Sensor counts how many ARP packets sent by each Node. If the ARP requests are sent more than the specified value, Genian ZTNA suspects the ARP Bomb and designates the Node as critical.

### 15.6.1 Possible Causes

The following is a short list of some commonly known causes of elevated ARP traffic.

- Looped switch configuration
- Duplicate IP's on the Network
- Failing Network Interface in a device
- Invalid Subent Mask on a device
- Denial of Service attack leveraging ARP (typically from malware infected endpoints)

If an ARP Bomb anomaly is detected in your network, but you confirm that there is no problem, you can reduce the sensitivity of the ARP Bomb detection, or assign an exempt node group under the **Policy > Node Policy > Anomaly Definition > ARP Bomb** .

### 15.6.2 Configure Settings for ARP Bomb in Anomaly Definition

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Anomaly Definition** in the left Policy panel.
3. Click **ARP Bomb.**
4. Find **Anomaly Event** section to configure more options.
   - For **Event Duration**, optional setting to specify how long the ARP request packets are sent:
   - For **Number of Allowable ARP Requests**, optional setting to specify the threshold to trigger the anomaly detection.
   - For **Attribute to Match**, optional setting to find a Node sending the excessive ARP packets.
5. Click **Update.**

### 15.6.3 Create Node Group For ARP Bomb Nodes

1. Go to **Policy** in the top panel.
2. Go to **Policy > Group > Node** in the left Policy panel.
3. Click on **Tasks > Create**
4. For **ID:** ARP Packet Bombed.
5. For **Status:** Enabled.
6. For **Boolean Operator** select **OR.**
7. Find and click on **Add** in **Condition** section.
8. For each **Anomaly** you want to add use the followings:
   - **Options:** Anomaly.
   - **Operator:** Detected is one of.
   - **Value:** ARP Bomb.
9. Click **Add.**
10. Keep adding **Conditions** as needed.
11. Click **Save.**

## 15.7 MAC+IP Clones

Genian ZTNA can detect MAC / IP theft in a variety of ways. The Network Sensor periodically sends an ARP request to check the operation status of Nodes. If two MAC's answer to a request for one IP, Genian ZTNA designates the more recently detected Node as a critical Node.

In addition, if the user changes the MAC on the endpoint where the Agent is installed and the MAC is already being used by another device, that device is then designated as a critical Node. Genian ZTNA provides industry-leading platform detection to detect when a Node is changing to another platform, allowing administrators to see when changes are made, and to block devices when unauthorized platform changes are detected.

### 15.7.1 Configure Settings for MAC+IP Clones in Anomaly Definition

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Anomaly Definition** in the left Policy panel.
3. Click **MAC+IP Clones.**
4. Find **Anomaly Event** section to configure more options.
   - For **MAC Spoofing Detection**, optional setting to specify whether an interface's MAC address is manually changed is also detected.
5. Click **Update**

### 15.7.2 Create Node Group For MAC+IP Cloned

1. Go to **Policy** in the top panel.
2. Go to **Policy > Group > Node** in the left Policy panel.
3. Click on **Tasks > Create**
4. For **ID:** MAC+IP Cloned.
5. For **Status:** Enabled.
6. For **Boolean Operator** select **OR.**
7. Find and click on **Add** in **Condition** section.
8. For each **Anomaly** you want to add use the followings:
   - **Options:** Anomaly
   - **Operator:** Detected is one of
   - **Value:** MAC+IP Clones
9. Click **Add.**
10. Keep adding **Conditions** as needed.
11. Click **Save.**

## 15.8 Multi-Homed / Ad hoc Network

A Genian Agent can immediately detect a multi-homed configuration and Ad hoc network connections in a variety of ways. If a computer having more than one IP address configured connects to more than one network and one of them is not on the trusted network, then Genian ZTNA designates the Node as a critical one.

This anomaly definition requires installing an Agent on the endpoint and enabling an Agent Action In the node policy.

See: *Controlling Network Interface*.

### 15.8.1 Configure Settings for Multi-Homed / Ad hoc Network in Anomaly Definition

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Anomaly Definition** in the left Policy panel.
3. Click **Multi-Homed / Ad hoc Network.**
4. Find **Anomaly Event:** section to configure more options
5. For **Trusted Network Scope:** (*An option may be configurable in Policy > Object > Network.*)
6. For **Sensor Network as Trusted:** (*This prevents from not being on the trusted network if a Sensor changes its management scope.*)
7. For **Agent Control** select **Yes** to configure more options and you may specify the followings:
   - **Response:** Disabling Device or Generating Logs.
   - **Interface Disabled Notification:** Yes or No.
   - **External Device Exceptions:** optional setting to specify the device to be an exception to this Anomaly. (*The name must be the exact match, therefore, you had better configure Interface Type Exception instead*)
   - **Interface Type Exception:** Wired, Wireless or Virtual.
8. Click **Update.**

### 15.8.2 Create Node Group For Multi-Homed / Ad hoc Network Connected

1. Go to **Policy** in the top panel.
2. Go to **Policy > Group > Node** in the left Policy panel.
3. Click on **Tasks > Create**
4. For **ID:** Multi-Homed / Ad hoc Network Connected.
5. For **Status:** Enabled.
6. For **Boolean Operator** select **OR.**
7. Find and click on **Add** in **Condition** section.
8. For each **Anomaly** you want to add use the followings:
   - **Options:** Anomaly.
   - **Operator:** Detected is one of:
   - **Value:** Multi-Homed / Ad hoc Network.
9. Click **Add.**
10. Keep adding **Conditions** as needed.
11. Click **Save.**

## 15.9 Port Scanning

Genian ZTNA can detect port scanning run in a variety of ways. The Network Sensor monitors the network traffic flow to check the access event of ports. If a port scan is run to find a virtual IP address in order to exploit a known vulnerability, Genian ZTNA suspends the Port Scan and designates the Node as a critical one. In addition, if the ports are scanned more than the specified value within a period of time, then designated as a critical Node.

### 15.9.1 Configure Settings for Port Scanning in Anomaly Definition

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Anomaly Definition** in the left Policy panel.
3. Click **Port Scan.**
4. Find **Anomaly Event** section to configure more options.
   - For **Event Duration**, optional setting to specify how long the port scan is run:
   - For **Number of Allowable Ports**, optional setting to specify the threshold to trigger the anomaly detection.
   - For **Attribute to Match**, optional setting to find a Node running the port scan.
5. Click **Update.**

### 15.9.2 Create Node Group For Port Scan Run

1. Go to **Policy** in the top panel.
2. Go to **Policy > Group > Node** in the left Policy panel.
3. Click on **Tasks > Create**
4. For **ID:** Port Scan Run.
5. For **Status:** Enabled.
6. For **Boolean Operator** select **OR.**
7. Find and click on **Add** in **Condition** section.
8. For each **Anomaly** you want to add use the followings:
   - **Options:** Anomaly
   - **Operator:** Detected is one of
   - **Value:** Port Scanning
9. Click **Add.**
10. Keep adding **Conditions** as needed.
11. Click **Save.**

## 15.10 Rogue Gateway

A Genian Agent can immediately detect a rogue gateway configuration in a variety of ways. If a gateway address (or default gateway) configured on a Node is not on the trusted network, Genian ZTNA designates the Node as a critical one.

This anomaly definition requires installing an Agent on the endpoint and enabling an Agent Action In the node policy.

See: *Controlling Network Interface*.

### 15.10.1 Configure Settings for Rogue Gateway in Anomaly Definition

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Anomaly Definition** in the left Policy panel.
3. Click **Rogue Gateway.**
4. Find **Anomaly Event** section to configure more options.
5. For **Trusted Network Scope:** (*An option may be configurable in Policy > Object > Network.*)
6. For **Sensor Network as Trusted:** (*This prevents from not being on the trusted network if a Sensor changes its management scope.*)
7. For **Agent Control** select **Yes** to configure more options and you may specify the followings:
   - **Response:** Disabling Device or Generating Logs.
   - **Interface Disabled Notification:** Yes or No.
   - **External Device Exceptions:** optional setting to specify the device to be an exception to this Anomaly. (*The name must be the exact match, therefore, you had better configure Interface Type Exception instead*)
   - **Interface Type Exception:** Wired, Wireless or Virtual.
8. Click **Update.**

### 15.10.2 Create Node Group For Rogue Gateway Configured

1. Go to **Policy** in the top panel.
2. Go to **Policy > Group > Node** in the left Policy panel.
3. Click on **Tasks > Create**
4. For **ID:** Rogue Gateway Configured.
5. For **Status:** Enabled.
6. For **Boolean Operator** select **OR.**
7. Find and click on **Add** in **Condition** section.
8. For each **Anomaly** you want to add use the followings:
   - **Options:** Anomaly
   - **Operator:** Detected is one of
   - **Value:** Rogue Gateway
9. Click **Add.**
10. Keep adding **Conditions** as needed.

11. Click **Save.**

## 15.11 Spoofed ARP

Genian ZTNA can detect any spoofed ARP packets sent in a variety of ways. The Network Sensor listens for ARP replies on a network and checks of them whether there may be any changes or differences between the ARP sender MAC address and the Ethernet source MAC address. If two responses are sent are different from each other, Genian ZTNA suspends the spoofed ARP packets sent and designates the Node with the Ethernet source MAC address as a critical one. In addition, if the number of response packets allowed are more than the specified value, that Node is then designated as a critical one.

**Note:** If you use Virtual Router Redundancy Protocol (VRRP), the sender MAC address may differ from the Ethernet source MAC address, a real MAC address. Genian ZTNA discovers any cases of VRRP, HSRP or GLBP so that these cases will not be detected as an Anomaly.

### 15.11.1 Configure Settings for Spoofed ARP in Anomaly Definition

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Anomaly Definition** in the left Policy panel.
3. Click **Spoofed ARP.**
4. Find **Anomaly Event** section to configure more options.
   - For **Event Duration**, optional setting to specify how long the spoofed ARP response packets are sent:
   - For **Number of Allowable Spoofed ARP Responses**, optional setting to specify the threshold to trigger the anomaly detection.
5. Click **Update.**

### 15.11.2 Create Node Group For Spoofed ARP Sent

1. Go to **Policy** in the top panel.
2. Go to **Policy > Group > Node** in the left Policy panel.
3. Click on **Tasks > Create**
4. For **ID:** Spoofed ARP Sent.
5. For **Status:** Enabled.
6. For **Boolean Operator** select **OR.**
7. Find and click on **Add** in **Condition** section.
8. For each **Anomaly** you want to add use the followings:
   - **Options:** Anomaly
   - **Operator:** Detected is one of
   - **Value:** Spoofed ARP
9. Click **Add.**

10. Keep adding **Conditions** as needed.
11. Click **Save.**

## 15.12 Unauthorized Service Request

Genian ZTNA can detect an unauthorized service requested in a variety of ways. The Network Sensor monitors the network traffic flow to check the access event of ports. If an unwanted service is requested on any virtual IP addresses, Genian ZTNA suspends the Unknown Service Request and designates the Node as a critical one. In addition, if the service requests are more than the specified value within a period of time, then designated as a critical Node.

### 15.12.1 Configure Settings for Unauthorized Service Request in Anomaly Definition

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy > Anomaly Definition** in the left Policy panel.
3. Click **Unauthorized Service Request.**
4. Find **Anomaly Event** section to configure more options:
   - For **Event Duration**, optional setting to specify how long the unauthorized services are requested:
   - For **Number of Allowable Service Requests**, optional setting to specify the threshold to trigger the anomaly detection.
   - For **Attribute to Match**, optional setting to find a Node sending the excessive unauthorized service requests.
5. Click **Update.**

### 15.12.2 Create Node Group For Unauthorized Service Requested

1. Go to **Policy** in the top panel.
2. Go to **Policy > Group > Node** in the left Policy panel.
3. Click on **Tasks > Create**
4. For **ID:** Unauthorized Service Requested.
5. For **Status:** Enabled.
6. For **Boolean Operator** select **OR.**
7. Find and click on **Add** in **Condition** section.
8. For each **Anomaly** you want to add use the followings:
   - **Options:** Anomaly.
   - **Operator:** Detected is one of:
   - **Value:** Unauthorized Service Request.
9. Click **Add.**
10. Keep adding **Conditions** as needed.
11. Click **Save.**

CHAPTER

# SIXTEEN

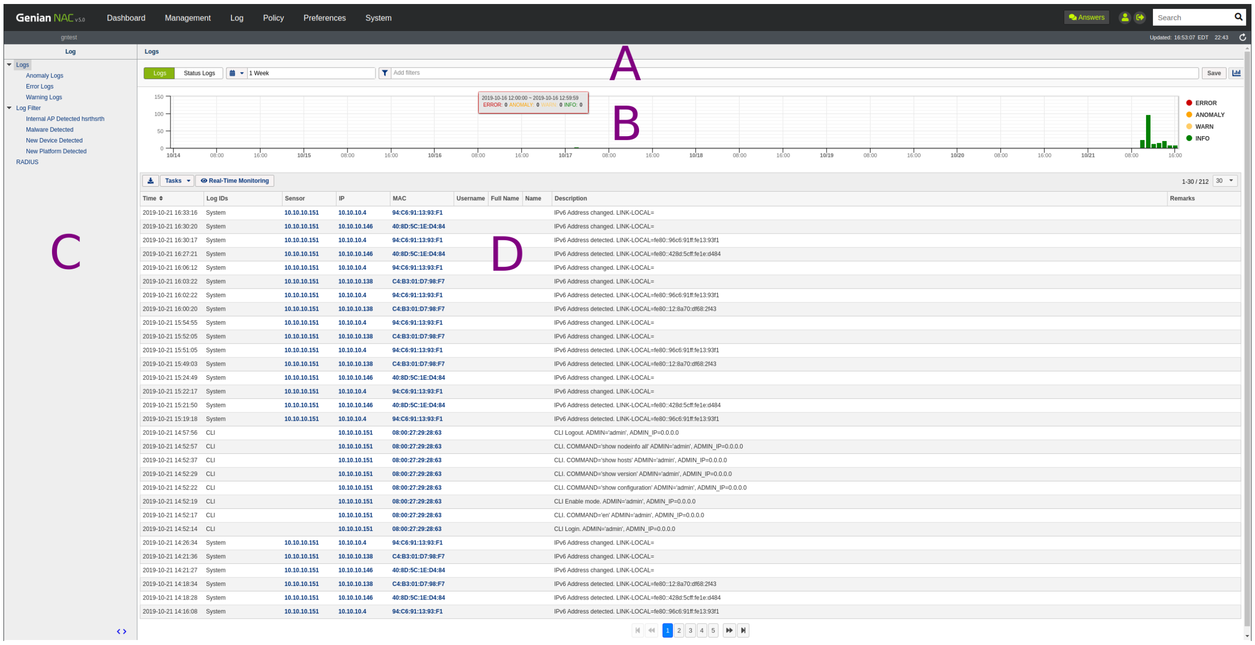
# MANAGING LOGS AND EVENTS

The Policy Server provides a centralized Log View. Information collected from endpoint devices, network devices, and other third-party devices are used to generate logs for security and management purposes. From here, Logs can then be sent outwards to another storage location, such as a SIEM solution.

Log view consists of four main sections.

- Panel A: Status and Filter.
- Window B: Time Graph and Chart.
- Panel C: Predefined Logs that are grouped by severity, or popular use cases.
- Window D: Result window of your searching and filtering.

Log display and generation options may be configured under **General > Log** in the **Preferences** section.



| Time | Log IDs | Sensor | IP | MAC | Username | Full Name | Name | Description | Remarks |
|---|---|---|---|---|---|---|---|---|---|
| 2019-10-21 16:33:16 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 16:30:20 | System | 10.10.10.151 | 10.10.10.146 | 40:8D:5C:1E:D4:84 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 16:30:17 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address detected. LINK-LOCAL=fe80::96c6:91ff:fe13:93f1 | |
| 2019-10-21 16:27:21 | System | 10.10.10.151 | 10.10.10.146 | 40:8D:5C:1E:D4:84 | | | | IPv6 Address detected. LINK-LOCAL=fe80::428d:5cff:fe1e:d484 | |
| 2019-10-21 16:06:12 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 16:03:22 | System | 10.10.10.151 | 10.10.10.138 | C4:B3:01:D7:98:F7 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 16:02:22 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address detected. LINK-LOCAL=fe80::96c6:91ff:fe13:93f1 | |
| 2019-10-21 16:00:20 | System | 10.10.10.151 | 10.10.10.138 | C4:B3:01:D7:98:F7 | | | | IPv6 Address detected. LINK-LOCAL=fe80::12:8a70:df68:2f43 | |
| 2019-10-21 15:54:55 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 15:52:05 | System | 10.10.10.151 | 10.10.10.138 | C4:B3:01:D7:98:F7 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 15:51:05 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address detected. LINK-LOCAL=fe80::96c6:91ff:fe13:93f1 | |
| 2019-10-21 15:49:03 | System | 10.10.10.151 | 10.10.10.138 | C4:B3:01:D7:98:F7 | | | | IPv6 Address detected. LINK-LOCAL=fe80::12:8a70:df68:2f43 | |
| 2019-10-21 15:24:49 | System | 10.10.10.151 | 10.10.10.146 | 40:8D:5C:1E:D4:84 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 15:22:17 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 15:21:50 | System | 10.10.10.151 | 10.10.10.146 | 40:8D:5C:1E:D4:84 | | | | IPv6 Address detected. LINK-LOCAL=fe80::428d:5cff:fe1e:d484 | |
| 2019-10-21 15:19:18 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address detected. LINK-LOCAL=fe80::96c6:91ff:fe13:93f1 | |
| 2019-10-21 14:57:56 | CLI | | 10.10.10.151 | 08:00:27:29:28:63 | | | | CLI Logout. ADMIN='admin', ADMIN_IP=0.0.0.0 | |
| 2019-10-21 14:52:57 | CLI | | 10.10.10.151 | 08:00:27:29:28:63 | | | | CLI. COMMAND='show nodeinfo all' ADMIN='admin', ADMIN_IP=0.0.0.0 | |
| 2019-10-21 14:52:37 | CLI | | 10.10.10.151 | 08:00:27:29:28:63 | | | | CLI. COMMAND='show hosts' ADMIN='admin', ADMIN_IP=0.0.0.0 | |
| 2019-10-21 14:52:29 | CLI | | 10.10.10.151 | 08:00:27:29:28:63 | | | | CLI. COMMAND='show version' ADMIN='admin', ADMIN_IP=0.0.0.0 | |
| 2019-10-21 14:52:22 | CLI | | 10.10.10.151 | 08:00:27:29:28:63 | | | | CLI. COMMAND='show configuration' ADMIN='admin', ADMIN_IP=0.0.0.0 | |
| 2019-10-21 14:52:19 | CLI | | 10.10.10.151 | 08:00:27:29:28:63 | | | | CLI Enable mode. ADMIN='admin', ADMIN_IP=0.0.0.0 | |
| 2019-10-21 14:52:17 | CLI | | 10.10.10.151 | 08:00:27:29:28:63 | | | | CLI. COMMAND='en' ADMIN='admin', ADMIN_IP=0.0.0.0 | |
| 2019-10-21 14:52:14 | CLI | | 10.10.10.151 | 08:00:27:29:28:63 | | | | CLI Login. ADMIN='admin', ADMIN_IP=0.0.0.0 | |
| 2019-10-21 14:26:34 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 14:21:36 | System | 10.10.10.151 | 10.10.10.138 | C4:B3:01:D7:98:F7 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 14:21:27 | System | 10.10.10.151 | 10.10.10.146 | 40:8D:5C:1E:D4:84 | | | | IPv6 Address changed. LINK-LOCAL= | |
| 2019-10-21 14:18:34 | System | 10.10.10.151 | 10.10.10.138 | C4:B3:01:D7:98:F7 | | | | IPv6 Address detected. LINK-LOCAL=fe80::12:8a70:df68:2f43 | |
| 2019-10-21 14:18:28 | System | 10.10.10.151 | 10.10.10.146 | 40:8D:5C:1E:D4:84 | | | | IPv6 Address detected. LINK-LOCAL=fe80::428d:5cff:fe1e:d484 | |
| 2019-10-21 14:16:08 | System | 10.10.10.151 | 10.10.10.4 | 94:C6:91:13:93:F1 | | | | IPv6 Address detected. LINK-LOCAL=fe80::96c6:91ff:fe13:93f1 | |

## 16.1 Managing Logs

You can find specific data by searching, filtering, tagging, and visualizing in real time. By default, Genian ZTNA provides Logs based on severities, and pre-defined Log Filters based on common usage.

### 16.1.1 Configuring Log Options

You can configure options about when Logs are generated and what additional info may be recorded, such as nodes, host names, node platforms, and node descriptions.

1. Connect to the Web Console.
2. Go to the **Preferences > General > Log** menu.

#### Remarks Column Elements

1. In the Logs option selection, check the items you want to add.
2. Click the **Update** button below.
3. Go to the top Log menu and verify that the newly added Audit Log Remarks column displays additional information.

#### Available Columns:

- Node Name
- Node Description
- Hostname
- Domain
- DNS
- Platform
- Job Title
- Switch Name
- Switch Port
- Sensor Group Name

#### Generating Node Status Logs

- Select `On` or `Off` for recording node status (Up/Down)

### Generating Agent Status Logs

- Select `On` or `Off` for recording Agent status (Running/Inactive)

## 16.1.2 Searching Logs

Using the **Search** section you can search for specific information within the logs. You can also use **Operators**, and **Special Characters** to assist you in your searches.

1. Go to **Log** in the top panel.

In the top of the view pane, configure search parameters from left to right:

1. Select either **Logs**, and/ or **Status Logs**.
2. Select your desired time period to search.
3. **Select Add filters to configure the following parameters:**
    - IP
    - MAC
    - Username
    - Full Name
    - Name
    - Sensor
    - Remarks
    - Description
    - Log Types (Error, Anomaly, Warning, Information)
    - Log ID's (Agent, Authentication, Policy, SSID, System, and many more)
4. Click **Search.**

**Note:** Clicking the "?" next to "Filter" will bring up help options to assist you with using special characters in your searches.

## 16.1.3 Time Graph and Chart

### Time Graph

The Time Graph shows you the amount of log activity per day. By default, Genian ZTNA shows the Time Graph in a **Stacked** format meaning that all Log Types that are received for that time are sorted and stacked onto one another graphically. You can choose to see these same logs in a Logarithmic view by clicking on the **Graph Icon** in the top right side of the view pane and selecting **Logarithmic.**

**Note:** If you want to disable the Time Graph from being seen you can simply un-check the **Time Graph check box**

### Chart

The Chart function allows you to see popular Log data for that seven-day period. These include **Top 10 IPS, MACs, Devices,** and more. You can access this function by clicking on the **Graph Icon** in the top right side of the view pane.

## 16.1.4 Real Time Monitoring

You can view logs in real-time as the events occur so that you can react quickly and take immediate action. You can view these events within in the same browser or you can view events in a new separate window.

### Viewing Logs in Real-Time

1. Click **Log** in the top panel.
2. Find and click on **Real-Time Monitoring.**
3. Find **Update Interval** option on the upper right corner to set your refresh rate. (*e.g. 5,10,15,30,60 Seconds*)
4. Find and click on **View in New Window** to view in a separate window.

## 16.1.5 Creating Log Filter

By default there are a few Log Filters that are provided, but you can create custom **Log Filters** and save them as your commonly used filters for easy access.

### Create a New Log Filter

1. Go to **Log** in the top panel.
2. Click on **Logs.**
3. Find the top of the view pane and enter your search criteria for which log set and time period to search, as well as which filters to apply.
4. Click **Save** in the top right.
5. For **Name**, type unique name.
6. For **Description**, type what this Log Filter contains.
7. For **Tree & Log Monitor:** (Checked displays New Filter under **Log Filter**, unchecked will keep it hidden from list)
8. For **Columns to Display:**, Choose which columns you would like to display in your New Log Filter.
9. Configure notifications if desired. See: *Sending Events*
10. Click **Save.**

### Edit Log Filters

1. Go to **Log** in the top panel.
2. Go to **Log Filter** in the left Log panel.
3. Find and click the **"Magnifying Glass"** Icon.
4. Use the *step 3* from above to reconfigure the search.
5. Click **Edit** to proceed or configure additional settings.
6. Click **Update.**

### Delete Log Filters

1. Go to **Log** in the top panel.
2. Select **Log Filter** in the left **Log** panel.
3. In main window find **Log Filter Name**, click on **Checkbox.**
4. Click **Tasks > Delete.**
5. Click **OK.**

## 16.1.6 Tagging Assets Using Event

### Assign Tag using Log Filter

1. Create a Log Filter as shown in :*Creating Log Filter* through step 4.
2. Click the **dropdown-list** beside **Tag** and select the **Assign:**

- **From**: This option acts as a conditional statement. If the origin of the log is of the selected class (**Node**, **External device**, **User**, or **WLAN**) , then a tag will be assigned to the attribute defined in the **To** option.
- **To**: The [Node/External device/User/WLAN] to which the tag is assigned.
- **Tag**: Select which **Tag** to assign.

**Note:** If you want to delete a Tag, Select the **clear**

### Verification:

- Click on the IP after searching for the target to which the tag is assigned.
- Check the Tag assigned to the target in the **General Tab**.

## 16.2 Sending Events

The Policy Server can send events internally to administrators, end users, networking devices, or externally to third-party security products such as SIEM using various protocols.

**Note:** To send emails notifications, Outbound email and admin email notification settings must both be configured. See *Setting up Outbound Mail Server ( SMTP )* , *Administrator Accounts*.

### 16.2.1 Define Event Criteria for Export

#### Use an existing Log Filter or Create a new one

1. Select the **edit** option under the desired log filter.
2. Log export may be configured further by checking **Notification** (Local Admin), **SYSLOG**, **SNMP Trap**, and/or **Webhook**.

#### Add Macros To Log Export Message Box

Genian ZTNA uses Macros as a placeholder text that gets replaced with specific data when inserted into the Log Notifications message box. You can add and customize these Macros to present the data however you like. If the Log Notifications message block is left empty then a default set of Macros will be used.

1. Go to **Preferences** in the top panel.
2. Go to **General > Log** in the left **Preferences** panel.
3. Find **Log Options: Remarks column Elements** section in main **Log** panel.
4. Select options to **Enable** this data to be added to **Logs.** (*Node Status Logs and Agent Status Logs are optional*)
5. Go to **Workflow** in the top panel.
6. Go to **Event Hooks** in the left **Workflow** panel.
7. Find and click **Name.**
8. Click Edit at the top right of view pane.
9. Find and select **Notification**, **SYSLOG**, **SNMP Trap**, and/or **Webhook**.
10. Find and click **Help for Macro** button just above **Notification** section title.
11. Choose the desired **MACRO** to add to the message body. (*Some Message{_SWNAME}{SWPORT}*)
12. Click **Update.**

**Default Message Syntax**

- Notification

```
SMS - [site Name] {_HEADMSG}: Log Filter Name
Email Subject - [Site Name] {_HEADMSG}: Log Filter Name
Email Contents - {_DATETIME} {_LOGTYPE} {_LOGID} {_SENSORNAME} {_IP} {_MAC} {_FULLMSG}
↪ {_DETAILMSG}
```

- SYSLOG

```
Default - {_DATETIME} {_LOGTYPE} {_LOGID} {_SENSORNAME} {_IP} {_MAC} {_FULLMSG} {_
↪DETAILMSG}
CEF - CEF:0|GENIANS|Genian NAC|{_VERSION}|{_LOGFILTERNAME}|{_LOGFILTERDESC}|1|rt={_
↪DATETIME} cs1Label=Log Type cs1={_LOGTYPE} cs2Label=Log ID cs2={_LOGID} dvchost={_
↪SENSORNAME} dst={_IP} dmac={_MAC} msg={_FULLMSG} cs3Label=Detail Message cs3={_
↪DETAILMSG}
```

- SNMP Trap

```
{_DATETIME} {_LOGTYPE} {_LOGID} {_SENSORNAME} {_IP} {_MAC} {_FULLMSG} {_DETAILMSG}
```

**Note:** SMS Notifications are limited to 500 per-month.

- Webhook (POST)

```
{
"datetime": "{_DATETIMEZ}",
"ip": "{_IP}",
"mac": "{_MAC}",
"sensorip": "{_SENSORIP}",
"sensorname": "{_SENSORNAME}",
"logid": "{_LOGID}",
"logidstr": "{_LOGIDSTR}",
"logtype": "{_LOGTYPE}",
"userid": "{_USERID}",
"fullname": "{_USERNAME}",
"userdept": "{_USERDEPT}",
"position": "{_POS}",
"nodename": "{_NNAME}",
"hostname": "{_HOSTNAME}",
"platform": "{_PLATFORM}",
"nodedesc": "{_DESC}",
"domain": "{_DOMAIN}",
"dnsname": "{_DNSNAME}",
"switchname": "{_SWNAME}",
"switchport": "{_SWPORT}",
"detail": "{_DETAILMSG}"
}
```

### Macro Definitions

Administrators can select and send necessary information when sending events by using predefined macros.

- Hostname, platform, and switch information are not included when a new node is detected.
- Macros can be used when additional information is collected after the node scan is completed.
- **Please refer to the documents below for related information.**
  - *Genian Device Platform Intelligence (GDPI)*
  - *Understanding Network Nodes*
  - *Browsing Switches*

| Macro Format | Contents |
|---|---|
| {_FULLMSG} | Full Log Message |
| {_HEADMSG} | Log Message Header |
| {_TAILMSG} | Data After Header (KEY=VALUE, ...) |
| {_EXTRAINFO} | All Additional Information |
| {_IP} | Log Node IP |
| {_IP_HTML} | Log Node IP(Hyperlink) |
| {_MAC} | Log Node MAC |
| {_MAC_HTML} | Log Node MAC(Hyperlink) |
| {_SENSORIP} | Log Sensor IP |
| {_SENSORNAME} | Log Sensor Name |
| {_LOGID} | Log ID |
| {_LOGIDSTR} | Log ID String |
| {_LOGTYPE} | Log Type |
| {_DATETIME} | Log Time and Date (2025/11/27 14:22:32) |
| {_DATETIMETZ} | Log Time and TimeZone |
| {_DETAILMSG} | Log Details |
| {_USERID} | Authenticated User ID |
| {_USERNAME} | Authenticated User Name |
| {_USERDEPT} | Authenticated User Department |
| {_POS} | Authenticated User Job Title (Additional Information Required) |
| {_NNAME} | Node Name (Additional Information Required) |
| {_HOSTNAME} | Hostname (Additional Information Required) |
| {_PLATFORM} | Platform (Additional Information Required) |
| {_DESC} | Node Description (Additional Information Required) |
| {_DOMAIN} | Domain (Additional Information Required) |
| {_DNSNAME} | DNSName (Additional Information Required) |
| {_SWNAME} | Switch Name (Additional Information Required) |
| {_SWPORT} | Switch Port (Additional Information Required) |

- Macros containing **(Additional Information Required)** will only output data if the **Preferences > General > Log > Log Options: Remarks column Elements** setting is enabled.
  If this setting is disabled, the macro replacement result will be displayed as an empty value. (Default is disabled.)

**Note:** You can convert to uppercase or lowercase by appending **_upper** or **_lower** to existing macros.

### 16.2.2 Sending Logs (Event Hooks)

You can send Events to external locations like SIEM solutions using several methods.

**Note:** To send emails notifications, Outbound email and admin email notification settings must both be configured. See *Setting up Outbound Mail Server ( SMTP )* , *Administrator Accounts*.

You can perform validation/transformation operations on logs before sending events through Workflow.

- You can send logs using data validated/transformed through Workflow.
- Macros that can be used for event transmission are available in Workflow.
  - Macros such as {_NODE_IPSTR} can be used in Workflow in the format ${request._NODE_IPSTR}.

  - After executing the Workflow, the results can be used in each event transmission setting in the format ${workflow}, ${workflow.result}, and JSON results defined in the Workflow's Response Body Template can be used in the format ${workflow.jsonKey}.

1. Select a **log filter**, click **edit.**
2. Click **Checkbox** for **Notification** (Administrator email / sms), **Syslog**, **SNMP Trap**, or **Webhook**.
3. Configure settings and Update.

### Example Integration: Splunk

Integrate with Splunk using the following process:

1. In Splunk configure a Local UDP input under **Settings > Data Inputs.**
2. Configure your desired **data input port** and enter your Genians policy server IP into the "Only accept connection from" section. (optional)
3. In Genians ZTNA, select syslog under the log filter of your choice.
4. Input the **Sever Address** of your splunk server. For **Protocol**, select **UDP**, and for **server port**, select the **data input port** you defined on Splunk.
5. In the SYSLOG message section, enter the value: {_DATETIME},LOGTYPE={_LOGTYPE},LOGID={_LOGID},IP={_IP},MAC DETAIL={_DETAILMSG}

- This is necessary for the proper display of information in Splunk.

### SNMP Trap Example

SNMP Trap is mainly used for device-to-device event transmission, and the transmission setting method is as follows.

1. Check SNMP trap in selected search filter of Genian ZTNA.
2. Enter the server address of the SNMP Trap server.
3. Enter the Community string defined in the SNMP Trap server.
4. In the SNMP Trap message, enter values of {_DATETIME},LOGTYPE={_LOGTYPE},LOGID={_LOGID},IP={_IP},MAC={_M DETAIL={_DETAILMSG}.

## 16.2.3 Integration Guide For Slack

This document describes how to integrate Genian ZTNA with Slack using webhook. This integration provides the ability to send notifications for any Genian ZTNA log files to the Slack Workspace and channel of your choice. In this example, we will create a Slack Notification for newly detected MAC addresses.

The main steps of this integration are as follows:

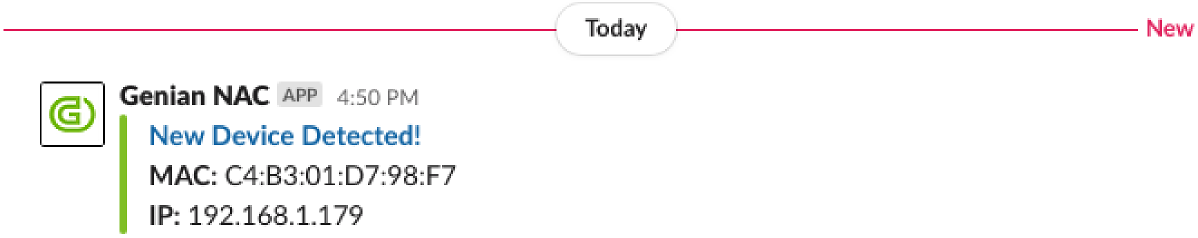
- Configure a Slack app to accept inbound Posts
- Test that the Slack app properly
- Configure a Genian ZTNA log filter to send Posts to Slack

### Slack App Configuration

The steps below demonstrate how to configure Slack to accept webhook Posts from Genian ZTNA.

1. Navigate to api.slack.com/apps, and select **Create an App**
2. Name your App and select a workspace to apply it to.
3. Select **Incoming Webhooks**, and set **Activate Incoming Webhooks** to **On**
4. Select **Add New Webhook to Workspace** and select one or multiple channels to post your message to. Save the channel URL as it will be input into Genian ZTNA later.
5. Use the curl utility in a command line to test sending a webhook to a channel.
6. Copy the sample Curl request from this page, and paste it into a command terminal. Ensure that the webhook URL in the sample request matches that of the channel you wish to test, as shown at in the channel list at the bottom of the page, and that the curl function is supported by your terminal.
7. After entering, if the message posts successful to your channel, Slack has been properly configured to receive webhook posts.

### Configuring Log Export to Slack



New Device Detected!
MAC: C4:B3:01:D7:98:F7
IP: 192.168.1.179

These steps will select logs from Genian ZTNA, and export them to the Slack webhook app, including those imported from external systems. To see how to import logs from external systems see: *Receiving Events*

1. Navigate to the **Log** tab, then select the **Add filters** option. Narrow your search to select which events to send to Slack. For our example we will search for "New MAC Detected" in the description, and click **Search**. Other filter variables may also be used to narrow your search. Ensure that your search returns only the desired results. Click **Save**
2. Next, assign a name and a description to your filter, then select **Webhook** from the bottom of the screen.
   - Set **Method** to **POST**
   - Set **URL** to the channel URL shown in the previous section of this guide.
   - Set **Character Set** as **UTF-8**
   - In the **POST DATA** section, select which log fields to send to Slack. For help with the syntax, click the question mark icon labelled **Help for Macro**
   - For this example we will show a way to post the newly detected MAC Address and the corresponding IP Address to the channel of your choice, as shown by the {_IP} & {_MAC} macros.
   - The **title_link** content will create a hyperlink from the message title to the newly detected MAC address on your Policy Server. Be sure to input your Policy Server IP or FQDN in the indicated area.

```
{
  "attachments":[
          {
          "fallback":"New Device Detected!",
          "color":"#7FBE26",
          "title":"New Device Detected!",
          "title_link":"POLICY SERVER ADDRESS/mc2/faces/frontpage.xhtml?
↪forceForwardUrl=1&folder=monitor&framePage=frame.xhtml&selectedTree=BBA&
↪selectedPage=nodeMgmt.xhtml?nid=All&mac={_MAC}&macequal=true&isselect=true",
          "text":"*MAC:* {_MAC}\n*IP:* {_IP}",

          }
]
}
```

- For **Content-Type** set to **Application/json**

## 16.3 Receiving Events

These options may be found under **General > Log** in the **Preferences** section.

**Note:** SNMP Trap is only available in On-Premise edition.

### 16.3.1 Receiving SNMP Traps

- Enable or Disable by selecting `On` or `Off` From the drop down menu to the right of the **SNMP Trap** Label.
- If enabled, enter a `community string` into the form.

### 16.3.2 Receiving Syslog

A Server Rule set must be added before receiving syslogs. For different receiving criteria, different rules may be configured.

1. Click the **Add** button to the right of the **Server Rules** label, and fill out the pop-up form.
2. Enter a name for the Rule.
3. For **Filter**,select a variable by which to evaluate incoming syslogs for allowance. Choose from **Program** , **Host**, **Match**, or **Netmask.** This option allows for syslogs from a given source location/ program, or a given message content to be allowed.
4. Define a **Filter Value.** If the **Filter** variable of the imported syslog matches the **Filter Value** , the syslog will be merged into the policy server logs.
5. Define a prefix for **IP**, **MAC** and **Username** values. This prefix will trigger the filter to import the values immediately following as IP Addresses, MAC addresses and Usernames.
6. Define the character set which the syslogs will be imported in.
7. Click **Add** at the bottom of the pop-up window.
8. Click **Update** at the bottom of the Log Preferences page.

Imported events can be used to assign tags to nodes, devices, users and Wlans, which can be used to dictate policy.

For more information see: *Tagging Assets Using Event*.

# 16.4 Report

A Report is a function that shows the information that an administrator wants in a chart and a table for easy viewing. Administrators can use reports to efficiently document and archive or report data. Types of reports include Query Reports, Time Graph Reports, and Automatic Reports.

## 16.4.1 Managing Reports

Query Report function, the Administrator can output the result of the query (SQL statement) desired by the Administrator as an Excel file in the report format. Query Reports define the report by setting up the query statement, and the report is created by the file creation operation on the defined report.

### Generate Query Report

1. Go to **Log > Report** in the top panel.
2. Go to **Tasks > Generate Query Report.**

Under **General:**

1. For **Title**, type unique name.
2. For **Description**, type what this report will do.
3. For **Status**, select **Enabled.**
4. For **Auto Generating**, select **Enable** for executing at set times.

Under **Advanced:**

1. For **File Format**, choose Excel or CSV from drop-down.
2. For **Query**, add custom query.
3. Click **Save.**

### Example Queries

### Collect Open Ports Of Nodes

```
SELECT NL_IPSTR as IP, NL_MAC as MAC, NL_FQDN as HOSTNAME, GROUP_CONCAT(NI_PORT) as␣
↪OPENPORT
 from vwNODELIST_ALL JOIN NODEINFOALL_OPENPORT ON (NI_NODEID = NL_NODEID)
 where NL_ACTIVE = ‘1’
 GROUP BY NL_NODEID
```

### List Of IPs With The Same MAC

```
SELECT * FROM (
 SELECT NL_IPSTR, COUNT(NL_MAC) CNT
   from vwNODELIST_VALID
   GROUP BY NL_IP
   ORDER BY NL_IP
) A WHERE CNT > 1

The Administrator uses the Time Graph Report to show the information about the
Node Group and the whole Node, the operation, the Agent installation, and the
number of operation Agent Nodes in a Graph Format.
```

### Generate Time Graph Report

1. Go to **Log > Report** in the top panel.
2. Go to **Tasks > Generate Node Report.**

Under **General:**

1. For **Title**, type unique name.
2. For **Description**, type what this report will do.
3. For **Status**, select **Enabled.**
4. For **Auto Generating**, select **Enable** for executing at set times.

Under **Advanced:**

**Note:** Repeat these steps under **Advanced** to add more **Node Options** to the report.

1. For **Node Options**, select **All Nodes** or **Node Group** from drop-down.
2. If **Node Group** is selected then for **Node Group** select desired group from drop-down.
3. For **Criteria**, select what to report on.
4. For **Name**, use default or type unique name.
5. For **Description**, type what this report will do.
6. For **Graph Type**, select **Line, Bar,** or **Face graph** from drop-down.
7. For **Graph Color**, select desired color from drop-down.
8. For **Generating Logs**, select desired criteria from drop-down.
9. Click **Add** then **Update.**
10. Go to **Report Definition >Time Graph Report.**

Under **Graph** tab:

1. Select desired **Time Period** and click **Generate**

Under **Table** tab

1. Select desired **Time Period** and click **Generate.**
2. Click **Export** to export report locally in **Excel** format.

### Create Automatic Reports

Automatic Report creation is the automatic generation and emailing portion of the Query Report.

**Note:** To send emails notifications, Outbound email and admin email notification settings must both be configured. See *Setting up Outbound Mail Server ( SMTP )* , *Administrator Accounts*.

1. Go to **Log > Report** in the top panel.
2. Go to **Automatic Report** in left **Report** panel.
3. Go to **Tasks > Create** to create Automatic Report.

Under **General:**

1. For **Name**, type unique name.
2. For **Description**, type what this report will do.
3. For **Recipient**, select **Administrator** or **Admin Role.**
4. Double click available names in left column.
5. For **Report**, Double click available reports.
6. For **Auto-generating**, select **Enable** from drop-down and choose how often to run this report.
7. Click **Save.**

### Exporting Reports

1. Go to **Log > Report** in the top panel.
2. Go to **Report Definition**, click on desired **Report** name in left **Report** panel.
3. Click **Tasks > Generate Report.** (*File should appear to click on*)
4. Click on **Report Filename** to download. (*e.g. 20180801110000.xlsx*)
5. Open **Report Filename** and save locally.

### How to Delete Reports

1. Go to **Log > Report** in the top panel.
2. Find **Report Definition** in the main window and click **Checkbox.**
3. Go to **Tasks > Delete.**
4. Click **OK** to verify deletion.

## 16.5 How to add additional information elements in Logs

Genian ZTNA can add additional information in audit logs or generate Agent/Node status Logs.

| Remarks Column Elements | description |
|---|---|
| Node Name | Display Node Name in Node details |
| Node Description | Display Description in Node details |
| Hostname | Display Hostname in Node details |
| Domain | Display Domain in Node details |
| DNS | Display DNS Name in Node details |
| Platform | Display Platform in Node details |
| Job Title | Display Authenticated User's Job Title |
| Switch Name | Display the name of connected Switch |
| Switch Port | Display the name of connected Switch port |
| Sensor Group Name | Display the name of node's sensor group name |

### 16.5.1 How to configure Remarks Column Elements

1. Go to **Preferences** in the top panel
2. Go to **General > Log** in the left Preferences panel
3. Find **Log Options > Remarks Column Elements** and choose elements Click **checkbox**
4. Click `update` button

### 16.5.2 How to Generate Node/Agent Status Logs?

1. Go to **Preferences** in the top panel
2. Go to **General > Log** in the left Preferences panel
3. Find **Generating Node Status Logs** and choose **On**
4. Find **Generating Agent Status Logs** and choose **On**
5. Click `update` button

CHAPTER

SEVENTEEN

# MANAGING SYSTEMS

Systems consist of Policy Server and Network Sensor. You can customize admin interface, manage admin roles, configure network settings, and control systems maintenance.

## 17.1 Site Management

This is the management page for configuring SASE. Through Site Management, you can create Service Edges (ZTNA Gateway, Hub) in the Cloud and configure Branches to connect to them.

### 17.1.1 Site Types

Sites can be created as either **Hub type** or **Branch type**.

#### Hub Type

A Hub site acts as an intermediary for **IPsec tunnels** with Branch sites and serves as a network access point.

- If there are multiple Hub sites, you can configure tunnels between the Hub sites.

#### Branch Type

The Branch type only routes traffic for the Branch site's network.

- When selecting a Parent Hub site, an IPsec tunnel can be configured to the Hub.

#### Site Connection Methods

- You can connect to the Hub by running IPsec on the ZTNA Gateway.
- Integration between Hub sites in ZTNA and dedicated IPsec devices (e.g., Cisco, Fortinet) is possible.
- If direct routing between the Hub and Branch is possible, you can connect via routing.

## 17.1.2 How to Configure a Site

1. Click **System -> Site**
2. Click **Select Action -> Create**
3. Enter basic information:
    - Enter the **Site Name**
    - Set the type (Hub, Branch)
    - **Configure the infrastructure (Cloud, On-Premises)**
        - For **Cloud**, you must configure **Cloud Provider**, **Region**, and **VPC ID**
        - Use a previously created Cloud Provider. If none exists, refer to *How to create a Cloud Provider* to create one.
        - Set the **Region** that matches the location.
        - Select the **VPC ID** to configure the site. When you select a **VPC ID**, the **Network Address** is automatically set to the VPC range.
        - For **On-premises**, manually set the IP range of the site in **Network Address**.
    - Select options to be used per site. [ ZTNA-IPsec, ZTNA-Client, Routing, Collector, URL Filter ]

## 17.1.3 Site Options

The available site options are ZTNA-Client, ZTNA-IPsec, Routing, Collector, URL Filter.

### Collector

The Genian ZTNA Cloud Collector collects node information in the cloud environment and provides visibility into the cloud for users.

According to the configured execution cycle, the Cloud Collector queries the Cloud Service Provider to collect node information and cloud-related details.

### How to Configure the Collector

To enable the Genian ZTNA Collector option, both *Cloud Provider Settings* and *Site Settings* must be configured.

1. After configuring the site, change the **Application Mode** under the Collector option at the bottom to "Enabled".

2. If there is a Proxy server used for external communication, configure **Proxy HostName** and **Proxy Port**.

3. Go to System - Sensor Management. Check whether a Cloud sensor has been created with the site name you configured.

4. If the Cloud sensor has been created, go to **Management - Node** to verify whether the Cloud sensor correctly registered instances within the Hub site's VPC range.

5. The information collected by the Collector can be viewed by clicking the node registered by the Cloud sensor.

### ZTNA-Client

ZTNA-Client is a feature that allows remote users (branch offices, home offices, mobile, etc.) to securely access designated site resources via SSL-based VPN tunnels in a ZTNA environment.

It is primarily used with the ZTNA Agent. In environments where agent installation is difficult (lack of permissions, servers, special OS, etc.), connection is possible via an OpenVPN compatible client.

This implements consistent security policy enforcement, session visibility, and centralized access control.

#### How to Configure ZTNA-Client

Before configuring ZTNA-Client, you must first proceed with *Site Settings*.

1. Change **ZTNA-Client Application Mode** to **Enabled** and proceed with detailed settings.

| Feature Name | Description and Sub-options | Description |
|---|---|---|
| SDP | Secures remote access and uses the Connection Manager. | |
| Connection Manager | Select the VPN to use for network connection. (Genian ZTNA, Axgate VPN, SSLPNS) | |
| | Client Network | Set the management sensor to manage clients. |
| | Use Virtual Network | By default, the sensor's management network is used, but when set to On, a virtual network is used. |
| | VXLAN Tunneling | Supports VXLAN connection between gateway sensors so that devices connecting to different ZTNA Gateways can use the same IP. |
| | Access Network | Specify the network range that the ZTNA Client will access. If unspecified, all networks are connected through the ZTNA Client tunnel. |
| | Static IP | Fixes the user's IP. |
| | Isolation | Access from outside and direct communication between other users are blocked. |
| | OpenVPN Compatibility | Provides a Config file usable with OpenVPN. |
| | Custom Server Domain | Set the server domain name or IP for the ZTNA Client to connect to. If not set, the sensor's IP or the gateway's public IP is automatically used. |
| | External Certificate | Set a trusted external certificate for the server domain that the ZTNA Client will connect to. |

**Note:** When changing ZTNA-Client to use a virtual network, a TAP interface is created on the ZTNA sensor, and the Client IP is set via DHCP through the TAP interface.

2. To connect using SDP, separately configured SDP settings must be entered.

Reference : understanding-sdp

| Feature Name | Description |
|---|---|
| Controller Domain | Enter the connection domain of the SDP Controller. |
| Controller Secret | Enter the secret key for authenticating to the SDP Controller. |
| SPA Port | Enter the port number for the client to send SPA (Single Packet Authorization) to SDP upon initial access. |
| User Authentication Port | Enter the port number to perform user authentication procedures after SPA transmission. |
| Authentication Method | Select the authentication method used to perform user authentication after SPA transmission. \ User Authentication, Certificate + User Authentication |

3. Add **ZTNA Connection Manager** to **Node Policy - Node Action**.

4. In the **ZTNA Connection Manager** node action settings, click **Assign** and add the site created earlier.

5. Go to System - Sensor - Click Sensor - Sensor Settings - Node tasks - Sensor Settings of the interface used by the sensor (**Existing Interface, Created TAP Interface**) - Set **Sensor Operation Mode to Inline, Operation Scope to Global**.

> **Note:** If Inline and Global modes are not set, ZTNA-Client packets may not be processed correctly.

6. Install the agent. [ https://Policy Server IP/agent ]

7. Right-click Agent - **Network Access** - Click the configured **Site** name.

8. Enter user information and click **Connect**.

### How to Check ZTNA-Client Sessions

Once connected to the site via the Agent or OpenVPN client, you can check the sessions accessing each site in the Web Console.

- Click **System - Site**, and click the number in the ZTNA-Client tab on the screen displayed in the Web Console to check the sessions connected to that site.
- In the **ZTNA Client Sessions** screen, you can check the connected **User ID, Hub Name, Device Name, User IP, Assigned IP, Packet Volume, Packet Count, Creation Time, and Last Communication Time**.

### Related Links

- To use 2-Factor Authentication, refer to the *ZTNA-Client Passkeys Authentication* document.
- To use SAML Authentication, refer to the *SAML ZTNA Client VPN Authentication* document.

### ZTNA-IPsec

ZTNA-IPsec is a feature that configures a Site-to-Site (IPsec) tunnel between an On-premises or Cloud branch and a ZTNA-Gateway.
It allows branch traffic to securely communicate with the Internet via the gateway or interconnect with headquarters/cloud resources.

### How to Configure ZTNA-IPsec

To use ZTNA-IPsec, *Cloud Provider* settings and *Hub Type Site Settings* are required in advance.

1. Go to System -> Site -> Click the created **Hub Type Site**, and change ZTNA-IPsec Application Mode to **Enabled**.
2. Configure **Pre-Shared Key** value and **Advance** settings.

> **Warning:** To configure IPsec tunneling with third-party VPN dedicated equipment, the **Pre-Shared Key** value and **Advance** options must be identical.

| Item | Item Description | Remarks |
|---|---|---|
| Pre-Shared Key | Secret key shared in advance for connection between Hub and Branch | |
| IKE Version | IKE version to use for IPsec connection | Supports IKEv1, IKEv2 |
| IKE encryption | Algorithm to encrypt authentication information | Supports AES-128, AES-256, blowfish-128, blowfish-192, blowfish-256, Twofish-128, Twofish-192, Twofish-256 |
| IKE integrity | Encryption algorithm for integrity assurance | Supports SHA1, SHA2-256, SHA2-384, SHA2-512 |
| Pseudo random function | Encryption algorithm for providing randomness | Supports None, SHA1, SHA2-256, SHA2-384, SHA2-512 |
| IKE DH group | Symmetric key exchange algorithm to generate keys for encrypting authentication information | Supports Off, DH group(5,14,15,16,17,18) |
| IKE Lifetime | Cycle for generating new keys | |
| ESP encryption | Algorithm to encrypt data packets | Supports AES-128, AES-256, blowfish-128, blowfish-192, blowfish-256, Twofish-128, Twofish-192, Twofish-256 |
| ESP integrity | Encryption algorithm for integrity assurance | Supports SHA1, SHA2-256, SHA2-384, SHA2-512 |
| ESP DH group | Encryption algorithm to generate keys for encrypting data packets | Supports Off, DH group(5,14,15,16,17,18) |
| Lifetime | Tunnel maintenance time | |

3. Go to System -> Site -> Select Tasks -> Click Create, and create a **Branch Type Site**.

   - **Site Name** : Enter the name to be used as the site name.

- **Type** : Select the Hub site to proceed with IPsec connection.
- **Infrastructure** : Select the configuration environment of the equipment to connect (Cloud, On-prem). If Cloud is selected, set Cloud Provider, Region, and VPC ID together.
- **Network Address** : Enter the network range to use. If Cloud, enter the configured VPC range.

4. Change **ZTNA-IPsec Application Mode to Enabled**, and proceed with detailed settings.

- **Public IP** : Enter the public IP of the VPN equipment.
- **Pre-Shared Key** : Enter the Pre-Shared Key configured in the Hub site.
- **Networks** : Enter the subnet of the VPN equipment.
- **Assigned Sensor** : Select the sensor to run the VPN of the Branch site. Do not select if using VPN equipment.

5. After configuration is complete, go to System -> Site -> **Created Hub or Branch Site** -> Click **Top Tab ZTNA IPsec Status** -> Check if the IPsec tunnel is connected normally.

## 17.2 Cloud Provider Management

This is the configuration screen to register and manage cloud accounts for various cloud-related operations.

1. From the top menu, go to System > Cloud Provider.
2. Click "Select Action" then click "Create".
3. Enter a name for the configuration (e.g., 'AWS Cloud').
4. Select one of the following for the Cloud: "AWS", "AZURE", "NHN", "NAVER", "LINODE".
5. Refer to the 'Input method for each cloud type' section below to enter the required information.
6. Click Create.

### 17.2.1 Input Method for Each Cloud Type

#### AWS Credential Information

1. Access Key: In the AWS Console, click the user email at the top right > Select "Security credentials" > Check and enter the 'Access key'.
2. Secret Key: When creating the Access key, click 'Show' to check and enter the 'Secret key'.

- **Policies that must be enabled in the AWS account's IAM**
- Path: AWS Console > IAM > Users > Select user ID > Permissions > Policy name
- AdministratorAccess: Provides full access to AWS services and resources.
- AmazonEC2FullAccess: Full access to Amazon EC2 through the AWS Management Console.
- AmazonRoute53FullAccess: Full access to Amazon Route 53 through the AWS Management Console.
- AmazonS3FullAccess: Full access to all buckets through the AWS Management Console.
- AWSMarketplaceFullAccess: Allows subscribing and unsubscribing from AWS Marketplace software, managing Marketplace software instances on the 'Your Software' page, and managing EC2 access.
- AWSSupportAccess: Grants access to the AWS Support Center.
- CloudFrontFullAccess: Grants full access to CloudFront Console and the ability to list Amazon S3 buckets.

- CloudWatchEventsFullAccess: Grants full access to Amazon CloudWatch Events.
- CloudWatchFullAccess: Grants full access to CloudWatch.
- SecurityAudit: Provides read-only access to security configuration metadata. Useful for software auditing AWS account configuration.

### AZURE Credential Information

1. Client ID: Azure Portal > Azure Active Directory > App registrations > Check and enter the 'Application ID'.
2. Client Secret: Home > Azure Active Directory > App registrations > Certificates & secrets > Check and enter the 'Value'.
3. Subscription ID: Home > Subscriptions > Check and enter the 'Subscription ID'.
4. Tenant ID: Home > Azure Active Directory > App registrations > Check and enter the 'Directory ID'.
5. Resource Group Name: Home > Subscriptions > Subscription Name > Resource groups > Check and enter the 'Name'.

- **IAM roles required for the Azure account**
- Path: Access control (IAM) > View my access > Current role assignments > Role field
- Contributor: Full access to manage all resources, except assigning roles in Azure RBAC, managing assignments in Azure Blueprints, or sharing image galleries.
- User Access Administrator: Can manage user access to Azure resources.
- Managed Application Operator Role: Can read and perform operations on managed application resources.

### NHN Credential Information

1. User Name: Enter the NHN Console login 'ID'.
2. Tenant ID: Go to Compute > Instance > Management page > Click API endpoint settings button > Check and enter the 'Tenant ID'.
3. Password: Go to Compute > Instance > Management page > Click API endpoint settings button > Set and enter the desired API 'Password'.

- **Project role settings for NHN account's IAM**
- Path: Login to the corresponding console > Member Management > IAM Members
- Set the role for the project to ADMIN.

## 17.3 Troubleshooting

- *Genian ZTNA log collection method*
- *Genian ZTNA diagnosis Method*
- *Network Sensor is not displayed in Web Console*
- *Sensor link state is displayed as Down*
- *Network Sensor is displayed as Failsafe*

CHAPTER

EIGHTEEN

# API GUIDE

**Note:** This feature requires Enterprise Edition

Genian ZTNA provides the REST API to get desired information from the policy server or to set security policy and various objects. An API key is required to call the API from the outside to the policy server. API Keys are created for each administrator and can be accessed or set according to the privileges granted to the administrator.

To create or verify an administrator API Key:

1. Go to **Management > User** in the top panel
2. In the left panel, select **Administrators**
3. Click **administrator name** to generate the API Key
4. Select **Administrator** tab
5. On **API Key**, Click **Generate API Key** button
6. Click **Update** at the end of the page

The API key set through the above process should be passed as parameter of Request URL as follows.

```
curl -X GET "https://nac.company.com/mc2/rest/logs?apiKey={API Key}"
```

List of APIs provided by Genian ZTNA can be found below.

- **https://[Policy Server IP or FQDN]:8443/mc2/swagger/index.html** (Admin must be authenticated to the Policy Server)
- API Reference Guide for Enterprise Edition
- API Reference Guide for MSSP

CHAPTER

NINETEEN

# LOG FORMAT

The logs generated by the Genian ZTNA consist of a column containing specified column values such as IP, MAC, and detailed text. The format of the text column is:

```
Log Messages. key1=value1, key2=value2, key3="value 3" . . .
```

CHAPTER

TWENTY

# NODE GROUP TEMPLATES

You can import node group templates into your Policy Server to more easily organize and manage your network.

See: *Managing Node Groups*

## 20.1 Common Vulnerabilities

`Ripple 20 by CVE Code`

`Urgent 11 by CVE Code`

CHAPTER

TWENTYONE

# FREQUENTLY ASKED QUESTIONS

## 21.1 What is the difference between ZTNA and existing NAC products?

The following features have been added to implement Zero-Trust security policies on top of the capabilities of existing NACs. Support for dynamic destination access control for communication/internal network->Cloud/from-home access between sensor managed nodes. ZTNA Client functionality to provide enhanced terminal security and secure communication environment for telecommuters. Cloud information collection for visibility and zero trust access control of the Cloud server band. Cloud Gateway functionality to provide dynamic access control for cloud server bandwidth and Internet access. Cloud Security Group Management for Automated Security Policy Management on Cloud Servers. Netflow (IPFIX)-based NTA capabilities that provide visibility into network traffic. Security news feeding service that informs you of the latest security news and related nodes. New Dashboard / Extended Node Type / Platform Image Based Grid View.

## 21.2 What is Zero Trust security policy and how does ZTNA provide it?

Any device that accesses a network is a concept that takes by default a policy that does not allow other than the services/servers that are essential to that device. To do this, the origin and destination must be categorized very precisely according to their role. (Micro Segmentation) ZTNA can manage node groups for destinations, including origin and Cloud, through node groups that provide more than 500 conditional expressions. The new ZTNA allows node groups to be used when setting up network access that is allowed to finely classified user terminals. When destination control is enabled through node groups, the security policy is automatically updated based on status/properties/Tags, etc.,away from the IP/Subnet security policy provided by existing products.

## 21.3 Do I need new equipment or network configuration for dynamic destination control?

No, no new equipment or network configuration changes are required when operating ZTNA in an existing sensor-installed environment. Dynamic access control is possible without configuration changes through communication between sensors through standard VXLAN SGT. Genians' patented ARP-based virtual in-line access control method allows in-band access control by configuring out-of-band or building an in-line gateway sensor, so you can choose the appropriate method depending on the deployment environment.

## 21.4 How can dynamic destination control be applied when accessing servers (workloads) that exist in the cloud?

Cloud access control can be applied in two ways. The first method is to manage the IP list of devices that have access to the server by synchronizing it with a node group through the Security Group feature provided by the Cloud. The second method is to configure the Cloud Gateway to allow all communications to pass through the Cloud Gateway for access control. In this case, you can use an SSL-VPN-based G2C method for specific terminals only or a G2G method using IPSec for network-level connections.

## 21.5 Is the user's network traffic visibility provided when performing dynamic access control?

Yes, ZTNA provides standard Netflow (IPFIX)-based audit records for connections through sensors/gateways. This provides 5 Tuples, Policy information, as well as GeoIP, BGP AS, HTTPS Encrypted Traffic Analysis (ETA), HTTP Request information, etc.

## 21.6 What is the difference between the dynamic access control provided by ZTNA and the controller-type SDN?

The SDN method, which handles dynamic access control for all connections on one central controller, has a problem that all communication is interrupted in the event of a controller failure. In contrast, Genian ZTNA's dynamic access control method uses the standard VXLAN SGT method, and dynamic access control of previously authorized terminals operates normally even in the event of a policy server failure. In addition, it is provided through Genian's own ARP virtual inline method, so there is no need to change the physical network configuration or network settings at all.

## 21.7 What happens if a ZTNA sensor failure occurs when using dynamic destination access control?

If you are operating in out-of-band host sensor mode, the network access control function is disabled in case of sensor failure. If you're operating in an In-Band manner with Cloud Gateway, you can recover faster than your On-Prem Appliance system with simple instance reboot/replayability.

## 21.8 What are the benefits of ZTNA offered in ZTNA over traditional VPNs?

By default, ZTNA provides IPSec, SSL-VPN capabilities provided by traditional VPNs. The ZTNA Client is integrated within the NAC Agent and supports Zero Config. The PoP can be located in the Cloud, dramatically reducing WAN segment traffic and providing faster network access to users compared to traditional VPN methods where all traffic enters the company. The PoP can be located in various countries/continents, making it suitable for global companies. (Multiple PoP and Latency-based PoP automatic selection) Only devices that have passed the device integrity check provided by the NAC Agent can be controlled to allow network access, and access is controlled through continuous device health check while the network is in use.

## 21.9 Does ZTNA support Multi Cloud environments?

The use of one or more Cloud services is becoming more common due to the complexity of the Cloud environment. ZTNA provides an easy way to simplify and automate the establishment of different security policies for different Cloud providers. When security policies for Cloud servers/services are defined through ZTNA, security groups are automatically applied through the industry standard Terraform without the need for separate UI/API/CLI for each Cloud service.

## 21.10 Can Cloud Security Group Management be applied only to Public Cloud?

No, it is also applicable to private clouds such as VMWare/Citrix, or to HCI and Hybrid clouds such as Nutanix. Furthermore, you can support a variety of providers, including switches, security equipment, and SaaS services. We are providing sequential support according to your request.

## 21.11 What is the difference between ZTNA and SASE?

SASE's approach to service is to ensure that all network access control is through the Cloud Gateway, placing all security systems in the Cloud. This shifts the On-Premises-centric security system to Cloud-centric. ZTNA provides the ZTNA and Cloud Gateway you need to do this. Cloud Gateway offers a variety of tunneling methods, including IPSec, SSL-VPN, GRE, and VXLAN, to help different branch and telecommuters create secure communication channels. ZTNA allows users to create their own built-in SASE services.

## 21.12 Does ZTNA support Multi-Tenancy?

ZTNA supports Kubernetes-based multi-tenant environments that can serve multiple tenants in addition to traditional products for single tenants. This allows you to build a system that provides independent, managed services for multiple domains within the client company.

## 21.13 What is the product release cycle?

Genian ZTNA releases a new minor version every one months.

## 21.14 Can I downgrade my software version?

No, downgrade is not supported. For a downgrade, you should create a backup before you upgrade, and then reinstall software and restore backup data.

## 21.15 Is the communication between each component encrypted?

Yes, communication between each component is encrypted through TLS.

## 21.16 What if I exceed the license amount?

See step 1 on *Sizing Software and Hardware*

## 21.17 How can I check Windows update of endpoints?

See step 1 on *Update Windows*

## 21.18 How come the blocked Nodes cannot open the CWP through Genian ZTNA?

See step 1 on *Blocked Nodes are not redirected to CWP page*

## 21.19 What Regex engine does Genian ZTNA utilize?

Genian ZTNA utilizes Perl Compatible Regular Expressions. For information including syntax reference the following resources:

- Perl Compatible Regular Expressions
- PCRE CheatSheet
- Regex Debugger

## 21.20 Can User Credentials from Active Directory be used to access the Web Console?

Yes. To configure, you must configure authentication integration AND user database synchronization with an AD domain controller. Lastly the Active Directory user must be selected in the Genians user database and configured with a superAdmin role.

- *Integrating User Directories*
- *Synchronizing User Directories*
- *Administrator Roles*

## 21.21 Can Node info be imported from a wireless controller via SNMP?

No, this function is not supported.

## 21.22 Why can't I collect domain information from my Agentless environment?

Domain name and host name information in an Agentless environment is collected via two methods:

Method 1 - The Sensor extracts domain name and host name from netbios packets. Be sure to add a sensor interface in the subnet you wish to collect this information for.

Method 2 - WMI collection of domain, host name and other information is possible if configured. Reference the following information on how to configure this feature if domain or host name information is not being populated by the Sensor.

*WMI Node Info Scan*

## 21.23 Why is the Agentless device host name not collected?

Domain name and host name information in an Agentless environment is collected via two methods:

Method 1 - The Sensor extracts domain name and host name from netbios packets. Be sure to add a sensor interface in the subnet you wish to collect this information for.

Method 2 - WMI collection of domain, host name and other information is possible if configured. Reference the following information on how to configure this feature if domain or host name information is not being populated by the Sensor.

*WMI Node Info Scan*

## 21.24 Why can't I collect device information in my Agentless environment, even after configuring Agentless WMI collection?

In Windows 10 version 2004 there are known issues with WMI functioning properly due to DCOM version issues. The recommendation is to upgrade to a later version. If upgrading to a later version is not possible, please contact your technical support representative.

## 21.25 Why there is 'Agent Not Installed' policy even though we are using Agentless?

The default enforcement policy is created based on Agent-installed. you can use it after creating/deleting a policy according to your environment.

## 21.26 When is the update cycle of Genian data?

The Genian data is automatically updated at the set period when the inspection cycle is set at **Web Console > Preferences > Miscellaneous > Genian data settings > Scan interval** and the bottom **Automatic Update** item is set as `On`.

## 21.27 How can I collect wireless LAN SSIDs?

Please refer to the following documents. *Controlling WLAN*

## 21.28 How do I control access to the terminal wireless LAN?

Terminal wireless LAN access control can be performed in two ways. There are ways to `Disable` wireless network adapter (*Controlling Network Interface*)` and restrict wireless LAN AP access using *Controlling WLAN*.

## 21.29 How do you control terminals that share and use networks using wired/wireless?

Anomaly definition policies (*Understanding Anomaly Detection*) can be restricted using the `Multi-Homed / Ad hoc Network` policy.

## 21.30 How do you control unnecessary administrator web access?

Session management(session-control) allows unnecessary access sessions to be forcibly terminated.

## 21.31 Can I access the web console using user credentials in Active Directory?

> Available by setting up authentication interworking and information synchronization; AD domain controller and database synchronization; finally, AD users must select and configure from Genians user databases integrate-external, LDAP .

## 21.32 What is the node type and platform classification operation method?

Node type and platform classification are classified through the operational data NMDB and GPDB GDPI .

## 21.33 How do I collect agent logs?

Right-click the agent tray icon -> Click Program Information -> Click Error Reporting -> Check C:GnAgentDate.zip File

## 21.34 What is the difference between node action and node action in enforcement policy?

Node actions enable all registered agent plug-ins, but only the specified plug-ins are available for node actions used by control policies.

## 21.35 A device using a wireless network is detected on a different platform

> A false positive occurs when you use another manufacturer's OUI while changing the MAC address to RANDOM MAC as a function of mobile and PC. The RANDOM MAC setting is located in the wireless lan profile detail setting and can be taken action by setting the MAC address type to the MAC of the terminal. *Wireless LAN User Devices Are Detecting as Wrong Platform*

## 21.36 What are Agent Sensor and Network Sensor?

- Agent Sensor: Collects asset information on the same network by installing the agent on some endpoints.
- Network Sensor: Collects asset information present on the network by setting up a physical server.

## 21.37 How do I use the Agent Sensor feature?

- Web Console → Policy (top menu) → Click the node policy to apply → Click Assign Agent Actions, move 'Sensor' to Selected and click Edit. Then click Edit at the bottom and click Apply Changed Policy (top right) to enable the Agent Sensor feature.

## 21.38 How do I set up the Network Sensor?

- Refer to the guide: Installing Network Sensor to configure a physical server (mini PC, desktop, server, etc.).

## 21.39 What information can I collect and view via the Agent Sensor?

- Automatically collects the IP, MAC, and host name of endpoints connected to the network and helps you easily identify them.

## 21.40 What information can I collect and view via the Network Sensor?

- Automatically collects and lets you easily view device type (PC, Network Appliance, Mobile Device, etc.), IP, MAC, host name, platform, NIC vendor, open ports, and service list.

## 21.41 What is the capacity of the trial license?

- You can automatically register and identify up to 300 endpoints.

## 21.42 Can I manage device/equipment information separately?

- Yes.
- Device: Management → Nodes → Click a device → In the Device Information tab, you can enter and manage manufacture date, vendor, serial number, etc.
- Node: Use the Description field, or manage with custom fields if categorization is needed.

## 21.43 Why do I see the agent Location Service permission pop-up on Windows 11 (24H2)?

- What changed? Starting with Windows 11 24H2, by Microsoft policy, apps that use Location Services must ask for permission the first time.
- Why does it appear? The plugin needs location permission to retrieve Wi-Fi lists, scan, and manage connections.
- Affected features: Interface control, network information collection, wireless LAN control, wireless connection manager.
- If you don't allow Location Services, these plugins may not function properly.

CHAPTER

# TWENTYTWO

# TROUBLESHOOTING

**This section describes common errors, their potential causes and how to resolve them.**

## 22.1 Genian ZTNA log collection and diagnostic method

### 22.1.1 Genian ZTNA log collection method

Genian ZTNA supports debug dumps for each component when an issue arises. The dump file is used for issue analysis.

#### How to Collect the Agent Log

#### Collecting via Web Console

1. Navigate to the **Management > Node** tab
2. Click the check-box beside the Node(s) you wish to collect logs from, and select to **Tasks > Bulk Actions**, or select an individual node IP.
3. Select **Run Node Tasks** from the dropdown, or use the **Node Tasks** menu if viewing a single node.
4. Select **Collect Agent Logs** and click **Run** if applicable.
5. After collection is complete, the logs can be viewed and searched in **Log > Debug Logs**.

#### Collecting via Endpoint

- Right-Click the **Agent Icon** on the endpoint
- Select the **About Genian Agent(A)**
- Click the `Save Error Logs`
- Log dump file is stored in **C:** on Windows , **/Users/Shared/Genians** on Mac
- In form of GnAgent _[DateTime].zip on Windows and Genians _[DateTime].zip on Mac

**Note:**

- Log collection in an Active Directory environment requires domain administrator-level privileges.
- For LINUX devices, you must go directly to the debug storage path and collect it. **/var/log/genians**.

### How to Collect the Policy Server and Network Sensor

The Policy Server and Network Sensor come with a feature for centrally collecting and exporting error logs. The log can be uploaded to a JIRA issue or saved locally.

#### Collecting via Web Console

1. Navigate to the **System** tab
2. Click the check-box beside the Appliance you wish to collect logs from.
3. Select to **Tasks > SysCollect**
4. Select if Center, Sensor, and/or Agent logs should be included for collection, and click **Start**.
5. After collection is complete, the logs can be viewed and searched in **Log > Debug Logs > system > agent**.

#### Collecting via Command Line Interface

Follow the below steps, as shown in the code box:

- Connect to the Policy Server or Sensor through console or SSH.
- Login.
- Enter configuration mode.
- Enter shell mode.
- Use the command `syscollect.sh` to generate a compilation of the component logs.
- Select if you would like to upload logs.
- Select which components to collect logs from.

```
genian> en

genian# @shell

Genians$ syscollect.sh

Do you want upload to GENIANS IMS ? (Y/n)
Do you want to trace centerd ? (y/N)
Do you want to trace sensord ? (y/N)
Do you want to collect agent logs ? (y/N)
```

### Collect network communication packets between components

#### Usage example

```
tcpdump -i eth0 port 80 and udp
- Capture for udp through 80 port on interface eth0

tcpdump -i eth0 -e
- Include ethernet information on interface eth0 and capture it.

```

(continues on next page)

(continued from previous page)

```
tcpdump -i eth0 net 192.168.
- Captures a packet starting at 192.168 on interface eth0

tcpdump -i eth0 host [IP address] and ARP[7] == 2
- Capture for arp Reply packets on interface eth0

tcpdump -i eth0 -w file1 port 80 and udp
- Save captures for port 80 and udp packets on interface eth0 as ABC files
```

### Option Definition

```
-v: When parsing and printing, produce (slightly more) verbose output. For example,␣
↪the time to live,
    identification, total length and options in an IP packet are printed. Also␣
↪enables additional packet
    integrity checks such as verifying the IP and ICMP header checksum.
-n: Don't convert addresses (i.e., host addresses, port numbers, etc.) to names
-e: Print the link-level header on each dump line. This can be used, for example, to␣
↪print MAC layer addresses
    for protocols such as Ethernet
-w: Write the raw packets to file rather than parsing and printing them out.
-A: Print each packet (minus its link level header) in ASCII.
-q: Quick (quiet?) output. Print less protocol information so output lines are␣
↪shorter.
```

### Conditional expression

```
host : Capture all packets containing the IP address you entered.
dst host : Filter by Destination IP Address
src host : Filter by Source IP Address
ether host : Capture all packets that contain the entered MAC address.
ether dst : Filter by Destination MAC addr of Ether Frame
ether src : Filter by Source MAC addr of Ether Frame
net : Capture to the network subnet
dst net: Capture to the network destination subnet.
src net: Capture to the network source subnet.
```

### Export Log Files From Genian ZTNA

Genian ZTNA shell mode supports the SCP command for sending files through SSH.

Navigate to **/disk/data/temp/** and use the follwing command format to send the logs to their destination:

### Usage example

```
scp [filename] [username]@[destinationIP]:[destinationPath]
```

## 22.1.2 Genian ZTNA diagnosis Method

This section provides an overview of the major processes used by Genian ZTNA that can be examined to troubleshoot issues.

### Genian ZTNA Process Description

### Policy Server Processes

```
centerd: Policy and node management processes
sensord: Network Sensor Process
mysql: Node and policy information is stored in the database
apache2: Web service Daemon
java: As a Java process for running the WebUI, Interworking between Web and Database
procmond: A process monitor daemon used by Genian ZTNA, Monitor abnormal termination␣
↪and perform re-execution
sshd: Daemon for providing SSH remote access
syslog-ng: SYSLOG Daemon
hbd: A daemon that performs actions (such as reboot) to normalize the system after a␣
↪certain period of time if a hardware or software failure occurs
mysqld_safe: Script to save restart and runtime information in Mysqld_error when␣
↪mysqld server fails
gnlogin: Providing services for executing CLI commands
crond: A daemon that performs scripts and commands on a specified cycle
```

### Network Sensor Processes

```
sensord: Network Sensor Process
nmap: Scan tool that Network information of Node
procmond: A process monitor daemon used by Genian ZTNA, Monitor abnormal termination␣
↪and perform re-execution
sshd: Daemon for providing SSH remote access
syslog-ng: SYSLOG Daemon
hbd: A daemon that performs actions (such as reboot) to normalize the system after a␣
↪certain period of time if a hardware or software failure occurs
```

### Agent Processes

```
Process name : GnAgent.exe
Description : Genian Agent
Function : Agent integrity check, node policy reception and GnPlugin run management
Execution cycle: Always
Execution condition: Always after Windows logon

Process name: GnPlugin.exe
Description: Genian Action Plugin
Function: Perform action policy of node policy and send result
Execution cycle: Always
Execution condition: Always when an action policy exists in a node policy

Process name: GnStart.exe
Description: Genian Starter
Function: Agent integrity check, GnAgent execution management, Keep Alive transfer
Execution cycle: Always
Execution condition: Always

Process name: GnAccount.exe
Description: Genian User Account Manager
Function: when running the GnAgent process with a specific account instead of an OS logon account
Execution cycle: When an event occurs
Execution condition: Node Policy>Execution Account

Process name: GnDump.exe
Description: Genian Agent Dump Utility
Function: Dump Agent Debug Logs
Execution cycle: None
Execution condition: Operates only when executed manually

Process name: GnExLib.exe
Description: Genian External Module
Function: Register external authentication module (ex. dll)
Execution cycle: None
Execution condition: Works only when executed manually

Process name: GnScript.exe
Description: Genians Software Install Manager
Function: Install Agent
Execution cycle: None
Execution condition: Performed only during agent installation

Process name: GnUpdate.exe
Description: Genian Updater
Function: Update Genian Agent automatically
Execution cycle: 6 hour
Execution condition: None

Process name: GnUtil.exe
Description: Genian Agent Utility
Funcfiton: Compute the SHA1 hash value of a specific file
Execution cycle: None
Execution condition: Works only when executed manually
```

## System Log Description

### Policy Server Log

**Location:** `/disk/data/logs`

#### Elasticsearch

```
GENIAN.log: Elasticsearch process abnormal termination and restart error log, etc.
```

#### apache2

```
Error_log: apache2 error log
Mod_jk.log: Apache and Tomcat communicate using Apache JServ Protocol (AJP) to␣
↪communicate with each other and configure it using a module called mod_jk
- Apache and tomcat related error log
```

#### mysqld

```
Initdb.log: Logs generated during database initialization
Check whether the table is abnormal when driving

Mysqld.error: error log during mysql operation
Slowquery.log: SQL Query Log for long-running jobs
- Refer to when a specific action takes a long time during ZTNA operation
```

#### system

```
Agent: Agent log stored in PC is called from policy server and stored
 - call command: centerd -dfg

centerd: Logs of actions performed by the Policy Server
 - Policy Server status, Node role status, Authentication, integration, Data sync etc

sensord: Save the operation and error log performed by the network sensor
 - Network Sensor status, Node detection, UP / Down, policy reception etc

messages: Hardware status related messages like dmesg

procmond: Process terminated abnormally and restart log
scanraw: Network scan  information of Node for the platform's detection of the node
updown: Agent Up / Down status log
authsync: Database synchronization related logs
dbmigration: Save database migration results
gnlogin: console Login History Saving
radius.log: Saving RADIUS Status and Node Authentication Logs
```

### tomcat

```
Catalina.out: The catalina.log file contains all log messages that are written to Tomcat's system.out and system.err streams.
The catalina.out file can include:
 - Uncaught exceptions printed by java.lang.ThreadGroup.uncaughtException(..)
 - Thread dumps, if you requested them via a system signal
```

### System Inspection

Check script for the status of the Genian ZTNA system.

- Follow the below steps, as shown in the code box:
- Connect to the Policy Server Console directly or by SSH.
- Enter configuration mode.
- Enter shell mode.
- Use the `sysinspect.sh` command to check the system status.

```
genian> en

genian# @shell

Genians$ sysinspect.sh


   ==========Regualr Inspection==========
   1) Check Server/Service infomation
   2) Check Service status
   3) Check Disk & Memory information
   4) Check Smartctl
   5) Check Slow Query
   6) Check Total Inspection
   9) Check Setup Config
   ======================================
   Enter Select Number :
```

### Check Server/Service information

- ServerRole: Refer to the configuration of the server to indicate the role of the server.
- H/W duplication: Check if the server is redundant. If redundant, check if the server is master or slave.
- DB replication: Check if the DB is redundant
- ALIVE: If DB replication status of Master / Slave server is normal, ALIVE
- MISMATCH or result is broken: If DB replication state of Master / Slave server is abnormal
- System Uptime: Number of Users in Server, Server CPU Load
- Platform: The model name of the server
- Version: The version of the image installed on this server
- MAC Address List: MAC Address list output

- Service Version: The version of services used by the server
- Elasticsearch indices Health check: Check the status of ElasticSearch indexes
- green: normal, Yellow / Red: abnormal
- Last 7 days Log Backup Check(Today Warning): Ensure Log backup is working properly
- Last 7 days DB Backup Check(Today Warning): Ensure Policy / Node backup is working properly

### Check service status

Verify that all necessary processes are running on Genian ZTNA.

Necessary processes by component:

```
Policy Server:
Mysqld, elasticsearch, java, centerd, sensord, apache2, procmond, sshd, syslog-ng,␣
↪radius (Need confirmation if using RADIUS server), vrrpd (Need confirmation if␣
↪using HA configuration)

Network Sensor:
sensord, procmond, sshd
```

### Check Disk & Memory information

Check the server's hard disk capacity and memory. If the hard disk is full or there is no free memory, Genian ZTNA may encounter the following problems.

- Genian ZTNA operation is slow or does not work
- When a backup file is not created

### Check Smartctl

Check hard disk status If the RAW_VALUE value of Reallocated_sector_ct is not 0, there is a problem with the hard disk. Genian ZTNA operation may be defective, requiring hard disk replacement

### Check Total Inspection

The server state described above is output at once

### Check Setup Config

- Check for any missing basic settings
- How to check sensor and node status through CLI command

How to Check Network Sensor Status:

```
genian# show enforcer
interface | mode | active | local | request | strict | max
bond0.100 |    2 |    OFF |    ON |     OFF |    OFF | 10
bond0.101 |    2 |    OFF |    ON |     OFF |    OFF | 10
```

How to Check Node Status:

```
genian# show nodeinfo filter [IP address]
    IP               | MAC                | device | sta | up |     age |    idle |    ␣
↪expire | noderole
    172.29.20.183    | 00:E0:4C:36:0D:F8 | eth0   |   1 |   1 | 1728088 |       5 |    -
↪3118306 | Denied by IPAM(10)

ARP Poisoning list
genian# show nodeinfo poisoning [IP address]
IP=172.29.111.55 MAC=00:05:1B:A3:E2:07 IF=bond0.111
TARGET=172.29.111.56   ACTIVE=1 LASTREQ=832    DSTTOXIC=0
TARGET=172.29.111.254  ACTIVE=1 LASTREQ=0      DSTTOXIC=0
```

## 22.2 Network

### 22.2.1 Network Sensor is not displayed in Web Console

#### Symptom

The Network sensor is not visible in Web Console.

#### Cause

- After the network sensor is installed, it registers with the policy server using port 443.
- If registration communication between policy server and network sensor fails, the sensor will not be recognized, and it will not be shown in the Web Console.

#### Resolution

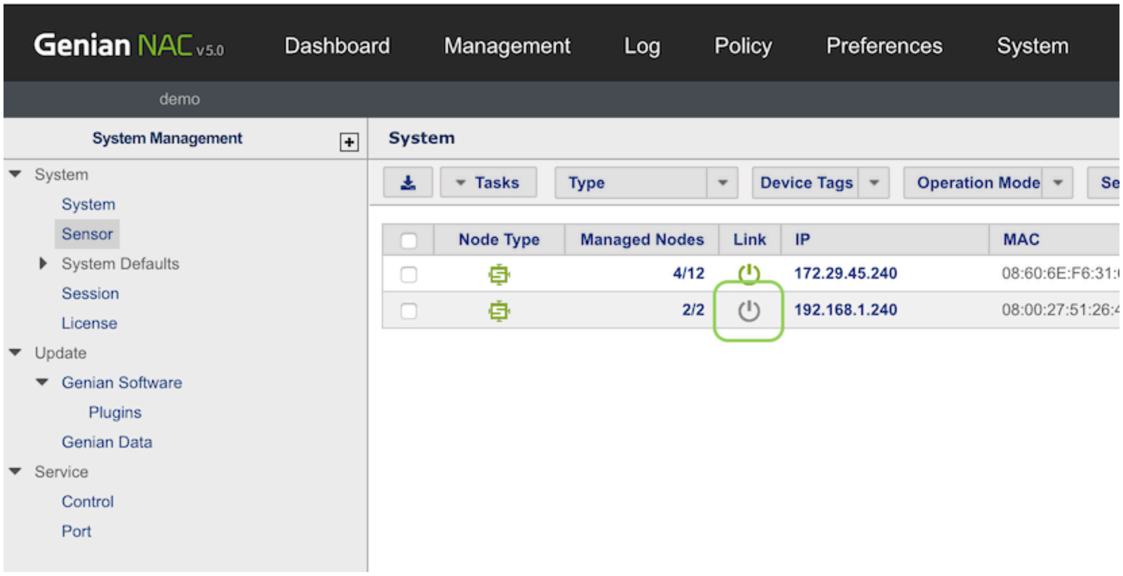
#### Check Connectivity

- Verify communication path between Policy Server and Network Sensor on port 443. Ensure necessary exceptions on firewalls or other appliances.
- Through SSH on the Policy Server and Network Sensor, inspect traffic using the command: `tcpdump -i eth0 host [Policy server or network sensor IP]` (If accessing Policy Server console, use Network Sensor IP for tcpdump host IP , and vice-versa)

### 22.2.2 Sensor link state is displayed as Down

#### Symptom

Sensor link state is displayed as Down in the node management or sensor management screen.



System

| □ | Node Type | Managed Nodes | Link | IP | MAC |
|---|---|---|---|---|---|
| □ | | 4/12 | | 172.29.45.240 | 08:60:6E:F6:31: |
| □ | | 2/2 | | 192.168.1.240 | 08:00:27:51:26: |

## Cause

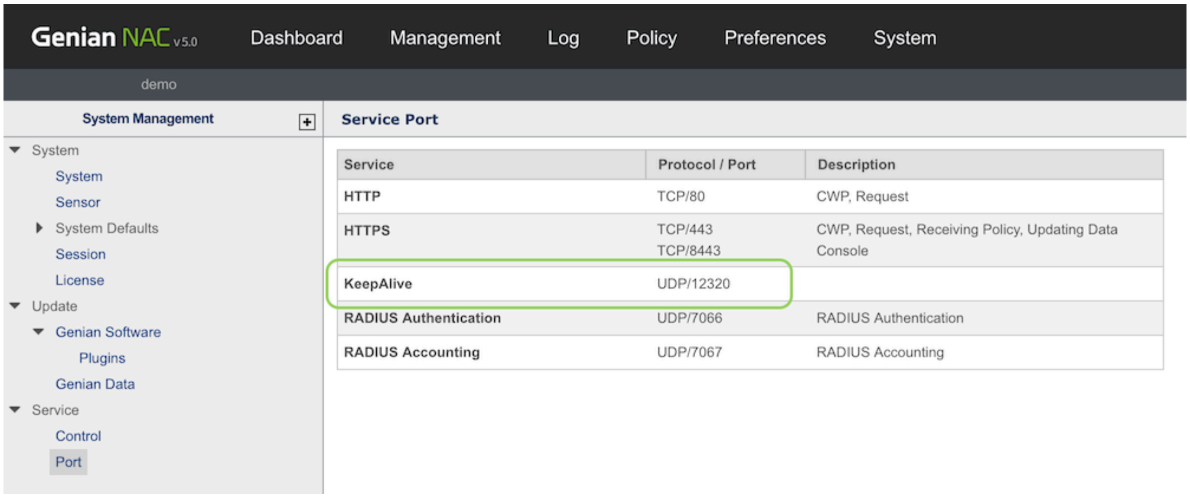
The network sensor periodically sends a keep-alive packet to the policy server to inform that it is operating normally. If this packet is not forwarded to the policy server, the link status is displayed as Down.

### The keep-alive packet communicates on the following ports:

**On-Premeses**
Allow for UDP / 3870 ports

**Cloud-managed**
(Varies)

Go to **System> Service > Port** and allow port in **Keepalive** section



Service Port

| Service | Protocol / Port | Description |
|---|---|---|
| HTTP | TCP/80 | CWP, Request |
| HTTPS | TCP/443<br>TCP/8443 | CWP, Request, Receiving Policy, Updating Data<br>Console |
| KeepAlive | UDP/12320 | |
| RADIUS Authentication | UDP/7066 | RADIUS Authentication |
| RADIUS Accounting | UDP/7067 | RADIUS Accounting |

### Resolution

In this case, the following should be confirmed:

1. The network sensor is turned on.
2. A communication path exists between policy server and network sensor on the keep-alive port. Ensure necessary exceptions on firewalls or other appliances.
3. Through SSH on the Policy Server, inspect traffic using the command to see if the keep-alive packet is reaching the policy server: `tcpdump -i eth0 host [Network Sensor IP] [keep-alive port]` , to check for keep-alive packet.

## 22.2.3 Network Sensor is displayed as Failsafe

### Symptom

The Network Sensor is displayed as Failsafe in the Node management or Sensor management.

### Cause

The Network Sensor periodically sends a UDP keepalive packet to the Policy Server, which will reply in the same session with an acknowledgement. If there is a Policy update, the Policy Server will notify the Sensor in the acknowledgement.

If the Sensor is made aware of new policy information, it will attempt to start a TCP session with the Policy server over HTTPS on port 443. If this TCP session fails to initiate 5 times, the Sensor status will display as Failsafe.

### Resolution

### Check Connectivity

- Verify communication path between policy server and network sensor on port 443. Ensure necessary exceptions on firewalls or other appliances.
- Through SSH on the Policy Server and Network Sensor, inspect traffic from the other component using the command: `tcpdump -i eth0 host [source IP]`

### Check Network Sensor Interface Status

- Through SSH on the Network Sensor, enter the command: `show interface eth[#]`
- Default interface is eth0.

#### Check Policy Server / Network Sensor Debug

Using SSH on the Policy Server and Network Sensor follow the steps below:

```
genian> en

genian# @shell

Genians$ Cat /disk/data/logs/system/centerd | grep ”ERRMSG=SOAP”> network_err

Genians$ Cat ./network_err | grep [Policy Server or Network Sensor IP Address] 443
```

### 22.2.4 Running Genian Agent is not Detected in WebUI

#### Symptom

The node is currently up, and the agent is running, but the agent is marked as down in the Web Console.

#### Cause

The Genian Agent sends a keep-alive packet to the Policy Server once every two minutes to let you know its operational status.

The policy server changes the agent's operation status to "no action" by default when it does not receive the keep-alive packet from the Genian Agent for 10 minutes.

The following situations can disrupt this keep-alive packet resulting in a false down status:

1. Packet control in a firewall between Policy Server and Genian Agent.
2. A PC's antivirus solution preventing Genian Agent process from sending data.
3. The Agent is not properly generating the keepalive packet.

#### Resolution

#### Checking communication between Policy Server and Genian Agent

- Using SSH on the Policy Sever and Network Sensor follow the steps below:

```
genian> en

genian# @shell

Genians$ tcpdump -i eth[interface number] host [Node IP address] [keep-alive port]
```

Example syntax: `tcpdump -i eth0 host 10.10.10.245 24378`

**If no traffic keep-alive traffic is detected:**

- Verify communication path between policy server and agent on the keep-alive port. Ensure necessary exceptions on firewalls or other appliances.
- (Windows) Enable local logging to determine that the agent is generating and sending the keepalive packet.

  - In the Registry, find `HKEY_LOCAL_MACHINE\SOFTWARE\Geni\Genian\Option` or `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Geni\Genian\Option`
  - Set `DWORD:DebugPrint (1)`

**If keep-alive traffic is detected:**

- There may be a problem with the Agent installation or Policy Server
- Use the Syscollect function on the Policy Server to send info to Genians engineers.
- Obtain logs from Agent and send to Genians engineers.

See: *Genian ZTNA log collection method*

## 22.2.5 Agent is Installed but not Running

### Symptom

The Genian Agent is showing as installed in the "Programs" section of an endpoint but it is not shown as running in the processes or services. It is not the shown as installed in the Web Console.

### Cause

The Genian Agent sends a keep-alive packet to the Policy Server once every two minutes to let you know its operational status.

The policy server changes the agent's operation status to "no action" by default when it does not receive the keep-alive packet from the Genian Agent for 10 minutes.

The following situations can break the installation of the agent and render it inoperable:

1. Proper installation of agent is not possible due to hard disk problems. there may be associated error logs in the Web Console for Data Corruption.
2. An agent deployed via GPO may partially uninstall due to Node policy settings for **"Deleting Agent Not Running"**

### Resolution

### Check Node Policy Settings for Agent Deletion

- Navigate to the last known node identity for the device, and check the **"Deleting Agent Not Running"** setting for the node. If the node has not been detected by the policy server for longer than the time sepcified, the agent has been uninstalled. The program registry itself preserved upon the agents deletion in GPO Deployments.

### Check Agent File Integrity Logs

- Check the main Web Console Logs section for Agent Data Corruption
- Use the Syscollect function on the Policy Server to send info to Genians engineers.
- Obtain logs from Agent and send to Genians engineers.

See: *Genian ZTNA log collection method*

### Reinstall Agent

- In all cases, reinstalling the agent (Standard Install or GPO based) has the potential to fully restore the agents function.
- If data corruption problems persist, check your operating system and device hardware, and contact Genians Support.

## 22.2.6 502 Proxy Error

### Symptom

Information in the Web Console is not up to date, and the error message `ERRMSG='Error 502 fault: SOAP-ENV:Server [no subcode] "HTTP/1.1 502 Proxy Error"'` is present in the logs.

### Cause

- In large networks, the information takes time to be sent from the Sensor, to the Policy Server. This may exceed the default timeout values for connection and data transmission.

### Resolution

### Increase the timout values

1. Access the Policy Server by CLI
2. Check the timeout values using the **show configuration** command.
3. Enter Global configuration mode using the **conf t** command.
4. Increase the timeout values for connection and data transmission.
5. Wait for the new configuration to save.
6. Exit the command line.

```
genian> en

genian> show configuration
genian# conf t

genian(config)# management-server connection-timeout [value in seconds]
genian(config)# management-server data-timeout [value in seconds]
genian(config)# exit

Genians# exit
```

## 22.2.7 Switch is showing a macflap error

### Symptom

The switch you have installed a Genians Network Sensor to is reporting a mac flap involving the port that the sensor is connected to.

### Cause

The Network Sensor sends a spoofed Virtual MAC as part of its internal AP detection mechanism, which occasionally results in a mac flap.

For more info see: *Detecting Internal SSID*

### Resolution

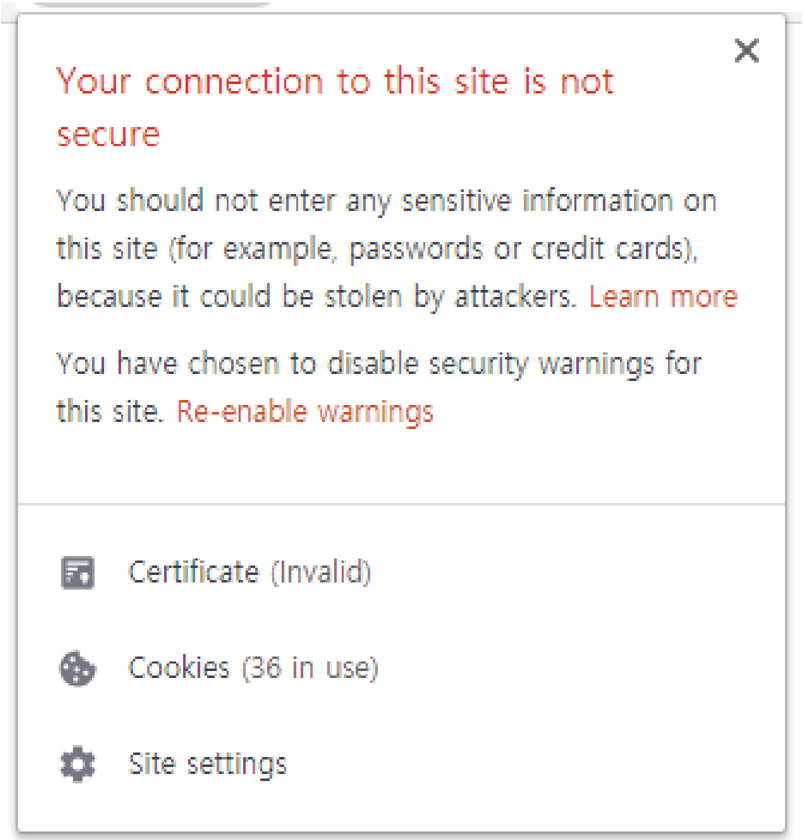
This feature can be disabled.

1. Log in with an Administrative account.
2. Go to **Preferences** in the top panel
3. Navigate to the **WLAN** section.
4. Under **Internal AP Detection** change **Virtual MAC** to **Off**
5. Click **Update**

## 22.2.8 How to solve SSL Certificate error

### Symptom

The SSL certificate error "Your connection to this site is not secure" occurs when a web browser can't verify the SSL certificate installed on a site



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

### Cause

- SSL certificates have a validity period. After this period has passed, browsers display a warning on the webpage, signifying that the SSL certificate expired (or invalid).

### Resolution

Uploading public certificate to resolve cert error

**If you have your own certificate:**

- Log in to the ZTNA Web Console
- Go to **Preferences > General > Certificate**
- Upload your own certificate
- Go to **System > Service > Control**
- Restart Web Console

**If you need certificate:**

- Log in to the ZTNA Web Console
- Go to **Preferences > General > Certificate > SSL Certificate**
- Enter Common Name, Country Code, Organization, Email to generate CSR
- Get certificate (.PEM) from Certificate Authority (such as VeriSign, Thawte, GeoTrust)

- Upload your new certificate
- Go to **System > Service > Control**
- Restart Web Console

**Note:** Please restart web service (httpd) after uploading certificate

## 22.3 Configuration

### 22.3.1 Node is not displayed in Web Console

#### Symptom

Case 1: None of the nodes except the Network Sensor are visible in the network subnet where the Network Sensor is installed.

Case 2: Only some nodes are visible while other active nodes are not detected.

#### Cause

Genian ZTNA can not scan nodes when the switch port configuration is mismatched with the Sensor interface settings.

Additionally, remote device/node discovery can be impacted when Radius Accounting, endpoint agent, or external API are not functioning properly.

#### Resolution

#### Switch

- Ensure that the port Genian ZTNA is on is properly configured to access the VLAN(s) you wish to monitor.
- Only Standard access ports (untagged) and 802.1Q Trunk (tagged) ports are supported by Genian ZTNA.

#### Network Sensor

- Check the interface settings by accessing the command line and using the command `show interface eth[#]`
- Be aware that interface eth0 can only function when attached to an access port or in the presence of a native VLAN on a trunk port.
- All tagged VLAN traffic can only be seen by a defined sub interface on that VLAN. For configuration, see: *Adding and Deleting Network Sensors*
- Try to ping resources on the subnet from the network sensor to ensure a communication path exists.

**If using a Virtualized Sensor**

- Ensure your hypervisor is properly configured to interface with the network and your switches. Hypervisors frequently require non-standard configurations to communicate across a LAN, or to accept traffic from a trunked interface.
- Refer to: /install/installing-genian-nac , under "**Prepare Network Connection**."

### Endpoint Agent

- Without the presence of a Sensor, the agent may be used to register nodes.

See:

- *Installing Windows Agent*
- *Installing macOS Agent*

### RADIUS

- Without the presence of a Sensor, RADIUS Access-Request packets may be used to register nodes.

See RADIUS Section:

- *Authentication using RADIUS (802.1x)*

### API

- Without the presence of a Sensor, REST API may be used to register nodes.

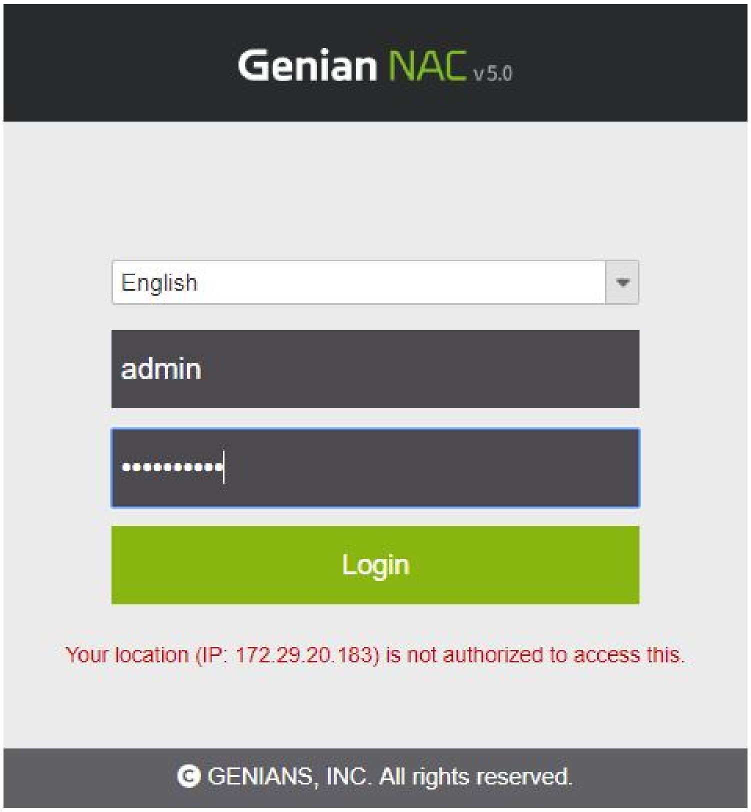
See:

- *API Guide*

## 22.3.2 Web Console login Failed

### Symptom

Authentication fails, and the message "Your location is not authorized to access this" is displayed.



Your location (IP: 172.29.20.183) is not authorized to access this.

### Cause

- The Policy Server controls access to Web Console with an Access list, which is specific to each administrative account.
- Access List is managed by a SuperAdmin account under "Web Console IP", under the administrator tab of each individual account.
- If the administrator's IP address is not in the "Web Console IP" list, the administrator can not access Web Console.

### Resolution

Verify that you have another account to login to Web Console with User Management modify permissions.

**Next:**

- Login to the WebConsole
- Navigate to Management > User > Click the User that you try login > Click the Administrator tab
- Confirm that the target IP is included in "Web Console IP1"
- Add IP address if IP address is not included. Hosts, subnets or 0.0.0.0/0 for all are accepted values.

If you do not have a login account for the Web Console:

- Follow the below steps, as shown in the code box.
- Login to Policy Server Console directly or through SSH.

- Enter Configuration mode.
- Allow your current IP access the the Policy Servers internal Data-Server.
- Set a password for the Data-Server.
- Enter shell mode.
- Authenticate to access the Mysql database.
- Update the allowed IP for the desired admin account.

```
genian> en

genian# conf t

genian(config)# data-server access-list [IP accessing console]
genian(config)# data-server password [Password]
genian(config)# exit
genian# @shell

Genians$ mysql -p[Password] -A ALDER
Genians$ update ADMIN set ADM_ALLOWIP1 = '0.0.0.0/0' where ADM_ID = 'admin'
Genians$ exit
```

### 22.3.3 SSH Login Failed

#### Symptom

SSH connection attempt fails with "Connection refused" message

#### Cause

- For security reasons, SSH connection is only allowed from designated IP addresses.
- If there is no IP address in the setting, the connection will not be established.

#### Resolution

#### Add Approved SSH Source IP

1. Go to System in the top panel.
2. Click the desired appliance's IP Address.
3. Click the Appliance tab.
4. Put into the IP Address in Approved SSH Source IP 1 or 2.
5. Click Update.
6. Check if SSH connection is available.

## 22.4 Operation

### 22.4.1 Lost Console Password

#### Symptom

The password for the Console has been lost.

#### Cause

Administrators can manage many solutions and neglect password management.

#### Resolution

**The Console password can be changed via the Web Console.**

1. Log in with an Administrative account.
2. Go to System in the top panel
3. Check the "checkBox" of the Policy Server IP Address.
4. Click the Tasks > Change CLI Password > Enter a new CLI Password to Reset Password.

### 22.4.2 A problem in which the node is assigned the wrong policy due to platform false positives

#### Symptom

Nodes that were defined as blocking exceptions due to node type conditions detected in the enforcement policy are assigned to a different policy and blocked.

#### Cause

The condition for the Node Group that corresponds with the Blocking Exceptions Enforcement Policy is based on Node-Type. If the detected platform of the node changes, it may no longer meet the conditions of the blosking exceptions Node Group and Enforcement Policy. The detected platform may chnage over time as more scans are conducted by the sensor, or the behavior of the node changes.

#### Resolution

Detected node types and node platforms may experience intermittent typos, or innaccurate detection. Therefore, the condition `detected is equal to` is not appropriate as a condition of exception handling policy.

If you want to use node-type conditions for defining blocking exceptions, you should use conditions such as `node type - Admin-Confirmed is equal to` and `node type - is - defined by Administrator`.

Method 1: To use exception group conditions as `node type - Admin-Confirmed is equal to` (recommended)

1. Go to **Web Console > Management > Status & Filter > Node Type** and select the node type to define the exception.

2. Select the upper left check box of the list screen to check the check box of all nodes in the list.
3. Select **Choose Task > Node and Device > Edit Node Fileds**.
4. `Admin-Confirmed Node Type` Item and `Admin-Confirmed Platform`` Check the item and click the bottom `modify` button.
5. Repeast the process with other node types if desired.
6. In the **Preferences > General > Node > Detection** topic, change the **Auto-Confirm Detected Platform** option to **On**.
7. Go to the **Enforcement Policy** menu and select the node group criteria for the exception handling policy **NodeType > Admin-Confirmed is equal to** condition to add the node type to define the exception.
8. If you have added all node types, click the 'Update' button and click the `Apply` button at the top of the screen to apply the policy.

> **Attention:** Verified node types and platforms are field values that mean information verified by the administrator **Status & Filter > Change Management** If the administrator does not check and change them directly in the **Node Details** screen, the administrator does not change them. The first detected platform and node type are maintained information due to setting number 6.
>
> Information that detects a node's platform and type differently than before can be monitored in the **Management > Status & Filter >Change Management** menu and the Dashboard widget **Detected / Admin-Confirmed Conflict**.

Method2: To use an exception group condition as the `node type - is - defined by Administrator`

1. Go to **Web Console > Management > Status & Filter > Node Type** and select the node type to define the exception.
2. Select the upper left check box of the list screen to check the check box of all nodes in the list.
3. Select **Choose Task > Node and Device > Edit Node Fileds**.
4. Check the `New Node Type` item, select the node type to be assigned, and click the `Save` button at the bottom.
5. Repeast the process with other node types if desired.
6. Go to the **Enforcement Policy** menu, add the node group conditions of the exception handling policy **node type > is > defined by Administrator** conditions, click the `Update` button, and click the `Apply` Policy button at the top of the screen to apply the policy.

> **Attention:** If the group condition is defined as node type - is - `defined by Administrator`, any node type that is defined by an administrator will be added to the group, regardless of the node type.
>
> In case of manually specifying node type, the node type will not be updated due to scanning, so it is possible to set up a policy with the `detected is equal to`, which will group nodes based on their originally detected type/platform.
>
> The newly registered nodes must also be monitored to specify the node type to avoid accidentally blocking nodes that you intend to exempt from blocking.

Method 3: Use exception node group criteria as existing type/platform and disable scanning for the node(s)

1. Go to **Web Console > Management > Status & Filter > Node Type** and select the node type to define the exception.

2. Select the upper left check box of the list screen to check the check box of all nodes in the list.
3. Select **Task > Node and Device > Edit Node Options**.
4. Check the **Node Platform / Open Port Scan** item, select the **Off** option, and click the `Save` button at the bottom.

> **Attention:** If you set node scanning scan OFF, scanning to that node is not performed. This does not result in node detection information renewal, which does not cause node type changes.
>
> You must continue to perform these settings on newly added nodes that you wish to block.

### 22.4.3 Wireless LAN User Devices Are Detecting as Wrong Platform

#### Symptom

Apple Mobile, MAC Book, Android Phone, Windows PC and other wireless endpoint devices are detected on other platforms

#### Cause

Conditions:

1. A device using a wireless LAN
2. When using wireless LAN, use a RANDOM MAC address rather than the MAC address of the device
3. If the OUI of the RANDOM MAC address is from another manufacturer

If platform detection is performed by connecting to the network under the above conditions, false positives may occur on other platforms that are not expected.

#### Resolution

- Disables the RANDOM MAC function to connect the network with the MAC on the device.

**Method 1: Disable RANDOM MAC function on Apple Mobile device (iOS & iPadOS)**

1. **Open Settings App**.
2. Go to **Wi-Fi**.
3. Select the **(i) icon** next to the currently connected network.
4. **Disable the Private Wi-Fi Address** option **OFF**.
5. Reconnect because the network disconnects and reconnects.

**Method 2: Disable RANDOM MAC function on Android mobile device**

1. **Settings** Open the app.
2. **Go to Network and Internet (Wi-Fi)**.
3. Select **Wi-Fi**, and then press and hold the **Network currently connected or click (Settings icon)**.
4. **Looks for the Advanced**Ehms**Personal MAC Enable** option.
5. Select **MAC Address Type** or **Random MAC**.

6. **Change to Device MAC (Device MAC)** option.

> **Attention:** For some manufacturers (Samsung, Xiaomi, OnePlus, etc.), menus may be available in the form of **Security and Privacy > Wi-Fi MAC Address**

**Method 3: Disable RANDOM MAC Features on Windows PCs**

1. **[Win + i]** Press the key to open **Settings**.
2. **Go to Network & Internet**.
3. Select **Wi-Fi** and click **Mange known networks**.
4. **Select your Wi-Fi network** and click **Properties**.
5. **Random hardware addresses** Set the option to **OFF**.
6. Reconnect your Wi-Fi to apply the changes.

> **Note:**
>
> Local Group Policy Editor (Windows Pro & Enterprise)
>
> 1. Run gpedit.msc
> 2. Computer Configuration → Administrative Templates → Network → WLAN Services → WLAN Settings
> 3. **Sets random hardware address acceptance option to Disabled**
>
> Registry Editor with Windows Home
>
> 1. Run regedit
> 2. HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlClass{4d36e972-e325-11ce-bfc1-08002be10318}
> 3. **Change key values related to random MAC functions** (Different manufacturers)

**Method 4: Disabling RANDOM MAC Function in macOS**

1. **Go to Apple Menu** > **System Settings**.
2. **Choose Network > Wi-Fi**.
3. **Click the (?) button** next to the network you are currently connected to.
4. **Disables the use of private MAC addresses** option for Wi-Fi networks.
5. Reconnect your Wi-Fi to apply the changes.

> **Attention:** Additional Notes
>
> Random MAC features are set individually for each SSID, so you must turn them off on all wireless networks in use.
>
> In some enterprise environments, mobile device management (MDM) solutions can also be used to force off the feature.
>
> In Windows and macOS environments, you can disable random MAC features through registry and group policy settings.

### 22.4.4 Cisco Switch-port Information Is Not Showing

#### Symptom

Switches are visible but but the switch ports are not visible in node management, node info or the switch management views.

#### Cause

If using SNMPv3 , some IOS versions may require you to configure the snmp-server group to view all contexts you wish to monitor.

#### Resolution

In this example, the SNMP group used to gain switch visibility is not authorized to view the VLANs assigned to the switch ports. To gain visibility of the switch ports, the group must be given privilege for the contexts. (VLANs)

#### View Contexts

```
switch>en
switch#>conf t
switch(Config)>show snmp context
vlan-1
vlan-2
vlan-3
```

#### Enable Access

```
switch>en
switch#>conf t
switch(Config)>snmp-server [groupname] v3 priv context vlan-1
switch(Config)>snmp-server [groupname] v3 priv context vlan-2
switch(Config)>snmp-server [groupname] v3 priv context vlan-3
```

### 22.4.5 Blocked Nodes are not redirected to CWP page

With all systems utilizing Captive Portal technology, there are some inherent issues that are present due to the underlying protocols and functionality associated with a Captive Portal environment. This document will discuss the most common issues and available workarounds.

### Symptom 1

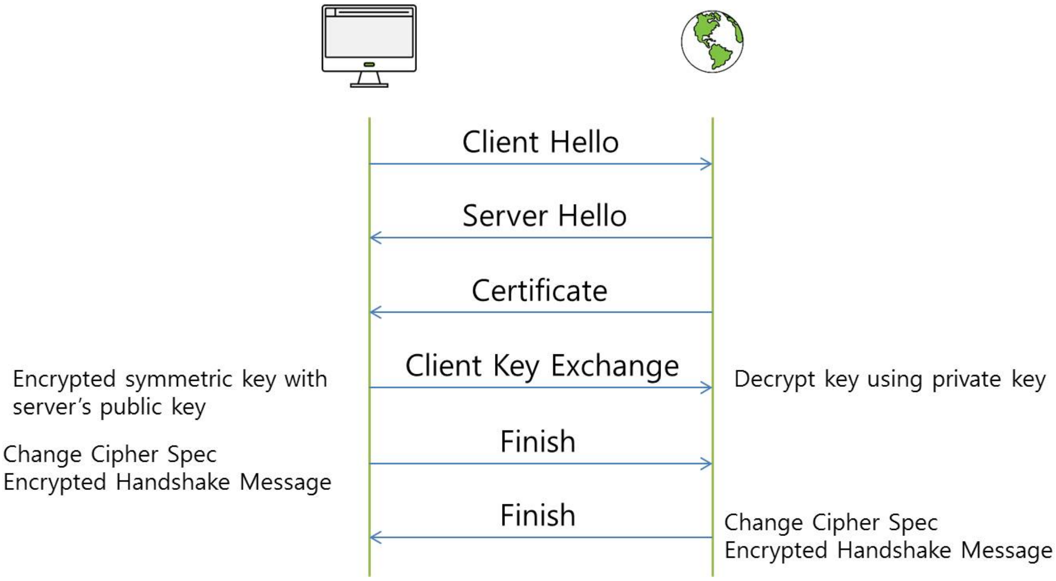
**Certificate Warnings**

The first issue is certificate warning messages being displayed to the end user upon a Captive Portal redirect. Language may vary but typically a message similar to "Your connection is not private" may be displayed to the end user as a warning. This issue is well known in Captive Portal environments and is the expected behavior.

### Cause 1

The cause of this issue is the technology that is used during a Captive Portal redirect for an HTTPS website.

The diagram below depicts the flow when a host accesses an HTTPS website when no Captive Portal is present:

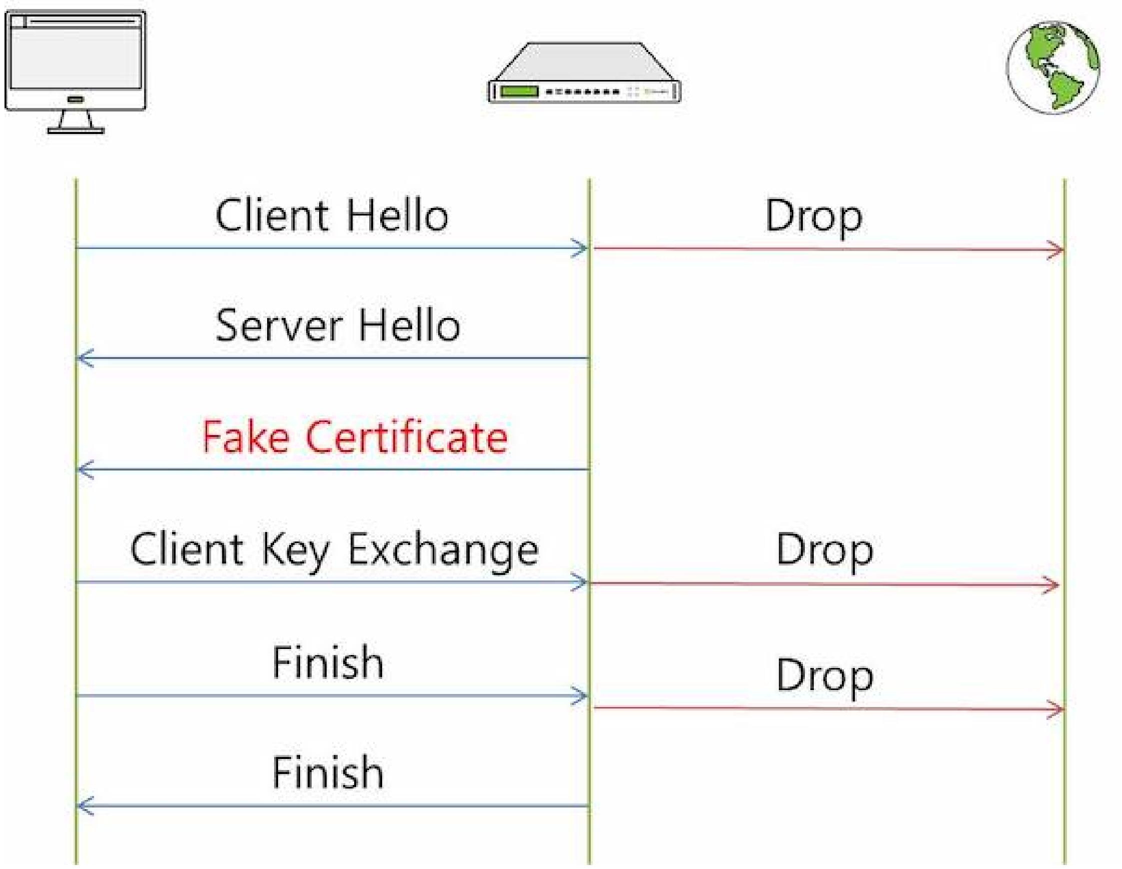

Client Hello
Server Hello
Certificate
Encrypted symmetric key with server's public key
Client Key Exchange
Decrypt key using private key
Change Cipher Spec
Encrypted Handshake Message
Finish
Finish
Change Cipher Spec
Encrypted Handshake Message

HTTPS communication requires intercommunication between the Web Server and the PC for encrypted communication before creating a cryptographic session.

1. Client hello: PC notifies Web Server of HTTPS communication request
2. Server Hello, Certificate: The server passes the certificate to the client, the client determines that the certificate is a trusted certificate
3. Client Key Exchange: The client sends the pre-master-secret key to the Web Server, Symmetric key sharing
4. Finish: After the end of the negotiation process, communication is exchanged by a symmetric key exchange

After that, encrypted communication is established between the PC and Web Server using the encrypted channel.

For comparison, the diagram below depicts the flow when a host accesses an HTTPS website when a Captive Portal is present:



The important point here is that the server certificate is transmitted to the CA certificate (FAKE Certificate) of the Captive Portal system so that the encrypted communication is not connected to the original target Web Server, but instead the session is established with the Captive Portal Web Server.

### Resolution 1

For the reasons listed above, end users must acknowledge the certificate warning, typically by clicking “Continue” before being redirected to the Captive Portal page.

Most modern operating systems now have built-in Captive Portal detection capability. Windows 10 Captive Portal Detection, Apple Captive Network Assistant and Android Connectivity Manager are all examples of this feature. These features function by sending out HTTP requests to various URLs pre-defined at the OS level to determine if the device is behind a Captive Portal. If no response is received, it is assumed the device is behind a Captive Portal. At that point, the operating system will automatically invoke an HTTP request using the default browser. Because the request is HTTP and not HTTPS, Captive Portal redirection occurs without any issues.

Captive Portal detection in general is not a perfect science, however, ensuring all packets are blocked the moment a device connects results in a higher probability of Captive Portal detection functioning properly, thereby bypassing the issue of certificate warnings. Genian ZTNA is constantly improving features and a new feature is being implemented which should ensure that the majority of the time endpoint device Captive Portal detection is triggered. This document will be updated with additional information when the feature is available.

### Symptom 2

**HSTS Websites – Browser Does Not Allow Redirect**

What is HSTS? At a high level HSTS (HTTP Strict Transport Security) is a policy that, when enabled, forces a browser to use an HTTPS connection over a HTTP and allows for the SSL certificate to be cached on the browser for a predetermined length of time. With HSTS enabled, clients are protected from protocol downgrading, man in the middle attacks (which is what a Captive Portal redirection is) and cookie hijacking.

### Cause 2

Most modern browsers (Google Chrome, Mozilla Firefox, Microsoft Edge) come preloaded with a list of sites supporting STS (Strict Transport Security). Once enabled a timeout will be sent with the HTTPS header that contains a HSTS TTL "Strict-Transport-Security: max-age=31536000" (one year). The certificate received from the site will be honored until the timeout expires. Future attempts to access the site will reference the certificate and, if the certificate does not match, the browser will not allow the connection to site to be established. For users behind a Captive Portal, this is where they reach a dead end because accepting a certificate warning will not allow them to proceed.

### Resolution 2

For users visiting an HSTS website behind a Captive Portal the only option is to browse to a non-HSTS website. Therefore, when enabling a Captive Portal for the first time in a new environment, it is key to communicate to end users to visit a particular website (perhaps the organization's website as long as it is not HSTS) if they are unable to access the other websites. This will allow users to be redirected to a captive portal properly. Some organizations even setup a specific page for this purpose (onboard.company.com, register.company.com, etc) and notify users in advance.

### Symptom 3

**CWP redirection fails in environments using Proxy Server**

### Cause 3

Captive portals may not be able to provide proper redirection if internal hosts on the network are configured to use a proxy server.

### Resolution 3

By making the proper proxy exceptions on your proxy server, this will ensure captive portal redirection functions properly.

See: *Configuring Captive Web Portal* for info on creating proxy server exceptions.

### 22.4.6 Changing Sensor Operation Without Web Console Access

**Note:** This applies to on-premise systems only.

#### Symptom

You are unable to access the Web Console, but need to de-activate Network Sensors in your environment.

#### Cause

There are many reasons this may occur, for example:

- Blockage of HTTPS traffic by Genians or another security system
- Failure of the Web Console to properly load

#### Resolution

#### Control Sensors through the Policy Server CLI

- Use SSH on the Policy Sever as shown below, and access the shell:

```
genian> en

genian# @shell

Genians$
```

- To STOP sensors, use command `centerd -dfS [Sensor]`
- To stop one sensor, use the command referencing a single sensor IP: `centerd -dfS 10.10.10.100`
- To stop multiple sensors, use the command referencing a multiple sensor IPs(up to 32) separated by comma: `centerd -dfS 10.10.10.100,10.10.20.100`
- To stop all sensors, use the command referencing all sensors: `centerd -dfS all`
- To START sensors, use command `centerd -dfR [Sensor]`
- To start one sensor, use the command referencing a single sensor IP: `centerd -dfR 10.10.10.100`
- To start multiple sensors, use the command referencing a multiple sensor IPs(up to 32) separated by comma: `centerd -dfR 10.10.10.100,10.10.20.100`
- To start all sensors, use the command referencing all sensors: `centerd -dfR all`

#### Check Sensors Status through the Policy Server CLI

- Type `exit` to exit the shell mode and re-authenticate.
- To show sensors, use command `show sensor [option]`
- Use the available options to filter results by sensor status: `all`, `active`, `passive`, `unknown`

### 22.4.7 ARP Enforcement does not block network access

#### Symptom

A node which should be blocked from network access by an Enforcement Policy still has network access even though the Enforcement Policy is enabled and the associated Sensor is set to Enforcement Mode, and the local config on the sensor shows that the node is being blocked.

#### Cause

- Some IDS/IPS or EDR solutions may detect and block the ARP Enforcement action of the sensor, because it is incorrectly identified as a network attack.

#### Resolution

#### Add Exceptions for Genian ZTNA in conflicting Security Products

To resolve the issue, make an exception for the Sensor IP(s). Depending on the configuration of your enforcement policies, and your other network security solutions, additional exceptions may be required.

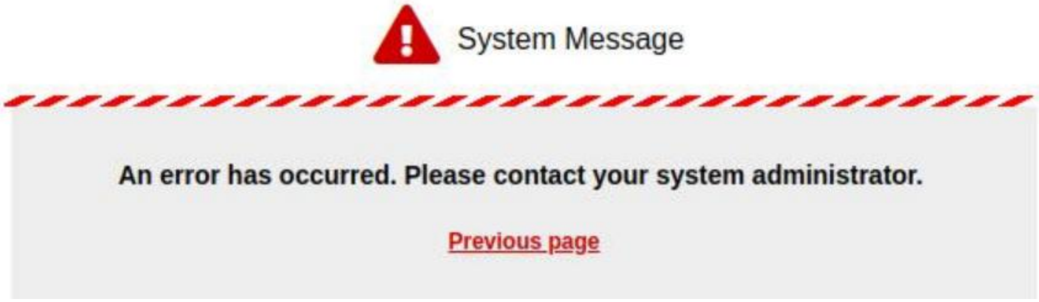
Example exception: ESET Endpoint Security

## 22.5 System

### 22.5.1 Web Console Error Page

#### Symptom

Error page appears when clicking specific menu in WebConsole:



System Message

An error has occurred. Please contact your system administrator.

#### Cause

This can happen if there is an error in the Java process that supports the link between the Web APP and the Policy Server Database.

#### Resolution

- Follow the below steps, as shown in the code box:
- Log in to the Policy Server console directly or by SSH.
- Enter Configuration mode.
- Enter shell mode.
- Use the `tail -f` command to display the most recent contents of the error log file in real time.
- Attempt to reproduce the error message by performing the action that created the error in the Web Console.
- Check for error logs to appear in the console. Document and share with Genians engineers.

```
genian> en

genian# @shell

Genians$ tail -f /disk/data/logs/tomcat/catalina.out
```

### 22.5.2 Compliant Node is Blocked

#### Symptom

In Enforcement Policy, the node is assigned Perm-all authority, but its network communication is blocked. In the Web Console, the policy appears correctly applied to the node, but the policy is not actually applied.

#### Cause

When a policy assigned to a node changes, the Policy Server instructs the Network Sensor to change the policy status of the node. In some cases the Network Sensor may not receive or act upon this input.

#### Resolution

#### Check Connectivity

- Verify communication path between Policy Server and Network Sensor on port 443. Ensure necessary exceptions on firewalls or other appliances.
- Through SSH on the Policy Server and Network Sensor, inspect traffic using the command: `tcpdump -i eth0 host [Policy server or network sensor IP]` (If accessing Policy Server console, use Network Sensor IP for tcpdump host IP , and vice-versa)

### Checking Network Sensor Policy

You can view which Enforcement Policy the network sensor is applying to a node through the Command Line Interface.

- Enter the terminal for the Network Sensor and use the command `show nodeinfo filter [Node IP Address]`
- Check if "noderole" is properly assigned to the node.

### Check Policy Server and Network Sensor Logs

The Policy Server houses its internal logs in a file called **centerd**, while the Network Sensor uses a file called **sensord**. These files can be monitored to see if the node role have seen changed.

- Follow the below steps, as shown in the code box.
- Log in to the Policy Server or Network sensor console directly or by SSH.
- Enter Configuration mode.
- Enter shell mode.
- Use the `tail -f` command to display the most recent contents of the error log file in real time.
- Attempt to make a policy change to a node through the Web Console.
- Check for error logs to appear in the console.

```
genian> en

genian# @shell
```

**On the Policy Server:**

```
Genians$ tail -f /disk/data/logs/centerd
```

Example node role logs from centerd:

```
Jul 17 16:06:26 Genians centerd[5788]: DBG|rolemgr.cpp|1720| 8015| Role Assign␣
↪Node=10.10.10.245 MAC=08:00:27:28:C9:1E NLVALID=1 StartBy=Changing IPAM Policy␣
↪QuickCheck=1491340468 Join=0

Jul 17 16:06:26 Genians centerd[5788]: DBG|rolemgr.cpp|1500| 8015| Role Assign Node.␣
↪ADDR=10.10.10.245 MAC=08:00:27:28:C9:1E NLVALID=1 StartBy=IPAM compliance status␣
↪changed.
```

**On the Network Sensor:**

```
Genians$ tail -f /disk/data/logs/sensord
```

Example node role logs from sensord:

```
Jul 17 16:15:22 Genians sensord[6340]: DBG|eventframe.|1067| 8068| RECV Event NOTIFY ␣
↪    SRC=10.10.10.4 DST=10.10.10.4 SEQ=6406 ID=NODEROLECHANGED(19) FLAGS=0 KERN=0

Jul 17 16:15:22 Genians sensord[6340]: DBG|eventframe.|1067|17655| SEND Event NOTIFY␣
↪ACK SRC=127.0.0.1 DST=10.10.10.4 SEQ=6406 ID=NODEROLECHANGED(19) FLAGS=1 KERN=1
```

### 22.5.3 Wrong Link State Displayed for Node

#### Symptom

The link status showing in the Web Console is incorrect.

#### Cause

- The Network sensor routinely confirms nodes link status. If many nodes are being managed by a sensor, there may be a delay time before the nodes link state is updated.
- This process can be impacted if the if there is a breakdown in communication between the Node and the Network Sensor, or the Policy Server and the Network Sensor.

#### Resolution

#### Check Communication from the Sensor to the Node

- Follow the below steps, as shown in the code box.
- Log in to the Policy Server console directly or by SSH.
- Enter Configuration mode.
- Enter shell mode.
- Use the `arping -I` command to initiate a mac address request for that nodes IP, sent from the defined interface. this will serve to test communications from the Sensor to the Node.
- Check for errors appear in the console. Document and share with Genians engineers.

```
genian> en

genian# @shell

Genians$ arping -I [interface number] [IP Address]
```

Example Syntax: `arping -I eth0.10 192.168.10.10`

#### Gather System Logs

- There may be a problem with communications from the Policy Server to the Sensor.
- Use the Syscollect function on the Policy Server to send info to Genians engineers.

See: *Genian ZTNA log collection method*

### 22.5.4 Recovering from database crashes

Every Genian ZTNA's system configures, policies, collection stored on database. If a database problem occurs by H/W or S/W error, you can recover database by using backup file.

#### Symptom

Web Console login failure, policy assignment and policy renewal failure, setting lookup failure, etc.

#### Cause

Crashes occur in databases due to various problems. H/W problems Internal database engine problems, setup problems, etc.

#### Resolution

Recover the database using the database information in the backup file.

```
Step 1 If the backup file is inside the equipment you want to restore, navigate to Step3.

genian> en
genian# @shell
!!! WARNNING !!! - SHELL PROMPT IS JUST FOR MAINTENANCE.
!!! WARNNING !!! - USE AT YOUR OWN RISK.
Genians$ cd /disk/data/DBBACKUP
Genians$ rz [Backup File]
Genians$ ls
drwxr-xr-x    2 root     root          4096 May 11 09:43 ./
drwxr-xr-x   36 root     root          4096 Apr 21 13:50 ../
-rw-r--r--    1 root     root     193863371 May 11 09:43 ALDER-93180-20210511-094236.tar.gz

Step 2 Connect to the gnlogin CLI.

genian$ gnlogin

Step 3 Verify the backup files at the time you restore them.

genian# show backup

Backup lists
---------------------------------
ALDER-93180-20210511-094236

Step 4 Restore the database (select Database Only under Options).

genian# do restore [Backup File Name]
Are you sure to restore configuration files (y/N): n
Are you sure to restore agent files (y/N): n
Are you sure to restore custom files (y/N): n
Are you sure to restore database (y/N): y
Do you want to start service after restore? (Y/n): y
```

(continues on next page)

(continued from previous page)

```
Step 5 If the system is restarted and the database restore is successful, all systems␣
↪will function normally.
```

## 22.5.5 Upgrade button is not displayed

### Symptom

ZTNA provides an upgrade button in the web console. (**System > Genian Software**) but the upgrade button may not be displayed for several reasons.

### Cause

- Your Server is already running the latest released version.
- Your current software version is Beta (5.0.XX-B)

### Resolution

- You can download the software when the next version is released
- You have to manually upload Release (5.0.XX-R) image once and click the manual upgrade button. (**System > Tasks > Update Specific System Image**)

## 22.5.6 Check and change the various network ports in use on the system

### Symptom

Genian ZTNA system service is not running normally.

### Cause

Problems can arise if normal communication for service execution fails.

### Resolution

#### Check the network port used by the system

You can check the port information for each service used by the Genian ZTNA system.

You can check whether communication between each configuration is performed normally by referring to the information during deployment.

1. Go to **System** on the top panel.
2. Select **Port** from the **Service** item on the left.

| Item | Explanation | Remarks |
|---|---|---|
| HTTP | The ports used by the CWP and IP Request systems are displayed. | Changeable |
| HTTPS | Ports used by CWP, IP Reuest system, policy reception, and node information update are displayed. | Changeable |
| HTTPS | The port used for WebUI access is displayed. | Changeable |
| KeepAlive | The port used for event transmission/reception and Sensor/agent operation status check is displayed. | Unchangeable |
| Syslog | The port used for the syslog listening service is displayed. | Unchangeable |
| Radius Authentication | The port used for Radius user authentication is displayed. | Changeable |
| Radius Accounting | The port used for Radius Accounting listening is displayed. | Changeable |
| Distribution Server | The port used by operating system update search and download, and agent file distribution is displayed. | Unchangeable |
| Data Server | The port used for the Database service is displayed. | Changeable |
| Log Server | The port used for log search and cluster service is displayed. | Changeable |
| SSH | The port used for the product remote CLI access service is displayed. | Changeable |

### Changing the network port used by the system

If using a known port is determined to be a problem, use that function to change the port.

### Changing HTTP service port

In Genian ZTNA system, services provided through HTTP protocol include Captive Web Portal (CWP) and IP Request system, and services are provided through known port 80.

The HTTP port in use can be changed through the following process.

**Note:** HTTP services are provided only by the Policy Server.

### Changing the Policy Server Port

1. Connect to the policy server in CLI mode using SSH. (Refer to *CLI Console* for SSH connection method.)
2. Enable to Globe configuration Mode.

```
genian> enable
genian# configure terminal
```

3. Change the port using the *management-server http-port* command.

```
genian(config)# management-server http-port 20000
```

### Changing HTTPS service port

**Services provided through HTTPS protocol in Genian ZTNA system include Captive Web Portal (CWP), IP Request system, policy reception, and node information update.**

The service is provided over the known port 443, and you can change the port through the following process.

**Note:** HTTPS port is applied to policy server, network sensor, and agent by using policy reception and node information update function.

### Changing the Policy Server Port (HTTPS)

1. Connect to the policy server in CLI mode using SSH. (Refer to *CLI Console* for SSH connection method.)
2. Enable to Globe configuration Mode.

```
genian> enable
genian# configure terminal
```

3. Change the port using the `management-server https-port` command.

```
genian(config)# management-server https-port 22000
```

### Changing the network sensor port (HTTPS)

1. Connect to the network sensor in CLI Mode using SSH. (Refer to *CLI Console* for SSH connection method.)
2. Enable to Globe configuration Mode.

```
genian> enable
genian# configure terminal
```

3. Use the `node-server port` command to change to the same port as the policy server.

```
genian(config)# node-server port 22000
```

### Changing the web console connection port

The Genian ZTNA system supports the administrator's Web UI access through a custom HTTPS port. The service is provided over port 8443 and you can change the port with the following process.

### Changing the Policy Server Port (WebUI)

1. Connect to the policy server in CLI mode using SSH. (Refer to *CLI Console* for SSH connection method.)
2. Enable to Globe configuration Mode.

```
genian> enable
genian# configure terminal
```

3. Change the port using the `management-server mgmt-port` command.

```
genian(config)# management-server mgmt-port 28443
```

### Changing the Radius Authentication Service Port

When using a Genian ZTNA device as a Radius Authentication Server, you can change the port. The service is provided through the known port 1812, and you can change the port with the following process.

1. Go to **Preferences** in the top panel.
2. Select **RADIUS Server** from the **Service** item on the left.
3. Enter **Authentication Port** in the **Authentication Server** settings.
4. Click the **Update** button.

### Changing the Radius Accounting service port

When using the Radius Accounting service on a Genian ZTNA device, you can change the port. The service is provided through the known port 1813 and you can change the port with the following process.

1. Go to **Preferences** in the top panel.
2. Select **RADIUS Server** from the **Service** item on the left.
3. Enter **Accounting Port** in the **Accounting Server** settings.
4. Click the **Update** button.

### Changing the Data Server service port

When using database service on Genian ZTNA device, you can change the service port. The service is provided through the known port 3306 and you can change the port by the following process.

**Note:** Separate work is required for individual database configuration and replication configuration.

1. Connect to the policy server in CLI mode using SSH. (Refer to *CLI Console* for SSH connection method.)
2. Enable to Globe configuration Mode.

```
genian> enable
genian# configure terminal
```

3. Change the port using the *data-server port* command.

```
genian(config)# data-server port 23306
```

### Changing the LOG Server service port

When using Log Server for Genian ZTNA device, you can change the log search port and port for cluster configuration. The service is provided through known ports 9200 (log search) and 9300 (cluster), and the port can be changed through the following process.

**Note:** Separate settings are required for Log Server individual configuration and cluster configuration.

#### Changing the Log Server Port (Log Search)

1. Connect to the policy server in CLI mode using SSH. (Refer to *CLI Console* for SSH connection method.)
2. Enable to Globe configuration Mode.

```
genian> enable
genian# configure terminal
```

3. Change the port using the `log-server http-port` command.

```
genian(config)# log-server http-port 29200
```

#### Changing Log Server Port (Cluster)

1. Connect to the policy server in CLI mode using SSH. (Refer to *CLI Console* for SSH connection method.)
2. Enable to Globe configuration Mode.

```
genian> enable
genian# configure terminal
```

3. Change the port using the `log-server tcp-port` command.

```
genian(config)# log-server tcp-port 29300
```

### Changing the SSH service port

You can change the port for SSH remote access to the Genian ZTNA device. The service is provided through the port 22 used, and the port can be changed through the following process.

1. Connect to the policy server in CLI mode using SSH. (Refer to *CLI Console* for SSH connection method.)
2. Enable to Globe configuration Mode.

```
genian> enable
genian# configure terminal
```

3. Change the port using the *ssh port* command.

```
genian(config)# ssh port 23910
```

# 22.6 Interworking

## 22.6.1 Windows Update Failure

### Symptom

Windows does not update on node.

### Cause

- Genian ZTNA can control the windows update process in the following ways:
- Which Updates will be required.
- Update Scheduling.
- Defining which location that the Windows checks for available updates (Genian ZTNA, Genian Proxy, or Microsoft Servers).
- Where the Windows downloads the updates from (Genian ZTNA, or Microsoft Servers).
- This level of customization introduces many different points of failure.

### Resolution

### Check the Windows Update Logs

The exact nature of an update failure can be determined through the log files.

For more Information, See:

- https://docs.microsoft.com/en-us/windows/deployment/update/windows-update-logs
- https://docs.microsoft.com/en-us/windows/deployment/update/windows-update-errors

## 22.6.2 LDAP Search Failed - Operations Error

### Symptom

LDAP authentication integrations or synchronization fails.

### Cause

LDAP errors can have many causes.

### Resolution

Checking the error messages to determine the cause of the failure.

- Refer to: https://ldap.com/ldap-result-code-reference/

## 22.6.3 "Secret key mismatched" error occurs testing external RADIUS integration

### Symptom

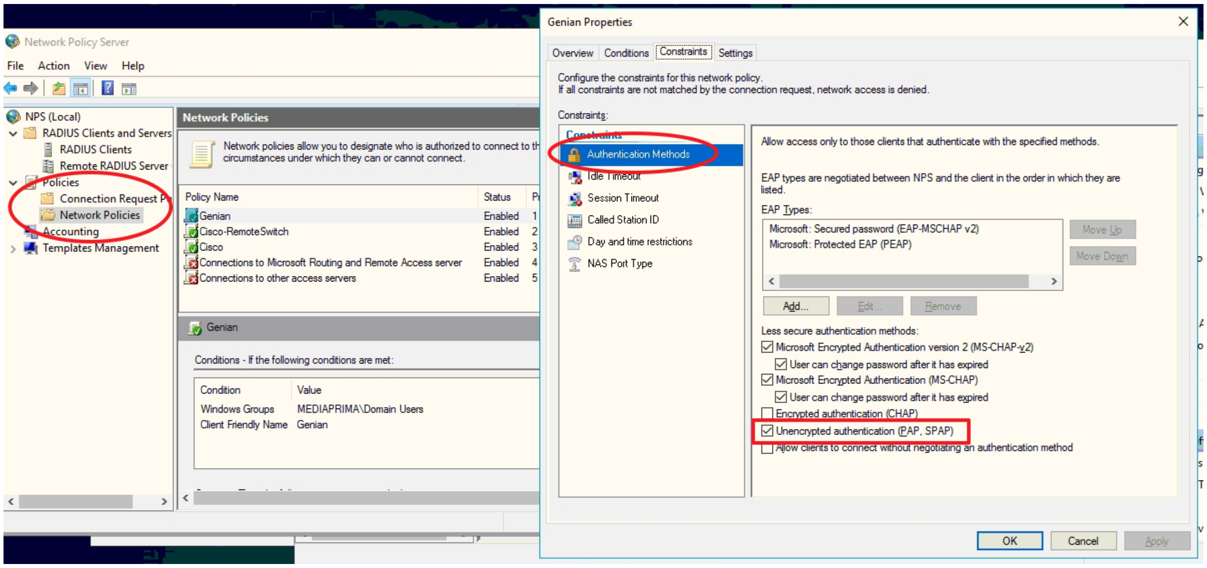
`secret key mismatched` error occurs when testing an integration of Genian ZTNA with an external RADIUS (Windows) server, using the built in test feature in the Web Console.

### Cause

If the Genian ZTNA Policy Server requests authentication with an unencrypted(PAP) method, but the RADIUS server does not allow non-encrypted authentication requests, the authentication is rejected and the authentication test window displays this error message.

### Resolution

Enable the RADIUS server to accept unencrypted authentication requests



Network policies allow you to designate who is authorized to connect to th circumstances under which they can or cannot connect.

| Policy Name | Status | P |
|---|---|---|
| Genian | Enabled | 1 |
| Cisco-RemoteSwitch | Enabled | 2 |
| Cisco | Enabled | 3 |
| Connections to Microsoft Routing and Remote Access server | Enabled | 4 |
| Connections to other access servers | Enabled | 5 |

Conditions - If the following conditions are met:

| Condition | Value |
|---|---|
| Windows Groups | MEDIAPRIMA\Domain Users |
| Client Friendly Name | Genian |

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Secured password (EAP-MSCHAP v2)
Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  ☑ User can change password after it has expired
☑ Microsoft Encrypted Authentication (MS-CHAP)
  ☑ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☑ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method

CHAPTER

TWENTYTHREE

# RELEASE NOTES

## 23.1 What's New in Genian ZTNA

### 23.1.1 New UI Themes

- Improved unity of UI Components, Controls, and Elements
- Brighter and flatter UI by increasing UI color brightness

### 23.1.2 Improved UX

- Node management/switch management detailed screen in one screen
- Added Node Management Grid View
- Information synchronization UX improvement
- Node group setting UX improvement
- Dashboard UX Improvements
- Security consent page support in CWP design template

### 23.1.3 Cloud infrastructure support

- Policy server operation in the cloud
- Added Collector to collect information of cloud resources
- Added CLI-based cloud control function in control policy
- Added cloud security policy management function

### 23.1.4 Remote work infrastructure Support

- Added ZTNA Gateway/Client function using SSL-VPN
- Added FIDO (Biometric) authentication for MFA
- Always on ZTNA function to always use only ZTNA connection

### 23.1.5 Zero Trust Security policy support

- Permission policy added for intuitive role-specific permission assignment during micro segmentation
- Improved to use dynamic node group for the destination network of permission object
- Provides ZTNA Gateway for cloud-based security gateway configuration
- Provides IPSec tunneling that securely connects ZTNA Gateway and head office/branch offices

### 23.1.6 Traffic/Application Visibility and Control

- Netflow collection and application identification for packets passing through ZTNA
- Control at the application level when granting permission through control policy
- Provides Secure Web Gateway (Proxy) for URL-based application control

### 23.1.7 IP Mobility Support

- Standard VxLAN-based IP Mobility support via network sensor
- Private IP static via Always on ZTNA (using same IP at work/home)

### 23.1.8 Enhanced user authentication

- Passkeys (FIDO2) authentication for administrator, Captive Web Portal and ZTNA Client
- Google Authenticator, Passkey Support for Captive Web Portal
- Hardware security chip TPM EK-based device authentication

## 23.2 LTS Roadmap

| LTS Version | StartDate | EndDate | Status |
|---|---|---|---|
| 6.0.35 | 2025.08 | 2027.08 | Available |
| 6.0.26 | 2024.09 | 2026.07 | Available |
| 6.0.16 | 2023.07 | 2024.07 | Not Available |

## 23.3 Current Versions

### 23.3.1 Genian ZTNA 6.0.42 (R) Release Notes (2026-01-05)

Last Updated: 2026-01-05

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 144111 | GN-31038 | WebUI | Added an automatic log file cleaning function for gnmicro services | |
| 144111 | GN-31026 | Windows Agent | Improved to enable macros in agent notification messages | |
| 144111 | GN-31001 | WebUI | Fixed an issue where network objects were displayed in Korean in the Models section of Swagger UI | |
| 144111 | GN-30994 | WebUI | Improved so that you can search by monitor model name or serial number in the search bar of node management | |
| 144111 | GN-30978 | WebUI | Improved so that additional parameters can be set if OIDC authentication is required | |
| 144111 | GN-30936 | Windows Agent | Improved the Penta SSO plug-in to check the normal authentication status of other repositories when there are multiple token stores | 5.0.51, 4.0.153, 6.0.11 |
| 144111 | GN-30935 | WebUI | Improved so that the number of MACs actually managed is displayed in the MACS information on the switch management screen | 5.0.0, 6.0.0 |
| 144111 | GN-30929 | WebUI | Added help on basic settings during information synchronization settings | |
| 144111 | GN-30910 | Center | Improved so that the Mac agent can recognize the port by adding a port to the IP information when the multi-center HAVIP automatic transmission option is set | 5.0.0, 6.0.0 |
| 144111 | GN-30901 | WebUI | Improved so that an audit log is recorded when the administrator performs a command on a node | |
| 144111 | GN-30899 | Windows Agent | Improved so that CPU information is collected normally on Surface Laptop 7th PC | |
| 144111 | GN-30890 | Center, CLI/gnlogin, Sensor | Secure Coding Check (CodeRay-XG) Source Vulnerability Remediation NAC Engine | |
| 144111 | GN-30883 | WebUI | Improved usability of the risk score management screen | |
| 144111 | GN-30797 | WebUI | nCloud collects NHN security vulnerability information and adds node grouping conditions | |
| 144111 | GN-30772 | Sensor | Added an option to allow settings related to TFTP SERVER and Bootfile in the bootp field of DHCP options | |
| 144111 | GN-30751 | WebUI | Azure collects K8S security vulnerability information and adds node grouping conditions | |
| 144111 | GN-29935 | WebUI | Improved completion notification method after adding ZTNA Gateway | |
| 144111 | GN-29574 | SDP | [SDP] Audit log Syslog TLS transmission function added | |
| 144111 | GN-29553 | macOS Agent | Added logic for enforcing macOS local network permissions | |

## Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 144111 | GN-31053 | WebUI | An issue where reserved IPs are included in the reallocatable list in the unused IP query REST API | 6.0.4, 5.0.48 |
| 144111 | GN-31034 | Center | When deleting an announcement, the deleted announcement may be displayed because it is not delivered to the agent | 6.0.41 (R-1), 5.0.81 (R-1) |
| 144111 | GN-31031 | WebUI | An issue where the link in the top list is not being clicked in the status of the node group in the Status 현황 & 필터의 노드그룹 현황에서 상단 목록의 링크가 클릭되지 않는 문제 Filter | 6.0.40 |
| 144111 | GN-30995 | WebUI | An issue where the audit log is left 2 times when logging in to the management console with a Cloud CSM account | 6.0.0, 5.0.45 |
| 144111 | GN-30993 | macOS Agent | Fixed an issue where the engine date of the macOS antivirus information plug-in ESET Endpoint Security was not displayed properly | 6.0.34, 5.0.74 |
| 144111 | GN-30992 | WebUI | System > Control tab page - UI alignment error fixed + icon replacement + CSS refactoring | |
| 144111 | GN-30961 | CWP | A problem where only OIDC is used as the authentication method in the node policy, and the password authentication window is displayed together | 6.0.40, 5.0.80 |
| 144111 | GN-30951 | Linux Agent | Linux Agent, an issue where the file distribution execution option is not applied | 6.0.8, 5.0.50 |
| 144111 | GN-30947 | WebUI | A problem where usage and status are not displayed properly when changing management roles in the user registration wizard | 5.0.51, 6.0.11 |
| 144111 | GN-30943 | WebUI | Operation errors that occur frequently with node UP/DOWN status events after creating a cloud site | |
| 144111 | GN-30937 | | Fixed an issue where the engine date of ESET Anti-Virus was not displayed properly in the antivirus information collection plug-in | |
| 144111 | GN-30926 | Center, Sensor | A problem where the DHCP IP allocation restriction function is used and the node registration is not correct even if a DHCP packet is received for the unused MAC after deleting the MAC | 6.0.30, 5.0.70 |
| 144111 | GN-30923 | Windows Agent | Improved the phenomenon where the button is pushed when generating a URL button in the title bar of the agent authentication window | 5.0.17, 6.0.0 |
| 144111 | GN-30921 | Sensor | Modify the total disk capacity collected by the sensor to be the same as the result of df | 4.0.M7, 3.5.1, 3.4.7 |
| 144111 | GN-30908 | WebUI | An issue where the administrator timeline is not applied in the custom report Excel file | |
| 144111 | GN-30898 | WebUI | A problem where regular expression matching at the end of polling does not work properly in Workflow HttpRequest process polling settings | |
| 144111 | GN-30876 | macOS Agent | Symptoms where the macOS agent and firewall agent permission notification window appears and then disappears | 6.0.39 |
| 144111 | GN-30872 | IPMGMT | The problem of not being able to use other sensor bands when using the IP application system with automatic login | 6.0.39, 5.0.79 |
| 144111 | GN-30865 | WebUI | An issue where If/Else does not work properly when testing the workflow in the UI | 6.0.38 |
| 144111 | GN-30864 | IPMGMT | A problem where the IP application system's user browser search button does not work on mobile terminals | 6.0.31, 5.0.71 |
| 144111 | GN-30823 | WebUI | A problem where the untag time is not displayed properly on the node tag settings screen in the node list task selection menu | 6.0.20 |
| 144111 | GN-30770 | Windows Agent | Removed an issue where the appearance and personalization plug-in forced the screen saver to be disabled | 5.0.18, 6.0.0 |
| 144111 | GN-30736 | WebUI | Some menu icons are broken (not displayed) and button style inconsistency issues | |

### 23.3.2 Genian ZTNA 6.0.35 (LTS) Release Notes (2025-12-01)

Last Updated: 2025-12-01

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 142317 | GN-30800 | WebUI | Tomcat version upgrade (9.0.108 -> 9.0.111) | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 | 2.2 |
| 140235 | GN-30205 | WebUI | Improve issues where node and user management policies can be modified and policies can be applied with limited rights through web browser control | | 3.1 |
| 140165 | GN-30382 | WebUI | Improved so that files that can execute scripts are not uploaded | | 3.1 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 142816 | GN-30739 | Ubuntu(Debian) | [General-purpose OS] Improved to limit the storage capacity of systemd journal logs | |
| 142305 | GN-30448 | Database | Fixed so that the agent desktop icon was not generated when upgrading from 5.0 to 6.0. | |
| 141126 | GN-30558 | WebUI | Management console vulnerability action (Access-Control-Allow-Origin, password change response) | |
| 140774 | GN-27147 | macOS Agent | Improved to be able to change the screen saver/wallpaper image of the Appearance and Personalization plug-in on macOS Sonoma (14.x) and above | 5.0.45, 6.0.2 |
| 138957 | GN-30056 | macOS Agent | macOS agent supports newly released macOS 26 (codename Tahoe) | |
| 138874 | GN-30310 | Center | Added a way to generate an audit record on the VPN server when the ZTNA VPN server fails to allocate DHCP | |
| 138852 | GN-30322 | Sensor | Improved so that the IP assigned when the VPN connection is terminated can be assigned to another client | |
| 137873 | GN-29866 | GNOS | CT64/SS64 Broadcom NetXtreme-C/E 10/25/40/50 gigabit ethernet card support | |
| 137873 | GN-29797 | WebUI | Add security level to Admin > Node Status Filters | |
| 137873 | GN-29790 | WebUI | Add risk rating to Admin > Node Status Filters | |
| 137873 | GN-29732 | WebUI | Added a REST API to send emails | |
| 137873 | GN-29590 | WebUI | Added a search filter function to a list where choices can be assigned from the new UI | |
| 137873 | GN-29584 | Linux Agent | Linux Agent adds the ability to apply action policies based on internal and external conditions of the terminal network | |
| 137873 | GN-29511 | WebUI | Improved so that API key or token information required for integration is not displayed in Workflow | |
| 137873 | GN-29473 | WebUI | Change the icon to an image icon font awesome | |
| 137873 | GN-29444 | WebUI | Add workflow validation options to log filters | |
| 137873 | GN-29294 | Windows Agent | Managing PNS Client Versions in ZTNA Connection Manager | |
| 137873 | GN-29271 | Linux Agent | Linux Agent extends ARP management plug-in functionality | |
| 137873 | GN-29035 | Linux Agent | Linux Agent adds plug-in for external transfer of agent information | |
| 137873 | GN-28763 | Ubuntu(Debian) | [General-purpose OS] Improved so that it can be executed as a /etc/init.d/ script | |
| 137873 | GN-28615 | IPMGMT | Improved to induce password changes when logging in to the IP application system if the account password has expired | |
| 137873 | GN-27888 | Center | Number of interfaces used by the agent installation terminal Add node group conditions | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 142783 | GN-30866 | Windows Agent | File download traffic temporarily increases every time the File Distribution V2 plug-in is updated. | 6.0.15, 5.0.56 |
| 142699 | GN-30836 | Sensor | [SS64] Repeated node up/down problem in sensor devices | 6.0.26 (LTS), 5.0.66 |
| 142001 | GN-30748 | Sensor | A problem where the sensor is unable to assign an IP to the VPNServer | 6.0.0 |
| 141888 | GN-30571 | WebUI | A page error occurs when logging in as an administrator with management roles and menu access restrictions | 6.0.34 |
| 141765 | GN-30783 | WebUI | An issue where the Connect Network Sensors page does not display properly | 5.0.65 (LTS), 6.0.26 (LTS) |
| 141753 | GN-30686 | syslog | [General-purpose OS] An issue where a new log file cannot be created in some cases in the Syslog audit log | 5.0.44, 6.0.1 |
| 141614 | GN-30378 | WebUI | An issue where fields set to read-only in agent deployment options become editable when modified | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56, 5.0.57 |
| 141597 | GN-30543 | WebUI | If the pop-up is blocked by the browser during SAML2 authentication, there is no response when clicking the SAML authentication button | 5.0.19 |
| 141411 | GN-30506 | WebUI | An issue where unsupported representative sensor functions are output in sensor settings in system management in 6.0 beta versions and above | 6.0.33 |
| 141315 | GN-30627 | CLOUD | Symptoms of Cloud NAC backups failing in Naver Cloud environments due to the awscli v2 upgrade | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.37, 5.0.77 |
| 141113 | GN-30653 | Center | 24.04 Problem with not uploading Ubuntu NAC sensor software to Policy Server 20.04 | 6.0.25, 5.0.65 (LTS) |
| 141099 | GN-30609 | Center | [General-purpose OS] A full DB connection occurred due to a problem where the number of sessions on the Percona MySQL server increased by 1 per day | 6.0.24, 5.0.64 |
| 140481 | GN-30581 | WebUI | A problem where the tag assignment REST API does not set when only the expiration date (expireDate) is entered for each tag release | 5.0.55, 5.0.65 (LTS), 6.0.26 (LTS), 5.0.66 |

continues on next page

Table 1 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 140471 | GN-30350 | WebUI | User registration An issue where user registration is not possible in the REST API | 6.0.28, 5.0.68 |
| 140423 | GN-29631 | Windows Agent | Fixed an error where the interface control plug-in misjudged wireless as a wire and blocked it | 5.0.0, 6.0.0 |
| 140331 | GN-30604 | CWP | Pages are intermittently not redirected during CWP redirection | 6.0.32, 5.0.72 |
| 140241 | GN-30535 | macOS Agent | macOS agent, AD authentication disabled when updated | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 |
| 140213 | GN-30439 | WebUI | NAC V6.0 Dashboard Widget Failure to Display Overall Status | 6.0.16 |
| 139819 | GN-30473 | Center, dbmigration | An issue where dbmigration fails due to a timeout | |
| 139723 | GN-30516 | Sensor | A problem where the information synchronization authentication integration fails due to communication failure when using a VPN tunnel and source routing | 5.0.42, 6.0.0 |
| 139696 | GN-30372 | Center | Symptoms of authentication failure because the VPN connection was disconnected after the sensor register operation and the connection was not reconnected | 5.0.42, 6.0.0 |
| 139140 | GN-30446 | Windows Agent | An issue where the distribution server list is not applied in operating system updates when using multiple distribution server features | 6.0.23, 5.0.63 |
| 139084 | GN-30488 | Center | An issue where the center daemon shuts down abnormally when registering an agent sensor | 6.0.1 |
| 139050 | GN-30398 | Center | When uploading software (policy server deb file) to the Ubuntu NAC policy server, it cannot be uploaded due to an integrity check failure | 5.0.20, 6.0.1 |
| 139048 | GN-30325 | macOS Agent | macOS agent crashes intermittently right after running daemon | 5.0.0, 6.0.0 |
| 139037 | GN-30340 | Center, ElasticSearch | An issue where ES logs are not saved because a 5.0 GNOS template was created from the Ubuntu NAC ES template information | |
| 138990 | GN-30228 | Windows Agent | Improvement of the network slowing down due to abnormal operation of the network AP information collection thread during wireless LAN control actions | 5.0.30, 6.0.0 |
| 138936 | GN-30265 | WebUI | Security agreement page, an issue where it cannot be created due to an error when adding a new automatic user | 6.0.17 |
| 138922 | GN-30412 | Sensor | When setting the policy server as a PMS proxy server, the update search fails because the domain options that allow connection are not reflected | 5.0.12, 6.0.0 |

continues on next page

Table 1 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 138908 | GN-30096 | Sensor | When setting up a distribution server proxy, an operating system update fails if the domain that allows connections contains a '/' character | 5.0.0, 6.0.0 |
| 138890 | GN-30274 | Center | When collecting domain information through an agent, domain information cannot be updated between the same DEVID if the information has already been collected | 5.0.0, 6.0.0 |
| 138857 | GN-30459 | Center, Sensor | An issue where static route settings in the Ubuntu NAC version are not applied after rebooting | 5.0.0, 6.0.0 |
| 138841 | GN-30373 | Center, Sensor | An issue where an English audit log is output because Preferences -> Management Console -> Advanced settings (some) cannot be transferred to the sensor | 6.0.30, 5.0.70 |
| 138633 | GN-30434 | Center, Sensor | An issue where logrotate does not work on cloud and compose policy servers/sensors | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 |
| 138576 | GN-30318 | WebUI | A problem where the changed approver cannot be imported normally when the approval is changed step by step in the IP application system | 4.0.156, 6.0.16, 5.0.55 |
| 138527 | GN-30419 | Center | An issue where emails are not being sent due to a Cloud NAC AWS CLI version upgrade | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 |
| 137873 | GN-30263 | procmond | A problem in the process monitoring daemon (procmond) that prevents center process from being restarted if it hangs | 6.0.20, 5.0.60 |
| 137873 | GN-30176 | Sensor | Symptoms of sensord shutting down intermittently when collecting information with wmic | 5.0.25 |
| 137873 | GN-30172 | Center | An issue where the 'Use certificate' settings linked to LDAP authentication are not saved or deleted | 6.0.32, 5.0.72 |
| 137873 | GN-30168 | WebUI | 6.0 An issue where the percentage display on the node platform dashboard is displayed the same as COUNT | 6.0.16 |
| 137873 | GN-30150 | WebUI | An issue where generating a query report from a custom report fails | 6.0.35 (LTS), 5.0.75 (LTS) |
| 137873 | GN-30127 | WebUI | The problem of not being able to connect to WEB SSH | 6.0.31 |
| 137873 | GN-30003 | Center, Sensor | [DKNS] An issue where snmp information cannot be provided even when using sensor SNMP agent settings | 6.0.32, 5.0.72 |

continues on next page

Table 1 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 137873 | GN-29903 | CWP | Problem where department names are not displayed on the cwp new user registration page | 6.0.31 |
| 137873 | GN-29810 | WebUI | An issue where exported PDF files do not open properly when exporting a pie chart with the number of nodes by security level from the dashboard | 6.0.34 |
| 137873 | GN-29774 | WebUI | A problem where some columns are not output when exporting from System and Sensor Management. | 5.0.30, 6.0.0 |
| 137873 | GN-29757 | WebUI | An issue where useful life expiration date and manufacturing date settings cannot be deleted in node lifecycle management | 6.0.29, 5.0.69 |
| 137873 | GN-29709 | Windows Agent | A problem where the ID/PWD value longer than the length of the field cannot be entered when using the wired 802.1x GenianGTC authentication module | 5.0.17, 6.0.0 |
| 137873 | GN-29702 | SDP | [SDP] An issue where the input window is infinite when updating settings in the CLI | 6.0.34 |
| 137873 | GN-29654 | Linux Agent | A problem where the same notification message is continuously generated in the item when the execution cycle of the Linux Agent user notification message plug-in is set to “always execute” | 6.0.26 (LTS) |
| 137873 | GN-29637 | Linux Agent | A problem where Linux Agent and Internet Kill Switch duplicate rules cannot be registered and repaired | 6.0.9 |
| 137873 | GN-29636 | Authsync, CLOUD | [CLOUD] An issue where audit logs are not recorded during information synchronization (authsync) | 4.0.114, 5.0.11, 6.0.0 |
| 137873 | GN-29629 | WebUI | Fixed an issue where the settings pop-up window was not fully displayed depending on the resolution | 6.0.22 |
| 137873 | GN-29613 | Linux Agent | Linux Agent incorrectly collects password usage time information for accounts that do not have a password enabled | 5.0.41, 6.0.0 |
| 137873 | GN-29609 | WebUI | An issue with log filters showing a previously specified date when reselecting a date after changing the calendar period | 4.0.M7 |
| 137873 | GN-29570 | WebUI | A system error is displayed on the status widget for each wireless LAN group within the wireless LAN group of the Status Filter | 6.0.29 |
| 137873 | GN-29551 | SDP | [SDP] Problem with missing KEY=VALUE format messages in Gateway Debug | 6.0.33 |
| 137873 | GN-29547 | SDP | [SDP] An issue where automatic certificate issuance using the Workflow function fails | |
| 137873 | GN-29527 | CWP | An issue where the help message (markdown) on the CWP user authentication page is different from the preview in the management console and the actual CWP page output | 5.0.55, 5.0.56, 6.0.19, 5.0.59, 4.0.159 |
| 137873 | GN-29520 | WebUI | Update node group list UI broken | 6.0.29, 5.0.69 |
| 137873 | GN-29516 | WebUI | An issue where the sorted state is not exported when exporting a list of nodes after sorting | 5.0.38 |
| 137873 | GN-23225 | Center | If a virtual sensor is deleted, it may be registered as a deleted virtual sensor when registering a new node | 5.0.32, 6.0.0 |

### 23.3.3 Genian ZTNA 6.0.26 (LTS) Release Notes (2025-12-01)

Last Updated: 2025-12-01

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 142316 | GN-30800 | WebUI | Tomcat version upgrade (9.0.108 -> 9.0.111) | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 | 2.2 |
| 140272 | GN-30205 | WebUI | Improve issues where node and user management policies can be modified and policies can be applied with limited rights through web browser control | | 3.1 |
| 140164 | GN-30382 | WebUI | Improved so that files that can execute scripts are not uploaded | | 3.1 |

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 142815 | GN-30739 | Ubuntu(Debian) | [General-purpose OS] Improved to limit the storage capacity of systemd journal logs | |
| 142306 | GN-30448 | Database | Fixed so that the agent desktop icon was not generated when upgrading from 5.0 to 6.0. | |
| 141127 | GN-30558 | WebUI | Management console vulnerability action (Access-Control-Allow-Origin, password change response) | |
| 140775 | GN-27147 | macOS Agent | Improved to be able to change the screen saver/wallpaper image of the Appearance and Personalization plug-in on macOS Sonoma (14.x) and above | 5.0.45, 6.0.2 |
| 138963 | GN-30056 | macOS Agent | macOS agent supports newly released macOS 26 (codename Tahoe) | |
| 138851 | GN-30322 | Sensor | Improved so that the IP assigned when the VPN connection is terminated can be assigned to another client | |
| 134660 | GN-29669 | Windows Agent | Windows Server 2025 support on agents | |
| 132971 | GN-29361 | Center, GeniUpdate | Fixed an issue where the latest operating information data update could fail | 6.0.16, 5.0.55, 5.0.60, 4.0.160 |
| 132679 | GN-29354 | | A problem where verification of the latest operating information data fails with Genian Sinker. | |

continues on next page

Table 2 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 130257 | GN-28738 | | Agent Windows Server 2022 support | |
| 130257 | GN-28564 | Sensor | [Mirror sensor] Structural improvements to improve performance | |
| 130257 | GN-28543 | WebUI | Provides a function to search for sensors in the management sensor section on the node registration screen | |
| 130257 | GN-28515 | macOS Agent | macOS agent improves tray icon update speed showing ZTNA connection status | |
| 130257 | GN-28498 | macOS Agent | Improved to enable OTP registration during OTP secondary authentication in macOS ZTNA Connection Manager | |
| 130257 | GN-28470 | Windows Agent | DNS control plug-in provides an option to set the sensor address as default DNS | |
| 130257 | GN-28469 | macOS Agent | Improved to enable OTP registration during OTP secondary authentication with the macOS agent authentication window | |
| 130257 | GN-28462 | Center | Improved to enable authentication queries after password conversion when linking LDAP authentication | |
| 130257 | GN-28446 | Linux Agent | UI and CLI improvements to guide apps other than Google OTP apps in Linux Agent and OTP secondary authentication | |
| 130257 | GN-28445 | Windows Agent | UI improvements to guide apps other than Google OTP apps in OTP secondary authentication with an in-layer window | |
| 130257 | GN-28444 | WebUI | Improved so that when using the SAML JIT Provisioning function, the IdP's group name works even if the group name is set different from the NAC (SP) management role (Adminstator Role) ID | |
| 130257 | GN-28441 | macOS Agent | macOS agent adds integrity check after successful connection to center | 5.0.0, 6.0.0 |
| 130257 | GN-28437 | Center | Improved so that different client profiles can be applied to wireless LAN policies with the same SSID | |
| 130257 | GN-28432 | macOS Agent | macOS ZTNA connection plugin OpenVPN update | 6.0.13 |
| 130257 | GN-28408 | WebUI | Improved so that the text size of big number type widgets can be displayed fluidly according to the size of the widget | |
| 130257 | GN-28379 | WebUI | Improved the OTP app installation screen in the new login UI of the management console so that apps other than Google OTP can be installed | |
| 130257 | GN-28371 | Windows Agent | Improved so that only site items are selected and linked regardless of the ZTNA connection method | |
| 130257 | GN-28369 | WebUI | UI improvements so that OTP secondary authentication shows that in addition to the Google OTP app, other apps such as MS Authenticator are also possible | |
| 130257 | GN-28339 | Center | Blocking malicious domains through DNS control | |
| 130257 | GN-28316 | CLOUD | [CLOUD] Improved to check the device's internal syslog log | |
| 130257 | GN-28275 | Windows Agent | Futuretech VPN integration added to ZTNA Connection Manager | |
| 130257 | GN-28189 | | Improved UI for setting node tags | |

continues on next page

Table 2 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 130257 | GN-27951 | | Improved so that if there are duplicate values when registering wireless LANs in batches, the duplicate values will be displayed in a message | |
| 130257 | GN-27765 | Linux Agent | Development of Linux Agent user notification message Linux Agent 사용자 알림메시지 & 공지사항 기능 개발 및 Main UI 적용 announcement function and application of Main UI | |
| 130257 | GN-27688 | WebUI | Improved to be able to set change items in convenient port-type emails | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 142784 | GN-30866 | Windows Agent | File download traffic temporarily increases every time the File Distribution V2 plug-in is updated. | 6.0.15, 5.0.56 |
| 142698 | GN-30836 | Sensor | [SS64] Repeated node up/down problem in sensor devices | 6.0.26 (LTS), 5.0.66 |
| 141999 | GN-30748 | Sensor | A problem where the sensor is unable to assign an IP to the VPNServer | 6.0.0 |
| 141766 | GN-30783 | WebUI | An issue where the Connect Network Sensors page does not display properly | 5.0.65 (LTS), 6.0.26 (LTS) |
| 141626 | GN-30378 | WebUI | An issue where fields set to read-only in agent deployment options become editable when modified | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56, 5.0.57 |
| 141599 | GN-30543 | WebUI | If the pop-up is blocked by the browser during SAML2 authentication, there is no response when clicking the SAML authentication button | 5.0.19 |
| 141365 | GN-30686 | syslog | [General-purpose OS] An issue where a new log file cannot be created in some cases in the Syslog audit log | 5.0.44, 6.0.1 |
| 141314 | GN-30627 | CLOUD | Symptoms of Cloud NAC backups failing in Naver Cloud environments due to the awscli v2 upgrade | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.37, 5.0.77 |
| 141112 | GN-30653 | Center | 24.04 Problem with not uploading Ubuntu NAC sensor software to Policy Server 20.04 | 6.0.25, 5.0.65 (LTS) |

continues on next page

Table 3 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 141100 | GN-30609 | Center | [General-purpose OS] A full DB connection occurred due to a problem where the number of sessions on the Percona MySQL server increased by 1 per day | 6.0.24, 5.0.64 |
| 140421 | GN-29631 | Windows Agent | Fixed an error where the interface control plug-in misjudged wireless as a wire and blocked it | 5.0.0, 6.0.0 |
| 140240 | GN-30535 | macOS Agent | macOS agent, AD authentication disabled when updated | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 |
| 140212 | GN-30439 | WebUI | NAC V6.0 Dashboard Widget Failure to Display Overall Status | 6.0.16 |
| 139818 | GN-30473 | Center, db-migration | An issue where dbmigration fails due to a timeout | |
| 139792 | GN-30372 | Center | Symptoms of authentication failure because the VPN connection was disconnected after the sensor register operation and the connection was not reconnected | 5.0.42, 6.0.0 |
| 139724 | GN-30516 | Sensor | A problem where the information synchronization authentication integration fails due to communication failure when using a VPN tunnel and source routing | 5.0.42, 6.0.0 |
| 139125 | GN-30446 | Windows Agent | An issue where the distribution server list is not applied in operating system updates when using multiple distribution server features | 6.0.23, 5.0.63 |
| 139103 | GN-30325 | macOS Agent | macOS agent crashes intermittently right after running daemon | 5.0.0, 6.0.0 |
| 139083 | GN-30488 | Center | An issue where the center daemon shuts down abnormally when registering an agent sensor | 6.0.1 |
| 139049 | GN-30398 | Center | When uploading software (policy server deb file) to the Ubuntu NAC policy server, it cannot be uploaded due to an integrity check failure | 5.0.20, 6.0.1 |
| 139036 | GN-30340 | Center, ElasticSearch | An issue where ES logs are not saved because a 5.0 GNOS template was created from the Ubuntu NAC ES template information | |
| 138987 | GN-30228 | Windows Agent | Improvement of the network slowing down due to abnormal operation of the network AP information collection thread during wireless LAN control actions | 5.0.30, 6.0.0 |
| 138935 | GN-30265 | WebUI | Security agreement page, an issue where it cannot be created due to an error when adding a new automatic user | 6.0.17 |
| 138921 | GN-30412 | Sensor | When setting the policy server as a PMS proxy server, the update search fails because the domain options that allow connection are not reflected | 5.0.12, 6.0.0 |
| 138907 | GN-30096 | Sensor | When setting up a distribution server proxy, an operating system update fails if the domain that allows connections contains a '/' character | 5.0.0, 6.0.0 |

continues on next page

Table 3 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 138856 | GN-30459 | Center, Sensor | An issue where static route settings in the Ubuntu NAC version are not applied after rebooting | 5.0.0, 6.0.0 |
| 138632 | GN-30434 | Center, Sensor | An issue where logrotate does not work on cloud and compose policy servers/sensors | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 |
| 138577 | GN-30318 | WebUI | A problem where the changed approver cannot be imported normally when the approval is changed step by step in the IP application system | 4.0.156, 6.0.16, 5.0.55 |
| 138526 | GN-30419 | Center | An issue where emails are not being sent due to a Cloud NAC AWS CLI version upgrade | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 |
| 137792 | GN-30263 | procmond | A problem in the process monitoring daemon (procmond) that prevents center process from being restarted if it hangs | 6.0.20, 5.0.60 |
| 137698 | GN-29907 | Center | A problem where RADIUS audit records are not stored in ES | 6.0.25, 5.0.65 (LTS) |
| 136941 | GN-30110 | macOS Agent | macOS Agent crashes while updating tray icons due to policy changes | 5.0.0, 6.0.0 |
| 136937 | GN-30105 | Center | An issue where the policy server's SOAP communication is not normal | 5.0.0, 6.0.0 |
| 136801 | GN-30157 | Windows Agent | The problem of not being able to connect to the Policy Server when installing the agent with an MSI installation package | 6.0.22, 5.0.62 |
| 136789 | GN-30045 | Center, Sensor | The problem of not being able to upgrade the kernel on Ubuntu NAC S30H_R1 devices | |
| 136782 | GN-28992 | Authsync | An issue where users created by information synchronization fail to authenticate due to mismatched passwords | 4.0.119, 5.0.17, 6.0.0 |
| 136590 | GN-30136 | WebUI | “There was an error requesting the page.” A problem that causes a management console error called | 5.0.55, 5.0.65 (LTS), 6.0.26 (LTS), 6.0.29, 5.0.69 |
| 136372 | GN-27945 | Center | An issue where an audit log of DB query errors occurs when registering a wireless LAN by dividing the Mac in uppercase and lowercase letters | 4.0.0, 5.0.0, 6.0.0 |

continues on next page

Table 3 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 136247 | GN-29460 | Windows Agent | Fixed an error where an audit log was not left when blocking pop-up messages were turned off in the forced process termination plug-in | 5.0.25, 6.0.0 |
| 136184 | GN-29791 | Windows Agent | Fix a password validation window error in the password validation plug-in | 5.0.55, 5.0.65 (LTS), 6.0.26 (LTS), 6.0.31, 5.0.71 |
| 135735 | GN-29885 | Sensor | An issue where DNS response IP is not updated when using FQDN network objects | 5.0.27 |
| 135533 | GN-29784 | macOS Agent | A problem where the macOS action execution type does not work according to the set options when the execution type is set at the specified time | 5.0.11, 6.0.0 |
| 135127 | GN-29847 | Enforcer | Problem with the new hardware Sxxx sensor not being able to redirect cwp to http | 5.0.0 |
| 135018 | GN-29666 | Windows Agent | The MAC address of an SSL VPN user is registered as a virtual MAC, so there is a risk of duplicate node IDs | 6.0.4, 5.0.48 |
| 134979 | GN-29513 | WebUI | An error occurs when clicking an IP usage application in violation of the IP management policy | 4.0.139, 5.0.37, 6.0.0 |
| 134972 | GN-29782 | Center | Fixed an issue where trying to upgrade to 20.04 NAC sensor version when automatically upgrading the Ubuntu 24.04 NAC sensor | 5.0.65 (LTS), 6.0.26 (LTS) |
| 134804 | GN-29717 | Center | A problem where the alarm transmission scheduler does not work on the cloud policy server | 5.0.54, 6.0.15 |
| 134619 | GN-29088 | Windows Agent | A problem where the collected information is not updated after the plug-in fails to send the collection information | 5.0.50, 4.0.153, 6.0.11 |
| 134606 | GN-29649 | Windows Agent | The removed network interface is still included in the network information collection plug-in collection list, and there is a risk of duplicate node IDs | 5.0.0, 6.0.0 |
| 134163 | GN-29548 | Center, ElasticSearch, Sensor, VRRPD | A phenomenon where CWP cannot be connected due to missing source routing in redundant sensors using VMAC | 6.0.19, 5.0.59 |
| 134148 | GN-29130 | Center, Genian Mobile | A problem where sending a mobile push alarm fails | 5.0.0, 6.0.0 |
| 133915 | GN-28588 | macOS Agent | An issue where the macOS agent and policy server have completed authentication but continue to request authentication | 5.0.0, 6.0.0 |
| 133802 | GN-29502 | Windows Agent | Fix password validation and change errors in the password validation plugin | 4.0.0, 5.0.55, 5.0.65 (LTS), 6.0.26 (LTS), 6.0.28, 5.0.68 |

continues on next page

Table 3 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 133786 | GN-29046 | | A problem where some information, such as the name of the management device, is not saved in the audit log when IP collision protection is set | 6.0.21, 5.0.61 |
| 133614 | GN-29358 | | If an administrator's expiration date is set, the problem is reset when the administrator modifies user information after logging in | 5.0.22, 6.0.0 |
| 133399 | GN-29145 | macOS Agent | An issue where the macOS wireless LAN control 'AP data collection validity time' option is not applied | 5.0.55, 5.0.65 (LTS), 6.0.26 (LTS) |
| 133364 | GN-29338 | Sensor | An issue where blocking is maintained intermittently when changing from a blocking policy to an acceptance policy | 4.0.123, 5.0.20, 6.0.0 |
| 133236 | GN-29433 | Center, macOS Agent | An issue where authentication information registered in the keychain disappears when changing the password through the macOS password validation plug-in | 6.0.21, 5.0.61 |
| 132897 | GN-28874 | Windows Agent | Fix an action execution error when booting the operating system when the PC time changes to the future and is restored after a certain period of time | 5.0.0, 6.0.0 |
| 132896 | GN-29339 | | Linux Agent, an issue where the action execution cycle continues to be executed for a certain period of time when the operating system is started | 5.0.42, 6.0.0 |
| 132813 | GN-29152 | WebUI | A problem where null is recorded in the audit log when agreeing to a security agreement and agreeing to user information | 5.0.57, 6.0.32 |
| 132666 | GN-29163 | WebUI | An issue where the operation mode of an interface that does not have an IP set during sensor settings can be changed to Host mode when using batch sensor commands | 4.1.3 |
| 132348 | GN-29302 | Center | An issue where upgrade directory permissions are changed to root when backing up GPDB/NMDB | 6.0.14, 5.0.55 |
| 132235 | GN-29245 | Linux Agent | Linux Agent periodically creates gnupdate zombie processes Linux Agent 주기적으로 gnupdate 좀비 프로세스 생성 & 증가하는 문제 growing issues | 6.0.22 |
| 132155 | GN-29159 | Center | A problem where the user authentication expiration processing scheduler does not work properly due to NTP changes during process operation | 4.0.143, 5.0.40, 6.0.0 |
| 132148 | GN-29185 | Center | A problem where policy changes due to node reservation tag assignment are not reflected in the sensor | 5.0.21, 6.0.0 |
| 131999 | GN-29180 | Center | A problem where ES index cannot be cleaned up due to an error that determines the execution result of a system command as a failure even if it is successful | |
| 131988 | GN-29225 | Authsync | A problem where setting the initial fixed password value does not work when using the REST API Server synchronization type | 5.0.38 |
| 131516 | GN-29033 | WebUI | A problem where all logs can be checked when exporting audit logs when the administrator's management scope (management sensor) is limited | 5.0.22, 6.0.0 |
| 131379 | GN-28959 | Center | A problem where the operating state of a node in the DOWN state is changed to UP and maintained during RADIUS authentication | 5.0.44, 6.0.1 |

continues on next page

Table 3 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 131361 | GN-29090 | Windows Agent | Password change via password validation plug-in fails on Windows 11 (24H2) | 5.0.0, 6.0.0 |
| 131262 | GN-29147 | Ubuntu(Debian) | [General-purpose OS] An issue where the management console (Tomcat) cannot run after upgrading an internally set device on a general-purpose OS device for a specific period of time | 6.0.25, 5.0.65 (LTS) |
| 130876 | GN-28991 | Center | The problem of not being able to assign a user IP when using a site user static IP | 6.0.14 |
| 130650 | GN-28798 | WebUI | An error occurs when updating the JIT Provisioning Additional Information section during SNMP authentication settings | 6.0.16, 5.0.55, 5.0.56, 6.0.24, 5.0.64 |
| 130524 | GN-28843 | dbmigration | An issue where the SNMP Agent setting USERNAME value is not normal after migration | 6.0.25, 5.0.65 (LTS) |
| 130399 | GN-28969 | Center, Sensor | [General-purpose OS] An issue where an updated library path cannot be found and a reference error occurs | 6.0.16, 5.0.55 |
| 130257 | GN-29468 | Center | A problem where custom data in the PlatformDetect table is deleted and the node type is changed after updating to the latest version of GPDB in general OS | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.29, 5.0.69 |
| 130257 | GN-28896 | ulogd | A memory problem occurs when sending WebProxy (Squid) audit logs to FlowLog | 6.0.0 |
| 130257 | GN-28881 | DKNS | An issue where the log file size continues to grow because logrotate does not work in the DKNS environment | 6.0.0 |
| 130257 | GN-28856 | WebUI | An issue where some of the information contained in the XML received after downloading Metadata from the CWP SAML authentication integration settings UI is displayed as /mc2 | 6.0.22, 5.0.62 |
| 130257 | GN-28826 | Center | A problem where the sensor is not used as a distribution server for a certain period of time when an action is modified without changing the distribution file | 4.0.M3, 3.4.3, 5.0.0, 6.0.0 |
| 130257 | GN-28747 | | A problem where part of the item is missing when delivering the device group item on the device usage application form | 4.0.0, 5.0.0, 6.0.0 |
| 130257 | GN-28728 | WebUI | Operation errors that cannot be removed from the device list and node list when deleting cloud sensor devices | 6.0.26 (LTS) |
| 130257 | GN-28701 | dbmigration | An issue where SNMP Agent settings are not normal due to migration errors | 6.0.17, 5.0.57 |
| 130257 | GN-28695 | Sensor | A problem where the upgrade is treated as a success even if the upgrade fails due to a timeout when upgrading a sensor | 5.0.42 |
| 130257 | GN-28667 | | An issue where nodes are not discovered by IP in Inline sensor monitoring mode | 5.0.37 |
| 130257 | GN-28651 | Sensor | A problem where the sensor process terminates abnormally when using the real-time detection function for host name changes | 4.0.114, 5.0.11 |
| 130257 | GN-28630 | macOS Agent | An agent error occurred when updating the OS with the macOS update plug-in. ERRMSG= Audit log issues | 5.0.11, 6.0.0 |

continues on next page

Table 3 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 130257 | GN-28610 | | A problem where when changing the tag name in the tag settings on the node detail screen, the description of the changed tag is not automatically changed | 6.0.26 (LTS) |
| 130257 | GN-28565 | WebUI | A problem where 404 errors are displayed in the audit log when entering the control policy screen | 6.0.19 |
| 130257 | GN-28541 | | An issue where an error occurs in the agent version status widget | 4.0.159, 6.0.20, 5.0.60 |
| 130257 | GN-28499 | macOS Agent | macOS agent disconnects from wireless LAN when using wireless LAN control plug-in on macOS Sonoma 14.5 | 5.0.0, 6.0.0 |
| 130257 | GN-28495 | Windows Agent | An issue where domain information from a node cannot be collected (when using workgroups) | 6.0.16, 5.0.55, 5.0.56, 6.0.20, 5.0.60 |
| 130257 | GN-28483 | Windows Agent | An issue where English characters are displayed when the first numeric key is entered in the agent authentication window | 4.0.120, 5.0.17, 6.0.0 |
| 130257 | GN-28447 | | An issue where mouse selection is intermittently not correct when the submenu is displayed in a dropdown form from the top menu | 6.0.17 |
| 130257 | GN-28423 | macOS Agent | An issue where verification information such as macOS offline integrity and electronic signatures is not sent to the audit log | 6.0.20 |
| 130257 | GN-28420 | Linux Agent | Linux Agent, problem of not being able to send certain offline logs | 6.0.20 |
| 130257 | GN-28409 | WebUI | A problem where the output information is displayed as undefined when there is abnormal data in the node details | 5.0.42, 6.0.16 |
| 130257 | GN-28405 | WebUI | An error showing the operator account in the IP Management Console's administrator list | 5.0.11, 6.0.0 |
| 130257 | GN-28399 | macOS Agent | Improved reboot-related wording for the macOS operating system update plug-in | 5.0.55, 6.0.17 |
| 130257 | GN-28375 | WebUI | A problem where SAML authentication in CWP does not work properly when setting a custom port other than 443 (https) port | 5.0.49, 6.0.7 |
| 130257 | GN-28372 | GNOS | [GNOS] Error log issue when checking udp communication with Policy Server during installation | 5.0.31, 6.0.0 |
| 130257 | GN-28310 | | An issue where the REST API for the node group list (/nodegroups) does not output the number of nodes applied to the node group | 4.0.159, 6.0.20, 5.0.60 |
| 130257 | GN-28309 | | An issue where an email with the application result is not sent when all SMS text notifications and e-mails are entered in the user application form | 5.0.0, 6.0.0 |
| 130257 | GN-28285 | WebUI | An issue where additional options are not applied properly when creating additional fields | 6.0.19, 5.0.59 |
| 130257 | GN-28272 | | Change the help and some image icons to awesome and unify the color style | 6.0.5 |
| 130257 | GN-27741 | WebUI | Problems where applications cannot be made if the department within 'Device Control > Device Use Application Form' does not exist | 5.0.0, 6.0.0 |

continues on next page

Table 3 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 130257 | GN-27606 | WebUI | A problem where the untagging time of the set tag is set to an unlimited number of times when the rest API assigns a tag with a set period | 5.0.49, 6.0.8 |

## 23.4 Previous Versions

### 23.4.1 Genian ZTNA 6.0.41 Release Notes (2025-12-01)

Last Updated: 2025-12-02

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 143079 | GN-30881 | Windows Agent | Improved to be able to display detailed screens for consistency in network connection information | |
| 143079 | GN-30831 | WebUI | Changes to AWS's vulnerability information collection structure and modification of grouping conditions | |
| 143079 | GN-30810 | macOS Agent | Added the macOS antivirus information plug-in to collect Kaspersky Endpoint Security information | 5.0.9 |
| 143079 | GN-30808 | WebUI | Certificate Services List Sorting Function Added | |
| 143079 | GN-30805 | WebUI | Improved the Nodes API to import a list of department (authenticated users) nodes by adding a department code parameter | |
| 143079 | GN-30801 | WebUI | Improved warning text about not being able to display mirror sensors in IP Matrix View | 6.0.41 (R), 5.0.81 (R) |
| 143079 | GN-30789 | Windows Agent | Improved disk space issues caused by temporary Internet folders when the agent runs as a local system account | |
| 143079 | GN-30747 | Center | Improved to display the top memory occupancy process items when the resource warning threshold is exceeded for the policy server's memory status | |
| 143079 | GN-30741 | WebUI | Agent Sensor setting function through a notification message when the administrator logs in to the CLOUD | |
| 143079 | GN-30726 | Linux Agent | Linux Agent adds macro functionality for agent action [File] options | |
| 143079 | GN-30724 | WebUI | Security enhancements for using the REST API | |
| 143079 | GN-30700 | Linux Agent | Linux Agent and gncli autocomplete functions have been improved so that they can operate according to policies | |
| 143079 | GN-30681 | Windows Agent | Process control function added to the Windows firewall control function | |
| 143079 | GN-30646 | WebUI | Improved so that a console warning is not output when the color is not set in the dashboard chart widget | |
| 143079 | GN-30597 | Center, ElasticSearch, GeniUpdate | Improved so that CVE2 operation information data can be updated due to CVE feed changes | |
| 143079 | GN-30593 | Linux Agent | Linux Agent adds the ability to automatically set local firewall rules according to the control policy permissions received | |
| 143079 | GN-30564 | WebUI | ZTNA top navigation bar responsive UI improvements | |
| 143079 | GN-30551 | WebUI | Process object functionality added | |
| 143079 | GN-30466 | WebUI | Improved functionality so that the management view editing function can be used in device usage applications | |
| 143079 | GN-30387 | WebUI | Improved so that the option filter is applied when there are many option items in the node group conditions displayed in the form of a dropdown | |
| 143079 | GN-30359 | Linux Agent | Linux Agent, gncli 5.0 support work | |
| 143079 | GN-30356 | Sensor | Improved so that DHCP DELETION packets are not processed for IPs that have a no-change policy | |
| 143079 | GN-29641 | WebUI | Improved so that announcements can be set and output for each node group | |
| 143079 | GN-25670 | | CWP secondary authentication level UI unification work | |
| 110830 | GN-24352 | CWP | Added an identity verification function using SMS/email to the security agreement page | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 143079 | GN-30918 | IPMGMT | The problem of not being able to log in when logging in to the IP application system if ~ is included in the password | 4.0.114, 5.0.11, 6.0.0 |
| 143079 | GN-30880 | WebUI | An issue where the Certificate Services search function does not work | 6.0.39 |
| 143079 | GN-30868 | Windows Agent | Improved so that the system shutdown plug-in "notification time before shutdown" can be expressed on a daily basis when set to 24 hours or more | 5.0.10, 6.0.0 |
| 143079 | GN-30860 | Linux Agent | Linux Agent, problem of not being able to use gncli commands in some environments | |
| 143079 | GN-30854 | WebUI | Problem with not being able to change from Settings > Properties Management > Usage Management > IP Usage > Device Change to Using Approver Email Approval | 6.0.6 |
| 143079 | GN-30853 | WebUI | Improved UI that doesn't handle multilingual messages and items displayed only in Korean | 5.0.33 |
| 143079 | GN-30851 | WebUI | An issue where the reason for the failure is not displayed when settings fail in some menus in the Administration Console > Settings | 6.0.22 |
| 143079 | GN-30848 | CWP | An issue where the Agent installation button is displayed when a mobile type node accesses the CWP page | 5.0.32, 6.0.0 |
| 143079 | GN-30830 | Windows Agent | Improved the phenomenon that screen saver (SCR) files are re-downloaded when the distribution server is changed | 5.0.0, 6.0.0 |
| 143079 | GN-30811 | macOS Agent | An issue where the macOS agent closes the input window after reissuing the authentication code when connecting to ZTNA | 6.0.37 |
| 143079 | GN-30807 | WebUI | Audit log Flow application chart area location error when resizing browser | 6.0.8 |
| 143079 | GN-30806 | WebUI | An issue where dashboard reports are generated when generating blank content | 6.0.39 |
| 143079 | GN-30781 | macOS Agent | The cursor is not focused on the ID field in the macOS agent and ZTNA connection manager | 6.0.16 |
| 143079 | GN-30762 | Windows Agent | An issue where Edge runs even if the default browser is changed to Chrome in Windows 11 | 5.0.0 |
| 143079 | GN-30755 | Windows Agent | Fixed a server load issue due to a large number of reconnections when setting multiple IPs on the network interface | 5.0.0 |
| 143079 | GN-30745 | WebUI | Checkbox + label text alignment error in System Administration > Security settings | 6.0.9 |
| 143079 | GN-30702 | WebUI | A problem where line break characters in flow application chart tooltips are displayed because they are broken | 6.0.24 |
| 143079 | GN-30666 | Linux Agent | Linux Agent, a problem where the installation file cannot be installed with a new installation file if the installation file already exists | 6.0.22 |
| 143079 | GN-30662 | WebUI | An authentication error occurs when logging in after changing the password on the login screen | 6.0.19 |
| 143079 | GN-30661 | WebUI | A phenomenon where FLOW logs are not output to Excel | 6.0.0 |
| 143079 | GN-30649 | WebUI | An issue where check boxes are displayed on discarded certificate items in the Certificate Services list | 6.0.39 |
| 143079 | GN-30645 | WebUI | An issue where pasting to the keyboard does not work when entering a numeric type field | 6.0.30 |
| 143079 | GN-30437 | WebUI | A problem where tag type information in user tags is output differently | 6.0.20 |
| 143079 | GN-30286 | WebUI | Fixed an issue where the changed department name was not displayed in the settings item on the node group list screen when the department name was changed | 6.0.32, 5.0.72 |
| 143079 | GN-30180 | WebUI | An issue where the error badge count in the top menu does not match the number of screens moved by clicking the icon | 5.0.22 |

### 23.4.2 Genian ZTNA 6.0.40 Release Notes (2025-11-03)

Last Updated: 2025-11-11

## New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 141783 | GN-30715 | Windows Agent | Change to enable agent sensors in Cloud ZTNA Basic Edition | |
| 141783 | GN-30701 | WebUI | Add the site name to the audit log found in Site Creation/Modification/Deletion | |
| 141783 | GN-30685 | WebUI | The ability to modify the “DHCP Service” item is limited when using the ZTNA Client sensor interface | |
| 141783 | GN-30684 | Center, Sensor | Improved so that VPN connection attempts are not attempted when the configured connection sensor is DOWN when linking authentication | |
| 141783 | GN-30683 | Center | Add a “if attribute value doesn't match a regular expression” condition to RADIUS policy conditions | |
| 141783 | GN-30665 | Sensor | Added a function to periodically check iptables rules while the broker VPN function is running | 5.0.42, 6.0.1 |
| 141783 | GN-30625 | Sensor | 2.91 version upgrade to address dnsmasq-related CVE vulnerabilities | |
| 141783 | GN-30623 | Center | Adding a default Azure CLI installation when building a cloud policy server | |
| 141783 | GN-30577 | macOS Agent | macOS ZTNA Connection Manager plug-in creates a log file when connecting to a VPN | 6.0.40 (R) |
| 141783 | GN-30570 | WebUI | Remove the part where the Google Map API Key used in the dashboard's sensor map is in the source code | |
| 141783 | GN-30559 | Sensor | Improved to leave detailed debugs for errors related to VPN connections | |
| 141783 | GN-30546 | Linux Agent | Linux Agent adds automatic registration function for SDP client certificates | |
| 141783 | GN-30529 | WebUI | Add node grouping conditions by collecting vulnerability information of EC2 instances when AWS Security Hub is enabled | |
| 141783 | GN-30522 | Sensor | Improved so that packets are not looped between sensor<-> gateways when the sensor is set to strict mode | 5.0.0 |
| 141783 | GN-30463 | WebUI | Improved notation for permission objects | |
| 141783 | GN-30442 | Authsync | Improved so that when synchronizing information (authsync), an audit log of the results of normal execution is left | |
| 141783 | GN-30424 | Linux Agent | Linux Agent, improved the function so that when the user mistyped the gncli command, the phrase that it was entered incorrectly appears | |
| 141783 | GN-30309 | WebUI | Admin Console sitemap feature added | |
| 141783 | GN-30270 | CWP | OIDC authentication function added | |
| 141783 | GN-30246 | WebUI | Top area > Multi-language selection Select menu Improved UI consistency issue in Safari environment | |
| 141783 | GN-30146 | WebUI | Improved so that the IP application form is saved by changing it to capital letters when entering MAC | |
| 141783 | GN-29970 | Windows Agent | PowerGate SSO integration plugin development | |
| 141783 | GN-29874 | WebUI | Added a feature to enable the cloud data collector to work in the K8S environment | |
| 141783 | GN-29761 | WebUI | Added a feature to display user tags as tooltips in the authenticated user item in the node list | |
| 141783 | GN-29737 | IPMGMT | Added a function to restrict the output of username/department information when an ordinary user applies on behalf of an IP application | |
| 141783 | GN-29593 | Windows Agent | Improved so that agents are allowed permission to use location services when there are features that require location services | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 141783 | GN-30728 | WebUI | An issue where unnecessary columns are output from tag items in the audit log filter | 6.0.35 (LTS) |
| 141783 | GN-30699 | VRRPD | A problem where the source routing is created incorrectly after changing the VRRP state | 4.1.M3 |
| 141783 | GN-30692 | Center, WebUI | An issue where the tomcat configuration file is not upgraded to a higher version when upgrading an image | 5.0.0, 6.0.0 |
| 141783 | GN-30689 | WebUI | An error that prevents Cloud Collector-related services from running on general-purpose OS | 6.0.39 (R-1) |
| 141783 | GN-30670 | WebUI | Fixed an error where the date input specified the maximum date was specified as the minimum date | 6.0.30 |
| 141783 | GN-30654 | Windows Agent | A problem where deleted items are still displayed on the server list registered in Genian Browser. | 5.0.42, 6.0.0 |
| 141783 | GN-30650 | macOS Agent | macOS agent disconnects from ZTNA when changing the network it belongs to | 5.0.13, 6.0.0 |
| 141783 | GN-30648 | Linux Agent | Linux Agent, the problem of not being able to connect to some sites when the browser is opened through the agent | |
| 141783 | GN-30644 | Windows Agent | A problem where the message is regenerated every cycle if the URL is blank in the user notification message action | 6.0.32, 5.0.72 |
| 141783 | GN-30640 | gnlogin | A problem where gnlogin (cli) does not execute the PING command when the domain contains a '-' hyphen | 5.0.9, 6.0.0 |
| 141783 | GN-30639 | WebUI | A problem where when linking SAML authentication to the management console does not apply to the changed locale when connecting to the login screen after changing the locale | 5.0.48, 6.0.6 |
| 141783 | GN-30635 | WebUI | Errors where the date in the Admin Console data table is displayed as a number (timestamp) | 6.0.30 |
| 141783 | GN-30633 | WebUI | Admin > Node > Status Filter > Problem where the sorting function does not work when searching for departments (authenticated users) | 5.0.33 |
| 141783 | GN-30631 | CWP | When accessing user information while cookies are deleted after user authentication via Passkey in CWP, normal query is not possible | 6.0.7 |
| 141783 | GN-30629 | WebUI | A problem where a blacklist settings file exists in the password policy, but the policy is not applied on the new settings page | 6.0.30 |
| 141783 | GN-30628 | Sensor | The problem of not being able to create a split tunnel | 6.0.21 |
| 141783 | GN-30620 | WebUI | Remove non-existing file references | |
| 141783 | GN-30608 | dbmigration | If the device group condition is used as 'all', the blocking device and the blocking exception device in the device control policy do not operate | 5.0.25, 6.0.0 |
| 141783 | GN-30599 | Sensor | A problem with repeated process restart logs due to abnormal shutdown of the gdcid daemon | 5.0.53, 6.0.14 |
| 141783 | GN-30595 | Sensor | A problem where the DHCP IP allocation restriction function does not work when the MAC being used is blocked | 6.0.30, 5.0.70 |
| 141783 | GN-30592 | WebUI | An issue where the number of available connections may be reduced because the DB Connection is not opened and closed | 5.0.0, 6.0.0 |

continues on next page

Table 4 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 141783 | GN-30589 | Windows Agent | An error where the agent is deleted regardless of policy using the agent installation information registered in the control panel | 5.0.0, 6.0.0 |
| 141783 | GN-30588 | WebUI | An issue where sub-items according to the version are not displayed when changing the SNMP version | 6.0.30 |
| 141783 | GN-30574 | IPMGMT | A problem where multiple applications are mixed with approvals/rejections, an email is sent with only the content of the refusal | 5.0.42, 6.0.0 |
| 141783 | GN-30563 | Center, Sensor | An issue where the sensor did not change the domain of the node, but the center updates the domain of the node to a blank | 5.0.25, 6.0.0 |
| 141783 | GN-30555 | WebUI | Site > An issue where the search function does not work in the ZTNA Client Sessions list | 6.0.0 |
| 141783 | GN-30520 | macOS Agent | Change the Radius log format when connecting to a VPN using the macOS ZTNA Connection Manager plug-in | |
| 141783 | GN-30512 | Database, dbmigration | [GNOS] A problem where a MySQL error log occurs on the policy server during policy/DB separation configuration | 5.0.58 |
| 141783 | GN-30505 | WebUI | An issue where the output date and time are not output to the administrator's timeline when exporting the audit log | 5.0.22 |
| 141783 | GN-30504 | WebUI | DHCP usage rate display, problem where DHCP band cannot be displayed properly in Matrix View | 5.0.42 |
| 141783 | GN-30432 | WebUI | An issue where 404 errors are recorded in the audit log due to references to resources that don't exist on some pages | 5.0.77 |
| 141783 | GN-30202 | Linux Agent | Linux Agent misses multilingual processing of some column names in monitor information | 6.0.12 |
| 141783 | GN-29901 | WebUI | A problem where some data displayed on the settings screen is output in the form of a 'value' | |
| 141611 | GN-30378 | WebUI | An issue where fields set to read-only in agent deployment options become editable when modified | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56, 5.0.57 |

## 23.4.3 Genian ZTNA 6.0.39 Release Notes (2025-10-01)

Last Updated: 2025-11-03

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 140682 | GN-30004 | WebUI | Lib version update/removal work with critical vulnerabilities | | 0.0 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 141433 | GN-29323 | Windows Agent | Added a tray menu to display personal client certificate information used in SDP | |
| 140682 | GN-30567 | Center | Improved distribution server priority order when using multiple distribution servers | |
| 140682 | GN-30562 | Center, RADIUSD | Improved ability to add attributes to RADIUS Access-Accept messages | |
| 140682 | GN-30534 | Windows Agent | Added a feature to change the color of the authentication button in the agent authentication window plug-in | |
| 140682 | GN-30530 | WebUI | Add a condition to a node group that uses the vulnerable AWS EC2 instance metadata service (IMDS) | |
| 140682 | GN-30498 | Sensor | Improved to collect traffic information for the bondx interface | |
| 140682 | GN-30471 | Windows Agent | Modified so that the password change window can be set via a separate URL when the password expires | |
| 140682 | GN-30468 | Windows Agent | Changed to exclude web apps (PWAs) installed in multiple browsers from the program removal list | |
| 140682 | GN-30455 | Windows Agent | Improved the problem that EDR Agent information cannot be collected in software information collection | |
| 140682 | GN-30444 | procmond | Improved so that bugrport is generated if a core file exists when the gdcid daemon is restarted | |
| 140682 | GN-30440 | WebUI | Added a sub-option (sensor location information change range) based on the IP application system's option whether to change sensor location information | |
| 140682 | GN-30423 | WebUI | When the type of the custom button is 'Information Collection', modified so that if you are not a user (node/device), it is output even in an unauthenticated state | |
| 140682 | GN-30390 | WebUI | Corrective feature limitations for sensor modes when using ZTNA Client sensor interfaces | |
| 140682 | GN-30385 | WebUI | Improved so that the width of the columns in the flowlog list can be adjusted | |
| 140682 | GN-30370 | WebUI | Improved the function to search for secondary sensor names when searching for sensor names in the sensor tree | |
| 140682 | GN-30361 | Linux Agent | A problem where the gncli module does not work when installing an agent with a Linux Agent or SSH connection | 6.0.9 |
| 140682 | GN-30339 | WebUI | Improved to output the correct port when there is no port information displayed in the Idp integration information | |
| 140682 | GN-30308 | Windows Agent | Improved execution function and encryption method after authentication in the agent authentication window | |
| 140682 | GN-30293 | syslog | Save PNS logs to audit logs through syslog integration | |
| 140682 | GN-30275 | macOS Agent | macOS agent, proactive response to changing network extended rights UI in macOS Tahoe | |
| 140682 | GN-30095 | SDP | [SDP] Improved to automatically set keyCloakHostName and CassandraSettings when installing a controller | |
| 140682 | GN-30052 | Linux Agent | Linux Agent adds a function to display the number of duplicates when receiving duplicate pop-up messages and improves UI | |

continues on next page

Table 5 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 140682 | GN-30042 | WebUI | Added a feature to prevent autocompletion of the password field on the user detail screen | |
| 140682 | GN-29765 | macOS Agent | Developing a user consent process for using macOS network extensions | |
| 140682 | GN-29718 | WebUI | Improved certificate information output | |
| 140682 | GN-29524 | WebUI | Improved so that '/' can be used in department names | |
| 140682 | GN-28785 | WebUI | Modified so that the CLI enable password for general-purpose OS devices can be changed in the management console | |
| 140682 | GN-28398 | Center, Genian Mobile | App push delivery added to the audit log filter alarm method | 5.0.0, 6.0.0 |
| 140682 | GN-28236 | macOS Agent | Applies to macOS ZTNA 6.0 Agent's firewall control plug-in NAC 5.0 | |
| 140682 | GN-25414 | WebUI | Improved certificate information output screen | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 140987 | GN-30643 | WebUI | An error where the server does not respond when using the SOAP API | 6.0.39 (R-1), 5.0.79 (R-1) |
| 140682 | GN-30544 | Sensor | A problem where permission information is missing from node information using sensor proc | |
| 140682 | GN-30542 | gnlogin | The problem of not being able to check interface information using cli | 4.0.9 |
| 140682 | GN-30502 | Windows Agent | Automatic rules operation error in Windows Firewall Control when the policy server address is a domain | 5.0.28, 6.0.0 |
| 140682 | GN-30441 | WebUI | An error where CVE information is not output due to an esQuery error | 5.0.39 |
| 140682 | GN-30431 | Linux Agent | Linux Agent, an issue where the agent module does not run intermittently (tray icon, ZTNA connection manager, etc...) | |
| 140682 | GN-30427 | WebUI | An issue where Korean is displayed in the date selector in tag settings when using the management console in English | 6.0.31 |
| 140682 | GN-30406 | Linux Agent | Linux Agent, an issue where the CWP page does not appear when the default web browser is Firefox on Ubuntu 22.04 and higher | 5.0.42, 6.0.0 |
| 140682 | GN-30401 | WebUI | A problem where the sensor and secondary sensor names are incorrect when there are multiple sensors with the same IP | 4.0.116, 5.0.13 |
| 140682 | GN-30381 | WebUI | Fixed an issue where dashboard widget restrictions were not applied in Administration > User Settings | 6.0.0 |
| 140682 | GN-30368 | WebUI | A problem where device application manager notifications do not occur | 5.0.42, 6.0.0 |
| 140682 | GN-30360 | Center | A problem where the user's VPN IP is not fixed when using a fixed user VPN IP | 6.0.26 (LTS) |
| 140682 | GN-30354 | Windows Agent | An issue where the help is displayed incorrectly when the '%' character is present in the agent authentication window help | 5.0.0, 6.0.0 |
| 140682 | GN-30341 | WebUI | An issue where the list does not appear with an error message when clicking on the quantity of the asset status monitor in the dashboard widget | 6.0.34, 5.0.74 |
| 140682 | GN-30324 | Windows Agent | A problem where multiple APs are output when collecting connected AP information through a wireless LAN control action. | 5.0.0, 6.0.0 |
| 140682 | GN-30244 | SDP | [SDP] Controller installation failure on Ubuntu 24.04 | 6.0.32 |
| 140682 | GN-30222 | WebUI | The problem of not being able to download when the custom button is a download when using the Custom CWP Port | 4.1.5 |
| 140682 | GN-30177 | WebUI | A problem where required input settings are not applied in the user settings list (check box) in the user addition field | 5.0.65 (LTS), 6.0.26 (LTS) |
| 140682 | GN-30165 | WebUI | Error occurs when " is included while entering SAML settings or OTP server settings in authentication-linked settings | 6.0.19, 5.0.59 |
| 140682 | GN-29971 | WebUI | SAML2 Authentication Integration > An issue where IdP Metadata upload does not work properly | 5.0.42, 5.0.48, 6.0.7 |
| 140682 | GN-29733 | WebUI | 6.0 An issue where horizontal scrolling of the list disappears when there is a command execution notification on the node list screen | |
| 140682 | GN-29525 | WebUI | A problem where an error page is displayed due to incorrect resource collection data on the equipment in system information in system management | 3.3.3 |
| 140682 | GN-29423 | WebUI | An issue where the list is not displayed when sorting by update time on the node group list screen | 5.0.41 |
| 138873 | GN-30425 | Center | Fixed so that the user account can be suspended when RADIUS authentication fails N times | 5.0.17 |

### 23.4.4 Genian ZTNA 6.0.38 Release Notes (2025-09-01)

Last Updated: 2025-10-13

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 140772 | GN-27147 | macOS Agent | Improved to be able to change the screen saver/wallpaper image of the Appearance and Personalization plug-in on macOS Sonoma (14.x) and above | 5.0.45, 6.0.2 |
| 139773 | GN-30443 | IPMGMT | Improved to batch process input value error verification in user changes in the IP application system | |
| 139268 | GN-30342 | Linux Agent | Linux Agent, Red Hat Enterprise Linux, and Oracle Linux OS support | |
| 139229 | GN-30348 | Windows Agent | Changed to exclude web apps (PWAs) installed in multiple browsers from the software collection list | |
| 139229 | GN-30344 | WebUI | Improved functionality so that specific services are restarted when they die in the general OS Ubuntu environment | |
| 139229 | GN-30338 | Sensor | Improved audit log that occurs when an upgrade is interrupted due to using the latest version | |
| 139229 | GN-30271 | | Font Awesome custom icon add rules to individual color css files | |
| 139229 | GN-30242 | Windows Agent | Initec NexessSSO integration plug-in development | |
| 139229 | GN-30219 | Center, syslog | Added an audit log for SOAP communication status errors | |
| 139229 | GN-30178 | Windows Agent | Improved so that software information is collected as soon as uninstallation is completed through the program removal plug-in | |
| 139229 | GN-29976 | WebUI | Add Base64 Encode/Decode functions to the workflow | |
| 139229 | GN-29902 | WebUI | Adding a Loop process to a workflow | |
| 139229 | GN-29753 | WebUI | Adding an If/Else Process to a Workflow | |
| 139229 | GN-29724 | WebUI | Add a Sendmail process that allows you to send mail via Workflow | |
| 139229 | GN-29008 | WebUI | Adding Crypto (AES, Hash, and HMAC support) processes to the workflow | |

## Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 140723 | GN-30571 | WebUI | A page error occurs when logging in as an administrator with management roles and menu access restrictions | 6.0.36 |
| 139782 | GN-30457 | WebUI | A problem where an error verification message is output repeatedly when the approver is a required item in a new IP application | 6.0.6, 5.0.49 |
| 139770 | GN-30487 | WebUI | A problem where an error occurs when the IP application form entry is set in the new application entry field for each purpose while the IP application form entry is on | 5.0.11, 6.0.0 |
| 139229 | GN-30418 | Authsync | A problem where only part of RESTAPI is synchronized when calling RESTAPI through information synchronization because the start page number is set incorrectly | 5.0.38, 6.0.0 |
| 139229 | GN-30345 | Center | Information Sync -> User Information -> A problem where user information that has already been synchronized is not updated even if the user information modification value is changed, so it cannot be corrected | 5.0.17, 6.0.0 |
| 139229 | GN-30302 | WebUI | Netflow Agent displays an error when there is no license | 6.0.30, 5.0.70 |
| 139229 | GN-30290 | Center | Fixed an issue where the error message in the user authentication failure log section was displayed as successful when the node authentication process failed after user authentication | |
| 139229 | GN-30283 | WebUI | Problems with overlapping CWP authentication page ID entry fields when the 'Protect ID in User Authentication' option of user authentication is on in the management console | 6.0.13 |
| 139229 | GN-30241 | Sensor | A problem where the blocking function does not work on the PNS sensor | 6.0.36 |
| 139229 | GN-30239 | WebUI | An issue where the license version shows up to the date when a deb image containing a codename is installed | 5.0.65 (LTS), 6.0.26 (LTS) |
| 139229 | GN-30231 | macOS Agent | When using the macOS software information collection action, there is a problem of repeatedly sending the information even though the information has not been changed | 5.0.11, 6.0.0 |
| 139229 | GN-30200 | WebUI | A problem where the main menu (top) menu order of the management console is Audit, Settings, and System, but the settings, audit, and system are displayed incorrectly | 6.0.34 |
| 139229 | GN-30188 | Windows Agent | PNS is not installed through the ZTNA Connection Manager plug-in on the policy server with NAT IP set. | 6.0.37 |
| 139229 | GN-30041 | WebUI | An issue where the sensor option for connecting to the server in the authentication connection is blank when there is no sensor | 6.0.30 |
| 139229 | GN-29939 | WebUI | An issue where an error message is not clearly provided when entering characters that cannot be used when creating a node group | 5.0.13, 6.0.0 |
| 139229 | GN-29373 | WebUI | A problem where when modifying IP or MAC address conditions with OR conditions while setting node group conditions, the details cannot be checked in the policy application changes | 5.0.11 |

### 23.4.5 Genian ZTNA 6.0.37 Release Notes (2025-08-04)

Last Updated: 2025-08-29

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 138352 | GN-30299 | Center | A problem where the policy server self-signed certificate is renewed every time the cloud policy server pod is restarted | |
| 137841 | GN-30151 | WebUI | Added robots.txt file to prevent web crawling | |
| 137841 | GN-30129 | WebUI | Add syntax to use time-related data in Workflow | |
| 137841 | GN-30128 | Center | Improved to leave an audit log when an unauthorized network sensor is accessed | |
| 137841 | GN-30114 | Linux Agent | Linux Agent improves functionality so that RPM packages can also be removed from program removal plug-ins | |
| 137841 | GN-30008 | macOS Agent | macOS agent improved to select user authentication method when authenticating SDP | |
| 137841 | GN-29906 | SDP | [SDP] Add certificate-related commands to CLI | |
| 137841 | GN-29905 | Windows Agent | Improved to select the user authentication method performed by SDP | |
| 137841 | GN-29830 | SDP | [SDP] Fixed an issue where an audit record was not left on the server device when an mTLS connection failed | |
| 137841 | GN-29801 | Windows Agent | Custom Plugin development for Escare PowerPack SSO integration | |
| 137841 | GN-29776 | SDP | [SDP] Improved so that the authentication method can be set | |
| 137841 | GN-29536 | Windows Agent | Improved browser auto login function of ZTNA Connection Manager (Chrome Extension auto install) | |
| 137841 | GN-29290 | WebUI | Improved so that only sensor groups managed in tree edit mode are displayed when the node management scope limit is 'Sensor Group' | |
| 137841 | GN-27827 | Linux Agent | Linux Agent adds Futuretech SSL VPN integration | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 138880 | GN-30386 | build, CLOUD, MGMT | A problem where SAML integration and Passkey registration do not work properly in a CLOUD environment | 6.0.37 (R-1), 5.0.77 (R-1) |
| 138789 | GN-30446 | Windows Agent | Fixed an error where the distribution server list could not be obtained when using multiple distribution server functions | 6.0.23, 5.0.63 |
| 137924 | GN-29701 | WebUI | SAML2 Authentication Integration > An error page is displayed when downloading Metadata | 6.0.22 |
| 137841 | GN-30251 | Linux Agent | Linux Agent, an issue where some messages may be missing when receiving many user message display policies at once | 6.0.20, 5.0.60 |
| 137841 | GN-30243 | macOS Agent | An issue where the "Monitor information change detected" audit log continues to occur when using the macOS monitor information collection plug-in | 5.0.17, 6.0.0 |
| 137841 | GN-30234 | Linux Agent | Linux Agent, an issue where the ZTNA connection menu is intermittently not displayed during initial installation | 6.0.2 |
| 137841 | GN-30212 | WebUI | A problem where the country code is not saved in the administrator notification information when registering or modifying a user in the management console | 6.0.30, 5.0.70 |
| 137841 | GN-30203 | Linux Agent | Linux Agent, an issue where icons are not displayed properly on the dock (taskbar) on ubuntu 24.04 and later | |
| 137841 | GN-30201 | syslog, Ubuntu(Debian) | [General-purpose OS] A problem where a syslog audit log filter is set without entering a filter value, the previously used log is not recorded | 5.0.42, 6.0.0 |
| 137841 | GN-30152 | Linux Agent | Linux Agent, an issue where the gnpopup module stops when clicking on a pop-up message linked to a URL | 6.0.12 |
| 137841 | GN-30140 | Linux Agent | Problems that cannot be repaired when the integrity of Linux Agent or Redhat Linux is damaged | 6.0.34, 5.0.76 |
| 137841 | GN-30132 | Center | An issue where the IP Utilization Alert Option feature causes threshold alerts on the number of nodes rather than the number of IPs | 5.0.0, 6.0.0 |
| 137841 | GN-30126 | build, MGMT | An issue where the IP management application system approval/rejection link does not open in the Docker Compose environment | 5.0.23, 6.0.0 |
| 137841 | GN-30014 | WebUI | A problem where a security group cannot be created because the relevant path is deleted when an error occurs during cloud security group policy creation | 6.0.1 |
| 137841 | GN-30002 | Ubuntu(Debian) | [General-purpose OS] A problem where the Smartctl command malfunctions with the maintenance script (Sysinspect.sh) | 5.0.0, 6.0.0 |
| 137841 | GN-29786 | WebUI | When setting the user tag period, the time cannot be allocated if the unlimited cancellation time check box is unchecked | 6.0.31 |
| 137841 | GN-29785 | Linux Agent | Linux Agent, an issue where policy updates are repeated indefinitely | 5.0.41, 6.0.0 |
| 137841 | GN-29739 | WebUI | An issue where the status filter on the node management page is not detected when clicking on the quantity of a node in the agent operating system specific widget | 5.0.17, 6.0.0 |
| 137841 | GN-28980 | WebUI | An issue where agent plug-in names containing Hangul appear broken in the policy application window | 6.0.37 (R-1), 5.0.77 (R-1) |

### 23.4.6 Genian ZTNA 6.0.36 Release Notes (2025-07-07)

Last Updated: 2025-08-29

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 138949 | GN-30056 | macOS Agent | macOS agent supports newly released macOS 26 (codename Tahoe) | |
| 138873 | GN-30310 | Center | Added a way to generate an audit record on the VPN server when the ZTNA VPN server fails to allocate DHCP | |
| 138640 | GN-30322 | Sensor | Improved so that the IP assigned when the VPN connection is terminated can be assigned to another client | |
| 137073 | GN-29974 | Sensor | Added a function to enable the sensor function to operate on the PNS gateway device | |
| 136995 | GN-30121 | Packaging, Ubuntu(Debian) | [General-purpose OS] Improved upgrade script (timeout, retry added) | 6.0.16, 5.0.55 |
| 136995 | GN-30116 | Windows Agent | Collection of vaccine information for Symantec Endpoint Protection version 14.3.11232 or higher products | |
| 136995 | GN-30104 | Linux Agent | Linux Agent, Rocky Linux support | |
| 136995 | GN-30080 | macOS Agent | Improved to leave an audit log when blocking a process by forcibly terminating the macOS process | |
| 136995 | GN-30043 | Linux Agent | Linux agent, 5.0 version CentOS support | |
| 136995 | GN-29995 | Center | Improved so that the password for the backup file can be entered when recovering a backup file via CLI | |
| 136995 | GN-29985 | Windows Agent | Added the ability to change the IP of the policy server to which the agent connects | |
| 136995 | GN-29972 | Windows Agent | Improved communication errors caused by specific programs when using the DLL injection blocking function | |
| 136995 | GN-29945 | SDP | [SDP] An issue where event transmission fails when the controller's domain is not set to the gateway | 6.0.0 |
| 136995 | GN-29928 | WebUI | Enhanced user ID verification function when creating accounts with user import (CSV) | |
| 136995 | GN-29665 | WebUI | Improved so that information on the reason for the application can also be used when using Excel upload in the IP application system | |
| 136995 | GN-29612 | Windows Agent | Fixed so that wireless connections are not directly authenticated by the GTC authentication module. | |
| 136995 | GN-29606 | WebUI | Operation status display function added to device node information | |
| 136995 | GN-29579 | Linux Agent | Linux Agent, system shutdown plug-in added | |
| 136995 | GN-29574 | SDP | [SDP] Audit log Syslog TLS transmission function added | |
| 136995 | GN-29491 | Linux Agent | Linux Agent adds ZTNA connection function through SDP connection and authentication to ZTNA Connection Manager | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 139046 | GN-30398 | Center | When uploading software (policy server deb file) to the Ubuntu NAC policy server, it cannot be uploaded due to an integrity check failure | 5.0.20, 6.0.1 |
| 139041 | GN-30325 | macOS Agent | macOS agent crashes intermittently right after running daemon | 5.0.0, 6.0.0 |
| 139034 | GN-30340 | Center, ElasticSearch | An issue where ES logs are not saved because a 5.0 GNOS template was created from the Ubuntu NAC ES template information | |
| 139020 | GN-30409 | Sensor | A problem where assigning permissions using FQDN objects can be blocked even if permission is present | 5.0.27, 6.0.0 |
| 138982 | GN-30228 | Windows Agent | Improvement of the network slowing down due to abnormal operation of the network AP information collection thread during wireless LAN control actions | 5.0.30, 6.0.0 |
| 138933 | GN-30265 | WebUI | Security agreement page, an issue where it cannot be created due to an error when adding a new automatic user | 6.0.17 |
| 138919 | GN-30412 | Sensor | When setting the policy server as a PMS proxy server, the update search fails because the domain options that allow connection are not reflected | 5.0.12, 6.0.0 |
| 138905 | GN-30096 | Sensor | When setting up a distribution server proxy, an operating system update fails if the domain that allows connections contains a '/' character | 5.0.0, 6.0.0 |
| 138854 | GN-30459 | Center, Sensor | An issue where static route settings in the Ubuntu NAC version are not applied after rebooting | 5.0.0, 6.0.0 |
| 138836 | GN-30373 | Center, Sensor | An issue where an English audit log is output because Preferences -> Management Console -> Advanced settings (some) cannot be transferred to the sensor | 6.0.30, 5.0.70 |
| 138630 | GN-30434 | Center, Sensor | An issue where logrotate does not work on cloud and compose policy servers/sensors | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 |
| 138573 | GN-30318 | WebUI | A problem where the changed approver cannot be imported normally when the approval is changed step by step in the IP application system | 4.0.156, 6.0.16, 5.0.55 |

continues on next page

Table 6 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 138524 | GN-30419 | Center | An issue where emails are not being sent due to a Cloud NAC AWS CLI version upgrade | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 |
| 137762 | GN-30269 | WebUI | An issue where the 'value' item in the Add Condition pop-up for setting conditions does not appear in RADIUS policies | 6.0.36 |
| 137252 | GN-28750 | Center | A problem where time-related data is displayed incorrectly when the time zone of the policy server and DB server is different | 6.0.17, 5.0.57 |
| 136995 | GN-30138 | Linux Agent | Linux Agent, an issue where some disk vendor information cannot be collected | 5.0.41, 6.0.0 |
| 136995 | GN-30123 | Linux Agent | Problem with Linux Agent not collecting LVM disk information | 5.0.41, 6.0.0 |
| 136995 | GN-30082 | Linux Agent | Linux Agent, an issue where actions are performed immediately when rebooting regardless of the periodic execution time object | 5.0.42, 6.0.0 |
| 136995 | GN-30018 | Windows Agent | Fixed an Alyac public installation error in the required software check plug-in | 5.0.33, 6.0.0 |
| 136995 | GN-30012 | WebUI | Fixed an issue where the default DATETIME macro for POST data was replaced with 'NONE' when calling a webhook from the audit log filter | 5.0.29, 6.0.0 |
| 136995 | GN-30006 | WebUI | An issue where some items on the page are displayed in Korean when using the English locale | 6.0.33, 5.0.73 |
| 136995 | GN-29973 | WebUI | An issue where node groups cannot be assigned in device control policies | 6.0.24 |
| 136995 | GN-29942 | macOS Agent | macOS Agent, problem with incorrect audit logs | 5.0.55, 6.0.26 (LTS), 6.0.31, 5.0.71 |
| 136995 | GN-29941 | Windows Agent | An issue where the Windows Actions plug-in leaves an incorrect audit log. | 5.0.6, 6.0.0 |
| 136995 | GN-29937 | Center, CLOUD, Docker | [AMI Cloud NAC] SFTP external backup failure issue | 6.0.4, 5.0.50 |
| 136995 | GN-29893 | Windows Agent | Fixed an issue where the external authentication integration plug-in failed to link authentication with a specific SSO | 5.0.0, 6.0.0 |
| 136995 | GN-29867 | Linux Agent | An issue where Linux Agent and ZTNA are not immediately reflected in the tray menu when disconnecting | 6.0.31 |
| 136995 | GN-29783 | WebUI | An issue where effective time processing is not normal because the administrator time zone is not reflected in the user tag allocation/deactivation time | 6.0.20 |

continues on next page

Table 6 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 136995 | GN-29766 | WebUI | An issue where icons for node types in the device in node details are not displayed | 6.0.33, 5.0.73 |
| 136995 | GN-29638 | Windows Agent | The wireless connection manager outputs a message saying incorrect account information even if the connection cannot be made due to a Radius failure | |
| 136995 | GN-29631 | Windows Agent | Fixed an error where the interface control plug-in misjudged wireless as a wire and blocked it | 5.0.0, 6.0.0 |
| 136995 | GN-28800 | WebUI | A problem where '/' is included in the network object ID, it is not properly reflected in the inclusion group of other network objects | 5.0.36, 6.0.0 |
| 136995 | GN-28714 | WebUI | A problem where input items are output at the bottom when outputting collected information on the CWP main screen | 5.0.9, 6.0.0 |
| 136995 | GN-28182 | WebUI | A problem where the notification registration time in CWP is not displayed properly when the server time zone and database time zone are different | 6.0.17, 5.0.57 |

### 23.4.7 Genian ZTNA 6.0.34 Release Notes (2025-05-07)

Last Updated: 2025-06-05

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 135042 | GN-29615 | WebUI | Added explanation and help for DB SID/NAME items on the information synchronization settings screen | 5.0.0, 6.0.0 |
| 135042 | GN-29607 | macOS Agent | Improved to collect macOS antivirus information ESET Endpoint Security 8.0 | |
| 135042 | GN-29529 | WebUI | Added a search filter function in the list (Addremove) where selections can be assigned from UI elements | |
| 135042 | GN-29519 | WebUI | Improved the Admin Console theme settings (hidden option) to be displayed in Settings > Preferences > Advanced Settings in Admin Console | |
| 135042 | GN-29507 | Linux Agent | Linux Agent adds tray menu related to Wake-on-LAN (WOL) | |
| 135042 | GN-29505 | macOS Agent | Added tray menu related to macOS Wake-on-LAN (WOL) | |
| 135042 | GN-29503 | WebUI | Improved so that when setting the IP policy on the node detail screen, it is converted to MAC address format and output in capital letters | |
| 135042 | GN-29463 | Windows Agent | Use the vaccine information collection plug-in to collect SentinelOne product version information | |
| 135042 | GN-29438 | macOS Agent | Added an execution account option to the macOS Agent Information External Transfer Plugin settings | |
| 135042 | GN-29417 | WebUI | Style improvements for advanced settings subitems in the settings UI in the management console | |
| 135042 | GN-29407 | Center | Provides a function to enable users to assign a static IP when assigning a VPN IP | 6.0.33 |
| 135042 | GN-29387 | SDP | [SDP] CLI (Command-line interface) function added | |
| 135042 | GN-29382 | WebUI | When secondary authentication is set, the UI for setting secondary authentication after primary authentication has been improved to be the same as the MFA recommendation setting UI | |
| 135042 | GN-29367 | Linux Agent | Add *Guest off-authorization users* option and *Owner exception* option to Linux Agent existing network shared folder plug-ins | |
| 135042 | GN-29315 | Windows Agent | Improved PassNinX server load for information queries in the PassNiNxSSO integration plug-in | |
| 135042 | GN-29282 | WebUI | Improved certificate information output function in the file upload component | |
| 135042 | GN-29155 | WebUI | Improved so that when adding columns for IP policy, MAC policy, and user authentication policy on the node management screen, the assigned content is displayed as a tooltip | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 135042 | GN-29809 | WebUI | An issue where Workflow is unable to properly parse JSON values containing newline characters | 6.0.34 (R-1), 5.0.74 (R-1) |
| 135042 | GN-29802 | WebUI | A problem where Korean is output when the risk score search conditions in the node group list are in English | 6.0.34 (R-1) |
| 135042 | GN-29744 | WebUI | A page error occurs when performing management restrictions by selecting a task in the All Manager during user management | 6.0.34 (R-1) |
| 135042 | GN-29736 | WebUI | Problems in which users in the assigned department are not displayed properly if the administrator's management scope is *user management scope restriction* | 6.0.24 |
| 135042 | GN-29713 | RADIUSD | An authentication failure issue occurred when registering a RADIUS EAP CA certificate configured as a bundle | 6.0.6, 5.0.49 |
| 135042 | GN-29690 | WebUI | SAML2 Authentication Integration > A phenomenon where existing input information disappears when downloading Metadata | 6.0.15, 5.0.55 (LTS) |
| 135042 | GN-29618 | WebUI | An issue where an error message is displayed in the report name in the user-defined report list | 6.0.1 |
| 135042 | GN-29588 | WebUI | A problem where the IP/MAC usage time on the node is set differently from the value entered when the administrator time zone and the browser time zone are different | 6.0.29, 5.0.69 |
| 135042 | GN-29526 | Linux Agent | A problem where many logs accumulate when the Linux Agent, Tray Icon, and gnpopup (message management) processes fail to run | 5.0.42, 6.0.0 |
| 135042 | GN-29495 | Windows Agent | Fixed an error where the screen saver was not turned off after setting the screen saver control in the Appearance and Personalization plug-in to Off | 5.0.18, 6.0.0 |
| 135042 | GN-29459 | SDP | A problem where SDP authentication fails because authentication information cannot be delivered to the gateway in an SDP controller redundant environment | 6.0.33 |
| 135042 | GN-29457 | SDP | [SDP] Fixed an issue where unnecessary NFTs rules were set when receiving SPA packets from the controller on the PNS gateway | 6.0.33 |
| 135042 | GN-29452 | SDP | [SDP] An issue where the session ID and gateway UUID are stored in reverse when the gateway joins the controller | 6.0.33 |
| 135042 | GN-29449 | macOS Agent | An issue where the button activation color is reversed in the macOS authentication window plug-in | 5.0.15, 6.0.0 |
| 135042 | GN-29440 | | Tooltip visibility error when hovering over a policy icon in the Administration > Node List table | |
| 135042 | GN-29439 | WebUI | A problem where data for the previous day, previous week, etc. is displayed as 0 in the node group and wireless LAN group items in the daily report | 6.0.30, 5.0.70 |
| 135042 | GN-29431 | SDP | [SDP] An issue where duplicate rules can be created in the nftable on the PNS SDP gateway | 6.0.33 |
| 135042 | GN-29429 | SDP | [SDP] TOTP authentication failure issue | 6.0.33 |
| 135042 | GN-29426 | SDP | [SDP] An issue where changed information is not updated to the controller when updating gateway settings | 6.0.32 |

continues on next page

Table 7 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 135042 | GN-29418 | WebUI | The phenomenon of not refreshing when a node is deleted through the *Destination Node Operation* dropdown in node details | 6.0.10 |
| 135042 | GN-29402 | WebUI | A problem where the ZTNA - Client does not check the node action being assigned in the basic information of the site | 6.0.0 |
| 135042 | GN-29389 | WebUI | An issue where the IP policy is not applied when changing the node's management sensor to the center | |
| 135042 | GN-29342 | | Settings>Consent Page>Delete security agreement window animation effects and fix UI errors | 6.0.18 |
| 135042 | GN-29341 | | Broken UI issues due to wrong bottom button position and missing styles | 6.0.18 |
| 135042 | GN-29304 | | Grippin Tower (Grippin Tower) OTP user secondary authentication failure issue | |
| 135042 | GN-29232 | WebUI | System > System Administration > System Information tab > FW policy and CLI settings output table UI margin error | 6.0.1, 6.0.34 (R-1) |
| 135042 | GN-29216 | WebUI | Edit UI style in Settings> Backup> Backup File Download Window | 6.0.5 |
| 135042 | GN-29199 | Center | An issue where the Alias IP band node of a sensor set to a distribution server downloads an agent installation file from the Policy Server | 4.1.3, 4.0.26, 3.5.22, 5.0.0, 6.0.0 |
| 135042 | GN-29129 | WebUI | An issue where some of the links in the dashboard widget contain special characters and cannot be queried | 5.0.42, 5.0.49, 6.0.8 |
| 135042 | GN-29072 | WebUI | A problem where the list is not displayed when clicking on the number of nodes for a node group item in the node report | 5.0.24, 6.0.0 |
| 135042 | GN-29048 | WebUI | A problem where when multiple applications are added to a new IP application, the results are not sent even if the processing result reception information is entered | 5.0.42, 6.0.0 |
| 135042 | GN-28903 | | An error page is displayed when searching (LIKE) if part of a specific string is the same in the node view search bar | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 135042 | GN-28838 | Center, Sensor, VRRPD | A problem where the Vrrp state is in the master state in the HA configuration, but the center (sensor) process runs in a slave state and does not act as a master | 5.0.0, 6.0.0 |
| 135042 | GN-28741 | WebUI | URL error when clicking approve/reject in the IP usage application approval email | 5.0.6, 6.0.0 |
| 135042 | GN-27945 | Center | An issue where an audit log of DB query errors occurs when registering a wireless LAN by dividing the Mac in uppercase and lowercase letters | 4.0.0, 5.0.0, 6.0.0 |
| 135042 | GN-26927 | | An issue where an audit log of creation failure is continuously recorded due to the remaining automatically generated report schedule when the administrator account is deleted | 4.1.5, 5.0.0, 6.0.0 |

### 23.4.8 Genian ZTNA 6.0.33 Release Notes (2025-04-07)

Last Updated: 2025-05-07

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 134355 | GN-29656 | Center | Improved so that a timeout can be set when setting up a webhook authentication link | 5.0.19, 6.0.0 |
| 134209 | GN-29384 | | [SDP] Controller+Keycloak integrated installation package added | |
| 134209 | GN-29374 | Center | [SDP] Improved to run SDP on PNS devices | |
| 134209 | GN-29370 | Center | [SDP] Improved to automatically issue certificates using the Workflow function of the policy server | |
| 134209 | GN-29322 | WebUI | Improved so that the department list displayed on the left side of the user management screen is output in tree format when the scope of user management is limited | |
| 134209 | GN-29314 | | [SDP] Separate keycloak into a separate installation package | |
| 134209 | GN-29311 | macOS Agent | Edit the name of the 'Allow everyone not permissions' option in the macOS network shared folder action | 6.0.4, 5.0.47 |
| 134209 | GN-29229 | WebUI | Daily report template improvements | |
| 134209 | GN-29156 | WebUI | Improved so that the output order of the drop-down list in the node type column on the node detail screen is displayed in order of name (in ascending order) | |
| 134209 | GN-28842 | WebUI | Recommended settings and added a settings screen when logging in to users without MFA | |
| 134209 | GN-28828 | WebUI | Added a function to display a set solicitation alarm when MFA is not set | |
| 134209 | GN-28805 | Center | Improved to generate a notification log before the ZTNA gateway VPN server certificate expires | |
| 134209 | GN-28198 | Zero Trust Security | [SDP] Development of additional functions for controllers and gateways | |
| 134209 | GN-28014 | WebUI | Added related features for Linode Cloud ZTNA G/W support | |
| 134209 | GN-27096 | WebUI | Change the label name of the item output in IPv4 format from an IP address to an IPv4 address | |
| 134209 | GN-26614 | WebUI | Improved batch modification of admin control settings | |

## Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 134995 | GN-29711 | WebUI | Problems that do not appear when searching for administrative department assignments after setting the administrator's management scope to *Limit User Management Scope* | 6.0.33 (R-1), 5.0.73 (R-1) |
| 134328 | GN-29708 | WebUI | An issue where the UBUNTUNS sensor image is not created when building a general-purpose OS, so it cannot be automatically upgraded | 6.0.33 (R-1) |
| 134209 | GN-29568 | WebUI | Administration > A problem where the risk rating column name in the node list is output in Korean when the name is in English | 6.0.32 |
| 134209 | GN-29534 | | A problem where an expression representing count is output in the daily report email | 6.0.33 (R-1), 5.0.73 (R-1) |
| 134209 | GN-29533 | macOS Agent | An issue where the pop-up window of the macOS user notification message action is not fixed | 6.0.21, 5.0.61 |
| 134209 | GN-29514 | WebUI | A problem where the content is not displayed when changing the tab after moving the software information data page on the node detail screen | 6.0.18 |
| 134209 | GN-29510 | | A problem where actions with an intermittent cycle are applied immediately when rebooting the PC | |
| 134209 | GN-29508 | Enforcer, Sensor | A problem where communication is not possible from the authorized terminal to the blocking device even when using the Stateful Inspection function of the sensor StrictMode | 4.0.116, 5.0.13, 6.0.0 |
| 134209 | GN-29467 | macOS Agent | ZTNA sites that can connect to macOS agents are displayed in duplicate | 6.0.32 |
| 134209 | GN-29460 | Windows Agent | Fixed an error where an audit log was not left when blocking pop-up messages were turned off in the forced process termination plug-in | 5.0.25, 6.0.0 |
| 134209 | GN-29436 | | [SDP] An error occurs when deleting nftable rules from PNS SDP devices | |
| 134209 | GN-29409 | WebUI | An issue where SP information is displayed as undefined when adding SAML authentication integration settings | 6.0.30 |
| 134209 | GN-29398 | | The problem of not being able to break the line when the setting value information is long in the Policy > 'Apply Change Policy' window | 6.0.5 |
| 134209 | GN-29392 | | go.sum file error on RELEASE-CLOUD build server | |
| 134209 | GN-29365 | CLI/gnlogin | Problem with *show data server replica status* command not working on server with DB port changed | 4.0.39, 4.0.116, 5.0.13 |
| 134209 | GN-29296 | WebUI | An issue where data does not appear in the node list that is moved when clicked on the new item count widget after the last login | 6.0.18 |
| 134209 | GN-29291 | Center, Sensor | Sensor (Agent) <->Proxy<->Center Configuration Failure to Relay Event Packets | 5.0.10, 6.0.0 |
| 134209 | GN-29285 | Authsync, Center | When department information is changed through department information synchronization, the changed content is not reflected in the group conditions | 5.0.0, 6.0.0 |
| 134209 | GN-29215 | WebUI | Table UI style broken in the quick search/import/ batch registration modal window | 6.0.5 |
| 134209 | GN-29192 | | A problem where IP management-related view items are not output when exporting nodes | 6.0.21, 5.0.61 |
| 134209 | GN-29117 | Authsync | A problem where a user defined query is executed during the information synchronization connection test | 3.4.M4, 4.0.0, 5.0.0, 6.0.0 |
| 134209 | GN-29087 | WebUI | An issue where some items on the page are displayed in Korean when using the English locale | 4.1.5, 5.0.11, 6.0.0 |
| 134209 | GN- | WebUI | A problem where the selected item is not reflected when saving | 6.0.17 |

### 23.4.9 Genian ZTNA 6.0.32 Release Notes (2025-03-04)

Last Updated: 2025-05-02

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 133114 | GN-26504 | WebUI | Vulnerability where internal network information can be queried through CWP | 5.0.0, 6.0.0 | 4.3 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 135005 | GN-29410 | WebUI | Improved so that the width can be specified in the node group filter conditions displayed in Dropdown | 6.0.29,<br>5.0.69 |
| 134658 | GN-29669 | Windows Agent | Windows Server 2025 support on agents | |
| 133114 | GN-29301 | Center | Improved so that multiple LDAP authentication linked servers can be set | |
| 133114 | GN-29214 | Sensor | Improved SNMP agent settings so that they can be customized and used | |
| 133114 | GN-29198 | WebUI | Fixed an issue where the management console login screen appeared in the 5.0 (old version) UI after the upgrade | |
| 133114 | GN-29176 | WebUI | Frontend rendering engine UI improvements | |
| 133114 | GN-29173 | Center | Enable FWDB application/update to provide an online upgrade function for the domestic version ON-prem policy server | |
| 133114 | GN-29106 | WebUI | Improved so that the list scroll area changes when the UI rendering engine details screen is displayed | |
| 133114 | GN-29096 | | Improved to display a list of sensors below the center in the sensor group assignment pop-up after creating a sensor group | |
| 133114 | GN-29081 | WebUI | Additional information added to the API for querying sensor resource information (H/W resources) | |
| 133114 | GN-29054 | Windows Agent | Improved so that the execution account can be selected as an execution option after connecting to a network in the ZTNA connection manager | |
| 133114 | GN-28946 | WebUI | Added the ability to set risk scores and view risk ratings | |
| 133114 | GN-28830 | macOS Agent | Improved so that the private Wi-Fi address option can be turned off on macOS Sequoia and higher devices | |
| 133114 | GN-28693 | macOS Agent | Connect to SDP with macOS Agent ZTNA Connection Manager | |
| 133114 | GN-28549 | macOS Agent | macOS agent, PNS integration with ZTNA connection manager | |
| 133114 | GN-27819 | Windows Agent | Connect to SDP with ZTNA Connection Manager for Windows | |
| 133114 | GN-27803 | WebUI | Create an information page for the Open Source included with the product | |
| 133114 | GN-27686 | WebUI | Improved so that MAC addresses can be searched without case sensitivity when searching for MAC addresses in audit logs | |
| 133114 | GN-26936 | Windows Agent | Added control over random hardware address options for connected SSIDs | 6.0.32,<br>5.0.72 |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 135016 | GN-29666 | Windows Agent | The MAC address of an SSL VPN user is registered as a virtual MAC, so there is a risk of duplicate node IDs | 6.0.4, 5.0.48 |
| 134976 | GN-29513 | WebUI | An error occurs when clicking an IP usage application in violation of the IP management policy | 4.0.139, 5.0.37, 6.0.0 |
| 134958 | GN-29550 | WebUI | An issue where emails are not sent when reception is set as a management role in the email sending definition | 6.0.17, 5.0.57 |
| 134807 | GN-29717 | Center | A problem where the alarm transmission scheduler does not work on the cloud policy server | 5.0.54, 6.0.15 |
| 134617 | GN-29088 | Windows Agent | A problem where the collected information is not updated after the plug-in fails to send the collection information | 5.0.50, 4.0.153, 6.0.11 |
| 134604 | GN-29649 | Windows Agent | The removed network interface is still included in the network information collection plug-in collection list, and there is a risk of duplicate node IDs | 5.0.0, 6.0.0 |
| 134291 | GN-29691 | Enforcer, Sensor | An issue where CWP redirection does not work when used as a CWP custom page | 6.0.32, 5.0.72 |
| 133575 | GN-29580 | Center, CLOUD | Symptoms of LDAP authentication failure because the VPN tunnel is broken after information synchronization is performed | 6.0.32, 5.0.72 |
| 133279 | GN-29530 | WebUI | An issue where OSS information and certificate service menu screen output are broken | 6.0.32 |
| 133144 | GN-29445 | Sensor | An issue where AP information cannot be collected because Ubuntu NAC does not include daemon binaries for wireless monitors | 5.0.42 |
| 133114 | GN-29435 | WebUI | An issue where the agent icon is not displayed on the settings screen | 6.0.30 |
| 133114 | GN-29434 | WebUI | Audit > An issue where detailed logs are not displayed when clicking on a log in the Flow log list | 6.0.29 |
| 133114 | GN-29392 | | go.sum file error on RELEASE-CLOUD build server | |
| 133114 | GN-29388 | | Problem of not being able to connect to the wireless connection manager when using MSCHAPv2+ 'user or computer authentication' | 5.0.0, 6.0.0 |
| 133114 | GN-29320 | Ubuntu(Debian) | An issue where the Windows update policy may not be displayed because the /disk/data/patches path does not exist when using an offline PMS on a general-purpose OS | 5.0.23, 6.0.0 |
| 133114 | GN-29201 | WebUI | An issue where the department name set in the user group conditions does not change when the department name is changed | 5.0.0, 6.0.0 |
| 133114 | GN-29177 | WebUI | Fixed an issue where the settings page didn't go to the top after editing | 6.0.22 |
| 133114 | GN-29158 | WebUI | An issue where a refresh does not occur after a task command when switching from the IP address management tab to the node management screen | 5.0.44, 6.0.1 |
| 133114 | GN-29142 | Center, Sensor | A problem where the status information of the nodes held by the center and sensor is not the same | 5.0.41, 6.0.0 |
| 133114 | GN-29093 | WebUI | System Administration > Control > Restart UI Alignment Error | |
| 133114 | GN-29080 | Linux Agent | A problem where two nodes are created with the same IP and the control policy may be applied incorrectly when connecting to the policy server after connecting to the Linux Agent and ZTNA | 5.0.45, 6.0.2 |
| 133114 | GN-28927 | WebUI | An issue where undefined appears in the message output field when the refresh button on the top menu is clicked | 6.0.0 |
| 133114 | GN-28539 | | A problem where only today's date can be selected from the calendar when the date limit for entering the end of use date on the IP application form is a time limit | 6.0.19, 5.0.59 |

### 23.4.10 Genian ZTNA 6.0.31 Release Notes (2025-02-03)

Last Updated: 2025-04-04

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 133040 | GN-29475 | | Utility update to verify operating information data with Genius Sinker (2.7.0) | 5.0.55 (LTS), 5.0.65 (LTS), 6.0.26 (LTS), 6.0.30, 5.0.70, 4.0.171 |
| 132361 | GN-29286 | WebUI | Improved UI rendering engine data table column width to be fixed | |
| 132361 | GN-29091 | | Apply cryptographic algorithms to http URL authentication plugins | |
| 132361 | GN-29060 | | UI rendering engine functionality improvements | 6.0.30 |
| 132361 | GN-29047 | CWP | An issue where visitor ID search results are not displayed when registering as a new CWP user on mobile | |
| 132361 | GN-29007 | | Improved time period selection window (calendar) on tag pages | |
| 132361 | GN-28863 | WebUI | Add a CONF component to generate server certificates | |
| 132361 | GN-28691 | Center | Added a certificate issuance option to the node policy so that certificates can be issued for user and terminal authentication through CWP | |
| 132361 | GN-28650 | Windows Agent | Adjust the width of the dialog box according to the password validation output guide | |
| 132361 | GN-28641 | Linux Agent | Linux Agent, interface control plug-in function extension | |
| 132361 | GN-28225 | Center | OneMore Security adds RADIUS FIDO secondary authentication integration | |
| 132361 | GN-27824 | Linux Agent | Added user authentication and information display functions to Linux Agent, tray menu, and MainUI | |
| 132361 | GN-26632 | | Cloud OS management system (GPMS) integration function development | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 134159 | GN-29548 | Center, ElasticSearch, Sensor, VRRPD | A phenomenon where CWP cannot be connected due to missing source routing in redundant sensors using VMAC | 6.0.19, 5.0.59 |
| 134144 | GN-29130 | Center, Genian Mobile | A problem where sending a mobile push alarm fails | 5.0.0, 6.0.0 |
| 134108 | GN-29608 | Enforcer | When the sensor interface is changed and used, the operation of the existing node cannot be properly confirmed | 5.0.0, 6.0.0 |
| 133912 | GN-28588 | macOS Agent | An issue where the macOS agent and policy server have completed authentication but continue to request authentication | 5.0.0, 6.0.0 |
| 133800 | GN-29502 | Windows Agent | Fix password validation and change errors in the password validation plug-in | 4.0.0, 5.0.55 (LTS), 5.0.65 (LTS), 6.0.26 (LTS), 6.0.28, 5.0.68 |
| 133778 | GN-29046 | | A problem where some information, such as the name of the management device, is not saved in the audit log when IP collision protection is set | 6.0.21, 5.0.61 |
| 133657 | GN-29501 | | An issue where the update patch file synced to Genian Sinker is missing | 4.1.0, 5.0.0, 6.0.0 |
| 133612 | GN-29358 | | If an administrator's expiration date is set, the problem is reset when the administrator modifies user information after logging in | 5.0.22, 6.0.0 |
| 133596 | GN-29468 | Center | A problem where custom data in the PlatformDetect table is deleted and the node type is changed after updating to the latest version of GPDB in general OS | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.29, 5.0.69 |
| 133496 | GN-29496 | WebUI | When the locale is en, when clicking Add Dashboard Widget, an error occurs because the license module column does not exist in the DB | 6.0.30 |
| 133391 | GN-29145 | macOS Agent | An issue where the macOS wireless LAN control 'AP data collection validity time' option is not applied | 5.0.55 (LTS), 5.0.65 (LTS), 6.0.26 (LTS) |
| 133362 | GN-29338 | Sensor | An issue where blocking is maintained intermittently when changing from a blocking policy to an acceptance policy | 4.0.123, 5.0.20, 6.0.0 |
| 133214 | GN-29433 | Center, macOS Agent | An issue where authentication information registered in the keychain disappears when changing the password through the macOS password validation plug-in | 6.0.21, 5.0.61 |
| 133053 | GN-29474 | Center | The problem of removing all certificates while removing unnecessary certificates when running ZTNA center | 6.0.31 |

continues on next page

Table 8 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 132962 | GN-29422 | WebUI | An issue where the validity of an account can be confirmed through information displayed in the REST API response when trying to log in to the management console | 6.0.31, 5.0.71 |
| 132361 | GN-29303 | | Fixed an issue where the export function worked when entering the Enter key in the input window when adding tags | 6.0.26 (LTS) |
| 132361 | GN-29298 | | An issue where the WBAuth plug-in function does not work. | 5.0.71 |
| 132361 | GN-29293 | Windows Agent | An issue with cmd.exe being able to run through an agent | 5.0.0, 6.0.0 |
| 132361 | GN-29292 | | An issue where html tags are displayed in the configuration information on the vaccine-related node group detail screen | 6.0.31, 5.0.71 |
| 132361 | GN-29276 | WebUI | A problem where the connection information of the switch port is not displayed | 6.0.29 |
| 132361 | GN-29233 | WebUI | A problem where filtering for log types does not work during node detail history management | 6.0.29, 5.0.69 |
| 132361 | GN-29227 | WebUI | An issue where text overlaps when the audit log data is longer than the table area | 6.0.29, 5.0.69 |
| 132361 | GN-29184 | Linux Agent | Problems caused by broken serial numbers in the Linux Agent and Device Information UI | 6.0.19 |
| 132361 | GN-29071 | Linux Agent | Linux Agent, an issue where the agent sends system information but cannot be updated | 5.0.41, 6.0.0 |
| 132361 | GN-28886 | macOS Agent | A problem where a process check failure log is left when a plug-in is not assigned to a macOS policy | |
| 132361 | GN-28862 | Windows Agent | Remove IPv6 options when using custom rules in the Windows Firewall Control plug-in | 6.0.31, 5.0.71 |
| 132361 | GN-28744 | | An issue where the tag name of the existing set group conditions is not changed when the tag name is changed | 5.0.12, 6.0.0 |
| 132361 | GN-28512 | WebUI | A symptom where the creation date of the log file in the debug log menu is displayed as 1970-01-01 09:00 | 5.0.40, 6.0.0 |
| 132361 | GN-28376 | WebUI | Unify table list items with sort-up/down icons, which are array sorting elements | 5.0.35 |
| 132361 | GN-27350 | WebUI | An issue where CWP does not output the changed content when registering a user after changing the user's purpose description in the cloud version | 5.0.19, 6.0.0 |

### 23.4.11 Genian ZTNA 6.0.30 Release Notes (2025-01-06)

Last Updated: 2025-03-07

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 132969 | GN-29361 | Center, GeniUpdate | Fixed an issue where the latest operating information data update could fail | 6.0.16, 5.0.55 (LTS), 5.0.60, 4.0.160 |
| 132832 | GN-29316 | WebUI | Improved related logic so that CSV Injection (Excel Macro Injection) cannot work | |
| 132825 | GN-29328 | CLOUD | Fixed an issue where it took a long time to view and delete ES templates when upgrading and installing Cloud | 5.0.33, 6.0.0 |
| 132677 | GN-29354 | | A problem where verification of the latest operating information data fails with Genian Sinker. | |
| 131783 | GN-28909 | WebUI | Improved notification window displayed when copying a node group (Policy > Group) | |
| 131783 | GN-28883 | | Added an API to check CA certificate details in certificate management on the new UI screen | |
| 131783 | GN-28625 | Sensor | Added the ability to limit DHCP IP assignments for blocked MACs | |
| 131783 | GN-28464 | WebUI | Improved to check whether the same IP is used on all interfaces of the same device when adding Alias IP in sensor settings | |
| 131783 | GN-28148 | WebUI | Added the option to view original text button (eye icon) in the password input component | |
| 131783 | GN-27477 | WebUI | Added the ability to limit dashboard widgets by license permission | |
| 131783 | GN-27475 | | Improved UI screen limit function for each license module | |
| 131783 | GN-27050 | Center, gnlogin | Added the ability to encrypt database backups | |
| 131783 | GN-26271 | WebUI | Added a permission restriction function based on the administrator authentication step by step settings | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 133061 | GN-29383 | WebUI | An issue where the update name is displayed incorrectly on the operating system update information tab | 6.0.29, 5.0.69 |
| 133049 | GN-29403 | WebUI | Error where batch sensor operation mode setting commands cannot be processed properly | 5.0.69 |
| 132885 | GN-29339 | Linux Agent | Problems that continue for a certain period of time when the action cycle is performed only once at the start of the operating system | 5.0.42, 6.0.0 |
| 132802 | GN-29152 | WebUI | A problem where null is recorded in the audit log when agreeing to a security agreement and agreeing to user information | 5.0.57, 6.0.32 (R) |
| 132664 | GN-29163 | WebUI | An issue where the operation mode of an interface that does not have an IP set during sensor settings can be changed to Host mode when using batch sensor commands | 4.1.3 |
| 132510 | GN-28825 | Sensor | A problem where deadlock monitoring takes a long time when fetching http information | 6.0.16, 5.0.57, 4.0.157 |
| 131783 | GN-29140 | WebUI | UI screen limit operation error for each license module | 6.0.30 |
| 131783 | GN-29136 | macOS Agent | An issue where some items are displayed in Korean on the macOS plug-in's English action settings page | 6.0.5, 5.0.48 |
| 131783 | GN-29121 | Center | A problem where a node's operating system update satisfaction status is classified as “not in use” when assigning an operating system update action through a label | 5.0.10, 6.0.0 |
| 131783 | GN-29066 | Center | An issue where the IP of the VPN client tap interface cannot be assigned intermittently | 6.0.0 |
| 131783 | GN-29053 | | An issue where synchronization fails when synchronizing G suite information when data fields are empty | 5.0.17, 6.0.0 |
| 131783 | GN-29040 | Center, Database | An issue where the license equipment maximum usage scheduler does not work according to the schedule set | 6.0.27, 5.0.67 |
| 131783 | GN-28976 | WebPlugin | Griffin Tower OTP integration failure problem | |
| 131783 | GN-28922 | WebUI | An issue where the interface settings button is displayed on the cloud version of the Policy Server node detail screen | 6.0.0 |
| 131783 | GN-28906 | | Style error overflowing with text when mousing over the menu displayed by Log>Log Filter> Left Tree | 6.0.5 |
| 131783 | GN-28846 | WebUI | UI style error in the 'Processing Results' item on the Application Management > Application Results Search page | 6.0.5 |
| 131783 | GN-28809 | WebPlugin | User Management > History Management > A problem where line breaks are not displayed properly when the description of audit log details is 4 lines or more | 5.0.22, 6.0.0 |
| 131783 | GN-28283 | WebUI | An issue where the management console refresh function does not work when installing extensions in a browser | 5.0.20, 6.0.0 |
| 131783 | GN-27339 | WebUI | An issue where clicking Audit > Log > Analysis Chart does not output properly | 6.0.0, 4.0.146, 5.0.53 |
| 131783 | GN-27071 | WebUI | An issue where the upload fails when uploading a file using an additional field in node attributes | 5.0.42, 5.0.50, 6.0.10 |

### 23.4.12 Genian ZTNA 6.0.29 Release Notes (2024-12-02)

Last Updated: 2025-02-06

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 131702 | GN-29143 | GenianOS | [General-purpose OS] Enhanced installation convenience using single command | |
| 130967 | GN-28954 | Sensor | Improved so that the server for ZTNA Client can be restarted in the event of an abnormal shutdown | |
| 130967 | GN-28918 | WebUI | Improved command transmission method for batch setting of sensor operation modes | |
| 130967 | GN-28853 | WebUI | Change the name of the OTP security key generation button | |
| 130967 | GN-28690 | WebUI | Modified to use regular expressions stored in the DB when checking emails for CWP new user registrations | |
| 130967 | GN-28482 | WebUI | Add a required option to the department selector in the Add User field | |
| 130967 | GN-28468 | Center | Added the ability to limit control policy assignments | |
| 130967 | GN-28336 | WebUI | Improved so that the applicant name and user name parts can be searched in the IP usage application form | |
| 130967 | GN-28208 | WebUI | Modified to keep existing items when added after searching in the management sensor assignment on the user details screen | |
| 130967 | GN-28199 | WebUI | Workflow UI added | |
| 130967 | GN-28088 | | Improved the quick search and search bar so that the device/IP owner can also be searched by name | |
| 130967 | GN-28077 | WebUI | Improved the message displayed when creating and authenticating Passkeys | |
| 130967 | GN-28022 | Genian Syncer | Improved so that the Genian Syncer package is included and distributed during NAC packaging | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 132346 | GN-29302 | Center | An issue where upgrade directory permissions are changed to root when backing up GPDB/NMDB | 6.0.14, 5.0.55 (LTS) |
| 132232 | GN-29245 | Linux Agent | Linux Agent periodically creates gnupdate zombie processes Linux Agent, growing issues | 6.0.22 |
| 132145 | GN-29185 | Center | A problem where policy changes due to node reservation tag assignment are not reflected in the sensor | 5.0.21, 6.0.0 |
| 132142 | GN-29159 | Center | A problem where the user authentication expiration processing scheduler does not work properly due to NTP changes during process operation | 4.0.143, 5.0.40, 6.0.0 |
| 131997 | GN-29180 | Center | An issue where ES index cannot be cleaned up due to an error that determines the execution result of a system command as a failure even if it is successful | |
| 131986 | GN-29225 | Authsync | A problem where setting the initial fixed password value does not work when using the REST API Server synchronization type | 5.0.38 |
| 131647 | GN-29122 | | An issue where duplicate nodes occur intermittently due to not being able to read the node ID during macOS updates | 5.0.9, 6.0.0 |
| 131513 | GN-29033 | WebUI | A problem where all logs can be checked when exporting audit logs when the administrator's management scope (management sensor) is limited | 5.0.22, 6.0.0 |
| 131392 | GN-29112 | WebUI | An issue where node information cannot be modified on the node detail page | 6.0.29, 5.0.69 |
| 131304 | GN-29065 | Windows Agent | Fix EDR related menu behavior errors in the integrated agent installation environment | 5.0.19, 6.0.0 |
| 130967 | GN-29044 | | External transfer of agent information; an issue where the file path selection option is missing input in the Windows Firewall Control plug-in | 6.0.17, 5.0.57 |
| 130967 | GN-28992 | Authsync | An issue where users created by information synchronization fail to authenticate due to mismatched passwords | 4.0.119, 5.0.17, 6.0.0 |
| 130967 | GN-28959 | Center | A problem where the operating state of a node in the DOWN state is changed to UP and maintained during RADIUS authentication | 5.0.44, 6.0.1 |
| 130967 | GN-28957 | Genian Syncer | An issue where the Genian Syncer download fails when packaging NAC when packaging the R or RC version is a branch | 6.0.29, 5.0.69 |
| 130967 | GN-28915 | Center | [General-purpose OS] Problem with not being able to connect to tls 1.0 and tls 1.1 when connecting to SSL from the httpd web server | 6.0.19, 5.0.59 |
| 130967 | GN-28914 | Sensor | An issue where the sensor is blocked due to the URL Filter function even though the sensor is not in active mode | 6.0.4 |
| 130967 | GN-28889 | | An error that causes the execution URL of the workflow list to be generated incorrectly | 6.0.29 |
| 130967 | GN-28884 | Center | A problem where the center daemon shuts down abnormally when the urlFilter function is enabled without using the ZTNA client | 6.0.4 |
| 130967 | GN-28859 | Authsync | A problem where newly created department information is not output when applying for an IP after synchronizing information | 5.0.19, 6.0.0 |
| 130967 | GN-28827 | Center | [General-purpose OS] Problem with apache service when the management port of the management console is set to 443 | 5.0.42, 6.0.16 |
| 130967 | GN-28760 | WebUI | Fixed an issue where the button UI appeared inconsistent due to missing application of the bottom button style class | 6.0.18 |
| 130967 | GN-28757 | Sensor | A problem where when collecting switch information using SNMP, the information is broken and stored when Hangul is included | 4.0.10, 5.0.0, 6.0.0 |
| 130967 | GN-28628 | Center, IPMGMT | A problem where IP policies are not reflected properly when setting IP policies for nodes registered under the center | 6.0.21, 5.0.61 |

## 23.4.13 Genian ZTNA 6.0.28 Release Notes (2024-11-04)

Last Updated: 2024-12-26

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 130493 | GN-26452 | WebUI | A vulnerability that can modify a user's immutable information | 5.0.0, 6.0.0 | 2.2 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 130387 | GN-28910 | Install Wizard | Improved to allow sensor installation tokens to be entered in the Install Wizard | |
| 130050 | GN-28764 | | Added a token-based mutual authentication feature for cloud sensors | |
| 130050 | GN-28742 | Ubuntu(Debian) | [General-purpose OS] Modified to start/stop MySQL via /etc/init.d/mysqld | |
| 130050 | GN-28683 | Backup | Improved so that when backing up a DB, the MySQL system tables_priv table is also backed up | |
| 130050 | GN-28662 | macOS Agent | macOS antivirus information collection improved to detect ESET Endpoint Antivirus 7.0 | |
| 130050 | GN-28631 | Linux Agent | Linux Agent adds a feature that automatically deletes agents when unable to connect to the center for a specific period of time | |
| 130050 | GN-28614 | WebUI | IP policy settings improved to allow hyphens when entering MAC | |
| 130050 | GN-28567 | Linux Agent | Linux Agent adds token verification function when installing agents | |
| 130050 | GN-28318 | Windows Agent | Change the web browser module used to display HTML from IE to Edge within the agent | |
| 130050 | GN-28296 | WebUI | System > Sensor Management > Create > Guide Window UI Style Unification | |
| 130050 | GN-28266 | macOS Agent | Improved to control model names in all options of the macOS device control plug-in | |
| 130050 | GN-27306 | Windows Agent | Added an SSL certificate verification function for agents to identify and authenticate policy servers | |
| 130050 | GN-27092 | Center, WebUI | Added a feature to enable mutual authentication between policy servers and agents/sensors | |
| 130050 | GN-26561 | WebUI | Vulnerability that exposes ES information in cloud environments | 6.0.15 |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 131513 | GN-29033 | WebUI | A problem where all logs can be checked when exporting audit logs when the administrator's management scope (management sensor) is limited | 5.0.22, 6.0.0 |
| 131413 | GN-29175 | WebUI | An issue where Cloud Policy Server is unable to modify sensor token usage items | 6.0.28, 5.0.68 |
| 131357 | GN-29090 | Windows Agent | Password change via password validation plug-in fails on Windows 11 (24H2) | 5.0.0, 6.0.0 |
| 131260 | GN-29147 | Ubuntu(Debian) | [General-purpose OS] An issue where the management console (Tomcat) cannot run after upgrading an internally set device on a general-purpose OS device for a specific period of time | 6.0.25, 5.0.65 (LTS) |
| 130739 | GN-28874 | Windows Agent | Fix an action execution error when booting the operating system when the PC time changes to the future and is restored after a certain period of time | 5.0.0, 6.0.0 |
| 130649 | GN-28798 | WebUI | An error occurs when updating the JIT Provisioning Additional Information section during SNMP authentication settings | 6.0.16, 5.0.55 (LTS), 5.0.56, 6.0.24, 5.0.64 |
| 130050 | GN-28868 | Linux Agent | A problem where the Linux Agent always tries to connect to the default port (443) even when the Center Port is set | 6.0.3, 5.0.46 |
| 130050 | GN-28857 | Center | A problem where sensor token usage items are enabled on the cloud policy server and can be set | 6.0.28, 5.0.68 |
| 130050 | GN-28836 | WebUI | An issue where node group names cannot be imported when importing node groups | 6.0.16, 5.0.55 (LTS) |
| 130050 | GN-28799 | macOS Agent | An issue where the macOS process behavior verification audit log is displayed in all versions | 5.0.27, 6.0.0 |
| 130050 | GN-28766 | Backup, CLOUD | [Cloud] An issue where restore is not performed normally with backed up NAC data | 5.0.37, 6.0.1 |
| 130050 | GN-28759 | Ubuntu(Debian) | [General-purpose OS] An issue where the latest agent update is not possible because the agent package is not copied when running | 6.0.16, 5.0.55 (LTS) |
| 130050 | GN-28755 | | A hidden error occurred in the collector tab when selecting cloud provider from the site's basic information and then changing it back to unset | 6.0.23 |
| 130050 | GN-28753 | | Linux Agent, an issue where certain network information cannot be collected in environments that do not use gnome shell | 5.0.41, 6.0.0 |
| 130050 | GN-28749 | Authsync, Center | [General-purpose OS] An issue where the authsync process terminates abnormally because the driver lib path cannot be found when linking DB2 information synchronization | 5.0.42, 6.0.0 |
| 130050 | GN-28735 | WebUI | Intermittent errors where the audit log cannot be retrieved after the product is running | 5.0.24, 6.0.0 |
| 130050 | GN-28710 | | An XSS false positive occurs when clicking Authenticated User (Authenticated User) in the switch management list if the link contains a colon (:) character in the returnURL | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 130050 | GN-28697 | | A problem where the date selection window (calendar) overlaps with the tab in node details and is output | 5.0.22, 6.0.4 |
| 130050 | GN-28685 | dbmigration | When using /disk/sys/conf/my.cnf, the DB migration fails and the department code is not hashed | 6.0.18, 5.0.58 |
| 130050 | GN-28537 | WebUI | A problem where the IP policy additional field item is not displayed in the IP policy on the node detail screen when applying the IP policy sensor band is on | 6.0.27, 5.0.67 |

### 23.4.14 Genian ZTNA 6.0.27 Release Notes (2024-10-07)

Last Updated: 2024-11-29

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 129272 | GN-23501 | | Change REST API calls to be made only through the management console port (8443) | | |

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 129272 | GN-28593 | Center | Improved so that an audit record is saved when the state of a node with an agent installed outside of the management band is changed | |
| 129272 | GN-28586 | macOS Agent | Improved to always display the macOS agent authentication window plug-in at the top level | 5.0.15, 6.0.0 |
| 129272 | GN-28563 | | Improved node group condition settings to include the parent department when selecting a user department | |
| 129272 | GN-28530 | Linux Agent | Linux Agent adds a pop-up function for expiration and pre-expiration notifications (user accounts, user authentication, passwords, etc.) | |
| 129272 | GN-28520 | Center, Database | Add to periodically store the maximum usage of the number of licensed devices | |
| 129272 | GN-28407 | WebUI | Improved so that the currently connected IP can be known when setting a common allowed IP in the management console | |
| 129272 | GN-28299 | Linux Agent | Linux Agent, gncli ID and password retrieval function added | |
| 129272 | GN-27188 | WebUI | Fixed an issue where Slowquery occurred when there was a lot of software information and the UI was not output | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 130875 | GN-28991 | Center | The problem of not being able to assign a user IP when using a site user static IP | 6.0.14 |
| 130514 | GN-28843 | dbmigration | An issue where the SNMP Agent setting USERNAME value is not normal after migration | 6.0.25, 5.0.65 (LTS) |
| 130397 | GN-28969 | Center, Sensor | [General-purpose OS] An issue where an updated library path cannot be found and a reference error occurs | 6.0.16, 5.0.55 (LTS) |
| 129272 | GN-28648 | | An issue where the control policy list on the node detail screen does not appear when a control policy corresponding to the regulation is assigned | 6.0.22 |
| 129272 | GN-28642 | WebUI | Problem when viewing site information without Cloud Provider set in the system site list | 6.0.23 |
| 129272 | GN-28594 | | A problem where department information is not sorted by default in the UI in the output sorting order when synchronizing department information | 5.0.35, 6.0.0 |
| 129272 | GN-28585 | procmond, Ubuntu(Debian) | [General-purpose OS] Modified so that procmond can be terminated via the /etc/init.d/procmon stop command | 5.0.29, 6.0.0 |
| 129272 | GN-28513 | WebUI | A problem where related nodes are not retrieved when clicking on the number of authentication nodes when the user ID starts with 'and' or 'or' on the list screen of user management | 6.0.17, 5.0.57 |
| 129272 | GN-28503 | WebUI | An issue where a 'Please enter verification code' message is displayed when trying to log in to the management console twice with a CSM account | 6.0.0, 5.0.45 |
| 129272 | GN-28255 | | An issue where the resource bundle ID is output in the audit log when modifying permission settings in the control policy | 4.0.157, 6.0.18, 5.0.58 |
| 129272 | GN-28028 | WebUI | Symptoms of collision protection not being set when approval after applying for equipment changes in the IP application system | 5.0.42, 5.0.45, 6.0.2 |
| 129272 | GN-27630 | | An issue where node group details are output in duplicate due to menu restrictions in adding new management roles | 5.0.31, 6.0.0 |

## 23.4.15 Genian ZTNA 6.0.25 Release Notes (2024-08-05)

Last Updated: 2024-10-07

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 128050 | GN-28531 | dbmigration | Added the ability to run a dashboard migration script when upgrading from 5.0 to 6.0 | 6.0.20 |
| 128050 | GN-28346 | | Image resizing issue when adding cwp2 custom button images | 5.0.0, 6.0.0 |
| 128050 | GN-28328 | WebUI | Reduced the number of devices in the free version from the global version (Community version) | |
| 128050 | GN-28311 | WebUI | REST API - Improved so that setting values are automatically entered using IdP's Metadata when setting up SAML IdP | |
| 128050 | GN-28305 | | Add a code sign so that the vaccine does not detect the agent configuration file as malware | |
| 128050 | GN-28300 | Center | Improved so that N host names can be entered as host names in node group conditions | |
| 128050 | GN-28298 | WebUI | Improved to encrypt parameters sent when logging in to the management console | |
| 128050 | GN-28289 | WebUI | Improved to prevent false positives with XSS for strings used as reserved words in NAC, such as ⓐ NETALL and ⓐ TEMP | |
| 128050 | GN-28268 | Database | Improved so that node groups can be configured with operating system names collected through Agentless WMI | |
| 128050 | GN-28251 | Authsync | Fixed an issue where synchronization failed due to exceeding the maximum membership string length (4096) when synchronizing AD information | 5.0.41, 6.0.0 |
| 128050 | GN-28086 | WebUI | Improved functionality so that when clicking on Site Assignment in Cloud Security Group Policy, the site is displayed depending on whether the security group is used or not | |
| 128050 | GN-27692 | | Improved the nodes/control policy list REST API to output the number of nodes to which policies have been applied | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 129214 | GN-28780 | | Agent using multiple deployment servers: An issue where sensor preferences are not changed when On is set | 6.0.23, 5.0.63 |
| 129146 | GN-28747 | | A problem where part of the item is missing when delivering the device group item on the device usage application form | 4.0.0, 5.0.0, 6.0.0 |
| 129137 | GN-28701 | dbmigration | An issue where SNMP Agent settings are not normal due to migration errors | 6.0.17, 5.0.57 |
| 129023 | GN-28712 | WebUI | An issue where the "Connection Method" pie (Pie) chart graph appears incorrectly in the dashboard widget | 6.0.0 |
| 128987 | GN-28695 | Sensor | A problem where the upgrade is treated as a success even if the upgrade fails due to a timeout when upgrading a sensor | 5.0.42 |
| 128968 | GN-28704 | | When copying a node group, an error message is displayed even if the ID name to be copied is entered | 6.0.25 |
| 128937 | GN-28708 | Ubuntu(Debian) | [General-purpose OS] An issue where the operating system update fails when connecting via NAC | 5.0.23, 6.0.0 |
| 128789 | GN-28548 | macOS Agent | macOS agent fails to authenticate through the authentication window after recovering integrity damage | 5.0.27, 6.0.0 |
| 128758 | GN-28667 | | An issue where nodes are not discovered by IP in Inline sensor monitoring mode | 5.0.37 |
| 128748 | GN-28651 | Sensor | A problem where the sensor process terminates abnormally when using the real-time detection function for host name changes | 4.0.114, 5.0.11 |
| 128050 | GN-28526 | RADIUSD | [RADIUSD] Issue with querying the wrong domain during AD authentication | 5.0.35 |
| 128050 | GN-28502 | Windows Agent | Problem of missing removal items when searching for astrick '*' through program removal plug-in | 5.0.22, 6.0.0 |
| 128050 | GN-28494 | WebUI | CWP design template preview error when changing the HTTPS port in the management console | 5.0.42, 5.0.50, 6.0.12, 5.0.53 |
| 128050 | GN-28461 | WebUI | Site list output error when clicking Site Assignment in Cloud Security Group Policy | 6.0.25 |
| 128050 | GN-28424 | | A problem where the site name in system management cannot be created/modified if the site name contains spaces | 6.0.19 |
| 128050 | GN-28342 | WebUI | An issue where traffic-related items are not displayed on the node list screen | 5.0.50, 6.0.11 |
| 128050 | GN-28303 | WebUI | A problem where the back button is displayed on the detailed screen that appears when clicking on the operation status chart of node management | 6.0.19 |
| 128050 | GN-28262 | GenianOS, Sensor | [GNOS] Problem when setting up SNMP Agent, sysObjectID is empty | 4.1.M8, 5.0.0, 6.0.0 |
| 128050 | GN-28165 | | A problem where the approval status changes to completed when an approval error occurs when applying for a new IP due to automatic approval | 4.1.4, 5.0.0, 6.0.0 |
| 128050 | GN-28080 | Center | A problem caused by the NAS-Port value and NAS-Port-ID value in the RADIUS audit record being reversed | 5.0.35 |
| 128050 | GN-27865 | WebUI | The tool that performs an Elasticsearch query and outputs a file has been improved to work with the latest version | 5.0.23 |
| 128050 | GN-27577 | WebUI | A problem where the tree menu is displayed in duplicate when clicking on the quantity link of a wireless LAN or user group | 6.0.19 |
| 128050 | GN-27436 | macOS Agent | An issue where the Mac settings window closes when controlling the macOS screensaver | 5.0.50, 6.0.9 |

### 23.4.16 Genian ZTNA 6.0.24 Release Notes (2024-07-01)

Last Updated: 2024-08-05

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 128412 | GN-28619 | Database | After upgrading to MySQL 8.0, change the default value of binlog from on to off | 6.0.18, 5.0.58 |
| 127367 | GN-28264 | Windows Agent | Wireless Connection Manager (WCM) 4 version cleaning function added after upgrading | |
| 127367 | GN-28256 | WebUI | Improved to enter the current password when changing the administrator's own password | |
| 127367 | GN-28253 | macOS Agent | macOS ZTNA login failure message segmentation | |
| 127367 | GN-28179 | Center | Add a node group condition that uses the motherboard serial number in system information | |
| 127367 | GN-28177 | WebUI | Improved so that the management console Locale can be set in the Top menu area | |
| 127367 | GN-28170 | WebUI | Fixed an issue where the calendar location of the period selection (window) was displayed incorrectly on the tag settings pop-up screen | |
| 127367 | GN-28163 | macOS Agent | Improved to be able to run scripts in the macOS file distribution plug-in | |
| 127367 | GN-28146 | WebUI | Uniform warning message output style | |
| 127367 | GN-28135 | Windows Agent | Network connection speed improvement with ZTNA Connection Manager | |
| 127367 | GN-28033 | Linux Agent | Linux Agent adds two-step authentication in ZTNA connections via gncli command | |
| 127367 | GN-28032 | Linux Agent | Linux Agent, OSID addition task | |
| 127367 | GN-28007 | Linux Agent | Linux Agent, when a user fails to log in, adds a lock function and improves the resulting message | |
| 127367 | GN-27998 | macOS Agent | Added Apex One and Bitdefender data collection features to the macOS Agent antivirus data collection plug-in | |
| 127367 | GN-27975 | Windows Agent | Provides authentication information integration function for PassNinX solutions | |
| 127367 | GN-27907 | | You can check the license agreement item (EULA) in the system management license. | |
| 127367 | GN-27862 | GenianOS | A problem where important information is displayed because there is no secret key setting in the syscollect archive | |
| 127367 | GN-27698 | WebUI | Replace the javascript library with the latest version where the vulnerability was detected | |
| 127367 | GN-27552 | WebUI | Improved so that when setting up a SAML IdP, settings are automatically entered using IdP's Metadata | |
| 126780 | GN-28021 | WebUI | Improved so that the paper size can be set when exporting dashboard reports | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 128637 | GN-28639 | Center | An issue where the agent plug-in cannot be uploaded to the VC directory due to insufficient permissions in the center | 6.0.24, 5.0.64 |
| 128601 | GN-28663 | CLOUD | The problem with Cloud NAC tomcat not running | 6.0.22, 5.0.62 |
| 128470 | GN-28611 | | A problem where events related to the change policy are not sent properly when the control policy is included when the change policy is applied | 5.0.42, 5.0.44, 6.0.1 |
| 128428 | GN-28618 | Center | An issue where updated policy information cannot be delivered due to a TIMEZONE processing error | 6.0.17, 5.0.57 |
| 128369 | GN-28587 | Windows Agent | A problem with connecting to past authentication information when authenticating the wireless connection manager MSCHAPv2 with a local system account | 4.0.5, 5.0.0, 6.0.0 |
| 128320 | GN-28600 | Windows Agent | A problem with connecting to past authentication information when authenticating GTC as a wireless connection manager | 6.0.10, 5.0.51 |
| 128252 | GN-28591 | WebUI | An issue where the collector does not work after registering on the Azure site | 6.0.20 |
| 128243 | GN-28440 | Ubuntu(Debian) | [General-purpose OS] Problem of not being able to install Ubuntu NAC on the cloud (aws, azure) | 5.0.42 |
| 128184 | GN-28570 | Center | [General-purpose OS] Unable to upload files from WebUI due to directory permission changes | 6.0.22, 5.0.62 |
| 128170 | GN-28557 | Center, WebUI | A problem where the MAC/IP blocking state is maintained when collision protection/change prevention is set on the MAC/IP blocking node | 6.0.21, 5.0.61 |
| 128037 | GN-28410 | | A problem where all logs can be checked in the real-time mode of the audit log when the administrator's management scope (management sensor) is limited | 5.0.45, 6.0.2 |
| 128003 | GN-28571 | Center | An issue where the agent is not installed on a node in the sensor band where the proxy service is set | 6.0.23, 5.0.63 |
| 127963 | GN-28521 | Center, Sensor | An issue where the dnsmasq daemon CPU is 100% used when there is no CLI name-server setting in ON-prem CT64/SS64 | 6.0.23, 5.0.63 |
| 127633 | GN-28478 | CLOUD | [CLOUD] An issue where information synchronization fails due to gndbserver changes due to a MySQL version upgrade | 5.0.0 |
| 127538 | GN-28389 | Windows Agent | A problem where a password is left in the log when the network connection fails in ZTNA Connection Manager | 6.0.0 |
| 127521 | GN-28422 | WebUI | An issue where the locale (Korean, English, etc.) cannot be changed on the management console login page | 6.0.16, 5.0.55 (LTS), 5.0.56, 6.0.17, 5.0.57 |
| 127367 | GN-28394 | WebUI | An issue where the Node Details Software Information tab is not displayed | 6.0.24 |
| 127367 | GN-28327 | WebUI | A problem where results retrieved from the quick search or node search bar are not processed properly when exported to Excel | 6.0.21, 5.0.61 |
| 127367 | GN-28301 | Center, WebUI | A problem where the block icon is displayed even when the new device is accessed from an IP that has MAC permission set | 4.0.8, 5.0.0, 6.0.0 |
| 127367 | GN-28237 | macOS Agent | Does not connect when trying to connect to ZTNA after disabling sleep mode on macOS | 5.0.13, 6.0.0 |
| 127367 | GN-28201 | WebUI | An issue where the Applications Detail data in the Flow log appears to be broken | |
| 127367 | GN-28157 | Windows Agent | Display an empty value in the 'Automatic Update' field due to collecting incorrect update settings through the operating system information collection plug-in | 5.0.0, 6.0.0 |
| 127367 | GN- | WebUI | A problem where an approval completion email is sent in du- | 5.0.42, 6.0.0 |

### 23.4.17 Genian ZTNA 6.0.23 Release Notes (2024-06-03)

Last Updated: 2024-06-28

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 127494 | GN-26117 | macOS Agent | macOS ZTNA Agent minimum supported OS upgrade | 6.0.0 |
| 127308 | GN-28368 | macOS Agent | macOS agent supports newly released macOS 15 (codename Sequoia) | 5.0.0, 6.0.0 |
| 126762 | GN-28150 | Center | When uploading an agent package (zip, gpf) from the center, the signature verification method was changed from RSA to RSA-PSS | |
| 126762 | GN-28140 | macOS Agent | macOS Agent changes electronic signature algorithm from RSA to RSA-PSS | |
| 126762 | GN-28138 | Linux Agent | Linux Agent changes electronic signature algorithm from RSA to RSA-PSS | |
| 126762 | GN-28137 | Windows Agent | Change the agent electronic signature algorithm from RSA to RSA-PSS | |
| 126762 | GN-28125 | WebUI | Improved to send a change event to the sensor when the self-signed certificate automatic renewal setting in the certificate management menu is changed | |
| 126762 | GN-28100 | WebUI | Enhancements to show UI for required input information for each cloud in Cloud Provider (*) | |
| 126762 | GN-28081 | WebUI | When Cloud Provider is selected in site creation, the screen is displayed depending on whether the collector function is present | |
| 126762 | GN-28023 | WebUI | Improved management console to enable signed requests when requesting SAML authentication | |
| 126762 | GN-28020 | Sensor | Improved so that the sensor device's SSL server certificate can be automatically renewed according to the expire date | |
| 126762 | GN-28002 | CWP | Improved to enable Signed Requests when requesting CWP SAML authentication | |
| 126762 | GN-27996 | WebUI | Tag assignment Change the initial location of the calendar that appears when you click the new UI allocation time | |
| 126762 | GN-27746 | Windows Agent | Improved so that agents can use multiple distribution servers when downloading distribution files | |
| 126762 | GN-27673 | Center | OTP2 level administrator authentication function added using third-party OTP server integration | |
| 126762 | GN-27628 | Center | Improved so that multiple distribution servers can be selected and used when downloading distribution files from the agent | |
| 126762 | GN-27567 | WebUI | Improved so that the IP list is sorted in the matrix view of IP address management when the sensor has an alias IP | |
| 126762 | GN-26639 | Center | An issue where some names are truncated and saved due to the short length of the username field | |
| 126762 | GN-24948 | macOS Agent | Added an external integration plug-in for macOS authentication information | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 127262 | GN-28401 | macOS Agent | An issue where the macOS password validation plugin doesn't work with Sonoma | 6.0.21, 5.0.61 |
| 127204 | GN-28418 | Windows Agent | An issue where the scheduled install/check option is not applied in Windows Update Actions | 5.0.0, 6.0.0 |
| 127159 | GN-28370 | WebUI | An issue where settings are not displayed when clicking Interface Settings in Sensor Management > Sensor Settings > IP Settings | 5.0.42, 6.0.16, 5.0.55 (LTS), 5.0.56, 5.0.57 |
| 127106 | GN-28411 | | An issue where Genian.scr is applied instead of the uploaded scr when controlling the screensaver with the appearance and personalization plug-in. | 6.0.23, 5.0.63 |
| 126839 | GN-28306 | Center, Sensor | A problem where the process runs abnormally because execution results cannot be obtained intermittently when executing system commands | 5.0.42 |
| 126762 | GN-28270 | macOS Agent | macOS agent, agent does not work when installed as an installation file containing a hyphen (-) in the domain name | 5.0.35, 6.0.0 |
| 126762 | GN-28254 | WebUI | An issue where the screen appears to be refreshed every 5 seconds when the audit log search filter is modified | 6.0.20 |
| 126762 | GN-28210 | WebUI | A problem where the DHCP server appears to be off even though it is on in sensor management | 5.0.1 |
| 126762 | GN-28203 | WebUI | An issue where the administrator account node management scope limit is a sensor that includes Alias IP, the application form applied for the Alias IP band is not displayed | 4.0.116, 5.0.13 |
| 126762 | GN-28181 | Authsync | A problem where an audit log of the deletion of departments that do not exist in the data source is left when synchronizing information | 4.0.128, 5.0.25 |
| 126762 | GN-28160 | Linux Agent | Network connection failure problem with Linux Agent and ZTNA Client | |
| 126762 | GN-28122 | Center | An issue where Windows update policies cannot be created after uploading GenianData via Genian Syncer | 6.0.19, 5.0.59 |
| 126762 | GN-28109 | Genian Syncer | An issue where the progress bar is displayed as 60% when the upload to the center is completed with gnSyncer | 4.0.146, 5.0.44, 6.0.1 |
| 126762 | GN-28094 | macOS Agent | An issue where the agent malfunctions when the macOS file distribution plug-in is empty and an action is assigned | 6.0.16, 5.0.55 (LTS), 5.0.56 |
| 126762 | GN-28062 | WebUI | A problem where the session management menu is not visible when menu restrictions are set during the administrator's management role | |
| 126762 | GN-28060 | | A problem where sensor group targets are searched in full when searching in the search bar of the node list | 5.0.42, 6.0.0 |
| 126762 | GN-28035 | WebUI | Error where correction choices are not preserved on the Auditor Manager's dashboard/log screen | |
| 126762 | GN-28000 | WebUI | An issue where the image appears broken in the status group section on the Policy > Group > Node screen | 6.0.0 |
| 126762 | GN-27977 | Sensor | [DKNS/Universal OS Sensor] A problem where connections may be blocked due to FQDN assigned to terminal permissions when using FQDN objects | 5.0.27 |
| 126762 | GN-27965 | WebUI | Differences in the position of the X button in the modal window and the unification of the effects (hovers) that occur when the button mouse is raised | |
| 125997 | GN-28047 | Sensor | [General-purpose OS] An issue where the snmp daemon does not work on the sensor | 6.0.15, 5.0.55 (LTS) |

## 23.4.18 Genian ZTNA 6.0.22 Release Notes (2024-05-07)

Last Updated: 2024-06-03

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 126175 | GN-26723 | WebUI | Vulnerability fixes that are not immediately reflected when the administrator's rights are changed | | 3.3 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 126175 | GN-28061 | WebUI | Improved so that Markdown can also be applied to the IP application system notice text | |
| 126175 | GN-28012 | gnlogin | CLI - Improved to sort the results of the show backup command by date | |
| 126175 | GN-27995 | WebUI | Change the CWP SAML settings UI user creation or update term to JIT provisioning | |
| 126175 | GN-27985 | Genian Syncer | Improved to obtain a list of files not displayed on the policy server from GeniansInker | |
| 126175 | GN-27979 | WebUI | Create SBOM using CyclondeDX and SPDX | |
| 126175 | GN-27978 | CWP | Single Logout (SLO) function added when linking CWP SAML authentication | |
| 126175 | GN-27952 | WebUI | Improved so that the time zone can be freely set as an audit log search condition | |
| 126175 | GN-27931 | WebUI | Added copy function for readonly items when setting up SAML IdP | |
| 126175 | GN-27916 | Linux Agent | Linux Agent, gncli log function added | |
| 126175 | GN-27887 | | Linux Agent, gncli Agent deletion function added | |
| 126175 | GN-27872 | WebUI | Improved functionality so that users can also check the results on the application processing results screen of the IP application system | |
| 126175 | GN-27849 | WebUI | Change the default logo to Genian ZTNA V6.0 SP1 | |
| 126175 | GN-27846 | WebUI | Improved to leave an audit log of authentication failures and authentication failures when an attempt to reuse authentication information is detected | |
| 126175 | GN-27842 | Windows Agent | Windows Agent modernizes data encryption methods | |
| 126175 | GN-27821 | | Linux Agent, resource bundle work for gncli multi-language support (en, ko) | |
| 126175 | GN-27813 | macOS Agent | macOS Agent modernizes data encryption methods | |
| 126175 | GN-27800 | WebUI | A problem where authentication can be retried by changing the IP when the number of password authentication failures is exceeded | |
| 126175 | GN-27793 | WebUI | Improved to force access when the same user's session exists during SAML authentication in the management console | |
| 126175 | GN-27771 | WebUI | Improved functionality to add Azure Cloud to ZTNA Gateway | |
| 126175 | GN-27766 | Linux Agent | Linux Agent modernizes data encryption methods | |
| 126175 | GN-27744 | WebUI | Improved so that EULA is printed differently depending on domestic/global | |
| 126175 | GN-27690 | Windows Agent | Edge and Chrome security options extended to web browser option control plug-ins | |
| 126175 | GN-27683 | Linux Agent | Linux Agent adds gncli autocomplete feature | |
| 126175 | GN-27644 | macOS Agent | Added an SSL certificate verification function for macOS agents to identify and authenticate policy servers | |
| 126175 | GN-27643 | Linux Agent | Added SSL certificate verification function for identification and authentication of Linux agents and policy servers | |
| 126175 | GN-27539 | WebUI | Added SAML authentication linked Single Logout (SLO) function to the management console | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 126732 | GN-28295 | Center | An issue where the entire audit log is deleted when the connection to the policy server database fails | 4.1.3 |
| 126677 | GN-28288 | WebUI | An issue where some types of node names (sensor names) cannot be modified | 6.0.21 |
| 126657 | GN-28274 | WebUI | MAC is allowed when using the IP policy sensor band - A problem where MAC policy is not reflected when the node has prohibited changes | 6.0.21, 5.0.61 |
| 126530 | GN-27955 | | An issue where policies are not applied to HA slave devices | 5.0.42, 4.0.156, 6.0.16 |
| 126505 | GN-28265 | Sensor | An issue where SNMP information from an external NAC device cannot be obtained even though the SNMP agent function is set | 5.0.57 |
| 126466 | GN-28271 | | An issue where when updating the agent from version 4 to the new (5.6) version, the installation token input dialog box is displayed and the update does not work automatically | 6.0.22, 5.0.62 |
| 126396 | GN-28228 | Sensor | [General-purpose OS] A problem where the sensor repeats up/down states | 5.0.42 |
| 126330 | GN-28231 | Sensor | An issue where the sensor reboots when using the sensor's DHCP service | 4.0.158, 6.0.19, 5.0.59 |
| 126175 | GN-28174 | Sensor | Failure to collect system information through WMI in an agentless environment (0x80010111) | |
| 126175 | GN-28131 | Center | The problem of not being able to register certificates for the management console and RADIUS external certificates | 5.0.42, 6.0.16 |
| 126175 | GN-28116 | Linux Agent | Linux Agent, an issue where the agent cannot be updated | 6.0.22 |
| 126175 | GN-28097 | Linux Agent | A problem where disconnecting via the tray icon is not reflected in the tray icon when connecting to Linux Agent or ZTNA | 6.0.22 |
| 126175 | GN-28065 | macOS Agent | The wireless LAN control plug-in does not work on macOS Sonoma | 5.0.33, 6.0.0 |
| 126175 | GN-28051 | WebUI | A problem where IP policy related items are output in duplicate in the search bar on the node list screen | 6.0.21, 5.0.61 |
| 126175 | GN-28029 | Sensor | [General-purpose OS] A problem where synchronization is not performed on the slave policy server and distribution server | 6.0.21, 5.0.61 |
| 126175 | GN-28017 | Windows Agent | Hardware data collection plug-in fails to collect information for hard disks larger than 4 TB | 5.0.0, 6.0.0 |
| 126175 | GN-27999 | Windows Agent | An issue where the appearance and personalization plug-in does not have a screen saver set but is incorrectly reported as “used” | 4.0.158, 6.0.19, 5.0.59 |
| 126175 | GN-27963 | WebUI | An issue where <ol>items marked up with sort list tags aren't displayed as numbers | 6.0.1 |
| 126175 | GN-27947 | Sensor | A problem where failure continuously occurs when the wireless detection mode is running erroneously | 6.0.22 |
| 126175 | GN-27946 | WebUI | An issue where additional information is not displayed in license warning messages | 5.0.22, 6.0.15 |
| 126175 | GN-27939 | WebUI | An issue where the default theme (Green24) of the management console is not applied during a new installation | 6.0.5 |
| 126175 | GN-27934 | CWP | An issue where the CWP authentication page does not display a link to the user registration page | 6.0.18, 5.0.58 |
| 126175 | GN-27908 | WebUI | An issue where the General-Purpose OS Management Console fails to generate a Passkey for administrator authentication | 6.0.7 |
| 126175 | GN-27884 | WebUI | A problem where security question settings are not displayed on the user authentication page in settings | 6.0.19, 5.0.59 |
| 126175 | GN- | CWP | An issue where the user authentication window is displayed | 5.0.42 |

## 23.4.19 Genian ZTNA 6.0.21 Release Notes (2024-04-01)

Last Updated: 2024-05-03

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 125554 | GN-28063 | WebUI | A problem where blind injection is possible in the node management search bar | | 2.2 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 125514 | GN-28027 | WebUI | Improved so that it is acceptable even if the IP of the local host is IPv6 when accessing the administrator login page | |
| 125410 | GN-27711 | RADIUSD | Improved so that a password prompt can be displayed when the user's password is changed on the AD server in a RADIUS and AD authentication integration environment | |
| 125410 | GN-27706 | WebUI | Improved to include the number of failed primary ID/PW login authentication during WEBUI 2-step authentication | |
| 125410 | GN-27697 | Center | Added so that passwords can be sent as ShaXX results when linking webhook authentication | |
| 125410 | GN-27499 | Windows Agent | Edit the description of allowed wireless LAN settings in the wireless LAN control plug-in | |
| 125410 | GN-27335 | Center | Improved so that if the IP of the terminal is included in the calling-station-id of the 802.1x account packet, it is treated as a Framed IP | |
| 125410 | GN-27294 | IPMGMT, Sensor | Improved so that IP policies can be created for each sensor | |
| 125410 | GN-26663 | macOS Agent | macOS password validation plugin added | |
| 125410 | GN-26589 | WebUI | Improved so that an unchangeable notification message is displayed on general-purpose OS and cloud devices where the CLI password cannot be changed | |
| 125410 | GN-25876 | WebUI | Add an audit log when an administrator fails two-step authentication | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 126131 | GN-28172 | | An issue where the node information item on the node detail page cannot be modified | 6.0.19 |
| 126038 | GN-28036 | WebUI | When logging out by clicking the Logout button at the top of the Administration Console, "The administrator logs out." Problems that do not leave an audit log | 5.0.42, 4.0.156, 6.0.16, 5.0.55 (LTS), 5.0.56 |
| 125997 | GN-28047 | Sensor | [General-purpose OS] An issue where the snmp daemon does not work on the sensor | 6.0.15, 5.0.55 (LTS) |
| 125634 | GN-28024 | Center, Sensor | A problem where ZTNA Client does not work when setting up multiple split tunneling networks | 6.0.5 |
| 125410 | GN-28008 | Center, IPMGMT | A problem that leaves an incorrect control policy when the IP policy sensor band application setting is set from ON to OFF | 6.0.21, 5.0.61 |
| 125410 | GN-27954 | Center | An issue where multiple nodes with the same IP/MAC are created while updating a node's IP with a RADIUS Account packet | 5.0.36 |
| 125410 | GN-27944 | WebUI | An issue where the tag UI is applied differently on the node detail screen | 6.0.20 |
| 125410 | GN-27911 | WebUI | An issue where the Subnet support option malfunctions in the IP settings to allow access in the management console | 6.0.21, 5.0.61 |
| 125410 | GN-27895 | Windows Agent | A problem where programs registered in the external authentication integration plug-in continue to run. | 6.0.18, 5.0.58 |
| 125410 | GN-27894 | Center | A problem where the new node host name restriction function does not work properly | 6.0.21, 5.0.61 |
| 125410 | GN-27848 | GNOS, Sensor | [GNOS] A problem where the syslog service on the sensor device is opened externally and works | |
| 125410 | GN-27808 | Center | An issue where unnecessary logs are left when the VPN function is turned off/on while the VPN connection fails | 5.0.42, 6.0.0 |
| 125410 | GN-27797 | WebUI | When an IP policy is applied as a sensor band, multiple IP searches are output in quick searches, etc. | 6.0.21, 5.0.61 |
| 125410 | GN-27733 | WebUI | A problem where the node list and the last operation time on the node detail screen do not match | 6.0.16, 5.0.55 (LTS) |
| 125410 | GN-27660 | Windows Agent | An issue where I-Sign+ (I-Sign+) cannot link authentication with the 'Penta SSO Alternative Authentication' plug-in even when logged in. | 5.0.51, 4.0.153, 6.0.11 |
| 125410 | GN-27657 | WebUI | An issue where the Excel file exported from the audit log does not open properly in Windows Excel | 6.0.11 |
| 125410 | GN-27494 | WebUI | Admin confirmation window and batch order correction window selection notifications, margins, and button UI modifications | 6.0.18 |
| 125410 | GN-27331 | WebUI | Fixed the pagination part alignment error in the list page header area and the select menu to be consistent | 6.0.5 |
| 125099 | GN-27993 | Sensor | [General-purpose OS] A problem where the DNS cache function cannot be turned off because the maximum DNS cache number setting in System > Preferences is not applied | 6.0.12, 5.0.53 |

## 23.4.20 Genian ZTNA 6.0.20 Release Notes (2024-03-04)

Last Updated: 2024-04-01

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 125406 | GN-27107 | WebUI | Service disabled by executing a Tomcat restart command by an unauthorized administrator | 5.0.41 | 2.7 |

## New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 125148 | GN-27973 | Center, macOS Agent, Sensor, Windows Agent | OpenSSL 3.0.13, 1.1.1w upgrade - excessive resource usage during X.509 policy constraint checking | 4.0.0, 5.0.0, 6.0.0 |
| 124647 | GN-27699 | WebUI | Improved so that when entering a WEBUI 2-step verification code, it is masked and displayed | |
| 124647 | GN-27694 | WebUI | Improved so that only xxx.xxx.xxx.1 to 254 is possible when setting the WEBUI management connection IP | |
| 124647 | GN-27651 | macOS Agent | Development of a macOS off-line log (audit record) transmission function | |
| 124647 | GN-27645 | Center, Sensor | Improved so that server connection timeout time can be set during FTP/SFTP backup | |
| 124647 | GN-27626 | Center, procmond | Improved the process inspection daemon (procmond) to make the center daemon SOAP API HealthCheck | |
| 124647 | GN-27620 | Center, Sensor | Improved so that a timeout can be set when downloading a file | 5.0.42, 6.0.3 |
| 124647 | GN-27551 | WebUI | New login page button UI improvements | |
| 124647 | GN-27544 | WebUI | Change the error message that is displayed when a timeout occurs on the new login page | |
| 124647 | GN-27537 | VRRPD | Improved to enable HA through VRRP Unicast mode in environments where multicast packet operation is not possible | |
| 124647 | GN-27524 | macOS Agent | Save debugging information to analyze the cause of the macOS agent's abnormal shutdown | |
| 124647 | GN-27518 | WebUI | JIT provisioning function support when linking the management console with SAML authentication | |
| 124647 | GN-27501 | Center, Sensor | Improved function so that nodes are registered as IP when using sensor inline mode | |
| 124647 | GN-27487 | Center, Sensor | Application domain regular expression/httpMethod condition added | |
| 124647 | GN-27450 | Linux Agent | Linux Agent, program removal plug-in development | |
| 124647 | GN-27444 | Center, gnlogin | Improved so that backup files can be restored on the Docker Compose policy server | |
| 124647 | GN-27441 | WebUI | Improved the File Upload API to provide a response to the file if it is a Cert file | |
| 124647 | GN-27372 | WebUI | Improved structure for retrieving the number of applied nodes in the node group list | |
| 124647 | GN-27065 | Center | Add an audit log when verification of the authentication code fails and add by information when the password is modified | |
| 124647 | GN-26946 | WebUI | Add Azure Collector | |
| 124647 | GN-26937 | Linux Agent | Linux Agent adds a feature to separate logs for individual actions | |
| 124647 | GN-26877 | Center | Added the ability to use macros in nodegroup conditions | |
| 124647 | GN-26847 | WebUI | Enhanced description of CWP Settings > Confirm button URL | |
| 124647 | GN-26595 | WebUI | Warning message output including the number of nodes applied when the policy was modified | |
| 124647 | GN-26182 | Linux Agent | Linux Agent, program information, and agent deletion UI developed with ZTNA's new UI design | |
| 124647 | GN-25587 | WebUI | App development to migrate the administrator's dashboard to match the new dashboard when upgrading from 5.0 to 6.0 | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 125366 | GN-27983 | Center | An issue where event packets sent from the 5.0/6.0 policy server are not handled by the 4.0.1 sensor | 5.0.42, 6.0.16 |
| 125348 | GN-27968 | WebUI | An issue where certificate-related uploads cannot be saved or modified in Certificate Management Settings | 6.0.19, 5.0.59 |
| 125291 | GN-27972 | | An issue where an SSL certificate is generated with an expiration date of 10 years | 6.0.15, 5.0.55 (LTS) |
| 125275 | GN-28003 | Windows Agent | A problem where the distribution file verification method is Sigstore Keyless Signing in the file distribution plug-in V2 fails | 5.0.42, 4.0.155, 6.0.15, 5.0.56 |
| 125238 | GN-28009 | WebUI | A problem where input is not possible if the last value is 0 when entering, such as 255.255.255.0 in the subnet mask input UI | 6.0.20 |
| 125166 | GN-27994 | Linux Agent | Linux Agent A problem where the distribution file verification method is Sigstore Keyless Signing in the file distribution plug-in V2 fails | 5.0.50, 5.0.53, 5.0.54, 6.0.15 |
| 125157 | GN-28005 | macOS Agent | A problem in macOS file distribution plug-in V2 that fails when the distribution file verification method is Sigstore Keyless Signing | 6.0.16, 5.0.55 (LTS), 5.0.56 |
| 125043 | GN-27986 | GenianOS | Addressing compatibility issues due to SLSA TUF certificate renewals | 5.0.42, 5.0.50, 6.0.15, 4.0.156 |
| 125040 | GN-27989 | Genian Syncer | An issue where integrity verification fails when syncing GenianData with GenianSinker | 4.0.156, 6.0.16, 5.0.55 (LTS) |
| 124918 | GN-27958 | WebUI | A problem where an error warning occurs in the audit log because the file referenced in the frontend page does not exist | 6.0.20 |
| 124895 | GN-27932 | Center | Improved load issues caused by large Keep Alive debug logs when upgrading or rebooting the center | 6.0.19, 5.0.59 |
| 124880 | GN-27904 | MySQL | A problem where MySQL 8.0 fails to run on SSD-enabled devices | 6.0.18, 5.0.58 |
| 124870 | GN-27936 | RADIUSD | The problem of not being able to connect due to authentication failure when connecting wired/wireless to TLS 1.0 after upgrading the Radius daemon | 6.0.19, 5.0.59 |
| 124825 | GN-27933 | WebUI | An issue where each setting is not possible when the tag is removed from the tag settings pop-up | 6.0.20 |
| 124647 | GN-27726 | WebUI | An issue where the service cannot be used when accessing an invalid path from the new login page | 6.0.19 |
| 124647 | GN-27722 | macOS Agent | An issue where the blocking policy ID is displayed incorrectly in the log when blocking a macOS device | 6.0.3, 5.0.46 |
| 124647 | GN-27709 | Windows Agent | A problem where a "real-time test" is reported as not working when performing an engine update for a newly identified vaccine | 6.0.19, 5.0.59 |
| 124647 | GN-27682 | Linux Agent | An issue where some UI characters are not visible in Linux Agent or System Dark mode | 6.0.17 |

continues on next page

Table 9 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 124647 | GN-27664 | WebUI | A problem where the DHCP pool usage status is output from only one sensor in the IP management sensor list | 5.0.42 |
| 124647 | GN-27632 | WebUI | Multilingual input device output issue when the management console language you are logged in to is not included in CWP supported languages | 5.0.31 |
| 124647 | GN-27622 | Sensor | An issue where earlyrole matching of permission policies does not work properly | 6.0.7 |
| 124647 | GN-27617 | Windows Agent | An issue where an AD account is locked due to an operating system information collection action to check whether an empty password is used on the AD server | 4.0.109, 5.0.6, 6.0.0 |
| 124647 | GN-27579 | CWP | Node Policy > A problem where the CWP user information confirmation screen does not work properly when the password usage option is turned off | 4.0.M8 |
| 124647 | GN-27576 | WebUI | An error where the nodegroup filter settings pop-up area leaves the screen | 5.0.31, 6.0.0 |
| 124647 | GN-27571 | WebUI | A phenomenon where the corresponding view item is increased when a new node view is created and used as an administrator with limited node views | 5.0.42 |
| 124647 | GN-27569 | WebUI | An issue where some dialog styles are displayed on the dashboard screen are different | 6.0.15 |
| 124647 | GN-27566 | WebUI | Fixed an issue where the agent OS icon was incorrect | 4.1.M5 |
| 124647 | GN-27543 | WebUI | Fixed an issue where an error occurred when using the CONF Update API | 5.0.20 |
| 124647 | GN-27536 | dbmigration | An issue where values are incorrectly converted when migrating data in registry settings | 6.0.5, 5.0.48 |
| 124647 | GN-27522 | WebUI | A problem where the name of the changed plug-in is not output when the policy is applied after changing the node action's plug-in | 5.0.45, 6.0.2 |
| 124647 | GN-27520 | WebUI | A problem where data is present when outputting a detailed CVE screen, but it is output on a blank screen | 5.0.50, 6.0.12, 5.0.53 |
| 124647 | GN-27498 | Windows Agent | An issue where the plug-in does not work according to the authentication status action check conditions | 5.0.0, 6.0.0 |
| 124647 | GN-27362 | WebUI | A problem where additional fields in the user and IP application form appear in a normal field format even when specified as a password form | 5.0.34 |
| 124647 | GN-27328 | Elastic-Search, WebUI | Added methods removed from Elasticsearch Export Utils | 6.0.11 |
| 124647 | GN-26376 | WebUI | The problem that when applying for general use of IP, results are not sent even if processing result reception information is entered on the application form | 5.0.13 |
| 124647 | GN-24361 | | An issue where the hsecmod.sh script does not work on the Cloud Policy Server | 5.0.42 |

## 23.4.21 Genian ZTNA 6.0.19 Release Notes (2024-02-05)

Last Updated: 2024-02-29

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 124617 | GN-27568 | Windows Agent | TLSv1.3 support for wired and wireless connection managers in 802.1x authentication (GTC) | |
| 123976 | GN-27612 | WebUI | Add a read-only option to an additional field in the multiline text input format | |
| 123976 | GN-27602 | WebUI | Add the READONLY option setting to the Add Multiline Input field item | |
| 123976 | GN-27473 | Windows Agent | Improved policy log of actions that are repeated every time a policy is reapplied | |
| 123976 | GN-27465 | macOS Agent | macOS action plugin options UX improvements | |
| 123976 | GN-27456 | WebUI | Reason for approval column added to ipmgmt application results | |
| 123976 | GN-27455 | Windows Agent | Hauri Byrobot API change (VrInfo.dll ver 2023.11.10.0) | |
| 123976 | GN-27447 | Linux Agent | Linux Agent improves software information collection so that software installed via Snap is also collected | |
| 123976 | GN-27374 | macOS Agent | When connecting to macOS ZTNA, if the connection window is lower than other windows, it will appear at the top | |
| 123976 | GN-27364 | Sensor | ZTNA Client TLSv1.3 support | |
| 123976 | GN-27357 | WebUI | Improvements to SAML idp's IP-Port output format and related code cleanup | |
| 123976 | GN-27348 | WebUI | Improved error page output | |
| 123976 | GN-27315 | WebUI | Improved dashboard 'Center/Sensor Equipment Status Status' widget | |
| 123976 | GN-27313 | WebUI | Improved so that it is possible to check even the set conditions in the application management list | |
| 123976 | GN-27260 | Linux Agent | Linux Agent improves electronic signatures so that they can be signed in an executable state | |
| 123976 | GN-27253 | Docker | NAC Docker development environment - Improved to use multiple OS versions of Containers | |
| 123976 | GN-27229 | WebUI | Add a mandatory field mark to the password field on the temporary user IP application form | |
| 123976 | GN-27225 | Windows Agent | Hauri Virobot Security 1.0 vaccine information collection | |
| 123976 | GN-27214 | WebUI | Change the Timezone default value in System Preferences to Browser Timezone | |
| 123976 | GN-27212 | WebUI | Improved so that policy server timezone can be set in cloud environments | |
| 123976 | GN-27199 | WebUI | Add IP/MAC additional fields to quick search criteria | |

continues on next page

Table 10 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 123976 | GN-27197 | Linux Agent | Linux Agent, network shared folder plug-in development | |
| 123976 | GN-27163 | Sensor | Added a function to periodically check whether the sensor daemon is deadlocked | |
| 123976 | GN-27133 | WebUI | Improved the dashboard sensor map so that the color of the marker is distinguished according to the sensor status | |
| 123976 | GN-27109 | macOS Agent | If the ZTNA connection fails after disabling the macOS agent sleep mode, the ZTNA connection window is displayed for reconnecting | |
| 123976 | GN-27108 | macOS Agent | Improved ability to save user connection information in the macOS agent ZTNA | |
| 123976 | GN-26667 | WebUI | Add the ability to apply actions in batches to policies | |
| 123976 | GN-26539 | WebUI | Change the location of the Edit button on the admin detail page | |
| 123976 | GN-26389 | macOS Agent | Network kernel module development for macOS | |
| 123976 | GN-26311 | WebUI | ZTNA new login page development (Frontend) | |
| 123976 | GN-26251 | WebUI | When creating a site, change the site name to only allow usable characters | |
| 123976 | GN-26189 | macOS Agent | macOS agent ZTNA DNS setting function | |
| 123976 | GN-25991 | macOS Agent | Firewall control plug-in for macOS Agent Internet Kill Switch | |
| 123976 | GN-25989 | Kubernetes | K8s Kata container-based DKNS support work | |
| 123976 | GN-25751 | WebUI | Change the search result output format when searching for a user name in IP/equipment owner settings | |
| 123976 | GN-25552 | Linux Agent | Development of user authentication management functions through Linux Agent and CLI | |
| 123976 | GN-25545 | Linux Agent | Linux Agent, device control function added | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 124626 | GN-27857 | WebUI | 504 error occurred during node discovery and quick search | 6.0.19, 5.0.59 |
| 124617 | GN-27464 | Windows Agent | GTC authentication failure Openssl3.0 no wireless connection via wireless connection manager applied to OpenSSL 3.0 (temporary action) | 6.0.19, 5.0.59 |

continues on next page

Table 11 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 124504 | GN-27670 | CWP | An issue where Markdown is not applied to the CWP user authentication component | 5.0.42, 4.0.156, 6.0.16, 5.0.55 (LTS), 5.0.56 |
| 124442 | GN-27769 | WebUI | An issue where some nodes are blocked due to policy application errors after changing the IP policy | 5.0.30, 6.0.0 |
| 124316 | GN-27648 | WebUI | An error occurred when the audit log reported the page. StatusCode=404, problem with 403 Warning logs | 6.0.19, 5.0.59 |
| 124082 | GN-27749 | WebUI | The problem of not being able to access the user information modification page in CWP | 6.0.16, 5.0.55 (LTS), 5.0.56, 6.0.18, 5.0.58 |
| 124025 | GN-27742 | Center | An issue where email delivery fails in Cloud NAC | 6.0.19, 5.0.59 |
| 123976 | GN-27678 | Windows Agent | An issue where the appearance and personalization plug-in is not collecting screen saver information | 5.0.59 |
| 123976 | GN-27623 | WebUI | An issue where the page that redirects when there is no login session is set up incorrectly | 6.0.19 |
| 123976 | GN-27619 | Center | An issue where Ubuntu NAC sensor software cannot be uploaded to GNOS Center | 5.0.42 |
| 123976 | GN-27593 | WebUI | An issue where the OTP guide screen on the new login page appears to be broken | 6.0.19 |
| 123976 | GN-27590 | WebUI | A problem where the vaccine name cannot be directly entered in the node group's vaccine information related conditions | 6.0.6, 5.0.49 |
| 123976 | GN-27580 | CWP | User creation or update is set to off during SAML authentication integration (CWP), but the SAML attribute settings are incorrect. Problems with leaving audit logs | 6.0.17, 5.0.57 |
| 123976 | GN-27572 | Backup | [Universal OS] An issue where the backup file contains an agent zip file, causing the capacity to increase | 5.0.31 |
| 123976 | GN-27521 | ulogd | DKNS > The log file size is increasing because the ULOGD log is not included in logrotate | 6.0.15 |
| 123976 | GN-27514 | Center | A problem where failure logs for some authentication methods are not left according to the order of the authentication methods in the node policy | 5.0.16 |
| 123976 | GN-27508 | Windows Agent | A problem where screensavers set to immediately apply actions to shapes and personalized actions do not work. | 4.1.M8, 5.0.0, 6.0.0 |
| 123976 | GN-27503 | Center, Sensor | Fix issues that occur after modifying the shell command to use it with specified permissions | 6.0.19, 5.0.59 |
| 123976 | GN-27482 | WebUI | An error occurs when copying a wireless LAN group | 4.1.4 |
| 123976 | GN-27458 | Center | An issue where the CLOUD version agent logs are not collected | 5.0.42 |
| 123976 | GN-27445 | Sensor | Problems where the application is not controlled by the URL path | 6.0.14 |

continues on next page

Table 11 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 123976 | GN-27443 | Windows Agent | A problem where the real-time monitoring status of the antivirus is reported as not working when booting the PC | 5.0.0, 6.0.0 |
| 123976 | GN-27442 | WebUI | A problem where the sorting of the last operation time column does not work on the node management list screen | 6.0.16, 5.0.55 (LTS) |
| 123976 | GN-27439 | WebUI | An issue where the administrator's dashboard is not displayed whose ID is not in English | 6.0.0 |
| 123976 | GN-27435 | WebUI | An issue where the Add button in Application Objects > Application Settings is not clicked when the browser size is small | 6.0.11 |
| 123976 | GN-27433 | Sensor | Problems that do not apply when an application object is modified | 6.0.7 |
| 123976 | GN-27429 | Center | The problem of not being able to read license information when using OpenSSL 3.0 | 6.0.19 |
| 123976 | GN-27426 | WebUI | An issue where image selection is not output properly in the ColorPicker component | 6.0.7 |
| 123976 | GN-27420 | WebUI | A problem where a sensor is added to a sensor group with a node management scope limit is not immediately reflected in the manager's tree | 5.0.31 |
| 123976 | GN-27413 | WebUI | An issue where the other language settings are not reflected when only Korean items are modified in the multilingual message component | 4.1.M3, 4.0.17 |
| 123976 | GN-27409 | Sensor | An issue where the Agentless AD SSO function does not work when installing the latest update on the AD server | |
| 123976 | GN-27405 | WebUI | Problems that cannot be corrected after copying the wireless LAN policy | 4.0.8 |
| 123976 | GN-27371 | WebUI | An issue where the same standalone plug-in with no scope of application can be assigned multiple times to a policy | 5.0.43, 6.0.0 |
| 123976 | GN-27308 | ElasticSearch, Ubuntu(Debian) | [General-purpose OS] A problem where a copy of Elasticsearch's nac_nodegrptreesnapshot index occurs when the log server is in single mode | |
| 123976 | GN-27285 | WebUI | A problem where password-type fields cannot be saved if they are empty regardless of the parent option | 6.0.17, 5.0.57 |
| 123976 | GN-27247 | WebUI | An issue where results are not displayed when moving the node list through a link in the WMI collection information widget | 5.0.33 |
| 123976 | GN-27238 | WebUI | An issue where the cloud version ID/password search phrase is unconditionally displayed in the English ID/password search phrase | 5.0.31 |
| 123976 | GN-27236 | WebUI | An issue where the text on the CWP session expiration page is output in the system locale | 5.0.14 |
| 123976 | GN-27227 | WebUI | JavaScript console error log output issue on the management console login page | 6.0.7 |
| 123976 | GN-27220 | Genian Mobile | The problem of not being able to log in to NAC Monitor (mobile) if the password contains'% ' | 6.0.14 |
| 123976 | GN-27218 | Database | "Unknown CODEMAP" Debugging of Policy Server by Operating System Information Gathering Action | 5.0.48, 6.0.6 |
| 123976 | GN-27179 | Sensor | A problem where the sensor does not work properly due to IPM policy reception failure when using DKNS | 5.0.42 |
| 123976 | GN-27173 | Center | A problem where the node's connection device/connection port information is not deleted when the switch is deleted | |

continues on next page

Table 11 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 123976 | GN-27125 | GenianOS | [General-purpose OS] Improved so that services do not run after image upgrades | |
| 123976 | GN-27120 | WebUI | A problem where an assigned item is not displayed in the allocatable list when the assigned item is canceled from the node action assignment in the node policy | 6.0.17, 5.0.57 |
| 123976 | GN-27099 | Sensor | Improved to check the active status of a node when assigning a DHCP IP to a global DHCP environment | |
| 123976 | GN-27080 | WebUI | An issue where the number of nodes in the permission control policy does not match the count in the control policy widget | 6.0.7 |
| 123976 | GN-27064 | Windows Agent | An issue that is controlled only by the previous policy when the device control plug-in version is changed after booting in safe mode | 5.0.0, 6.0.0 |
| 123976 | GN-26900 | Sensor | The problem of assigning the IP being used as a DHCP IP | 4.0.149 |
| 123976 | GN-26559 | WebUI | Improved to match the administrator's time zone when processing the time period setting on the user registration page | 4.1.M4 |
| 123976 | GN-26180 | WebUI | Activate the back button even when no items are selected on the management screen | 6.0.10 |
| 123133 | GN-27496 | Linux Agent | Linux Agent intermittently misses sending some action system information | 5.0.50, 6.0.15 |

## 23.4.22 Genian ZTNA 6.0.18 Release Notes (2023-12-19)

Last Updated: 2024-02-01

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 123781 | GN-26393 | WebUI | Vulnerability where information can be modified by directly entering a URL to an unauthorised page | | 3.1 |
| 123284 | GN-26390 | WebUI | File export permission bypass vulnerability for unauthorized administrators through the Audit Log REST API | | 3.1 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 123464 | GN-27625 | Sensor | Fixed an issue where pubilc IP cannot be imported when changing sensor operation modes and policies | |
| 122922 | GN-25063 | WebUI | 6.0 widget added | |
| 122821 | GN-27491 | WebUI | Improved so that IDP-enabled SSO authentication requests can be authenticated when linking SAML authentication | |

continues on next page

Table 12 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 122708 | GN-27476 | WebUI | Added a divider line to separate SAML login from existing login buttons, and improved login button output when setting multiple IdPs | |
| 122708 | GN-27344 | Center | Improved functionality so that secondary webhook authentication can be linked | |
| 122708 | GN-27320 | WebUI | Improvements to the alarm output when external access is permitted | |
| 122708 | GN-27249 | Linux Agent | Linux Agent modified to display an error message sent from the server when the ZTNA Client connection fails | |
| 122708 | GN-27243 | Authsync | Improved REST API Server-type information synchronization so that paging parameters included in response headers can be used | |
| 122708 | GN-27201 | WebUI | Added an IP/MAC additional field item to change node properties | |
| 122708 | GN-27140 | Sensor | Improved to sign with ZTNA Gateway server certificate center CA | |
| 122708 | GN-27100 | Center | ZTNA client fixed IP allocation failure message delivered to client | |
| 122708 | GN-27090 | Center | An issue where an audit record is not left when ZTNA fixed IP allocation fails | |
| 122708 | GN-27077 | Sensor | Improved exception handling for event socket unconfigured logs when creating an event socket | |
| 122708 | GN-27068 | WebUI | Improved to be able to browse the nodegroup criteria filter list | |
| 122708 | GN-27052 | WebUI | Improved so that an additional path path can be entered when entering Domain on the application definition screen | |
| 122708 | GN-26955 | -Unknown/None- | Improved the sysinspect script to work with the changed ES account when the ES account is changed | |
| 122708 | GN-26942 | WebUI | Fixed an issue where an error log was left when calling the device modification API | |
| 122708 | GN-26929 | Database | Add device information to add/delete 'USB information' audit log | |
| 122708 | GN-26921 | Windows Agent | Development of plug-ins linked to external authentication through agents | |
| 122708 | GN-26913 | Windows Agent | Exosphere vaccine information collection | |
| 122708 | GN-26909 | Zero Trust Security | [ZTNA] Add RADIUS accounting attribute generated when connecting to a client | |
| 122708 | GN-26907 | Center | Improved so that multiple URLs can be set when setting a search filter webhook | |
| 122708 | GN-26889 | Sensor | A problem where traffic information is not output when using ZTNA GW (Global-line) | |
| 122708 | GN-26873 | WebUI | Improved the quick search in the top menu to search for (IP/equipment) owners and ownership departments | |
| 122708 | GN-26860 | WebUI | Function to view process status information in the cloud collector | |
| 122708 | GN-26855 | MySQL | [General-purpose OS] Improved to prevent reuse of MySQL passwords | |

continues on next page

Table 12 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 122708 | GN-26842 | Center | mysqldump execution error when updating CLOUD GPDB | |
| 122708 | GN-26575 | IPMGMT | Disable access when the ipmgmt page function is not used | |
| 122708 | GN-26545 | GenianOS | GNOS kernel version upgrade (5.15.0) | |
| 122708 | GN-26482 | Authsync, Database | When storing department codes, compress them with a hash function to prevent oversize | 5.0.45, 6.0.2 |
| 122708 | GN-26325 | GNOS | Fixed an issue where procmond was executed repeatedly when running httpd-driven scripts | |
| 122708 | GN-26284 | Center | In-product self-signed certificate automatic renewal function | |
| 122708 | GN-26021 | Sensor | Apply URL+pathpattern and userAgent rules when detecting an application using APP DB | |
| 122708 | GN-25674 | WebUI | Errors outside the password rules guide phrase area when changing the ZTNA password | |
| 122708 | GN-25533 | Center | Added a cache deletion option when setting up the proxy service | |
| 104536 | GN-22567 | Database | GNOS MySQL 8.0 upgrade | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 123883 | GN-27681 | WebUI | System > System Management > Image Selection Upgrade Popup Window Error | 6.0.18 |
| 123767 | GN-27674 | MySQL | An issue where the daemon does not run after upgrading to the MySQL 8.0 version image on a device with an SSD | 6.0.18, 5.0.58 |
| 123721 | GN-27652 | Center | A problem where Google OTP authentication cannot be performed because the Google OTP security key issued by the center cannot be sent to the agent | 6.0.13 |
| 123497 | GN-27646 | Authsync | If a MySQL function is used in the user department ID column name of information synchronization, an incorrect policy may be assigned due to a failure in department synchronization | 6.0.18, 5.0.58 |
| 123435 | GN-27641 | WebUI | In the tomcat log, by the following code has not been detected to the pool, no symptoms of connecting to the web console after a large number of cases | 5.0.20 |
| 123340 | GN-27399 | macOS Agent | A problem where plug-ins don't work according to macOS internal/external conditions | 6.0.5, 5.0.48 |
| 123298 | GN-27573 | WebUI | A problem where the list is not displayed when clicking on the number of members in each group in the user group status | 4.0.156, 6.0.16, 5.0.57 |
| 123293 | GN-27401 | Sensor | A problem where the sensor process terminates abnormally when the same event is received from the sensor device | 4.0.64 |

continues on next page

Table 13 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 123291 | GN-27541 | Authsync | A problem where if the connection to the information synchronization server fails, it is treated as a deleted user and all users are deleted | 6.0.9 |
| 123281 | GN-27517 | WebUI | Errors where certain items are not modified in the Nodes REST API | 5.0.8, 4.0.111 |
| 123274 | GN-27550 | WebUI | A problem where tree-structured data components are not output | 6.0.16, 5.0.55 (LTS), 6.0.17, 5.0.57 |
| 123268 | GN-27460 | GenianOS | [General-purpose OS] An issue where aes256 commands are not executed during initial operation | 5.0.42, 6.0.16, 5.0.55 (LTS), 5.0.56 |
| 123266 | GN-26993 | WebUI | Information display error displayed as a tooltip on ip and mac on the audit log and node detailed history management screen | 6.0.4, 5.0.47 |
| 123166 | GN-27519 | Sensor | Symptoms where the sensor system stops due to a deadlock when changing the sensor mode continuously | 5.0.57, 4.0.157, 6.0.19 |
| 123133 | GN-27496 | Linux Agent | Linux Agent intermittently misses sending some action system information | 5.0.50, 6.0.15 |
| 123055 | GN-24708 | Center | In an environment where many sensor debugs are sent to the center, a load may be caused by deleting old debugs when the center is rebooted | 5.0.0 |
| 123046 | GN-27575 | Center | An issue where the log filter action does not work when the ES log filter query result is greater than 2K | 4.1.M6 |
| 122946 | GN-27574 | Center | An issue where ES index (nac-filter) for log filters is deleted during the ES log cleaning cycle | 5.0.50, 6.0.11 |
| 122840 | GN-27561 | Center | [General-purpose OS] An issue where the LDAPsearch command results fail due to the LDAP configuration file being set to the wrong file in the general-purpose OS | 5.0.42 |
| 122708 | GN-27500 | Windows Agent | "Outsider Extension (Registry)"Problems that cannot be decertified when applying the action for the first time | 4.0.0, 5.0.0, 6.0.0 |
| 122708 | GN-27438 | WebUI | An issue where existing tags are removed when adding tags in node details | 6.0.18 |
| 122708 | GN-27424 | WebUI | An issue where the dashboard tag cloud type widget continues to load | 6.0.14 |
| 122708 | GN-27419 | WebUI | An issue where the data area is not output when searching with invalid conditions in the Flow log | 6.0.0 |
| 122708 | GN-27397 | WebUI | Error creating and modifying RADIUS policies with the operator account | 5.0.30 |
| 122708 | GN-27389 | Center, CLOUD | An issue where generic OS sensor upgrades are not performed automatically when upgrading the CLOUD policy server | |
| 122708 | GN-27368 | WebUI | The problem of incorrect aggregation when generating daily reports for each administrator based on the scope of management | 6.0.17, 5.0.57 |
| 122708 | GN-27356 | Sensor | A problem where the cache service does not run even when the patch proxy service is set to ON | 5.0.55 (LTS), 4.0.157 |

continues on next page

Table 13 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 122708 | GN-27321 | WebUI | Node/control policy issues not being fixed | 4.0.157, 6.0.18, 5.0.58 |
| 122708 | GN-27293 | WebUI | An issue where error messages appear in irrelevant locations in the nodegroup filter settings popup | 6.0.14 |
| 122708 | GN-27268 | Sensor | A problem where RADIUS authentication requests are sent to the default gateway even if an interface to communicate with the policy server is specified | 6.0.14 |
| 122708 | GN-27148 | WebUI | An issue where the login failure count is not reset after a successful login when logging in to the management console using secondary authentication | 4.0.10 |
| 122708 | GN-27119 | Windows Agent | A problem where all the name value defined in the URL button in the agent authentication window is not output | 5.0.42, 6.0.0 |
| 122708 | GN-27111 | Authsync | A problem where rank synchronization fails when there is no rank information in the local DB during rank synchronization | 6.0.6, 5.0.49 |
| 122708 | GN-27110 | WebUI | The problem of not being able to authenticate when accessing the application results screen again after modifying the user information on the CWP user registration application result search screen | 5.0.32 |
| 122708 | GN-27059 | WebUI | A problem where tag names can be entered with a space (Space) | 4.0.M7 |
| 122708 | GN-27057 | procmond | An issue where when Tomcat is restarted, the audit log says tomcat9 even though it's not the tomcat9 version | 5.0.53, 6.0.15 |
| 122708 | GN-27048 | WebUI | An issue where the vertical layer area overlaps when entering 3 or more lines on the login screen | 6.0.8 |
| 122708 | GN-27040 | Center | An issue where “unknown” and “no information” date information collected from agents is displayed as “1970-01-01” | |
| 122708 | GN-27017 | ElasticSearch, gnlogin | An issue where the audit log is not saved when the log server authentication information is changed before the log server is running | |
| 122708 | GN-27006 | WebUI | The service control menu was removed from the CLOUD version, but an issue where it can be accessed from the top menu | 5.0.29 |
| 122708 | GN-26992 | Center | An issue where the agent plug-in operates based on the policy server's time zone | |
| 122708 | GN-26953 | WebUI | An issue where data-linked values are incorrectly delivered when the fields are not sorted in the real-time mode of the audit log | 6.0.2 |
| 122708 | GN-26951 | Windows Agent | A problem where virus treatment audits are not recorded with the vaccine information collection plug-in | 4.0.144, 5.0.41 |
| 122708 | GN-26941 | WebUI | An issue where items in ConfEngine's addRemove component are modified incorrectly | 5.0.18 |
| 122708 | GN-26933 | WebUI | An issue where calendar components used in some date input fields are displayed only in English | 5.0.20, 6.0.0 |
| 122708 | GN-26904 | WebUI | Node Management > Problem with the icon not being displayed in the Risk column | 5.0.53, 6.0.13 |
| 122708 | GN-26864 | Windows Agent | An issue where the latest information in the information collection plug-in is not updated intermittently | 5.0.0, 6.0.0 |
| 122708 | GN-26859 | Linux Agent | Linux Agent, an issue where unpartitioned storage device information is not collected | 5.0.41, 6.0.0 |

continues on next page

Table 13 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 122708 | GN-26777 | WebUI | An issue where the update time is not updated when modifying a node group in a node/control policy | 6.0.18 |
| 122708 | GN-26742 | Sensor | Using "NMAP TCP SCAN" in Sensor Node Information Check Settings Not Applicable | 5.0.40 |
| 122708 | GN-26415 | WebUI | An issue where policy updates fail when modifying security group policy conditions | 6.0.3 |
| 122708 | GN-26032 | WebUI | A problem where content is not visible as much as the bottom button area when vertical scrolling occurs in the dialog window | 6.0.1 |
| 122708 | GN-25805 | WebUI | IP Change Prohibited (Designated IP Band) in IP Matrix View - Single IP Violated icon is not displayed | 4.0.8 |

### 23.4.23 Genian ZTNA 6.0.17 Release Notes (2023-10-11)

Last Updated: 2023-12-19

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 122609 | GN-27492 | WebUI | Tomcat version upgrade (8.5.94 -> 8.5.96/9.0.81 -> 9.0.83) | | 7.5 |
| 121382 | GN-26315 | WebUI | Improved two-step verification to limit the number of times the verification code can be entered and the time limit | | 4.3 |
| 120862 | GN-27278 | WebUI | Tomcat version upgrade (8.5.94/9.0.81) | | 7.5 |
| 120382 | GN-26600 | WebUI | The problem of not being able to log in after an abnormal API call | 5.0.42, 5.0.49, 6.0.7, 4.0.156, 5.0.56 | 5.3 |

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 122686 | GN-27462 | Windows Agent | Improved to download only cosign files corresponding to the operating system (64/32 bit) when installing the file distribution V2 plug-in | 5.0.42, 4.0.155, 6.0.15, 5.0.55 (LTS), 5.0.56, 5.0.57 |

continues on next page

Table 14 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 122678 | GN-27340 | Sensor | Improved so that DKNS also provides information synchronization and authentication integration functions through an SSL tunnel | |
| 122661 | GN-25714 | WebUI | Added an option to set a security agreement expiration date | |
| 122232 | GN-27164 | VRRPD | [General-purpose OS] A problem where the redundant configuration switches to the slave state due to an interface status check failure after switching to the master state | 5.0.42 |
| 122211 | GN-27402 | WebUI | API improvements so that start/end times can be set when modifying MAC policies | |
| 122163 | GN-27390 | Center, WebUI | Improved so that data in the /disk/data/report directory is also deleted when setting the number of reports to be saved | |
| 121924 | GN-27241 | macOS Agent | Improved so that agents can validate server events when using macOS multi-policy servers | |
| 121886 | GN-27248 | Linux Agent | Linux Agent, improved so that agents can validate server events when using multiple policy servers | |
| 121740 | GN-26627 | WebUI | Improved so that the authentication screen is not displayed again on CWP Web after agent authentication while the CWP web page is output | |
| 121113 | GN-27269 | -Unknown/None- | Remove unnecessary permissions from apache/tomcat-related directories and files | |
| 120834 | GN-27319 | WebUI | Add ServerTimeZone settings to jdbc connection when Tomcat is running | |
| 120399 | GN-27146 | Center | A problem where the password entered by the user remains in the central debug file when linking external authentication via extauth fails | |
| 120324 | GN-27174 | WebUI | Improved so that you can select combo box data that is output by default in ConfEngine File (40) type | |
| 120324 | GN-27160 | Center | Modify the local DB account connection method when using a user domain when linking authentication | |
| 120324 | GN-27049 | | Improved to support regular expressions in macOS file distribution folders | |
| 120324 | GN-26875 | WebUI | Edit the message displayed in CWP when the host name is restricted | |
| 120324 | GN-26843 | Center | The problem of generating an agent package twice when the center daemon is initially running | |
| 120324 | GN-26827 | WebUI | Fix the pop-up message on the Start Now button to perform a backup | |
| 120324 | GN-26803 | Windows Agent | Add audit records for shared folder control through plug-ins | |
| 120324 | GN-26801 | WebUI | Fixed an issue where WEBUI's primefaces basic system error was output | |
| 120324 | GN-26775 | Linux Agent | Linux Agent adds the ability to check the full contents of popup messages | |
| 120324 | GN-26763 | WebUI | Improved to be able to select items added during the previous day in the daily report | |

continues on next page

Table 14 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 120324 | GN-26760 | WebUI | Improved to be managed by each administrator (according to the scope of management) when creating and sending daily reports | |
| 120324 | GN-26753 | WebUI | Improved to output an error message when entering a semicolon at the end of the query string in the query report | |
| 120324 | GN-26734 | WebUI | Improved error message when entering an incorrect date for the start date/expiration date in Administration > Nodes > Equipment Properties | |
| 120324 | GN-26681 | WebUI | Apply detailed screen splitting function in node management grid mode | |
| 120324 | GN-26668 | CWP | Change the default setting for using CWP SSL to On | |
| 120324 | GN-26665 | WebUI | Add drop-down UI of "Available OS Types" when allocating agent actions when creating policies | |
| 120324 | GN-26653 | WebUI | Node Management List > Improved so that only one item in the same category can be selected when changing node attributes | |
| 120324 | GN-26640 | WebUI | Change the previous item to be selected when continuing to add node group conditions | |
| 120324 | GN-26612 | WebUI | Improved so that the current location point can be displayed by toggling the dashboard sensor map | |
| 120324 | GN-26611 | WebUI | Added an Authentication Flow that forces agent installation when logging in to Keycloak | |
| 120324 | GN-26610 | Center | An issue where the agent is displayed in English when installing an agent regardless of the user's default locale setting | |
| 120324 | GN-26564 | GNOS | NanoPI sensor hardware support | |
| 120324 | GN-26555 | Sensor | Added a gnlogin command to check the IP information cached on the sensor when using FQDN on a network object | |
| 120324 | GN-26547 | WebUI | Application Management > IP New/Return > Application Processing (Approve/Reject) Reason Entry Popup Window UI Improvement | |
| 120324 | GN-26544 | GNOS | GNOS kernel latest patch applied (5.10.181) | |
| 120324 | GN-26538 | WebUI | Remove dashboard widget animations | |
| 120324 | GN-26524 | WebUI | Improved so that when calling the CommonData (confui, codemap, customdata) Rest API, the locale is treated as the value of Accept-Language in the header | |
| 120324 | GN-26491 | WebUI | Improved so that the content of the node management description column is output at the same size as the column | |
| 120324 | GN-26488 | Windows Agent | Added an option to create an agent shortcut icon on the Windows desktop | |
| 120324 | GN-26473 | Sensor | Improved separation of the entered SNMP Agent versions and regular expression checks for Community and Passwd | |
| 120324 | GN-26468 | WebUI | Improved the number of list outputs per page in the Software/History Management List in Node Details so that it is possible to change the number of list outputs | |
| 120324 | GN-26464 | WebUI | Fixed an issue where images were broken when uploading and previewing images in Settings > Announcements | |

continues on next page

Table 14 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 120324 | GN-26412 | WebUI | Fixed to switch to the login screen when the administrator session is forcibly terminated | |
| 120324 | GN-26410 | CWP, WebUI | When linking SAML authentication, no message is output when the SP fails after IdP authentication | |
| 120324 | GN-26407 | WebUI | Modified so that Policy Server can be displayed in the IP management matrix view | |
| 120324 | GN-26360 | Linux Agent, Zero Trust Security | Linux Agent adds two-step authentication function for ZTNA connection manager | |
| 120324 | GN-26344 | WebUI | Keycloak login page Genians theme added | |
| 120324 | GN-26312 | WebUI | A problem where subsequent tasks cannot proceed if there are duplicate csv nodes when registering nodes in batches | |
| 120324 | GN-26263 | WebUI | Improved diagram output in node details | |
| 120324 | GN-26152 | Center, DKNS, Sensor | HTTPS web-based application detection via compose environment SWG | |
| 120324 | GN-26133 | Linux Agent | Linux Agent, Linux security settings plugin development | |
| 120324 | GN-25759 | WebUI | An issue where an English message is output when a value that does not match the form is entered in the calendar | |
| 120178 | GN-27207 | Windows Agent | Improved so that agents can validate server events when using multiple policy servers | |

## Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 122586 | GN-27502 | Center | An issue where agent logon API processing is delayed when the agent/sensor downcheck process by Keepalive takes a long time | 5.0.42 |
| 122548 | GN-27495 | WebUI | Fixed so that the policy application event is not called when the close button is clicked in the Service Control > Policy Application dialog | 6.0.17,<br>5.0.57 |
| 122534 | GN-27480 | WebUI | A problem where department selection type conditions cannot be retrieved from node group conditions | 5.0.31, 6.0.0 |
| 122501 | GN-27504 | Center | Improved so that NodeID-related DB errors (Illegal mix of collations) audit logs do not occur when KeepAlive is received | |
| 122481 | GN-27451 | WebUI | Audit > An issue where the Flow log list is not sorted by time | 6.0.1 |
| 122475 | GN-27490 | CWP | An issue where an Invalid settings: sp_cert_not_found_and_required message is output when clicking the SAML login button in CWP | 6.0.13 |

continues on next page

Table 15 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 122451 | GN-27345 | WebUI | Modified so that the page is converted to markdown during the ready phase | 5.0.42, 4.0.156, 6.0.16, 5.0.55 (LTS), 5.0.56 |
| 122423 | GN-27510 | Center, Sensor | [General-purpose OS] An issue where added libraries cannot be found after upgrading the NAC package | 5.0.42 |
| 122374 | GN-27404 | Center, macOS Agent | An issue where the macOS update plug-in does not install properly when using the installation mode | 5.0.11 |
| 122301 | GN-27467 | WebUI | An issue where XSS is executed in the policy application popup screen when XSS is added to the node action description | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 122253 | GN-27437 | Center, macOS Agent | Symptoms where OS information on macOS Sonoma devices is classified as unknown | 6.0.16, 5.0.55 (LTS), 5.0.56, 6.0.17, 5.0.57, 4.0.157 |
| 122080 | GN-27383 | WebUI | Fixed an issue where the parameter value is invalid error occurred and characters in all languages can be entered in an input form where Hangul can be entered | 5.0.42, 4.0.156, 6.0.16, 5.0.55 (LTS), 5.0.56 |
| 122068 | GN-27385 | GenianOS | Fixed an issue where iptables commands could fail when running at the same time | 5.0.0, 6.0.0 |
| 121995 | GN-27417 | WebUI | Status Filter > Tags > Node tags are not output properly | 6.0.16 |
| 121910 | GN-27400 | CWP | The problem with Agent not being able to register Passkeys | 6.0.16 |
| 121877 | GN-27398 | Linux Agent | Linux Agent performs a condition-only check action, and the result cannot be updated even if the results change | 5.0.50, 6.0.15 |
| 121831 | GN-27446 | Center | A problem where the SOAP API processing process stops and 100% CPU is used when an empty password is entered when using external authentication (runauth) | 5.0.42, 6.0.16, 5.0.55 (LTS), 5.0.56, 5.0.57, 4.0.157 |
| 121705 | GN-27380 | Windows Agent | A problem where an action check condition terminates abnormally if a '%' character exists other than a macro supported by the agent | 5.0.0, 6.0.0 |
| 121652 | GN-27387 | WebUI | An issue where the export function does not work on the OpenPort status screen | 5.0.6 |

continues on next page

Table 15 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 121591 | GN-27393 | WebUI | A problem where the mapping column key set in the IP and MAC additional field user selector does not work | 6.0.16, 5.0.55 (LTS) |
| 121525 | GN-27270 | macOS Agent | The problem of not being authenticated when omitting .com in the allowed domain name in macOS AD alternative authentication | 4.0.108, 5.0.5 |
| 121504 | GN-27382 | WebUI | Additional fields - A problem where parameter value is invalid errors occur when Hangul and some special characters are included in the user selector | 5.0.42, 5.0.50, 5.0.53, 4.0.155, 6.0.15 |
| 121454 | GN-27394 | Center | A problem where backup fails when an absolute path is set to the SFTP storage path | 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 121442 | GN-27291 | WebUI | If the Alias sensor name contains special characters such as * , · parameter value is invalid error occurs | 5.0.42, 4.0.156, 6.0.16 |
| 121393 | GN-27388 | Center | [General-purpose OS] Problem with not being able to connect to webssh | 5.0.42 |
| 121197 | GN-27322 | Center, Sensor | [General-purpose OS] System Administration > Preferences > Time Zone Settings Not Working in Ubuntu NAC | 5.0.50 |
| 121158 | GN-27259 | Linux Agent | Linux Agent, an issue where the agent does not work when installing a specific package | 5.0.45, 6.0.2 |
| 121153 | GN-27221 | Linux Agent | A problem where the agent shuts down abnormally when collecting monitors that do not have an EDID value from the Linux Agent or monitor information collection plug-in | 6.0.12 |
| 121131 | GN-27359 | gnlogin, VR-RPD | An issue where the same event already exists in queue debug log occurs because event queuing works even in processes that do not require event retransmission processing | 5.0.42 |
| 121074 | GN-27289 | WebUI | An issue where a report file is not generated when creating a custom report | 6.0.17, 5.0.57 |
| 121015 | GN-27358 | Center | An issue where the centerd execution option's sensor service start/stop function does not work | 5.0.42, 4.0.156, 6.0.16, 5.0.55 (LTS), 5.0.56 |
| 120814 | GN-27262 | Center | A problem where the node's changed control policy cannot be delivered to the sensor when the timezone settings of the policy server and DB server are different | 6.0.17, 5.0.57 |
| 120771 | GN-24372 | CLOUD | Backup not working on Docker compose policy server | 5.0.42 |
| 120763 | GN-27211 | Sensor | An issue that does not apply when multiple access rights are granted through a rights control policy | 6.0.7 |
| 120693 | GN-27290 | WebUI | An issue where the sensor tree is not displayed properly when '%' is included in the sensor name | 5.0.43, 6.0.0 |

continues on next page

Table 15 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 120602 | GN-27279 | Center, Sensor | A problem where the settings only apply when trust-nodeserver-id is set on the center device, the sensor daemon must be restarted | 5.0.42, 4.0.156, 6.0.16, 5.0.55 (LTS), 5.0.56 |
| 120533 | GN-27091 | Center, procmond | A problem where the event log (procmond process) sent from the sensor cannot be saved due to an unknown center did error on the policy server | 5.0.42 |
| 120518 | GN-27113 | Center | A problem where update information (sysinfo) sent from a slave device fails to be updated to an unknown devid | 4.0.145, 5.0.42, 6.0.1 |
| 120505 | GN-27200 | Center | Symptoms where the BADQUERY=ILLEGAL MIX of collations error continues to occur in the slave center | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 120494 | GN-27177 | Backup | An issue where backup files include agent zip files that increase capacity | 6.0.16, 5.0.55 (LTS) |
| 120457 | GN-27153 | WebUI | A problem where the manager node management scope limit is set to a sensor group and the management sensor cannot be selected when registering a node | 5.0.31 |
| 120418 | GN-27210 | Enforcer | A problem where the control policy name is not left in the Netflow log | 6.0.16 |
| 120357 | GN-27191 | WebUI | An issue where the browser freezes on the audit log screen | 5.0.54, 6.0.15 |
| 120324 | GN-26976 | Center | [General-purpose OS] An issue where the device does not work properly when the update fails | 5.0.56, 6.0.17 |
| 120324 | GN-26899 | Center | The problem with self-signed certificates not being reissued | 5.0.45, 6.0.2 |
| 120324 | GN-26845 | WebUI | A problem where the agent is deleted when the Windows update action is assigned, but the output appears as if the agent exists in the node list | 4.0.M1, 5.0.0, 6.0.0 |
| 120324 | GN-26836 | WebUI | Node group conditions fail to retrieve department information if a department name containing a tag exists | 5.0.42, 6.0.0 |
| 120324 | GN-26815 | WebUI | Audit > Report > Node Report > Node Group Selection > Problem with content not being output | 5.0.24 |
| 120324 | GN-26771 | Center | A problem where the center daemon process does not run properly after enabling the policy server (node-server enable) through gnlogin | 5.0.42 |
| 120324 | GN-26746 | WebUI | An issue where the RADIUS policy's two-step authentication grace period is misexplained | 6.0.11 |
| 120324 | GN-26740 | WebUI | Errors that do not reflect application modification information | 6.0.13 |
| 120324 | GN-26721 | WebUI | An issue where the validation success log is left as an error log when the Agent is uploaded | 6.0.1 |
| 120324 | GN-26692 | WebUI | A phenomenon where progress does not end when the upload process is processed without selecting a file in the system management software | 5.0.2 |

continues on next page

Table 15 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 120324 | GN-26689 | Center | An issue where the node IP is incorrectly output when removing the no-change setting in the debug | 5.0.43, 6.0.0 |
| 120324 | GN-26680 | Center | An issue where the last line word in the password blacklist file is not prohibited (restricted) | 4.0.106 |
| 120324 | GN-26676 | gnlogin | [General-purpose OS] A problem where ADMIN and ADMINIP are not left in the audit record when gnlogin is commanded | 5.0.23 |
| 120324 | GN-26673 | Center | New node policy: If MAC is blocked, change prohibited (specified IP band) A problem where MAC allowed nodes are blocked when the IP usage time of the set node expires | 4.1.M5 |
| 120324 | GN-26652 | WebUI | Node Management List > A problem where the IP start/end time is 9 hours different from the entered value when importing node attributes | 4.1.M4 |
| 120324 | GN-26605 | Center | New wireless LAN AP detection, wireless LAN AP information change audit log format modification | 6.0.0 |
| 120324 | GN-26588 | WebUI | When adding a new dashboard tab, modify it to be sorted at the end of the tab list | 6.0.0 |
| 120324 | GN-26586 | WebUI | An issue where the 'Apply Change Policy' button is not displayed when copying a node group and is applied immediately | 5.0.31 |
| 120324 | GN-26581 | WebUI | Intermittent errors where the loading bar does not output | 6.0.17 |
| 120324 | GN-26578 | WebUI | A problem where the user ID and department name columns are displayed as blank when querying the results of the IP application form | 4.1.4 |
| 120324 | GN-26573 | WebUI | Check the management console settings, change the integration and change the language setting parameters | 6.0.0 |
| 120324 | GN-26560 | WebUI | The problem of not being searched when AND is present in the search term on the node management screen | 5.0.38 |
| 120324 | GN-26558 | WebUI | A problem that is not fixed when only the TTL value of the FQDN option is modified in the network address of a network object | 5.0.19 |
| 120324 | GN-26529 | WebUI | Improved error page output due to incorrect sensor IP/mask settings in the Sensor IP Usage Rate Top Status (old version) widget | 4.1.4 |
| 120324 | GN-26489 | Center | An issue where the thread ID in the debug file does not remain normal in the Ubuntu/cloud version | 6.0.0 |
| 120324 | GN-26487 | WebUI | Fixed an issue where an error page was displayed when there was no value on the CVE detail screen | 5.0.24 |
| 120324 | GN-26476 | WebUI | Correction of errors on the execution results status page for each action | 5.0.50 |
| 120324 | GN-26463 | GenianOS | A problem where syscollect may not work properly | 5.0.0 |
| 120324 | GN-26439 | Center, Sensor | Problems that are not allowed in SWG if it is an Application Category condition for an application object | 6.0.14 |
| 120324 | GN-26369 | WebUI | A problem where the date display is incorrectly displayed when searching for the previous year in the node/log/wireless LAN report | 5.0.34 |
| 120324 | GN-26235 | macOS Agent | macOS agent problem of not being able to obtain motherboard information for new model Macs | 5.0.41, 6.0.0 |

continues on next page

Table 15 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 120324 | GN-25815 | WebUI | A problem where the approval/rejection popup for a new IP application is active and the approval/rejection popup is enabled, the problem is that it is in a waiting state when approved/rejected | 4.1.3 |
| 120324 | GN-24713 | procmond | A problem where a daemon operation error occurs when changing the policy server to a sensor-only image | 5.0.0 |
| 120142 | GN-27237 | Center, Sensor | A problem where the node cannot be immediately re-registered by the sensor when the agent node registered to the sensor is deleted from the management console | 5.0.42 |
| 114063 | GN-26566 | WebUI | An issue where the changed information was updated and not displayed when the tab was moved after updating the node information | 5.0.50 |

### 23.4.24 Genian ZTNA 6.0.16 Release Notes (2023-07-21)

Last Updated: 2024-08-19

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 125554 | GN-28063 | WebUI | A problem where blind injection is possible in the node management search bar | | 2.2 |
| 125406 | GN-27107 | WebUI | Service disabled by executing a Tomcat restart command by an unauthorized administrator | 5.0.41 | 2.7 |
| 123781 | GN-26393 | WebUI | Vulnerability where information can be modified by directly entering a URL to an unauthorised page | | 3.1 |
| 123284 | GN-26390 | WebUI | File export permission bypass vulnerability for unauthorized administrators through the Audit Log REST API | | 3.1 |
| 122609 | GN-27492 | WebUI | Tomcat version upgrade (8.5.94 -> 8.5.96/9.0.81 -> 9.0.83) | | 7.5 |
| 121382 | GN-26315 | WebUI | Improved two-step verification to limit the number of times the verification code can be entered and the time limit | | 4.3 |
| 120862 | GN-27278 | WebUI | Tomcat version upgrade (8.5.94/9.0.81) | | 7.5 |
| 118988 | GN-27014 | WebUI | A problem where Passkey can be registered using the Passkey re-registration function without permission | | 3.9 |
| 118676 | GN-26383 | WebUI | Vulnerability where html/script code can be injected | | 5.3 |
| 118272 | GN-26935 | WebUI | Vulnerability where an html tag output as a department name is executed in a tree | 5.0.0 | 1.2 |
| 117073 | GN-26835 | Center | Command Injection vulnerability via SQL used to update data | | 6.6 |
| 116162 | GN-26833 | Sensor | nmap script tampering vulnerability during sensor NMDB update | | 4.1 |
| 114948 | GN-26696 | Sensor | Insufficient validation of incoming sensor events | | 6.3 |
| 114936 | GN-26694 | Center | Parameter injection vulnerability due to insufficient verification of download URLs | | 6.6 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 127494 | GN-26117 | macOS Agent | macOS ZTNA Agent minimum supported OS upgrade | 6.0.0 |
| 127308 | GN-28368 | macOS Agent | macOS agent supports newly released macOS 15 (codename Sequoia) | 5.0.0, 6.0.0 |
| 125148 | GN-27973 | Center, macOS Agent, Sensor, Windows Agent | OpenSSL 3.0.13, 1.1.1w upgrade - excessive resource usage during X.509 policy constraint checking | 4.0.0, 5.0.0, 6.0.0 |

continues on next page

Table 16 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 123464 | GN-27625 | Sensor | Fixed an issue where pubilc IP cannot be imported when changing sensor operation modes and policies | |
| 122922 | GN-25063 | WebUI | 6.0 widget added | |
| 122686 | GN-27462 | Windows Agent | Improved to download only cosign files corresponding to the operating system (64/32 bit) when installing the file distribution V2 plug-in | 5.0.42, 4.0.155, 6.0.15, 5.0.55, 5.0.56, 5.0.57 |
| 122232 | GN-27164 | VRRPD | [General-purpose OS] A problem where the redundant configuration switches to the slave state due to an interface status check failure after switching to the master state | 5.0.42 |
| 122211 | GN-27402 | WebUI | API improvements so that start/end times can be set when modifying MAC policies | |
| 122169 | GN-24332 | WebUI | Change the output page when blocked by a URL filter | |
| 122163 | GN-27390 | Center, WebUI | Improved so that data in the /disk/data/report directory is also deleted when setting the number of reports to be saved | |
| 121924 | GN-27241 | macOS Agent | Improved so that agents can validate server events when using macOS multi-policy servers | |
| 121886 | GN-27248 | Linux Agent | Linux Agent, improved so that agents can validate server events when using multiple policy servers | |
| 121113 | GN-27269 | -Unknown/None- | Remove unnecessary permissions from apache/tomcat-related directories and files | |
| 120399 | GN-27146 | Center | A problem where the password entered by the user remains in the central debug file when linking external authentication via extauth fails | |
| 120178 | GN-27207 | Windows Agent | Improved so that agents can validate server events when using multiple policy servers | |
| 120017 | GN-27206 | Center, Sensor | Added the ability to export trusted nodeids from the center to sensors and agents | |
| 119945 | GN-27013 | WebUI | Improved so that items set to markdown can be converted | |
| 119810 | GN-27121 | Center, macOS Agent | macOS agent support for new OS 14.0 (Sonoma) | |
| 119717 | GN-27142 | Windows Agent | Change the integration module to support the new version of the pill | |
| 119664 | GN-27031 | Center, Sensor | [General-purpose OS] Local privilege escalation vulnerability in Ubuntu OverlayFS module | |
| 119611 | GN-26789 | Genian Syncer | Electronic signature verification of operating information data synchronized with Genian Sinker | |
| 119336 | GN-27046 | WebUI | Added IP/MAC additional field items to node registration, batch node registration, and node attribute import | |
| 119305 | GN-27045 | WebUI | Added the ability to output additional IP and MAC fields newly added to the node management list | |
| 119025 | GN-27038 | WebUI | Fixed an issue where webssh could not be connected after the openssh version was upgraded | |

continues on next page

Table 16 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 118991 | GN-26987 | Linux Agent | Improved functionality so that the approval window is not displayed when using the Linux Agent and File Distribution Plug-in V2 | |
| 118795 | GN-26879 | WebUI | IP/MAC additional field management function added | |
| 118668 | GN-23316 | Center | Simplifying upgrades by including sensors/agents in the Policy Server image | |
| 118623 | GN-26778 | Center | Add node group conditions related to the IP/MAC additional field | |
| 118566 | GN-26988 | macOS Agent | Improved functionality so that the approval window is not displayed when using the macOS file distribution plug-in V2 | |
| 118438 | GN-26791 | WebUI | Expand up to 20 custom fields that can be used when registering nodes in batches (uploading csv files) | |
| 118275 | GN-26838 | Ubuntu(Debian) | [General-purpose OS] ICMP Timestamp support removed | |
| 118209 | GN-26981 | Center, Linux Agent, macOS Agent, WebUI, Windows Agent | Improved functionality so that the approval window is not displayed when using the distribution plug-in V2 | |
| 117819 | GN-26766 | Center, macOS Agent | Development of distribution plugins based on macOS Sigstore electronic signatures | |
| 117731 | GN-26730 | macOS Agent | macOS agent ZTNA applies a new icon and changes the connection display | |
| 117654 | GN-26724 | Sensor | Improved port module kernel upgrade (2.6.38->4.14.196) for Axgate 80D and 200AX models | |
| 117501 | GN-26729 | macOS Agent | Symptoms of not being able to collect AhnLab V3 information when using the macOS agent vaccine information collection plug-in | |
| 117501 | GN-26644 | Windows Agent | Change the Center CA certificate installation option to default ON and change the execution cycle | |
| 117501 | GN-26619 | Sensor | Improved so that it is possible to set whether or not to use HNAP-NSE as an option when performing an NMAP scan | |
| 117501 | GN-26563 | Sensor | Improved so that the sensor can manage the Alias IP band without setting Alias IP in the sensor interface | |
| 117501 | GN-26535 | wsdump | Improved so that the WLAN monitoring function works when the DKNS sensor is running | |
| 117501 | GN-26479 | Sensor | Improved so that the blocking node is unblocked when shutting down via the sensor reboot/poweroff command | |
| 117501 | GN-26450 | WebUI | Improved so that the scroll moves to the top when moving a page in the history management list | |
| 117501 | GN-26442 | GenianOS | [General-purpose OS] OpenVPN package added to ubuntu target | |
| 117501 | GN-26381 | WebUI | Add an organization name (USER_COMPANY) column to the user management list | |
| 117501 | GN-26330 | Integretion | Added provider so that NAC user DB can be used during Keycloak authentication | |

continues on next page

Table 16 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 117501 | GN-26300 | WebUI | The problem that the CWP device application form and alarm message do not match the time zone | |
| 117501 | GN-26187 | WebUI | Improved so that visitor searches on the user registration page can be queried by the administrator's email | |
| 117501 | GN-24976 | WebUI | Add the Flow Application Name statistics widget to the dashboard | |
| 117501 | GN-19829 | CLOUD | Enables on-prem backup files to be restored to the cloud | |
| 116677 | GN-26792 | Center, Sensor | Enhanced validation of policy server incoming events | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 136621 | GN-27541 | Authsync | A problem where if the connection to the information synchronization server fails, it is treated as a deleted user and all users are deleted | 6.0.9 |
| 128037 | GN-28410 | | A problem where all logs can be checked in the real-time mode of the audit log when the administrator's management scope (management sensor) is limited | 5.0.45, 6.0.2 |
| 127521 | GN-28422 | WebUI | An issue where the locale (Korean, English, etc.) cannot be changed on the management console login page | 6.0.16, 5.0.55, 5.0.56, 6.0.17, 5.0.57 |
| 127204 | GN-28418 | Windows Agent | An issue where the scheduled install/check option is not applied in Windows Update Actions | 5.0.0, 6.0.0 |
| 127159 | GN-28370 | WebUI | An issue where settings are not displayed when clicking Interface Settings in Sensor Management > Sensor Settings > IP Settings | 5.0.42, 6.0.16, 5.0.55, 5.0.56, 5.0.57 |
| 126839 | GN-28306 | Center, Sensor | A problem where the process runs abnormally because execution results cannot be obtained intermittently when executing system commands | 5.0.42 |
| 126732 | GN-28295 | Center | An issue where the entire audit log is deleted when the connection to the policy server database fails | 4.1.3 |
| 126396 | GN-28228 | Sensor | [General-purpose OS] A problem where the sensor repeats up/down states | 5.0.42 |
| 126076 | GN-28130 | Center, Sensor | An issue where NAC cannot function properly because the daemon terminates abnormally when sending event packets from the center daemon and sensor daemon | 5.0.42, 4.0.155, 6.0.16 |
| 126038 | GN-28036 | WebUI | 관리콘솔의 상단 로그아웃 버튼을 클릭하여 로그아웃 시 "관리자가 로그아웃 함." 감사 로그가 남지 않는 문제 | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56 |

continues on next page

Table 17 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 125997 | GN-28047 | Sensor | [General-purpose OS] An issue where the snmp daemon does not work on the sensor | 6.0.15, 5.0.55 |
| 125366 | GN-27983 | Center | An issue where event packets sent from the 5.0/6.0 policy server are not handled by the 4.0.1 sensor | 5.0.42, 6.0.16 |
| 125291 | GN-27972 | | An issue where an SSL certificate is generated with an expiration date of 10 years | 6.0.15, 5.0.55 |
| 125275 | GN-28003 | Windows Agent | A problem where the distribution file verification method is Sigstore Keyless Signing in the file distribution plug-in V2 fails | 5.0.42, 4.0.155, 6.0.15, 5.0.56 |
| 125166 | GN-27994 | Linux Agent | Linux Agent A problem where the distribution file verification method is Sigstore Keyless Signing in the file distribution plug-in V2 fails | 5.0.50, 5.0.53, 5.0.54, 6.0.15 |
| 125157 | GN-28005 | macOS Agent | A problem in macOS file distribution plug-in V2 that fails when the distribution file verification method is Sigstore Keyless Signing | 6.0.16, 5.0.55, 5.0.56 |
| 125099 | GN-27993 | Sensor | [General-purpose OS] A problem where the DNS cache function cannot be turned off because the maximum DNS cache number setting in System > Preferences is not applied | 6.0.12, 5.0.53 |
| 125043 | GN-27986 | GenianOS | Addressing compatibility issues due to SLSA TUF certificate renewals | 5.0.42, 5.0.50, 6.0.15, 4.0.156 |
| 124442 | GN-27769 | WebUI | An issue where some nodes are blocked due to policy application errors after changing the IP policy | 5.0.30, 6.0.0 |
| 124082 | GN-27749 | WebUI | The problem of not being able to access the user information modification page in CWP | 6.0.16, 5.0.55, 5.0.56, 6.0.18, 5.0.58 |
| 123721 | GN-27652 | Center | A problem where Google OTP authentication cannot be performed because the Google OTP security key issued by the center cannot be sent to the agent | 6.0.13 |
| 123435 | GN-27641 | WebUI | In the tomcat log, by the following code has not been detected to the pool, no symptoms of connecting to the web console after a large number of cases | 5.0.20 |
| 123340 | GN-27399 | macOS Agent | A problem where plug-ins don't work according to macOS internal/external conditions | 6.0.5, 5.0.48 |
| 123298 | GN-27573 | WebUI | A problem where the list is not displayed when clicking on the number of members in each group in the user group status | 4.0.156, 6.0.16, 5.0.57 |
| 123293 | GN-27401 | Sensor | A problem where the sensor process terminates abnormally when the same event is received from the sensor device | 4.0.64 |
| 123281 | GN-27517 | WebUI | Errors where certain items are not modified in the Nodes REST API | 5.0.8, 4.0.111 |

continues on next page

Table 17 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 123274 | GN-27550 | WebUI | A problem where tree-structured data components are not output | 6.0.16, 5.0.55, 6.0.17, 5.0.57 |
| 123268 | GN-27460 | GenianOS | [General-purpose OS] An issue where aes256 commands are not executed during initial operation | 5.0.42, 6.0.16, 5.0.55, 5.0.56 |
| 123133 | GN-27496 | Linux Agent | Linux Agent intermittently misses sending some action system information | 5.0.50, 6.0.15 |
| 123055 | GN-24708 | Center | In an environment where many sensor debugs are sent to the center, a load may be caused by deleting old debugs when the center is rebooted | 5.0.0 |
| 123046 | GN-27575 | Center | An issue where the log filter action does not work when the ES log filter query result is greater than 2K | 4.1.M6 |
| 122946 | GN-27574 | Center | An issue where ES index (nac-filter) for log filters is deleted during the ES log cleaning cycle | 5.0.50, 6.0.11 |
| 122840 | GN-27561 | Center | [General-purpose OS] An issue where the LDAPsearch command results fail due to the LDAP configuration file being set to the wrong file in the general-purpose OS | 5.0.42 |
| 122586 | GN-27502 | Center | An issue where agent logon API processing is delayed when the agent/sensor downcheck process by Keepalive takes a long time | 5.0.42 |
| 122534 | GN-27480 | WebUI | A problem where department selection type conditions cannot be retrieved from node group conditions | 5.0.31, 6.0.0 |
| 122501 | GN-27504 | Center | Improved so that NodeID-related DB errors (Illegal mix of collations) audit logs do not occur when KeepAlive is received | |
| 122481 | GN-27451 | WebUI | Audit > An issue where the Flow log list is not sorted by time | 6.0.1 |
| 122475 | GN-27490 | CWP | An issue where an Invalid settings: sp_cert_not_found_and_required message is output when clicking the SAML login button in CWP | 6.0.13 |
| 122451 | GN-27345 | WebUI | Modified so that the page is converted to markdown during the ready phase | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56 |
| 122423 | GN-27510 | Center, Sensor | [General-purpose OS] An issue where added libraries cannot be found after upgrading the NAC package | 5.0.42 |
| 122301 | GN-27467 | WebUI | An issue where XSS is executed in the policy application pop-up screen when XSS is added to the node action description | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |

continues on next page

Table 17 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 122253 | GN-27437 | Center, macOS Agent | Symptoms where OS information on macOS Sonoma devices is classified as unknown | 6.0.16, 5.0.55, 5.0.56, 6.0.17, 5.0.57, 4.0.157 |
| 122080 | GN-27383 | WebUI | Fixed an issue where the parameter value is invalid error occurred and characters in all languages can be entered in an input form where Hangul can be entered | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56 |
| 122068 | GN-27385 | GenianOS | Fixed an issue where iptables commands could fail when running at the same time | 5.0.0, 6.0.0 |
| 121995 | GN-27417 | WebUI | Status 현황 & 필터 > 태그 > 노드 태그가 정상적으로 출력되지 않는 문제 Filter > Tags > Node tags are not output properly | 6.0.16 |
| 121910 | GN-27400 | CWP | The problem with Agent not being able to register Passkeys | 6.0.16 |
| 121877 | GN-27398 | Linux Agent | Linux Agent performs a condition-only check action, and the result cannot be updated even if the results change | 5.0.50, 6.0.15 |
| 121831 | GN-27446 | Center | A problem where the SOAP API processing process stops and 100% CPU is used when an empty password is entered when using external authentication (runauth) | 5.0.42, 6.0.16, 5.0.55, 5.0.56, 5.0.57, 4.0.157 |
| 121705 | GN-27380 | Windows Agent | A problem where an action check condition terminates abnormally if a '%' character exists other than a macro supported by the agent | 5.0.0, 6.0.0 |
| 121591 | GN-27393 | WebUI | A problem where the mapping column key set in the IP and MAC additional field user selector does not work | 6.0.16, 5.0.55 |
| 121504 | GN-27382 | WebUI | Additional fields - A problem where parameter value is invalid errors occur when Hangul and some special characters are included in the user selector | 5.0.42, 5.0.50, 5.0.53, 4.0.155, 6.0.15 |
| 121454 | GN-27394 | Center | A problem where backup fails when an absolute path is set to the SFTP storage path | 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 121442 | GN-27291 | WebUI | Alias 센서명에 *, · 등의 특수문자가 포함된 경우 parameter value is invalid 에러 발생 | 5.0.42, 4.0.156, 6.0.16 |
| 121418 | GN-27209 | WebUI | An issue where the IP application is approved and the request is not notified by email | 5.0.46, 6.0.4 |
| 121393 | GN-27388 | Center | [General-purpose OS] Problem with not being able to connect to webssh | 5.0.42 |

continues on next page

Table 17 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 121367 | GN-27203 | Windows Agent | A problem where the action execution result is sent after a certain period of time (5 minutes) even if the action execution result changes unspecified | 5.0.0, 6.0.0 |
| 121158 | GN-27259 | Linux Agent | Linux Agent, an issue where the agent does not work when installing a specific package | 5.0.45, 6.0.2 |
| 121153 | GN-27221 | Linux Agent | A problem where the agent shuts down abnormally when collecting monitors that do not have an EDID value from the Linux Agent or monitor information collection plug-in | 6.0.12 |
| 121131 | GN-27359 | gnlogin, VR-RPD | An issue where the same event already exists in queue debug log occurs because event queuing works even in processes that do not require event retransmission processing | 5.0.42 |
| 121015 | GN-27358 | Center | An issue where the centerd execution option's sensor service start/stop function does not work | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56 |
| 120693 | GN-27290 | WebUI | An issue where the sensor tree is not displayed properly when '%' is included in the sensor name | 5.0.43, 6.0.0 |
| 120637 | GN-27292 | WebUI | A problem where options are not entered even when selecting an IP/MAC list when setting a policy in node details | 6.0.16, 5.0.55 |
| 120602 | GN-27279 | Center, Sensor | A problem where the settings only apply when trustnodeserver-id is set on the center device, the sensor daemon must be restarted | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56 |
| 120533 | GN-27091 | Center, procmond | A problem where the event log (procmond process) sent from the sensor cannot be saved due to an unknown center did error on the policy server | 5.0.42 |
| 120518 | GN-27113 | Center | A problem where update information (sysinfo) sent from a slave device fails to be updated to an unknown devid | 4.0.145, 5.0.42, 6.0.1 |
| 120505 | GN-27200 | Center | Symptoms where the BADQUERY=ILLEGAL MIX of collations error continues to occur in the slave center | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 120494 | GN-27177 | Backup | An issue where backup files include agent zip files that increase capacity | 6.0.16, 5.0.55 |
| 120418 | GN-27210 | Enforcer | A problem where the control policy name is not left in the Netflow log | 6.0.16 |
| 120411 | GN-27224 | Windows Agent | The input dialog box is not output when the screen is locked to the agent authentication window | 5.0.49, 6.0.7 |
| 120248 | GN-27187 | CLOUD | A problem where agent information is not displayed properly on the new Cloud Policy Server | 5.0.45, 6.0.2 |
| 120223 | GN-27198 | Sensor | A problem where ZTNA NAT does not work when multiple exception bands are set | 6.0.12 |
| 120220 | GN-26886 | Sensor | Fix ZTNA Client connection error in DKNS | 6.0.15 |

continues on next page

Table 17 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 120142 | GN-27237 | Center, Sensor | A problem where the node cannot be immediately re-registered by the sensor when the agent node registered to the sensor is deleted from the management console | 5.0.42 |
| 120129 | GN-27176 | macOS Agent | An issue where the macOS update plug-in works abnormally | 5.0.11 |
| 120103 | GN-26887 | WebUI | An issue where tooltips in the control policy column in the node list are not updated when switching sensor mode | 5.0.50, 6.0.11 |
| 120083 | GN-27136 | macOS Agent | macOS USB blocking not working | 5.0.50, 6.0.9 |
| 120000 | GN-27154 | WebUI | A problem where the link in the connected device column in the node list works even though the switch has been deleted from switch management | 5.0.38 |
| 119997 | GN-27000 | WebUI | A problem where an invalid parameter message is displayed when moving to the user details screen with a link in the Node Management List > Authenticated User column | 6.0.5, 5.0.50 |
| 119823 | GN-27137 | macOS Agent | An issue where the macOS message pop-up content is not visible | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 6.0.14 |
| 119801 | GN-27058 | Windows Agent | A problem where actions set to be performed according to internal and external conditions when restarting the PC malfunction | 5.0.43, 6.0.0 |
| 119771 | GN-27158 | WebUI | An error where node information cannot be updated when changing the IP addition field of the user settings list type | 6.0.16, 5.0.55 |
| 119745 | GN-27152 | WebUI | A problem where the wrong node is output in the matrix view when there are multiple nodes with the same IP | 4.0.8 |
| 119727 | GN-27183 | Center, Sensor | A problem where the re-registration event (REGISTER_REQ) sent from the policy server to the sensor is not processed by the sensor | 5.0.42 |
| 119536 | GN-27162 | Sensor | [General-purpose OS] An issue where the gdcid daemon does not run after booting the device | 5.0.42 |
| 119513 | GN-27151 | geniup | An issue where the migration is not performed properly due to the command being terminated during the migration | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 119403 | GN-27132 | gnlogin | A problem where the center works abnormally when a% string is present in the MySQL password | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 119373 | GN-27085 | WebUI | An issue where the existing connection is disconnected (forced login) function does not work when logging in to the management console with SAML | 5.0.48, 6.0.6 |

continues on next page

Table 17 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 119363 | GN-27084 | WebUI | An issue where audit logs are left due to false positives on parameters processed by URLEncode in XSS inspection logic | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 119352 | GN-27127 | Windows Agent | Failed to perform offline PMS through the Windows update plug-in | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56 |
| 119304 | GN-27088 | Center | The problem that the URL filter function does not work | 6.0.4 |
| 119154 | GN-27106 | Center | An issue where only some nodes are applied when the node policy is applied immediately | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 119116 | GN-26958 | Center | A problem where a new IP is assigned when ZTNA fixed IP is assigned | 6.0.13 |
| 119097 | GN-27089 | macOS Agent | A problem where GNDaemon restarts when an integrity check command is performed by the macOS Agent Management Console | 5.0.42, 5.0.54, 6.0.15, 5.0.56 |
| 119037 | GN-26674 | WebUI | A problem where the node management control policy column appears to be blocked (orange) even though the control policy applied to the node is allowed (PERM-ALL) | 6.0.7 |
| 119019 | GN-27053 | WebUI | An issue where the AUTHUSER (authenticated user) column cannot be used in the node attribute import function | 5.0.30 |
| 118998 | GN-26938 | Linux Agent | Linux Agent is unable to register a new node due to a local network change detection error | 5.0.51, 6.0.11 |
| 118978 | GN-27047 | WebUI | An issue where Elastic Percolate cannot be initialized due to an error during initialization related to Elastic when running Tomcat | 5.0.53, 6.0.14 |
| 118930 | GN-26972 | Center | An issue where a 'badQuery=illegal mix of collations' error occurs when a SLAVE device exists | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 118903 | GN-26467 | Windows Agent | As a password validation action, a pop-up window is intermittently displayed even after verification due to unverified reasons. | 5.0.6, 6.0.0 |
| 118837 | GN-27037 | MGMT | [General-purpose OS] A problem where apache does not run when the management console port and HTTPS port are set to the same | 5.0.42 |

continues on next page

Table 17 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 118781 | GN-27066 | Windows Agent | Fixed a CMD window display error when running a script in File Distribution V2 | 5.0.42, 4.0.156, 6.0.16, 5.0.55, 5.0.56 |
| 118736 | GN-26931 | Center | An issue where motherboard information (updateinfo) is not being deleted | 5.0.52, 6.0.13 |
| 118611 | GN-27012 | Center | A problem with trying to access a different sensor when connecting to a ZTNA client | 6.0.4 |
| 118611 | GN-26934 | Sensor | An issue where ZTNA Client session monitoring information differs from reality | 6.0.15 |
| 118598 | GN-26870 | WebUI | An issue where tags are not assigned to NAC nodes when setting response policies through NAC integration in EDR | 5.0.42, 5.0.45, 6.0.2 |
| 118470 | GN-26895 | macOS Agent | A phenomenon where software information cannot be collected on macOS Mac mini M2 models | 5.0.11 |
| 118460 | GN-25831 | WebUI | An issue where the input type changes when adding or removing field assignments in usage management | 4.0.11 |
| 118446 | GN-26957 | macOS Agent | An issue where an action is performed when an action is performed immediately regardless of the scope of application of the macOS plug-in | 6.0.5, 5.0.48 |
| 118434 | GN-26759 | WebUI | A problem where values are not displayed when modifying directly entered value items when adding conditions to a RADIUS policy | 6.0.11 |
| 118387 | GN-26973 | macOS Agent | An issue where macOS user notification messages do not pop up when running periodically | 5.0.42, 5.0.50, 5.0.53, 6.0.14 |
| 118364 | GN-27016 | Sensor | A problem where the localconf service port is changed to an unspecified value by the sensor daemon | NoVersion |
| 118288 | GN-26785 | Center | An issue where device control policies can be received from other node groups when using device control policies | 5.0.23 |
| 118267 | GN-26930 | Center | An issue where search filter-related functions do not work when disabling alarm transmission failure messages | 5.0.39 |
| 118221 | GN-26969 | WebUI | XSS false positives issue with Get Parameter (queryString) | 5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15 |
| 118180 | GN-26956 | WebUI | An issue where an Exception error message is output when modifying authentication integration settings | 6.0.16, 5.0.55, 5.0.56 |
| 117919 | GN-26970 | Center | A problem where the policy server processes events using the past event processing method even though it is an improved version of the Push Notification event processing agent | 5.0.42, 4.0.155 |
| 117685 | GN-26898 | WebUI | An issue where html is displayed as text in the dashboard license warning message | 6.0.15 |
| 117683 | GN-26511 | WebUI | An error where the log ID is entered incorrectly in the automatic report generation log | 6.0.1 |

continues on next page

Table 17 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 117592 | GN-26901 | Sensor | [AXGATERALINK] An issue where policies were not updated due to building with the wrong endian | 6.0.5, 5.0.48 |
| 117501 | GN-27617 | Windows Agent | An issue where an AD account is locked due to an operating system information collection action to check whether an empty password is used on the AD server | 4.0.109, 5.0.6, 6.0.0 |
| 117501 | GN-27442 | WebUI | A problem where the sorting of the last operation time column does not work on the node management list screen | 6.0.16, 5.0.55 |
| 117501 | GN-27396 | WebUI | A problem where the contents of the Last Operation Time column are incorrectly displayed when exporting a node list | 6.0.16, 5.0.55 |
| 117501 | GN-26840 | WebUI | A problem where when outputting collected node details, it is output differently from the output settings | 6.0.4 |
| 117501 | GN-26751 | Sensor | The problem of incorrectly checking the deadlock when sensord deadlock is detected | 6.0.16, 5.0.57 |
| 117501 | GN-26687 | WebUI | A problem where the time in the node management last operation time column is output without applying the administrator's time zone | 4.1.M4 |
| 117501 | GN-26643 | Windows Agent | An issue where the previously displayed authentication window continues to appear even if the agent self-authentication window action policy is removed | 5.0.0, 6.0.0 |
| 117501 | GN-26606 | macOS Agent | An issue where login is not performed when entering the enter key once in the macOS authentication window | 5.0.15 |
| 117501 | GN-26551 | macOS Agent | When the macOS agent checks conditions for performing multiple actions, only the results of the last condition are displayed | 5.0.21, 6.0.0 |
| 117501 | GN-26490 | Center | A problem with trying to connect to the default port when connecting to ZTNA when setting a custom server domain | 6.0.15 |
| 117501 | GN-26487 | WebUI | Fixed an issue where an error page was displayed when there was no value on the CVE detail screen | 5.0.24 |
| 117501 | GN-26459 | Sensor | An issue where ZTNA Client Split Tunneling does not work when using the IP fixed option | 6.0.11 |
| 117501 | GN-26432 | Windows Agent | A problem where the logo is displayed in the upper left corner of the Windows authentication window and wireless connection manager | 5.0.39, 6.0.0 |
| 117501 | GN-26431 | WebUI | 관리콘솔 접속 IP 확인시 "x.x.x.x, x.x.x.x" 형태로 접속IP 가 확인되는 경우 접속 가능 IP라도 접속이 되지 않는 문제 | 5.0.33 |
| 117501 | GN-26408 | Sensor | A problem where sensor daemons die intermittently when conditions that do not belong to the node group are added to the node group | 4.0.114, 5.0.11 |
| 117501 | GN-26382 | WebUI | Http Status 400 - Bad Request can occur when setting or adding SAML IdP in User Authentication > Authentication Integration > SAML2 Authentication Integration | 5.0.25 |
| 117501 | GN-26380 | WebUI | The problem of not being able to download the IP application form from IPMGMT | 5.0.43, 6.0.0 |
| 117501 | GN-26372 | Center, Sensor | An issue where ZTNA Client's web access is not communicated via SWG after URL Filter is enabled | 6.0.12 |
| 117501 | GN-26354 | Center | A problem displaying unconnected local DB account information when linking authentication | 5.0.53 |
| 117501 | GN-26341 | Authsync | A problem where information other than ID is not synchronized when synchronizing Tibero/AltiBase/DB2 information | 6.0.8 |

continues on next page

Table 17 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 117501 | GN-26314 | WebUI | A problem where the label is not displayed on the IP application form when the department name etc. are removed from the IP application list settings | 4.0.11 |
| 117501 | GN-26299 | Center | Authentication permission issue even if the domain is different from the user domain associated with authentication | 5.0.53 |
| 114063 | GN-26566 | WebUI | An issue where the changed information was updated and not displayed when the tab was moved after updating the node information | 5.0.50 |

## 23.4.25 Genian ZTNA 6.0.15 Release Notes (2023-05-17)

Last Updated: 2023-07-20

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 116655 | GN-26814 | Center | Code improvements to Bufferoverflow | | 2 |
| 115659 | GN-26725 | Linux Agent, macOS Agent, Windows Agent | [Agent] Added validation for events sent from the Center and sensors | | 6.3 |
| 114716 | GN-26368 | WebUI | Vulnerability where an administrator's API key is exposed to other administrators | | 5.3 |
| 114205 | GN-26392 | WebUI | Vulnerability that allows unprivileged administrators to download debug logs | | 2.9 |
| 113812 | GN-26222 | WebUI | A problem where redirection can be performed by modulating the returnURL parameter used when moving pages in the management console | | 1.9 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 117753 | GN-26702 | WebUI | A function that outputs a warning when external access is permitted from the policy server | |
| 117445 | GN-26769 | Linux Agent | Linux Agent, development of distribution plug-ins based on Sigstore electronic signatures | |

continues on next page

Table 18 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 117369 | GN-26755 | Center, Linux Agent, macOS Agent, WebUI, Windows Agent | Development of distribution plug-ins based on Sigstore electronic signatures | |
| 116763 | GN-26826 | geniup | A problem where a disk runs out when performing geniup on a UEFI system | |
| 116385 | GN-26844 | Center, Sensor | Display whether the sensor can be accessed externally in sensor information (public IP) | |
| 116215 | GN-26705 | Center | Electronic signature verification of update server distribution data via SLSA | |
| 115882 | GN-26786 | Center | Electronic signature verification for WSUSSCN2.CAB received from the update server | |
| 115309 | GN-26336 | Center | Improved so that RADIUS secondary authentication can be linked using ExtSVC | |
| 114491 | GN-26631 | Docker | Improved so that DKNS can run on Linux systems using nftables | |
| 114376 | GN-26043 | Sensor | Improved so that authentication and encryption algorithms can be selected when the SNMP Agent is running | |
| 114251 | GN-26328 | WebUI | Improved to include node group names when downloading node groups in Excel | |
| 114195 | GN-26568 | WebUI | Improved so that the node group conditions can be entered directly when setting the software name include/not included | |
| 113890 | GN-26359 | Windows Agent | Added a feature to force the use of Windows's 'Wi-Fi random hardware address option' | |
| 113812 | GN-26515 | Enforcer | DKNS Ubuntu 22.04 support | |
| 113812 | GN-26462 | WebUI | Improved so that customer information is not displayed on the management UI login screen | |
| 113812 | GN-26348 | WebUI | Improved the title of the node blocking rate status widget displayed in the control policy list | |
| 113812 | GN-26329 | Windows Agent | Added a feature that allows you to forcibly disable the Windows logon screen display settings when controlling the screen saver | |
| 113812 | GN-26321 | WebUI | A problem where the OS type combo box on the device group screen is output as an empty value | |
| 113812 | GN-26301 | WebUI | Improved info message style in the IP settings window that allows access | |
| 113812 | GN-26279 | WebUI | Dashboard widget added dialog UI/UX improvements | |
| 113812 | GN-26254 | WebUI | Improved so that ZTNA client information is displayed normally in a redundant environment | |
| 113812 | GN-26207 | Center, DKNS | Apply ztnaclient/urlfilter dynamic service port | |
| 113812 | GN-26192 | WebUI | SAML Service Provider Metadata Creation Function | |
| 113812 | GN-26186 | Center | Improved the part where the audit log type did not match due to event key mismatch | 5.0.33 |

continues on next page

Table 18 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 113812 | GN-26183 | WebUI | Fixed so that the end date of use of the IP application system is not displayed by default on the same day when applying for an IP | |
| 113812 | GN-26171 | CWP | Improved so that the administrator's ID is not displayed in CWP announcements | |
| 113812 | GN-26148 | Center | Improved so that when the agent logs on, node information can be updated immediately if it is determined that the device is different from the existing node | |
| 113812 | GN-26139 | Sensor | Improved so that ZTNA client session management works when policy servers are redundant | |
| 113812 | GN-26123 | WebUI | Improved the part where millisecond values are output in the DateTime value of emails sent after listening to the user | |
| 113812 | GN-26104 | Center | [General-purpose OS] Improved the flow log collection function to work (Filebeat added) | |
| 113812 | GN-26037 | WebUI | Improved so that a reason input pop-up window appears when approving/rejecting on the user application details page | |
| 113812 | GN-26031 | Center, Database | Adding node group conditions using system information (motherboard) collected by agents | |
| 113812 | GN-25782 | Linux Agent | Linux Agent adds password validation action function | |
| 113812 | GN-25540 | GenianOS | Change the CA certificate validity period to 10 years | |
| 113812 | GN-25196 | Sensor | Implementation of VXLAN connection function between ZTNA gateways (sensors) | |
| 113812 | GN-24116 | WebUI | Added an API function linked to external services | |
| 113812 | GN-22197 | Center | Added a function to enable OAUTH 2.0 ROPC authentication | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 117409 | GN-26213 | WebUI | An issue where an option value that does not change when assigning a node group after creating a node policy appears to have changed | 5.0.44 |
| 117204 | GN-26852 | Center, Genian Syncer | An issue where Mobilebrowser data cannot be updated when uploading Genie data via Syncer, and an issue where CVE data versions cannot be updated | 4.1.0 |
| 117179 | GN-26770 | Center, Sensor | [General-purpose OS] A problem where the sensor does not work as a distribution server | 5.0.29 |
| 116850 | GN-26839 | Center, Sensor | Policy Server/Sensor Memory Rick (Genie Update and Node Scan (https)) issues | 4.0.14 |
| 116693 | GN-26768 | WebUI | Node addition field - error not reflecting user selector setting options | 5.0.22 |
| 116649 | GN-26767 | WebUI | Missing license and notification message display | 6.0.0 |

continues on next page

Table 19 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 116622 | GN-26816 | WebUI | An error where the output is broken if the nodegroup's CWP message has a tag | 5.0.37 |
| 116612 | GN-26779 | WebUI | A problem where a warning message is output even when the log server (elasticsearch) is in a normal state | 5.0.23 |
| 116606 | GN-26773 | WebUI | An issue where node group conditions do not work in the node list query API | 5.0.54, 6.0.14 |
| 116577 | GN-26758 | Windows Agent | If the agent runs on a local system, the Store app fails to be deleted through the program removal plug-in | 5.0.42, 6.0.0 |
| 115782 | GN-26749 | Elastic-Search | [General-purpose OS] An issue where ES does not run properly intermittently because communication with Elastic is blocked by the Iptables policy | 5.0.31 |
| 115635 | GN-26727 | Sensor | [General-purpose OS] A problem where a DHCP server that assigns the same DNS as the sensor is detected as an abnormal DHCP server | |
| 115608 | GN-26706 | WebUI | Modify the search popup to work when the 'Add Node Field - User Selector' option does not allow text entry | 5.0.22 |
| 115567 | GN-26748 | WebUI | Audit > An issue where the loading image does not disappear due to a JavaScript error when clicking Application Detail on the Flow list screen | 6.0.8 |
| 115370 | GN-26719 | WebUI | An issue where when creating a time object from the Policy > Object > Time menu causes the date to be stored incorrectly if the System Timezone and Administrator Timezone are different | 5.0.34 |
| 115297 | GN-26601 | WebUI | An issue where unused IPs cannot be selected in the matrix view when the administrator's management scope is set to a sensor group | 4.0.117, 5.0.14 |
| 115246 | GN-26739 | CWP | Your security key has already been generated during the CWP security key issuance process during the initial authentication after user registration in Google OTP 2-step authentication. A phenomenon where the phrase “” is displayed | 6.0.13 |
| 115118 | GN-26428 | Center | A problem that may fail depending on the OS type when upgrading the deb image through the console UI | 5.0.42, 6.0.12 |
| 115105 | GN-26571 | Enforcer | An issue where the blocking node appears to be communicating due to a SYN-ACK response from the sensor even when CWP is disabled | 5.0.0 |
| 115040 | GN-26660 | Docker, Sensor | A problem where the DKNS sensor is registered as a new sensor every time the IP is changed | 6.0.0 |
| 115019 | GN-26607 | GenianOS | The problem of not being able to connect to the Genian Monitor program from the IP that allows access to the management WEBUI | 5.0.42, 5.0.50, 5.0.53, 6.0.13 |
| 114878 | GN-26654 | macOS Agent | macOS screensaver settings are not enforced when users manually change them | 5.0.45, 6.0.2 |
| 114830 | GN-26409 | Linux Agent | Linux Agent, Agent-related UI behavior errors (tray icon, etc.) due to failure to collect login user information | 6.0.15, 5.0.55 (LTS) |
| 114819 | GN-26647 | WebUI | Fixed an issue where Disk column content was not displayed on the system management screen | 5.0.23 |
| 114639 | GN-25626 | WebUI | An issue where regular users are searched even when the visitor's email approval target is an administrator | 4.0.M8 |

continues on next page

Table 19 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 114611 | GN-26629 | WebUI | A problem where the node management screen is moved through a quick search, and when performing a batch task after selecting all nodes, a message that no nodes have been selected is displayed | 4.0.114, 5.0.11 |
| 114555 | GN-25887 | WebUI | Subcategories are not displayed in the multi-level category structure within the status filter node group | 5.0.42, 5.0.45, 6.0.2 |
| 114516 | GN-26620 | Enforcer | IP collision protection An issue where collision protection is applied even on a normal Mac when unknown mac is set | 4.0.17 |
| 114498 | GN-26402 | Center, Sensor | An issue where the PROCMON daemon may hang when changing RADIUS settings | 6.0.3 |
| 114309 | GN-26597 | WebUI | A problem where query reports are not generated when the DB/Log server is separated | 5.0.37 |
| 114297 | GN-26532 | WebUI | Fixed an issue where the number of NIC vendor status did not match | |
| 114258 | GN-26609 | WebUI | An error occurs when registering a node using the node addition field (user selector-mapping column name) | 5.0.42, 5.0.50, 6.0.11 |
| 114230 | GN-26430 | WebUI | A problem where the department tree of the device usage application form does not appear in a cloud environment | 5.0.52, 6.0.13 |
| 114195 | GN-26465 | WebUI | An issue where existing settings are not selected as default values when modifying agent actions in node group conditions | 5.0.45 |
| 114195 | GN-26440 | WebUI | There is no change in the tag, but the node details are also updated and processed when the node details are modified | 5.0.22, 6.0.4 |
| 114195 | GN-26425 | WebUI | A problem where the data does not include the parent department when selecting the user department in the node group condition | 5.0.35 |
| 114150 | GN-26280 | Center | A problem where a multi-sensor device is registered in an approved state when re-registered after deleting it | 6.0.8, 5.0.50 |
| 114063 | GN-26566 | WebUI | An issue where the changed information was updated and not displayed when the tab was moved after updating the node information | 5.0.50 |
| 114007 | GN-26531 | WebUI | An issue where the tree list for all users by department does not appear | 6.0.7 |
| 113966 | GN-26587 | WebUI | Fixed an issue where the content in the node management department name column was not displayed properly | 6.0.5, 5.0.50 |
| 113812 | GN-26677 | Center | Unable to perform control actions within permission policies and Windows Firewall uncontrollable errors | 6.0.13 |
| 113812 | GN-26655 | WebUI | An error page occurred when exporting node management to Excel in the Compose version | 5.0.48, 6.0.6 |
| 113812 | GN-26549 | Sensor | Intermittent dnsmasq daemon restart symptoms | 6.0.12, 5.0.53 |
| 113812 | GN-26497 | Windows Agent | If you turn off server certificate verification for the wireless profile (EAP-TTLS) in the wireless connection manager, you cannot connect | 5.0.49, 6.0.7 |
| 113812 | GN-26411 | ulogd | A problem where disk capacity is insufficient due to a problem where logrotate does not work with ULOGD debug logs | 6.0.0 |

continues on next page

Table 19 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 113812 | GN-26377 | WebUI | Fixed an issue where batch sensor settings and operation modes were not applied | 6.0.8 |
| 113812 | GN-26363 | WebUI | A problem where the session expiration page is output and node information is not displayed properly when connecting to CWP | 6.0.15 |
| 113812 | GN-26350 | Center | A problem where the sensor is not authenticated because RADIUS is not automatically allowed when using the general-purpose OS ZTNA client | 6.0.10 |
| 113812 | GN-26335 | Windows Agent | An issue where the agent tray icon is not displayed when connecting remotely to a PC | 5.0.0, 6.0.0 |
| 113812 | GN-26317 | WebUI | An error occurred when adding the same conditions to the user/new application option in the visitor's purpose settings | 4.0.11 |
| 113812 | GN-26288 | WebUI | An error where the list output becomes strange after modifying a custom field | 4.0.11 |
| 113812 | GN-26272 | Center | SMTP authentication integration - Abnormal user authentication issue when using [account] @ [domain] ID format | 5.0.53 |
| 113812 | GN-26250 | Linux Agent | Linux Agent misses gathering some network interface information | 5.0.51, 6.0.12 |
| 113812 | GN-26236 | WebUI | Node Details Software Information Tab Pagination ui Unification | 6.0.4, 6.0.9 |
| 113812 | GN-26204 | Center | Problems with "File read failed.ERRMSG=Isa directory" debug during policy server installation | 5.0.42, 4.0.152 |
| 113812 | GN-26194 | Sensor | A problem where IPTABLES is created in duplicate when changing http/https port settings | 4.0.17 |
| 113812 | GN-26190 | Sensor | An issue where TCP packets are blocked in a redundant environment | 6.0.15 |
| 113812 | GN-26181 | Linux Agent | Linux Agent, an issue where the tray icon is not displayed when switching to a user who is already logged in | 5.0.41, 6.0.0 |
| 113812 | GN-26097 | WebUI | A problem where node management does not proceed when exporting to Excel | 4.0.2 |
| 113812 | GN-25955 | WebUI | A problem where some information is missing when copying device group policies | 6.0.3, 5.0.46 |
| 113812 | GN-25916 | Center | A problem where the number of IPs that can be assigned decreases after ZTNA authentication replacement fails | 6.0.14 |
| 113812 | GN-25148 | WebUI | Error where WebUI smart help settings are not displayed | 5.0.49, 6.0.7 |
| 113318 | GN-26444 | WebUI | Symptoms of not being able to search for Hangul in the software settings window under node group conditions | 5.0.35 |

## 23.4.26 Genian ZTNA 6.0.14 Release Notes (2023-04-12)

Last Updated: 2023-05-16

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 113417 | GN-26391 | WebUI | Vulnerability where an unauthorized administrator can view debug logs in real time | 5.0.0, 6.0.0 | 2.9 |
| 113217 | GN-26460 | Windows Agent | A vulnerability that allows an ordinary user to obtain PC administrator rights via an agent | 5.0.0, 6.0.0 | 4.6 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 113565 | GN-26098 | WebUI | Improved the issue where the browser is stuck (frozen) when the dashboard screen is displayed | |
| 113517 | GN-26494 | WebUI | Add data loading display to dashboard widgets | |
| 113466 | GN-26493 | WebUI | Improved management console login time verification method | |
| 112778 | GN-26167 | Authsync | Postgresql package upgrade to support SCRAM-SHA-256 authentication | |
| 112778 | GN-26138 | Center | A problem where users who are forced to change their password during ZTNA authentication cannot access the password change page due to client authentication failure | |
| 112778 | GN-26105 | WebUI | Improvement of the width (width) of the node management operation status chart | |
| 112778 | GN-26073 | Sensor | Change to not MASQUERDE for NAT exception bands only | 6.0.5 |
| 112778 | GN-25993 | Center | Ability to restore previous versions of GPDB/NMDB updates | |
| 112778 | GN-25990 | WebUI | User add/update function through SAML Assertion Attribute (user information) | |
| 112778 | GN-25959 | Center | Improved to leave an audit log when automatically returning | |
| 112778 | GN-25940 | Linux Agent | Linux Agent, offline installation package creation tool development | |
| 112778 | GN-25921 | Linux Agent | Linux Agent, log cleaning function added | |
| 112778 | GN-25882 | Linux Agent | Linux Agent Improves Action Plugin Policy Option UX | |
| 112778 | GN-25704 | Sensor | Fixed so that CWP redirect works even when connecting via PROXY | |
| 112778 | GN-25630 | Center | Improved to enable BULK transmission when linked to an external WEBHOOK function of the audit log search filter | |
| 112778 | GN-25613 | Linux Agent | Linux Agent, vaccine information collection and data conversion work | |
| 112778 | GN-25517 | WebUI | Improvement for columns that cannot be sorted due to the application of a converter in the node list | |
| 112778 | GN-25337 | WebUI | Improved so that audit logs generated during a specific time period can be set as a search filter every day | |
| 112778 | GN-25204 | Center, Sensor | Add application information to Flow audit records when accessing the Web via SWG | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 113764 | GN-25776 | Center | Improved so that password change expiration notifications are not displayed for users without a password and synchronized users (READ ONLY) | 4.0.18 |
| 113658 | GN-26554 | Sensor | Too many open file errors occur in Ubuntu NAC Center/Sensor Equipment and the sensor status goes down | 5.0.51, 6.0.11 |
| 113558 | GN-26448 | WebUI | An error where policy server information is not output from the system list after installing the Compose method | 5.0.6 |
| 113539 | GN-26540 | Windows Agent | Windows 11 is incorrectly displayed as Windows 10 when selecting the plug-in 'Applicable OS' in the English management console. | 5.0.42, 6.0.0 |
| 113484 | GN-26267 | WebUI | An issue where today's audit log is not output from Audit > Logs before 9:00 KST | 4.0.17 |
| 113398 | GN-26357 | WebUI | A problem where the old version of the detailed screen is displayed when returning to the basic status from the target node list on the new node group detail screen | 5.0.35 |
| 113369 | GN-26518 | Center | An issue where information collected by the agent (updateinfo) may be deleted | 5.0.52, 6.0.13 |
| 113354 | GN-26322 | macOS Agent | An issue where CPU usage increases when receiving macOS notification messages | 5.0.27 |
| 113340 | GN-26446 | Center | An issue where the center daemon's fd increases when the LDAP connection fails | 5.0.41, 4.0.145, 6.0.0 |
| 113318 | GN-26444 | WebUI | Symptoms of not being able to search for Hangul in the software settings window under node group conditions | 5.0.35 |
| 113230 | GN-26496 | CLOUD | An issue where log statistics data is not displayed when a cloud site is first created | 5.0.50, 6.0.12 |
| 113147 | GN-26296 | Windows Agent | A problem where other action policies malfunction when there are a large number of USB exception policies in the device control policy | 5.0.0, 6.0.0 |
| 113128 | GN-26353 | Authsync | An issue where a fixed value is not set when syncing Google G Suite information | |
| 113042 | GN-26414 | Windows Agent | A problem where the fixed option in the password verification window is periodically placed in the center of the screen even when the fixed option is off | 5.0.42, 6.0.12, 5.0.53 |
| 113035 | GN-26454 | Sensor | Sensor HA configuration, problem where the slave sensor does not generate a default application list and terminates abnormally | 6.0.14 |
| 113027 | GN-26433 | Sensor | An issue where sensor communication may not be possible due to an incorrect IP rule being created when adding a gateway IP | 5.0.42 |
| 112970 | GN-26367 | WebUI | A problem where the explanation for the two-step authentication settings in the RADIUS policy appears in Korean when changing multiple languages | 6.0.11 |
| 112778 | GN-26331 | WebUI | Add multilingual processing and chart time zone settings in dashboard widget settings | |
| 112778 | GN-26320 | WebUI | An issue where an error occurs when creating a security group policy due to in/outbound conditions | 6.0.3 |
| 112778 | GN-26233 | Windows Agent | An issue where the audit log is broken when connecting to a VPN via ztnaClient if Korean is present in the interface name | 6.0.0 |
| 112778 | GN-26132 | Center | A problem that does not apply when the ZTNA Client's existing sensor IP is specified as a different IP on the same network | 6.0.4 |
| 112778 | GN-26102 | WebUI | An issue where the calendar screen is hidden by the menu tab when the vertical view is small when setting a node | 6.0.4 |
| 112778 | GN-26099 | Center | "IP+User ID" node manual registration, problem that pre-registered IP is not assigned | 6.0.11 |
| 112778 | GN-26027 | Center | A problem where the IPM icon is not displayed when registering a node that has set a change ban on unused IPs | 4.0.8 |

### 23.4.27 Genian ZTNA 6.0.13 Release Notes (2023-03-13)

Last Updated: 2023-04-14

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 112768 | GN-26286 | WebUI | An issue where Google OTP 2-step verification can pass 2-step verification by receiving a new security key | | 6.5 |

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 112639 | GN-26337 | macOS Agent | Add a macro for the user path to the macOS action execution condition | |
| 112190 | GN-26255 | WebUI | Increase OTP input length to 32 characters | |
| 111909 | GN-26039 | Center | A problem where client alternative authentication fails due to IP that allows authentication when authenticating ZTNA clients | |
| 111909 | GN-25874 | Center | Change the center API status logging cycle (1 day to 10 minutes) | |
| 111909 | GN-25860 | WebUI | Improved so that comments can be saved in the audit log when adding tags | |
| 111909 | GN-25710 | Center | Add procmod to monitor syslog-ng | |
| 111909 | GN-25550 | WebUI | Improved so that a list of places of use can be output and deleted on the detailed screen of node/control actions | |
| 111909 | GN-25501 | WebUI | Passkeys authentication is supported as primary authentication - Management Console (MC) | |
| 111909 | GN-25035 | CWP | Passkeys authentication is supported as primary authentication - user (CWP) | |

#### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 112765 | GN-26160 | Authsync, Center | A problem that may fail when downloading CSV and synchronizing user information | 5.0.0 |
| 112751 | GN-26385 | Packaging | C30G and C50G equipment monitor output problems | 5.0.44, 6.0.1 |
| 112679 | GN-26339 | dbmigration | A problem where version information in 6.0 products is incorrectly output as version 5.0 | 6.0.5 |
| 112671 | GN-26259 | Elastic-Search | Error displaying shard information in the Elasticsearch management tool on the Advance page | 5.0.17 |

continues on next page

Table 20 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 112654 | GN-26319 | WebUI | A problem where when clicking on the management device name on the audit log screen, node management is not retrieved and all are output | 5.0.38 |
| 112637 | GN-26223 | WebUI | A problem where only 50 tags are output when assigning tags on the node detail screen | 5.0.22 |
| 112631 | GN-26276 | Elastic-Search | The problem with Elasticsearch redundancy not being configured | 5.0.51, 6.0.11 |
| 112600 | GN-26242 | WebUI | An issue where agents installed on cloud OS (Linux) are displayed as a Windows icon in the node list in the management console | 6.0.8, 5.0.50 |
| 112529 | GN-26316 | Center | A problem where past passwords can be changed to a recently used password even when using the function to prevent reuse of past passwords | 3.0_1007 |
| 112507 | GN-26227 | Center | [General-purpose OS] An INVALID COMMON NAME certificate error occurs because the server certificate does not have Subject Alternative Names | 5.0.23 |
| 112382 | GN-26208 | WebUI | An issue where XSS detection logs are left when entering a search term containing < characters in the search box | 6.0.7, 5.0.50, 4.0.152 |
| 112366 | GN-26178 | WebUI | An issue where an XSS discovery log is left due to -> included in the detailed audit log message | 6.0.7, 5.0.50, 4.0.152 |
| 112312 | GN-26198 | macOS Agent | macOS agent secondary authentication error when connecting to a second ZTNA network | 6.0.2 |
| 112119 | GN-25936 | WebUI | A problem where node task commands that work regardless of management role permission settings do not work | 5.0.44, 6.0.1 |
| 112097 | GN-26219 | WebUI | An issue where an error occurs when copying a policy if the action has a label | 4.0.113, 5.0.10 |
| 112062 | GN-26170 | WebUI | A problem where adding/deleting components of the CWP design template in the English management console does not work properly | 5.0.48, 6.0.7 |
| 111951 | GN-26200 | Center | An issue where the CVE list is not updated in the latest versions of ZTNA and NAC | 5.0.50, 6.0.12, 5.0.53 |
| 111909 | GN-26119 | Windows Agent | A problem where APs allowed to connect are blocked due to capitalization comparison errors in wireless LAN control | 4.0.0, 5.0.0, 6.0.0 |
| 111909 | GN-26118 | Windows Agent | An issue where some printers are excluded when virtual printer collection exclusion is set in printer information collection | 4.0.0, 5.0.0, 6.0.0 |
| 111909 | GN-26095 | Center | An issue where the ZTNA Client connection option is intermittently disabled | 6.0.6 |
| 111909 | GN-26053 | Sensor | An issue where ARP Promises work in sensor Inline Global mode | 5.0.37 |
| 111909 | GN-26020 | Windows Agent | Print blank information from the dashboard by collecting printer information without content | 4.1.0, 5.0.0, 6.0.0 |
| 111909 | GN-26019 | Center | An issue where international SMS transmission fails when {_FULLMSG} is included in the SMS content of the search filter alarm transmission | 5.0.19 |
| 111909 | GN-26009 | Elastic-Search | 6.0 ES (7.17.7) The problem of not being able to configure clusters | 6.0.11 |

continues on next page

Table 20 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 111909 | GN-26008 | WebUI | An issue where the policy copy function does not work on the node group details screen | 5.0.31 |
| 111909 | GN-26005 | Genian Syncer | A problem where files with Korean paths cannot be uploaded to Genian Sinker | 4.0.0, 5.0.0, 6.0.0 |
| 111909 | GN-25999 | Windows Agent | A problem where the wireless interface is blocked due to a false wire detection due to an interface control action | 5.0.0, 6.0.0 |
| 111909 | GN-25996 | WebUI | An internal error occurred due to cloud VPC when modifying site information | 6.0.2 |
| 111909 | GN-25927 | Ubuntu(Debian) | [General-purpose OS] Improved so that web server status monitoring (FTSS) can be performed | 5.0.23 |
| 111909 | GN-25926 | Sensor | An issue where DKNS on the ARM platform cannot be upgraded via WebUI | 6.0.12 |
| 111909 | GN-25908 | Center | [General-purpose OS] CENTERD STAT - modified to count APACHE2 instead of HTTPD | 5.0.50 |
| 111909 | GN-25893 | WebUI | 5.0 A problem where the node target task command for task selection cannot be executed after selecting a node in node details. | 5.0.44, 6.0.1 |
| 111909 | GN-25846 | Database | The "Automatically Include Known Networks" setting of Adhoc Network Connection Risk Detection is not applicable | 5.0.21 |
| 111909 | GN-25817 | WebUI | An issue where incorrect search conditions are added when moving pages and performing tasks after moving from the agent version status widget to the node list | 5.0.26 |
| 111909 | GN-24674 | WebUI | Error: The phrase is displayed on the department output screen when assigning a department in the device usage application form | 5.0.42, 6.0.0 |

### 23.4.28 Genian ZTNA 6.0.12 Release Notes (2023-02-10)

Last Updated: 2023-03-17

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 111883 | GN-26150 | WebUI | Tomcat version upgrade (9.0.68 -> 9.0.72, 8.5.78 -> 8.5.86) | | |
| 111842 | GN-26205 | Database | MySQL version upgrade 5.7.40 -> 5.7.41 | | |
| 111646 | GN-25869 | CWP | A problem where only an account (ID) is authenticated when CWP is authenticated using the agent user authentication menu when the IP management message is first on | 6.0.3, 5.0.46 | 3.4 |
| 111295 | GN-26000 | MySQL | MySQL version upgrade 5.7.33 -> 5.7.40 | | |
| 111254 | GN-26062 | Center, macOS Agent, Sensor, Windows Agent | OpenSSL 1.1.1t upgrade - Passing random pointers to memcmp calls can read memory contents or cause denial of service | | 7.4 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 111631 | GN-26135 | macOS Agent | Added macOS file distribution options and improved logic related to file execution | 5.0.35 |
| 111205 | GN-25739 | WebUI | Add management roles when registering users in batches | |
| 111186 | GN-25994 | macOS Agent | Adding USB device information to the macOS hardware information collection plug-in | |
| 111033 | GN-26163 | Sensor | Changed to use the Dnsmasq Cache feature | |
| 111033 | GN-25933 | Center, Database | Improved so that ZTNA Client can set up multiple server domains | |
| 111033 | GN-25928 | Genian Syncer | Remove patch collection settings that are unnecessarily printed on Genius Sinker | |
| 111033 | GN-25914 | Sensor | A problem where ZTNA Client does not work in an ARM environment | |
| 111033 | GN-25911 | Zero Trust Security | Secondary DNS settings are reflected when ZTNA fixed IP is enabled | |
| 111033 | GN-25866 | Center | Improved ZTNA RADIUS secret settings to take precedence over RADIUS client settings | |
| 111033 | GN-25762 | Center, Sensor | Improved so that the physical interface can be used when connecting to a ZTNA client | |
| 111033 | GN-25752 | WebUI | Segmentation of memory widget output and improved operation | |
| 111033 | GN-25748 | Linux Agent | Linux Agent monitor information collection plug-in development | |
| 111033 | GN-25726 | Sensor | Site NAT exception band settings | |
| 111033 | GN-25718 | Center | Support for same network assignment for multiple sensors at ZTNA sites | |
| 111033 | GN-25622 | build | Added a script to check the amount of real-time network interface traffic | |
| 111033 | GN-25440 | Center | Fixed an issue where some nodes were deauthenticated due to automatic logout of unused nodes when using device authentication | |
| 111033 | GN-25049 | Linux Agent | Linux Agent, Popup module development and user notification message action function added | |
| 111033 | GN-24094 | Sensor | Detailed sensor upgrade failure audit records | |

## Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 113135 | GN-26130 | macOS Agent | Crash issue when using the macOS hardware information collection plug-in | 5.0.38 |
| 113080 | GN-26040 | WebUI | Change node management An issue where the administrator confirmation function does not work when selecting all nodes | 5.0.26 |
| 111889 | GN-26072 | Linux Agent | A problem where the Linux Agent gets stuck when running without using the GUI module | 6.0.12 |
| 111835 | GN-26188 | IPMGMT | A problem where temporary users cannot automatically log in to the IP application system | 5.0.50, 4.0.153, 6.0.11 |
| 111735 | GN-25998 | Windows Agent | (Password Verification Plug-in) An issue reported because the account's password change time is constantly changing | 4.0.M5, 5.0.0, 6.0.0 |
| 111726 | GN-25565 | Center | Center daemon abnormally shuts down when sending Syslog TLS | 4.1.M7 |
| 111667 | GN-26175 | Center | The phenomenon of continuing to download GPDB from cloud services using GDPI | 5.0.41 |
| 111618 | GN-26106 | Windows Agent | A problem where sharing is not disabled when setting the sharing allowance time in network shared folder control | 5.0.42, 5.0.50, 6.0.11 |
| 111584 | GN-26137 | WebUI | An issue where the CWP page preview screen is not visible on the CWP design template settings page | 5.0.42, 5.0.50, 6.0.11 |
| 111581 | GN-26124 | WebUI | A problem where the chart is not output when the FLOW log period is full | 6.0.0 |
| 111571 | GN-26161 | GenianOS | Fix sshd restart error in procmond | 5.0.23 |
| 111408 | GN-26125 | ulogd | A problem where the control policy ID cannot be stored in FlowLog | 6.0.1 |
| 111211 | GN-26035 | WebUI | An error page occurred when clicking on the download image in the detailed view of the IP usage application | 5.0.42, 5.0.50, 6.0.10 |
| 111161 | GN-26063 | IPMGMT | An issue where the automatic login function for IP usage applications does not work in CWP | 5.0.50, 4.0.153, 6.0.11 |
| 111033 | GN-26006 | Center | [General-purpose OS] Problem with ZTNA Client not working on Policy Server | 6.0.11 |
| 111033 | GN-25979 | Center | A problem where the policy application queue does not work properly when the RADIUS policy is changed multiple times | 5.0.23 |
| 111033 | GN-25978 | WebUI | A problem where the password length error is displayed even though the password was not changed when editing on the switch detail screen | 5.0.17 |
| 111033 | GN-25888 | Center | Symptoms of not being able to issue a Google verification code when synchronizing information with the mail server | 5.0.16, 6.0.0 |
| 111033 | GN-25859 | Enforcer, Sensor | [General-purpose OS] Sensor malfunction due to failure to create nac.ko module for ubuntu kernel version | 5.0.39, 6.0.0 |
| 111033 | GN-25830 | Sensor | An issue where snmp collection is not performed properly when collecting node details | 6.0.4 |
| 111033 | GN-25801 | WebUI | A problem where the 2-step authentication settings screen is displayed on the full user list screen | 6.0.7 |
| 111033 | GN-25756 | Windows Agent | The problem of not setting a manual proxy when running the agent on a local system | 4.0.0, 5.0.0, 6.0.0 |
| 111033 | GN-25675 | Center | An issue where the Agentless AD SSO function does not work without LDAP authentication settings | 5.0.44, 6.0.1 |
| 111033 | GN-25002 | Center | A problem where the platform and type of a node registered with the NAT IP node registration function are changed to unknown | 4.0.27 |

### 23.4.29 Genian ZTNA 6.0.11 Release Notes (2023-01-10)

Last Updated: 2023-02-10

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 111015 | GN-25982 | WebUI | CSP and HSTS headers added to WebUI Response Headers | | |
| 110942 | GN-25849 | WebUI | WebUI lib vulnerability check | | |
| 110495 | GN-25875 | Windows Agent | A problem where agents have high privileges when running a web browser | 4.0.0, 5.0.0, 6.0.0 | 3.3 |
| 110354 | GN-25811 | IPMGMT | A problem where you can log in with only a user ID via frontpage in the IP application system | | 4.9 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 110821 | GN-25891 | Windows Agent | Added a function to limit the number of open ports collected | |
| 110801 | GN-25280 | WebUI | User creation wizard function added | |
| 110619 | GN-24938 | WebUI | Modified so that when an email is sent immediately, the email is sent with node group data at the time of execution | |
| 110535 | GN-25579 | Center | Node snapshot cleanup function missing | |
| 110495 | GN-25865 | Windows Agent | Improvement of center load problems caused by infinite repetitive transmission in a short time when transmission of information collected from agents fails | 4.0.0, 5.0.0, 6.0.0 |
| 110215 | GN-25741 | Center, WebUI | Add an authenticated user item when registering a node | |
| 110215 | GN-25735 | WebUI | Print if the license has a limit on the number of agents on the license status screen | |
| 110215 | GN-25731 | WebUI | Improved to search all nodes instead of searching from the selected sensor when selecting equipment items in node details | |
| 110215 | GN-25727 | Ubuntu(Debian) | [General-purpose OS] Timestamp output to history history | 5.0.0, 6.0.0 |
| 110215 | GN-25666 | Center | [RADIUS] Improved so that audit logs can be sent externally through log filters | |
| 110215 | GN-25656 | RADIUSD | [RADIUS] Changed to output detailed failure audit logs when linking AD authentication | |
| 110215 | GN-25623 | Center, DKNS | Improved to be able to operate on multiple sensors with the same ZTNA Client settings | |
| 110215 | GN-25604 | Center | An issue where the agent installation icon is not displayed when the CWP agent installation message is deleted | 3.0_0910 |
| 110215 | GN-25592 | Center | Support for fixed IP assignment function for ZTNA users | 6.0.11 |
| 110215 | GN-25576 | Windows Agent | Always on ZTNA feature development | |
| 110215 | GN-25564 | Linux Agent | Linux Agent detects when changing the local network and develops additional tasks related to it | |
| 110215 | GN-25480 | Sensor | [General-purpose OS] Improved so that block device information is collected when collecting disk information | |
| 110215 | GN-25269 | Center | Improved to allow the USER macro to be used for additional RADIUS policy attributes | |
| 110215 | GN-25232 | WebUI | Added Macro settings help in the assignment parameter topic of the control policy CLI tool command | |
| 110215 | GN-24836 | Center | ZTNA Client Access Secondary Authentication grace time feature added | |
| 110215 | GN-24755 | Center | Apply BP announcements through geniupdate to NAC | |

## Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 114610 | GN-25945 | Center | [ZTNA] Unable to perform control actions within the permission policy and Windows firewall uncontrollable errors | 6.0.7 |
| 111461 | GN-26028 | Windows Agent | Fixed an issue where forced termination of a process did not work when there were multiple action policies to forcibly terminate the process | 5.0.25 |
| 110993 | GN-26042 | Linux Agent | Linux Agent, permission issues due to dbus connection errors | 6.0.6 |
| 110979 | GN-26029 | CLOUD | Cloud NAC user information not syncing problem | 6.0.3, 5.0.50 |
| 110971 | GN-26045 | CLOUD | An issue where the GDPI API is not set to use when creating a new Cloud Site | 5.0.50, 6.0.10 |
| 110966 | GN-25749 | WebUI | Errors when applying service objects tcp-all and udp-all in nhn cloud and naver cloud when setting up a security group | 6.0.9 |
| 110790 | GN-26018 | WebUI | An error occurred during approval on the detailed view screen of the new/return application form | 5.0.49, 6.0.8 |
| 110778 | GN-25964 | Windows Agent | An issue where the execution option after authentication disappears after upgrading the agent authentication window | 5.0.42, 6.0.3, 5.0.46 |
| 110736 | GN-25832 | WebUI | An issue where the management console session time changes when the PC time is changed | 5.0.48, 6.0.7 |
| 110566 | GN-25965 | Center | A problem with different event names when tunneling ZTNA sensors | 6.0.0 |
| 110440 | GN-25880 | Center | [General-purpose OS] Problem with not being able to output favicons | 5.0.37 |
| 110376 | GN-25861 | WebUI | An issue where custom report files are not generated | 6.0.4 |
| 110373 | GN-25889 | WebUI | A problem where the delete function does not work in switch management | 6.0.4 |
| 110346 | GN-25931 | CWP | When using Domain with On Premise, authentication is not possible because an authentication request occurs with an IP address during SAML authentication | 5.0.48 |
| 110215 | GN-25797 | WebUI | Fixed a malfunction issue with the empty selection node basket function | 5.0.44, 6.0.1 |
| 110215 | GN-25763 | WebUI | An error where items cannot be output when modifying the client assignment network when setting ZTNA-Client | 6.0.0 |
| 110215 | GN-25760 | WebUI | An issue where the node's IP policy is not properly reflected | 4.0.116, 5.0.13 |
| 110215 | GN-25730 | WebUI | A problem where the operation method of a node registered as ZTNA VPN is displayed incorrectly on the node detail screen | 5.0.32 |
| 110215 | GN-25712 | Windows Agent | A problem where Hangul is included when controlling the Hosts file through the DNS control plug-in, it malfunctions | 4.1.0, 5.0.0, 6.0.0 |
| 110215 | GN-25694 | WebUI | Fixed an issue where a node's management sensor could be set as a sensor Alias | 4.0.119, 5.0.16 |
| 110215 | GN-25686 | Windows Agent | Wireless related menu display error on the tray icon when the wireless connection manager is off | 5.0.0, 6.0.0 |
| 110215 | GN-25677 | CWP | An issue where the SAML login button is not displayed on the user re-authentication screen when moving to the CWP user information modification screen in a SAML authentication linked environment | 5.0.45, 6.0.2 |
| 110215 | GN-25507 | WebUI | When setting conditions for node actions, tooltips are not displayed on icons that appear in the condition column | 4.0.M1 |
| 110215 | GN-25489 | WebUI | A problem that is displayed as' (1) 'regardless of the number of node deletion commands sent in node management | 5.0.44 |

### 23.4.30 Genian ZTNA 6.0.10 Release Notes (2022-12-05)

Last Updated: 2023-01-10

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 110207 | GN-25925 | IPMGMT, WebUI | IP Application System > IP Application Screen XSS Possible Problems | | 5.4 |
| 109988 | GN-25847 | WebUI | Added a re-authentication procedure when accessing the user information modification page on the CWP screen | | 4.2 |
| 109886 | GN-25740 | WebUI | Issues where XSS is possible in Audit > Logs > Log search bar | | 5.6 |

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 109570 | GN-25657 | WebUI | Revise the application processing results for temporary use applications to be able to add and delete menus in IP management | |
| 109570 | GN-25639 | CLI/gnlogin, Database | Improved so that changes to the ssh port are immediately reflected in the DB | |
| 109570 | GN-25625 | WebUI | Modified to indicate that an additional user field is required when creating a required field | |
| 109570 | GN-25567 | Linux Agent | Linux Agent improved to be able to collect multiple IP and DNS configuration information (IPv4, IPv6) when collecting network information | |
| 109570 | GN-25513 | Linux Agent | Added a function to send agent version information to the center regardless of whether the Linux Agent or software information collection action is applied | |
| 109570 | GN-25494 | Windows Agent | Modified so that the password validation window can automatically close when detecting a password change | |
| 109570 | GN-25470 | WebUI | Improved so that when clicking on the node management operation status chart, the history management tab on the node detail screen can be displayed without changing the screen | |
| 109570 | GN-25278 | Windows Agent | Publish the agent installation package on the Microsoft Store | |
| 109570 | GN-25186 | Center | Netflow log Start/Close/Update/Deny selection option added | |
| 109570 | GN-24968 | WebUI | Add a back button to the detail page when moving to the node detail page from another screen | |
| 109570 | GN-24820 | WebUI | Audit > Log data usage display function added to the log screen | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 110912 | GN-25900 | Linux Agent | A problem where the number of receiving policies from the server increases during long-term use of the Linux Agent | 5.0.41, 6.0.0 |
| 110215 | GN-25616 | WebUI | An issue where the default widgets on the new dashboard are not added when creating a cloud site | 6.0.1 |
| 110209 | GN-25903 | macOS Agent | An issue where the agent malfunctions when the macOS file distribution plug-in file is not uploaded | 5.0.31, 6.0.0 |
| 110173 | GN-25796 | Center | A problem where the node type changes even when a node type is specified when registering a new node by an agent | 5.0.33 |
| 110152 | GN-25885 | Sensor | A problem where switch port information cannot be collected | 6.0.4, 5.0.47 |
| 110059 | GN-25863 | WebUI | A problem where the node management search term does not work if is in the search term | 5.0.42, 5.0.49, 6.0.8 |
| 109972 | GN-25868 | Center | An issue where no node (agent) up/down logs are left intermittently | 5.0.49 |
| 109939 | GN-25699 | WebUI | Problems where the filter results of the agent action in Status 현황&필터 의 에이전트 액션의 필터 결과가 상세조회 내역과 다른 문제 및 엑셀다운로드가 안되는 현상 Filter differ from the detailed query history, and Excel cannot be downloaded | 6.0.4, 5.0.48 |
| 109915 | GN-25819 | WebUI | A problem where node management search through software status does not work properly | 6.0.7 |
| 109766 | GN-25488 | WebUI | If the management console session timeout exceeds 60 minutes, the remaining time is not normal | 6.0.1 |
| 109752 | GN-25818 | WebUI | When uploading an agent file, an out of memory error occurs on a device with low memory and cannot be uploaded | 6.0.8, 5.0.50, 4.0.152 |
| 109720 | GN-25750 | Windows Agent | A problem where a web browser opens with an incorrect URL in the authentication window | 5.0.0, 4.0.123 |
| 109570 | GN-25864 | Genian Mobile | The problem with Genian NAC Monitor not being able to connect to the center | 5.0.49, 6.0.9 |
| 109570 | GN-25745 | Linux Agent | Linux Agent Issues Not Running Files With Root Permissions in "File Distribution" Plug-in | 6.0.8, 5.0.50 |
| 109570 | GN-25734 | Windows Agent | IE is displayed when clicking a hyperlink in an agent notification message | 6.0.4, 5.0.47 |
| 109570 | GN-25723 | Sensor | An issue where iptables rules are not removed after disabling ZTNA IPsec | 6.0.1 |
| 109570 | GN-25652 | WebUI | When moving by clicking on the platform quantity in the CVE status widget on the dashboard, an error occurred when clicking the list button | 5.0.43, 6.0.0 |
| 109570 | GN-25621 | WebUI | An issue where the header image was added on the login page but it wasn't printed | 6.0.7 |
| 109570 | GN-25608 | Windows Agent | The problem of automatic authentication without receiving authentication information again after GTC authentication as a wired authentication manager | 5.0.17, 6.0.0 |
| 109570 | GN-25575 | WebUI | An issue where selecting a date from the calendar in the node report search bar selects a different date than the selected date | 5.0.8 |
| 109570 | GN-25553 | WebUI | A phenomenon where the detailed information content is broken when the audit log is exported to Excel | 5.0.21 |
| 109570 | GN-25549 | dbmigration | RADIUS Accounting does not work after creating a CLOUD customer site | 5.0.33 |
| 109570 | GN-25543 | WebUI | Fixed an issue where the icon was not displayed in the node list authentication user column after user authentication with SAML2 | 5.0.19 |
| 109570 | GN-25430 | WebUI | An issue where the agent action condition (agentActionName) is not queried in the search bar of node management | 6.0.7 |

### 23.4.31 Genian ZTNA 6.0.9 Release Notes (2022-11-11)

Last Updated: 2022-12-05

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 109583 | GN-25753 | WebUI | Improved so that CWP does not redirect to an illegal path via the PAGEFW parameter | | 4.2 |
| 109400 | GN-25746 | Center, Sensor | Secure coding inspection results vulnerability patch | | |
| 108915 | GN-25438 | Center, Sensor | Improved the _filelist.html file to be generated differently for each center | | 3 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 109642 | GN-25446 | Linux Agent | Linux Agent develops additional collection function for Sophos Linux vaccine information | |
| 109174 | GN-25570 | Center, WebUI, Windows Agent | Fixed an issue where a duplicate login process was required due to CWP when registering a security key when using Google OTP secondary authentication | 6.0.2 |
| 109081 | GN-25601 | WebUI | An issue where application information is disabled on the IP usage application modification screen | |
| 109071 | GN-25640 | WebUI | Modified the custom report tree menu to output only reports created by me | |
| 108915 | GN-25510 | WebUI | When adding a ZTNA gateway, an error message is output when selecting an unsupported site | |
| 108915 | GN-25496 | macOS Agent | Change the check cycle to enable automatic macOS agent update load balancing | |
| 108915 | GN-25479 | WebUI | Remove the html syntax of the device usage application processing notification message | |
| 108915 | GN-25477 | macOS Agent | Duplicate processing of popup messages when using the wireless LAN control plug-in in macOS sleep mode | |
| 108915 | GN-25457 | WebUI | Send an 'instance message' via REST API | |
| 108915 | GN-25450 | Linux Agent | Linux Agent adds a feature to clean up actions when an agent is deleted | |
| 108915 | GN-25416 | Linux Agent | Handling exceptions for using different time zones on the Linux Agent and Policy Server | |
| 108915 | GN-25407 | WebUI | UI division between calendar current date and selected date | |
| 108915 | GN-25388 | Windows Agent | Adding help to the Wireless LAN Control Plug-in for the "Allowed SSID-Regular" option | |
| 108915 | GN-25333 | RADIUSD | RADIUS EAP-TTLS support (MSCHAPv2, PAP) | |
| 108915 | GN-25322 | WebUI | Add each column to the user management view when the last authentication was deactivated | |
| 108915 | GN-25321 | Windows Agent | Action policy CONF settings UX improvements | |
| 108915 | GN-25312 | Linux Agent | Linux Agent, Always on ZTNA function development | |
| 108915 | GN-25231 | WebUI | Fixed an issue where loading takes a long time when clicking on the MAC address condition in node group conditions | |
| 108915 | GN-25212 | WebUI | Improved output of the period (date and time input format) input item on the CWP new user registration screen | |
| 108915 | GN-25134 | Linux Agent | Development of basic structures and VPN connection management functions for essential operations through Linux Agent and CLI | |
| 108915 | GN-25096 | Center | Improved so that RADIUS MAC authentication node group checks can be compared using Calling-Station-Id | |
| 108915 | GN-25077 | WebUI | Passkeys alternative authentication method added | |
| 108915 | GN-24841 | Linux Agent, WebUI, Windows Agent | Added the ability to delete the content set in the sub-item when changing the settings in the Windows Firewall Control plug-in's custom rules to All | |
| 108915 | GN-24705 | Windows Agent | Blocked page display function through Captive Portal Detection | |
| 108915 | GN-24504 | WebUI | Naver CLOUD (NCP) support | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 109403 | GN-25671 | WebUI | ZTNA between Hub-Branch - IPSec Pre-Shared Key Setup Error | 6.0.1 |
| 109323 | GN-25708 | macOS Agent | macOS agent crash issues | 5.0.45, 6.0.2 |
| 109233 | GN-25663 | macOS Agent | IP input window output when installing the macOS agent in an environment where the Internet connection is blocked | 5.0.27, 6.0.0 |
| 109217 | GN-25720 | IPMGMT | The problem of not being able to apply for a new temporary user IP | 4.0.149, 6.0.6, 5.0.49 |
| 109158 | GN-25645 | Center | A problem where platform detection data files (scanraw) created with the IP before the change cannot be cleaned up when the DHCP node IP is changed | 4.0.M7 |
| 109150 | GN-25589 | Center | Bad type conversion error occurs when deleting a node due to deleting an IP change node | 5.0.46, 6.0.5 |
| 108989 | GN-25698 | WebUI | Message size error when sending collector data | 6.0.0 |
| 108938 | GN-25669 | WebUI | A problem where the column size is adjusted in the node list and then updated, the adjusted size is not output | 6.0.7 |
| 108915 | GN-25574 | macOS Agent | An issue where message-related IDs within the macOS agent cannot be imported properly | 5.0.50, 6.0.9 |
| 108915 | GN-25568 | WebUI | A phenomenon where items are canceled when applied immediately after selecting all in the node policy | 6.0.4 |
| 108915 | GN-25559 | Windows Agent | The problem of not being able to connect due to incorrect registration of the Hangul SSID profile through the wireless connection manager | 4.0.5, 5.0.0, 6.0.0 |
| 108915 | GN-25498 | macOS Agent | An issue where the screensaver option in the macOS Appearance and Personalization plug-in doesn't apply | 5.0.15, 5.0.45, 6.0.2 |
| 108915 | GN-25462 | Genian Monitor | Web page error display issue when clicking on details in Genian Monitor for Windows | 5.0.19, 6.0.0 |
| 108915 | GN-25443 | Center | A problem where the certificate expiration log remains based on the device certificate even when using a custom certificate | 5.0.0 |
| 108915 | GN-25439 | Center | An issue where the agent installation node's platform changes to Unknown when manually updating GPDB | |
| 108915 | GN-25428 | Ubuntu(Debian) | [General-purpose OS] Problem of not being able to upload and download agent installation files after restoring agent files | 5.0.23, 6.0.0 |
| 108915 | GN-25418 | GenianOS | [General-purpose OS] An issue where the file export (Excel Export) function does not work | |
| 108915 | GN-25400 | WebUI | A problem where normal output is not displayed when the node list is moved and then re-searched or the page is moved through the status widget for each agent version | 5.0.42, 5.0.45, 6.0.2 |
| 108915 | GN-25399 | Center, Database | An issue where the number of nodes in the Windows update status is displayed incorrectly when assigning a Windows Update action label | 4.0.113, 5.0.10 |
| 108915 | GN-25390 | Sensor | An issue where permissions do not work properly when using FQDN network objects | 5.0.27 |

continues on next page

Table 21 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 108915 | GN-25381 | Center, CLOUD | Symptoms of a certificate not being reissued with the Reissue Certificate button in the CLOUD version | 5.0.45, 6.0.2 |
| 108915 | GN-25364 | WebUI | A problem where visible processing of child settings is not processed properly when the CONF On/Off button is set as the parent | 5.0.16 |
| 108915 | GN-25350 | WebUI | An issue where a logged-in administrator UI session ends after approving/rejecting an email for a new IP application | 4.1.0 |
| 108915 | GN-25345 | Center | [General-purpose OS] An issue where the automatic sensor upgrade function does not work when upgrading the policy server | 5.0.43, 6.0.0 |
| 108915 | GN-25340 | macOS Agent | An issue where the macOS operating system information collection plug-in fails to obtain the installation date | 6.0.4, 5.0.47 |
| 108915 | GN-25317 | Center | A problem where the time object is not released from the node group even after the end time of the node group condition | 4.1.3 |
| 108915 | GN-25289 | macOS Agent | macOS Device Control plug-in operation errors and log improvements | 6.0.3, 5.0.46 |
| 108915 | GN-25219 | Center | [General-purpose OS] An issue where master files are not synchronized to the Slave in an HA redundant configuration | |
| 108915 | GN-25159 | WebUI | An issue where all header lists set in URL calls are not deleted | 5.0.15 |
| 108915 | GN-25117 | WebUI | An issue where the node list is not detected when moving the agent-related widget | 5.0.33 |
| 108915 | GN-25081 | WebUI | An issue where device change approval is not processed in the IP application REST API | 5.0.7, 4.0.110 |

## 23.4.32 Genian ZTNA 6.0.8 Release Notes (2022-10-11)

Last Updated: 2022-11-08

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 109188 | GN-25561 | WebUI | Blind SQL Injection vulnerability in node search bar | | 5.3 |
| 108509 | GN-25184 | Sensor | Modified Dnsmasq to not cache query results in order to prevent DNS Cache Attacks | | 3.7 |
| 108074 | GN-23677 | Center, Sensor | Administrator approval system to enhance security when registering sensor policy servers | | 7.9 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 108806 | GN-25615 | Linux Agent | Linux agent registration and upgrade omissions added when installing and upgrading NAC | |
| 108767 | GN-25468 | WebUI | Allow spaces in registry values when setting action conditions | |
| 108676 | GN-25266 | Windows Agent | Show whether to use an empty password in the debug log when starting the password verification plugin | |
| 108630 | GN-25075 | WebUI | Added the ability to upload an image of an announcement | |
| 108274 | GN-24693 | Windows Agent | Background image support for authentication window lock screen | |
| 108074 | GN-25509 | Database | Initial Popup page changes for ZTNA | |
| 108074 | GN-25417 | macOS Agent | Prohibit closing the macOS agent authentication window | |
| 108074 | GN-25411 | WebUI | A problem where the loading bar is output after the Cloud Sensor is created, but the screen is not updated even after the Sensor is created | |
| 108074 | GN-25316 | GNOS | "Invalid DHCP Server Collection Information" - Always add output options to the relevant risk audit log | |
| 108074 | GN-25223 | Linux Agent | Linux Agent adds web browser integration downloaded from snap when connecting to a web browser via a tray icon | |
| 108074 | GN-25205 | WebUI | Node Details - Improved output of recent execution results on the Operating System Update Information tab | |
| 108074 | GN-25191 | WebUI | Provided so that the changed status can be checked with an image icon when 'agent service is stopped' | |
| 108074 | GN-25189 | CLI/gnlogin | Improved so that mgmt-local-port is applied when entering the mgmt-port CLI | 5.0.44, 6.0.2 |
| 108074 | GN-25176 | WebUI | File Upload component file name storage method and download improvements | |
| 108074 | GN-25161 | Center | Port bounce processing when the Switch Port VLAN is changed through the control policy | |
| 108074 | GN-25027 | WebUI | Expanded the character limit for input items in the audit log filter | |
| 108074 | GN-25015 | Linux Agent | Linux Agent, Genian Linux PAM (Pluggable Authentication Modules) development | |
| 108074 | GN-25006 | WebUI | Add an Application Name statistics pie chart to the Flow Log screen | |
| 107302 | GN-25095 | Linux Agent | Linux Agent develops file distribution action plug-in | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 108774 | GN-25482 | WebUI | New issues added when modifying condition settings in a policy group | 6.0.6, 5.0.49 |
| 108771 | GN-25481 | dbmigration | A data migration error related to registry settings occurred during an action condition | 5.0.48 |
| 108770 | GN-25032 | WebUI | Fixed an issue where the time period set for the tag was applied even when the untag time was set to an unlimited number | 5.0.21 |
| 108730 | GN-25086 | WebUI | An error occurred when clicking on a report item belonging to an unspecified category | 5.0.38, 6.0.0 |
| 108538 | GN-25560 | WebUI | Script error issue when moving the policy tab after performing a search on the node management screen | 6.0.4 |
| 108173 | GN-25532 | WebUI | An issue where the USER_LASTPWCHANGE value is not updated when the user password is changed in CWP | 6.0.6, 5.0.49, 4.0.151 |
| 108074 | GN-25456 | macOS Agent | Problem with duplicate entry logs when uploading macOS agents | 5.0.45, 6.0.2 |
| 108074 | GN-25402 | macOS Agent | macOS hostname change plug-in success error | 5.0.34, 6.0.0 |
| 108074 | GN-25386 | macOS Agent | macOS forced process termination plugin not working | 5.0.0, 6.0.0 |
| 108074 | GN-25361 | Windows Agent | Wireless LAN control plug-in operation error when the SSID of the allowed AP is in Korean | 5.0.0, 6.0.0 |
| 108074 | GN-25357 | WebUI | An error occurred during approval on the detailed view screen of the new/return application form | 5.0.13 |
| 108074 | GN-25354 | macOS Agent | An issue where information cannot be collected when the macOS shared folder name contains a period | 6.0.4, 5.0.47 |
| 108074 | GN-25339 | WebUI | The phenomenon of switching to the analysis chart page when the refresh button is clicked while the log search and search filters are modified | 5.0.22 |
| 108074 | GN-25319 | WebUI | An error page is displayed when multiple nodeType conditions are entered and queried in the node list | 5.0.42, 5.0.45, 6.0.2 |
| 108074 | GN-25279 | WebUI | A problem where the results are incorrectly displayed in the node type widget from the node list moved to links of some node types | 5.0.43, 6.0.0 |
| 108074 | GN-25271 | Center | Modified so that only the linked interface is checked when applying the primary/secondary DNS condition policy | 5.0.0 |
| 108074 | GN-25259 | Windows Agent | A problem where the result of performing the previous action remains even if the node policy is changed to OFF or not to use the agent | 5.0.0, 6.0.0 |
| 108074 | GN-25253 | Windows Agent | After blocking device control, it is output in the audit log in the form of "ID = number" and modified to the policy name | 5.0.25, 6.0.0 |
| 108074 | GN-25238 | WebUI | A problem where there is no X button in the department search pop-up in the node group condition addition UI, and the cancel button is not displayed in the second department search pop-up when there is no department information | 5.0.20 |
| 108074 | GN-25216 | WebUI | A problem where a file cannot be uploaded properly when uploading a file via the REST API | 5.0.42, 5.0.45, 6.0.2 |
| 108074 | GN-25152 | IPMGMT | Page error when applying for IP use while violating the IP management policy | 5.0.11 |
| 108074 | GN-25147 | WebUI | An issue where all of the default node groups have been updated, but it may show that there is an updatable quantity | 5.0.27 |
| 108074 | GN-25144 | Center | A problem where the server connection fails if the authentication-linked server address contains a space | |

### 23.4.33 Genian ZTNA 6.0.7 Release Notes (2022-09-06)

Last Updated: 2022-10-11

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 107755 | GN-25237 | WebUI | CSAP (SaaS) security certification audit source code vulnerability measures | | 0 |
| 107447 | GN-25387 | Database, WebUI | Issues where management roles are not applied to Policy > Cloud Security Group Policy | | 3.5 |
| 107144 | GN-25309 | Center, Sensor | CSAP (SaaS) Security Certification Audit Source Code Vulnerability Measures - C/C++ | | 7.5 |
| 107144 | GN-25250 | WebUI | Possible problems with XSS when/is appended after the HTML Tag string | | 4.9 |
| 107144 | GN-25239 | WebUI | Tomcat version upgrade (8.5.78 -> 9.0.65) | | 7.5 |
| 107144 | GN-25193 | WebUI | [Universal OS Ubuntu] Management Console > An issue where the 'X-Frame-Options' header on the CWP Design Template list page is displayed as allowall | | 6.5 |
| 107144 | GN-25119 | macOS Agent | Upgrade to the latest versions of macOS Agent, OpenVPN (2.5.7), and OpenSSL (1.1.1q) | | 5.3 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 108044 | GN-25409 | WebUI | Improved access permission settings on the debug log screen | |
| 107868 | GN-24699 | Windows Agent | Passkeys (biometric authentication) function added to secondary authentication in the agent authentication window | |
| 107717 | GN-24803 | WebUI | Improved functionality related to report email forms, settings, and list search | |
| 107144 | GN-25273 | GenianOS | [General-purpose OS] Improved to allow custom use of apache2 settings | 6.0.3 |
| 107144 | GN-25201 | macOS Agent | macOS agent status recheck function | |
| 107144 | GN-25164 | GenianOS | Improved so that an audit log is left only when the information is updated when the owner is reset each time the authentication is performed | |
| 107144 | GN-25160 | Windows Agent | Update Sophos Endpoint Agent vaccine information | |
| 107144 | GN-25138 | Windows Agent | Provides gNPMS execution results as a result message of Windows update actions | |
| 107144 | GN-25137 | Linux Agent | Linux Agent, ARP management action plug-in development | |
| 107144 | GN-25125 | WebUI | Change the output order on the user creation screen | |
| 107144 | GN-25112 | Linux Agent | Development of operating functions based on Linux Agent and agent deletion method options | |
| 107144 | GN-25078 | Windows Agent | Consider expanding the monitor while using screen lock with the agent authentication window | |
| 107144 | GN-25025 | Windows Agent | Provide "EAP-TTLS" authentication method through wireless connection manager | |
| 107144 | GN-24950 | Windows Agent | Provide "EAP-TTLS" authentication method through wired authentication manager | |
| 107144 | GN-24929 | Enforcer, Sensor | Network control (blocking) function through application identification | |
| 107144 | GN-24913 | Windows Agent | Passkeys-based secondary authentication function added to ZTNA Connection Manager | |
| 107144 | GN-24814 | CWP, WebUI | REST API related to Passkeys (FIDO2 - biometric authentication) | |
| 107144 | GN-24745 | CWP | Passkeys authentication is supported as secondary authentication - user (CWP) | |
| 107144 | GN-24744 | CWP, WebUI | Passkeys authentication is supported as a second factor authentication - Management Console (MC) | |
| 107144 | GN-22592 | CWP | A problem where the component position falls to the bottom when the CWP design template component setting is turned off and on | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 108688 | GN-25129 | CWP, WebUI | A problem where SAML authentication cannot be linked to a policy server operated as an AMI image on AWS | 5.0.19 |
| 107849 | GN-25478 | WebUI | Fixed an issue where the IPMGMT Font Awesome icon was not displayed | 6.0.7 |
| 107708 | GN-25308 | WebUI | An issue where the session persists even after the session timeout period elapses after the management console wakes up from an idle state | 5.0.42, 6.0.0 |
| 107422 | GN-25380 | Sensor | Switch registration failure when SNMP v2 Community settings include special characters | 6.0.4, 5.0.47 |
| 107221 | GN-25099 | WebUI | An issue where the expiration date of the user registration form is not reflected when the email is approved | 4.0.M8, 5.0.41 |
| 107144 | GN-25343 | Windows Agent | A problem where a shared control notification popup for the managed folder appears every time the PC is booted | 5.0.0, 6.0.0 |
| 107144 | GN-25318 | Windows Agent | An issue where the password validation pop-up window can be closed even when using a weak password | 5.0.13, 6.0.0 |
| 107144 | GN-25301 | macOS Agent | macOS network shared folder disconnection malfunction and broken text issues | 6.0.4, 5.0.47 |
| 107144 | GN-25296 | Windows Agent | In an English window, the default logo in the agent authentication window is displayed in Korean. | 5.0.8, 6.0.0 |
| 107144 | GN-25222 | Linux Agent | Linux Agent, intermittent database access errors during long-term use | 6.0.4, 5.0.47 |
| 107144 | GN-25218 | WebUI | Loading bar output problem when clicking on fontawesome icon | 6.0.3, 5.0.46 |
| 107144 | GN-25211 | WebUI | Settings > Preferences > Admin Console > Authentication > Session Timeout Setting Error | 6.0.1 |
| 107144 | GN-25209 | WebUI | An issue where the 'Notification Message' tab menu is hidden under the detailed view when the node does not have an agent installed | 6.0.5 |
| 107144 | GN-25181 | Windows Agent | Fixed an error that occurred during two-step authentication via Google OTP for the first time | 6.0.2 |
| 107144 | GN-25163 | Windows Agent | A problem where vaccine information cannot be collected immediately on a node that has been deleted and re-registered as a new one | 5.0.0, 6.0.0 |
| 107144 | GN-25151 | Center | A problem where node groups cannot be matched if the software versions are the same/different when there are multiple software with the same name | 5.0.37 |
| 107144 | GN-25136 | WebUI | A problem where the count of satisfied/unsatisfied columns is incorrectly displayed on the node management screen | 5.0.33 |
| 107144 | GN-25130 | Genian Monitor | Items and settings cannot be modified in Genian Monitor for Windows | 5.0.0, 6.0.0 |
| 107144 | GN-25115 | WebUI | An issue where the IP address column was removed from the IP management application results column in the management console, but it was not reflected | 5.0.10 |
| 107144 | GN-25103 | Sensor | A problem where the mobile OpenVPN app does not register a node when connecting to ZTNA | 6.0.0 |
| 107144 | GN-25080 | Authsync, Center | A problem where synchronization is not performed during the information synchronization cycle when changing settings in the management console | |
| 107144 | GN-25074 | Center | A problem where new functions using GPDB may not work properly when upgrading images in a closed network | 5.0.0, 6.0.0 |
| 107144 | GN-25029 | macOS Agent | Messages do not pop up when the macOS Agent blocks the wireless LAN control | 5.0.27, 6.0.0 |
| 107144 | GN-24914 | Genian Syncer | The problem of not being able to download patch files uploaded through Genian Sinker | 5.0.44, 6.0.1 |
| 107144 | GN- | WebUI | An error where the administrator session is maintained when | 5.0.14 |

### 23.4.34 Genian ZTNA 6.0.6 Release Notes (2022-08-08)

Last Updated: 2022-09-06

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 106934 | GN-25306 | WebUI | A problem where usable method information is output through an unused HTTP-method | | 5.3 |
| 106611 | GN-25110 | Linux Agent | Upgrading Linux Agent, OpenVPN (2.5.7), and OpenSSL (1.1.1q) to the latest versions | | 5.3 |

## New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 106673 | GN-24961 | WebUI | Show progress when exporting (downloading) a list of nodes | |
| 106611 | GN-25206 | macOS Agent | Complete process termination when the macOS agent daemon stops working | |
| 106611 | GN-25149 | Windows Agent | Improved to be able to collect information about Windows guest accounts | |
| 106611 | GN-25100 | Database | Remove port related warnings when running the MySQL client on a server where MySQL is not enabled | |
| 106611 | GN-25089 | WebUI | Manual link improvements | |
| 106611 | GN-25082 | WebUI | Cloud Sensor additional UX improvements | |
| 106611 | GN-25071 | Linux Agent | Linux Agent adds the ability to perform actions again when re-registering a node | |
| 106611 | GN-25054 | Linux Agent | Linux Agent adds full Agent log compression function for error reporting | |
| 106611 | GN-25047 | WebUI | Node custom field modification function added to node registration API | |
| 106611 | GN-25046 | Enforcer | Improved the kernel debug function so that permission information can also be output | |
| 106611 | GN-25033 | RADIUSD | RADIUS certificate registration improvements and an issue where EAP-TLS connections fail on Windows 11 terminals | 5.0.42 |
| 106611 | GN-25030 | WebUI | Added a storage selection option when adding a Cloud Sensor | |
| 106611 | GN-25001 | WebUI | Added a user search function by department name on the user screen | |
| 106611 | GN-24980 | Center, Database, Sensor | Add server domain settings to connect to ZTNA | |
| 106611 | GN-24978 | WebUI | Improved so that data can be output in the selected order when importing data from the dashboard Big Number widget as a query | |
| 106611 | GN-24975 | WebUI | Improved loading speed of Excel exported files | |
| 106611 | GN-24970 | Sensor | Softether Virtual-Hub Real Interface support | |
| 106611 | GN-24966 | WebUI | Added a parameter so that when moving the node list through a link on the policy management screen, it can be output from a node perspective | |
| 106611 | GN-24935 | WebUI | Add search filters, RADIUS, and Flow menus to the Audit menu submenu | |
| 106611 | GN-24930 | Sensor | A problem that occurs when the IP of the ZTNA terminal is missing from NAC WEBUI and the output occurs | |
| 106611 | GN-24925 | WebUI | Edit the description of authentication when using the REST API | |
| 106611 | GN-24903 | WebUI | Added a search function to the node group detail screen criteria list | |
| 106611 | GN-24884 | Linux Agent | Linux Agent appearance and personalization plug-in development | |
| 106611 | GN-24847 | WebUI | Develop a feature to authenticate management console authentication using SAML | |
| 106611 | GN-24791 | WebUI | Improved the function to check only the details of the set range when setting the management IP control range in the matrix view | |
| 106611 | GN- | macOS | Implementing the Always Connect to ZTNA Network option | 6.0.0 |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 107108 | GN-24990 | WebUI | A problem where the same verification message is output when uploading multiple IP applications if the purpose is not set | 4.0.106, 4.0.148 |
| 106968 | GN-25287 | WebUI | Node Detailed Policy > MAC Policy > IPMChange Event is not called when modifying a prohibited IP list | 5.0.41 |
| 106954 | GN-25298 | macOS Agent | When the macOS agent performs an action in the 'periodic execution' cycle, the execution result remains 'satisfied before execution' | 5.0.11, 6.0.0 |
| 106864 | GN-25242 | CLOUD | An issue where the elasticsearch index is not deleted when the cloud ztna site is deleted | 6.0.5 |
| 106664 | GN-25257 | WebUI | An error occurred when trying to download Excel from the node report's filter menu in the report menu | 5.0.36 |
| 106636 | GN-25277 | Windows Agent | Fix electronic signature verification errors when building agents | 4.0.0, 5.0.0, 6.0.0 |
| 106611 | GN-25225 | Windows Agent | GnPlugin.exe abnormally terminates due to monitor information collection plug-in | 5.0.0, 6.0.0 |
| 106611 | GN-25215 | Windows Agent | GNPlugin not working due to operating system information collection plug-in | 5.0.37, 6.0.0 |
| 106611 | GN-25200 | WebUI | An error in the English UI where a specific item is output in Korean within the restricted management role menu item | 4.1.0 |
| 106611 | GN-25127 | Zero Trust Security | A problem where the ZTNA isolation function does not work properly | 6.0.6 |
| 106611 | GN-25094 | macOS Agent | When using the macOS agent as an alternative authentication for AD accounts, re-authenticate repeatedly | 5.0.7, 6.0.0 |
| 106611 | GN-25091 | WebUI | Symptoms of not being able to search the node list when clicking the IP or MAC in the audit log after assigning a specific management role | 4.1.M1 |
| 106611 | GN-25083 | WebUI | An issue where custom reports of the query report type are not generated | 6.0.1 |
| 106611 | GN-25048 | Linux Agent | Linux Agent, Tray Icon intermittently not displayed | 5.0.42, 6.0.0 |
| 106611 | GN-25044 | WebUI | Problem when uploading Genian Software files | 5.0.2 |
| 106611 | GN-25039 | Center | Infinite loading issue when downloading ZTNA Profile | 6.0.0 |
| 106611 | GN-25018 | WebUI | An error in which an incorrect message is output to the collector when creating multiple sites | 6.0.3 |
| 106611 | GN-25016 | WebUI | Fixed a bug in outputting the conditions of vaccine information in the new node group | 5.0.31 |
| 106611 | GN-24998 | Authsync | A problem where synchronization does not work properly when synchronizing department information and rank information when data source classification values are changed | 4.0.0 |
| 106611 | GN-24947 | WebUI | An issue where the last password change time column is not modified when calling the user modification API | 5.0.43, 6.0.0, 4.0.146 |
| 106611 | GN-24835 | Center | A problem where MAC information may be stored in lower case when registering a node registered by an agent | 6.0.4 |
| 106611 | GN-24675 | Ubuntu(Debian) | [General-purpose OS] An issue where the NAC deb file creation time is displayed incorrectly in the management console | 5.0.41 |

## 23.4.35 Genian ZTNA 6.0.5 Release Notes (2022-07-11)

Last Updated: 2022-08-16

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 106029 | GN-25104 | Center, macOS Agent, Sensor, Windows Agent | Upgrading to the latest version of OpenSSL (OpenSSL 1.1.1q) | | 5.3 |
| 105858 | GN-24782 | WebUI | Library upgrades based on vulnerability checks | | 9.8 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 107045 | GN-21428 | macOS Agent | Apply action policies based on internal and external conditions of the macOS Agent terminal network | |
| 105858 | GN-24983 | Linux Agent | Linux Agent adds Sophos server protection information collection function | |
| 105858 | GN-24962 | WebUI | Added a UI that allows you to enter a description when registering a node | |
| 105858 | GN-24945 | WebUI | Modify the IP owner/IP ownership department output format when outputting the node list in Excel | |
| 105858 | GN-24942 | WebUI | An issue where MAC tags are assigned to all unused IP nodes when MAC tags are set to unused IPs, and improvements to the status filter screen | |
| 105858 | GN-24924 | WebUI | Added an authentication user ID parameter to the Get Node List (GET /nodes) API | |
| 105858 | GN-24922 | WebUI | Improved the search field autocomplete function in the Flow log search box so that columns displayed in the list UI are displayed first | |
| 105858 | GN-24921 | Center | Modified to enable LDAP server connection using a certificate in LDAP authentication integration and LDAP information synchronization | |
| 105858 | GN-24910 | Sensor | An issue where the setting change is not immediately reflected when the ZTNA Isolation option is changed | |
| 105858 | GN-24900 | Center | ZTNA Client OpenVPN compatibility option added | |
| 105858 | GN-24899 | Database | Adding an App Database Rule | 6.0.4 |
| 105858 | GN-24894 | Enforcer | When sending udp event packets from the NAC kernel (Enforcer), if the packet size is larger than the mtu size, the packet cannot be sent to the policy server | |

continues on next page

Table 22 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 105858 | GN-24879 | Linux Agent | Linux Agent, latest platform version information added | |
| 105858 | GN-24876 | WebUI | Added a MAC/device authentication restriction processing option for user applications | |
| 105858 | GN-24871 | WebUI | Site management function settings UX changes | |
| 105858 | GN-24865 | Center, DKNS, Sensor | ZTNA Client Split Tunneling | |
| 105858 | GN-24862 | WebUI | Added the ability to search for user names in IP/equipment owner settings | |
| 105858 | GN-24858 | Sensor | Improved so that debug messages are displayed as standard output when running SoftEtherVPN Foreground | |
| 105858 | GN-24850 | Sensor | Allowing communication between the same users during isolated operation between ZTNA client terminals | |
| 105858 | GN-24832 | WebUI | Improved so that unused IP can be output when selecting all nodes in the tree on the Administration > Node List screen | |
| 105858 | GN-24825 | Center | Add a default RADIUS policy with conditions if you are not a ZTNA client | |
| 105858 | GN-24818 | Zero Trust Security | Isolation between ZTNA client devices on the same site | |
| 105858 | GN-24816 | Windows Agent | Added an automatic password input switching function in the agent authentication window | |
| 105858 | GN-24787 | Center | Modified to display the name of the management device in the audit log related to the operation status as the sensor name | |
| 105858 | GN-24786 | WebUI | Fixed an issue where the web console did not run if there were spaces before and after the data-server username in local.conf | |
| 105858 | GN-24768 | Linux Agent | Linux Agent Process Forced Termination Plugin Development | |
| 105858 | GN-24753 | WebUI | The node list converter has been improved so that when calling Ajax, it calls multiple items in groups instead of a single one | |
| 105858 | GN-24672 | CLOUD | Improved so that DHCP IP can be fixed when using ZTNA Client | |
| 105858 | GN-24671 | WebUI | Add a link to the node list to the assigned IP on the ZTNA Client Sessions list screen | |
| 105858 | GN-24664 | Linux Agent | Linux Agent package e-signature function added | |
| 105858 | GN-24655 | RADIUSD | RADIUS authentication integration added to RADIUS server external authentication integration | |
| 105858 | GN-24600 | Center | User account startup time feature added | |
| 105858 | GN-24330 | Windows Agent | KB Kookmin Bank Pentasso modified so that authentication can be linked continuously | |
| 105858 | GN-24183 | Sensor | Porting sensor modules to X-gate MIPS-raLink machines | |
| 105858 | GN-23901 | WebUI | Improved UI screen output performance | |
| 105858 | GN-17371 | Windows Agent | Agent Debug Log English Culture | |

## Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 106536 | GN-25228 | WebUI | An error with collector settings working on the collection site | 6.0.0 |
| 106390 | GN-24967 | WebUI | A problem where information belonging to a department does not change when the information of a higher department is changed | 4.0.M9 |
| 106370 | GN-25220 | Backup | An issue where the backup fails because the password is encrypted | 6.0.3, 5.0.46 |
| 106363 | GN-25179 | Center | An issue where the attached file size is displayed as 0 kB and cannot be read due to an incorrect MIME format when sending an attached file email | 5.0.16 |
| 106305 | GN-25153 | WebUI | An issue where changed items on the new node detail screen do not appear to be reflected if there is no screen update | 6.0.1 |
| 106275 | GN-24904 | WebUI | Management (node/switch/wireless LAN/user) correction mode (on/off) error problem in the left menu | 6.0.5 |
| 106046 | GN-25090 | Sensor | A problem where the sensor dies due to missing exception handling for memory allocation failures when using the real-time detection function for host name changes | 4.0.114, 5.0.11 |
| 106009 | GN-25135 | Database | A problem where DB backup files are not created properly | 6.0.3 |
| 105959 | GN-25132 | WebUI | An error occurs when adding a node group condition to an item classified as 'agent status' in the Ubuntu version of the general-purpose OS | 5.0.42, 5.0.43, 6.0.1 |
| 105858 | GN-25043 | MGMT | The problem of not being able to run a web server (httpd) with a registered external certificate | 5.0.42 |
| 105858 | GN-24984 | Sensor | A problem where only the last Secondary IP band works for an interface with Secondary IP set to Subnet Scan | 5.0.42 |
| 105858 | GN-24981 | Windows Agent | MAC/IP Clone detection error when Teredo Tunneling Pseudo-Interface is present on the PC | 5.0.0, 6.0.0 |
| 105858 | GN-24977 | Zero Trust Security | An issue where profiles cannot be imported from the OpenVPN app | 6.0.0 |
| 105858 | GN-24946 | WebUI | Fixed an issue where error messages were displayed and change policies were not applied properly when modifying Radius policies | 5.0.30 |
| 105858 | GN-24939 | Authsync | A problem where the Paging parameter value is incorrectly applied when synchronizing information through the REST API Server and calling the API | 5.0.38 |
| 105858 | GN-24919 | WebUI | An error occurred when an email defined as a detailed report type was executed immediately | 5.0.43, 6.0.0 |
| 105858 | GN-24906 | Center | Symptoms of a node group not being able to change even if time-related node group conditions in vaccine information/agreement agreement information have passed | 3.0_0910 |
| 105858 | GN-24896 | WebUI | A problem where the subnet is not allocated by changing the IP when the IP multiple application list is larger than the IP processing band set for the purpose | 4.1.0 |
| 105858 | GN-24891 | DKNS | A problem that fails when performing an upgrade via WEBUI for Ubuntu 20.04 DKNS | 6.0.5 |

continues on next page

Table 23 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 105858 | GN-24867 | Windows Agent | The problem of not being able to control the printer's shared folder | 4.0.125, 5.0.22, 6.0.0 |
| 105858 | GN-24846 | WebUI | An issue where the IP list in the IP usage application form is not displayed as the IP allocation band set for the purpose | 5.0.13 |
| 105858 | GN-24845 | WebUI | An error occurs in the IP application system's automatic rejection processing API | 5.0.14 |
| 105858 | GN-24839 | WebUI | An error page occurs when exporting Excel from IP/MAC status | 4.0.M7 |
| 105858 | GN-24811 | Windows Agent | An issue where values are refilled after unsaving the user ID/PW in the wireless connection manager | 5.0.0, 6.0.0 |
| 105858 | GN-24798 | Center | An issue where authenticated users on a node are not detected when syncing Google G Suite information and linking SAML authentication | 5.0.19 |
| 105858 | GN-24792 | Linux Agent | A problem where the MAC policy function that allows authentication does not work on the Linux Agent | 5.0.41, 6.0.0 |
| 105858 | GN-24784 | IPMGMT | An error where the locale value is changed when querying the results of the IP application | 4.0.114, 5.0.11 |
| 105858 | GN-24741 | WebUI | A problem where the detailed screen of a node in the device is not displayed when moving to another node in the node details | 5.0.38 |
| 105858 | GN-24725 | Linux Agent | A problem where the tray icon is not displayed on platforms based on Linux Agent Debian 11 | 5.0.0, 6.0.0 |
| 105858 | GN-24663 | Center, Linux Agent, macOS Agent, WebUI, Windows Agent | A problem where condition settings malfunction when there is a comma (',') in the node action's condition settings | 5.0.0, 6.0.0 |
| 105858 | GN-24625 | Center | An issue where the upgrade status is incorrect on the dashboard due to the processing of a new agent software addition when the agent version is upgraded | 4.0.M8 |
| 105858 | GN-24580 | Windows Agent | There is no message displayed to the user when deletion fails in the document search delete custom plug-in | 5.0.42 |
| 105858 | GN-24551 | Sensor | A problem where sensor-related functions do not work properly on general-purpose OS | 6.0.4 |
| 105341 | GN-25000 | Linux Agent | Linux Agent, an issue where messages are displayed incorrectly as a result of performing actions | 5.0.42, 6.0.0 |

## 23.4.36 Genian ZTNA 6.0.4 Release Notes (2022-06-10)

Last Updated: 2022-07-11

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 105837 | GN-25064 | WebUI | Web service vulnerability improved so that Apache WAS information is not exposed | 4.0.119, 5.0.16 | 2.5 |
| 105203 | GN-23947 | Windows Agent | Windows Agent Secure Coding Check Results Vulnerability Patch | 5.0.0, 6.0.0 | |
| 103600 | GN-24583 | WebUI | A lib upgrade where a vulnerability was discovered in the Java lib used by WebUI | | 9.8 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 105730 | GN-25062 | macOS Agent | macOS agent support for macOS Ventura | |
| 105203 | GN-24918 | WebUI | Improved so that IP output is limited according to the management IP control range option when assigning an IP | 6.0.4, 5.0.47 |
| 105203 | GN-24728 | IPMGMT, WebUI | Encrypt email approve/reject button link parameters in IP usage applications | |
| 105203 | GN-24718 | WebUI | Add a preview image to the ZTNAC version dashboard widget palette | |
| 105203 | GN-24656 | WebUI | Flow log UI search period default value changed from 1 week to last 24 hours | |
| 105203 | GN-24643 | WebUI | Improved to output a list of nodes from the perspective (nodes/devices) based on widget data | |
| 105203 | GN-24639 | WebUI | Provides security violation detection logs as a default filter | |
| 105203 | GN-24636 | CLOUD | IPsecVPN encryption method applied to each hub | |
| 105203 | GN-24633 | WebUI | A problem where a unit other than the time unit cannot be set in the "within a specific time ~" condition when setting node group conditions | |
| 105203 | GN-24616 | Linux Agent | Development of integrity verification functions for Linux agents, policies, and management server information | |
| 105203 | GN-24614 | WebUI | In the case of the hub site, IPSec's Advance setting function was added | |
| 105203 | GN-24613 | WebUI | Improved image selection when adding cloud sensors | |
| 105203 | GN-24602 | WebUI | Modify the node management search bar style | |
| 105203 | GN-24599 | WebUI | Policies > Objects > Add Web Access UI | |

continues on next page

Table 24 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 105203 | GN-24594 | WebUI | Reset the status of the selected item when applying the node policy immediately and improve the popup that appears as a modal window | |
| 105203 | GN-24572 | WebUI | Added a function to allow a description to be entered when entering a network address | |
| 105203 | GN-24562 | Windows Agent | Change the default Web browser used by the agent to "Default Web browser" | |
| 105203 | GN-24548 | WebUI | Improved the Audit > Log > IP link to display node information as a tooltip | |
| 105203 | GN-24545 | WebUI | Added the sensor's subnet parameter to the IP application REST API so that it can be automatically assigned as an unused IP in that subnet | |
| 105203 | GN-24543 | WebUI | Fixed an issue where values in the Flow log destination IP column were not aligned | |
| 105203 | GN-24507 | Linux Agent | [CC] Linux Agent adds new platform (Hancom Cloud) information | |
| 105203 | GN-24501 | WebUI | Add a column on whether to set urlFilter to the site list | |
| 105203 | GN-24486 | WebUI | Added column sizing options to the node list screen | |
| 105203 | GN-24471 | WebUI | Improved to output items related to departments, ranks, and tags in the node list to the converter | |
| 105203 | GN-24468 | Zero Trust Security | Implementing controls for each Webfilter object and file type | |
| 105203 | GN-24464 | macOS Agent | Added installation time information to the macOS Agent operating system information collection plug-in | |
| 105203 | GN-24463 | Linux Agent | [CC] Linux Agent improved so that Cipher Suite is fixed during TLS communication | |
| 105203 | GN-24451 | macOS Agent | macOS network shared folder plug-in development | |
| 105203 | GN-24450 | Linux Agent | [CC] Linux Agent adds agent deletion function via authentication code | |
| 105203 | GN-24433 | Linux Agent | Linux Agent improved the latest OS update check to check for update items other than versions | |
| 105203 | GN-24373 | Zero Trust Security | Apply URL Filter control policies | |
| 105203 | GN-24333 | WebUI | Objectifying rules in web filters | |
| 105203 | GN-24328 | macOS Agent | Auto Proxy Configuration settings added to macOS PCs | |
| 105203 | GN-24156 | WebUI | MAC is allowed when registering nodes in batches - Improved so that no change (designated IP) can be set | |
| 105203 | GN-24024 | WebUI | Development of an integrated management screen with a node management list and detailed screen | |
| 105203 | GN-24008 | | URL filtering function added | |
| 105203 | GN-22495 | Windows Agent | Development of functions related to Internet Kill Switch | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 105827 | GN-25085 | Center | An issue where registration date/up/down status is incorrectly matched to node group conditions when creating a node | 4.0.0 |
| 105671 | GN-24936 | WebUI | Modify component items displayed in node group creation conditions | 5.0.31 |
| 105637 | GN-25060 | Center | A problem where agent platform information cannot be updated even after agent is reinstalled or logged on after deleting agent information due to prolonged downtime | 5.0.0, 4.0.61 |
| 105629 | GN-25067 | Center, Sensor | [General-purpose OS] A problem where debug logs are piled up in multiple files in duplicate | 5.0.42 |
| 105624 | GN-25003 | Sensor | A problem where the center restarts after the node fails to send DHCP information collected from the sensor | 4.0.114, 5.0.11 |
| 105616 | GN-25068 | macOS Agent | An issue where plug-ins close when using macOS appearance and personalization actions | 5.0.15, 6.0.0 |
| 105529 | GN-25037 | WebUI | An error occurred when searching again after checking the list through the node group menu of the status and filter on the node management screen | 5.0.38 |
| 105514 | GN-25050 | Enforcer | Memory allocation failure issue in Enforcer kernel module | 5.0.40 |
| 105410 | GN-24885 | WebUI | An issue where the table of contents page does not flow when uploading an image from the custom button | 5.0.12 |
| 105390 | GN-24999 | Sensor | A problem where only 32 virtual sensors are added | 5.0.32 |
| 105203 | GN-24971 | Sensor | Sensor daemon hang symptom problem | 4.0.117 |
| 105203 | GN-24905 | Center | A problem where the agent is down but the node changes to an UP state in an environment where nodes are registered using switch ARP table information | 6.0.4, 5.0.47 |
| 105203 | GN-24897 | macOS Agent | An issue that causes database errors related to macOS appearance and personalization actions | 5.0.45, 6.0.2 |
| 105203 | GN-24817 | WebUI | An issue where the user list for each subdepartment is not being output | 5.0.45, 6.0.4 |
| 105203 | GN-24802 | Windows Agent | The real-time surveillance enforcement control option for the V3 vaccine does not work. | 5.0.0, 6.0.0 |
| 105203 | GN-24797 | Sensor | Collection error due to incorrect data format when collecting SNMP information | 4.1.4 |
| 105203 | GN-24785 | Center | Google verification code issuance error in G Suite sync settings after changing the Google API client ID | 6.0.4 |
| 105203 | GN-24767 | Sensor | A problem where the domain information of a node is not updated by NETBIOS scans | 4.0.M3 |
| 105203 | GN-24733 | Windows Agent | If there is a lot of script content to be executed by the script execution plug-in, the action policy is not executed. | 4.0.16, 5.0.0, 6.0.0 |
| 105203 | GN-24729 | IPMGMT, WebUI | Error when approving multiple application items in batches when approving an IP application by email | 4.0.113, 5.0.10 |
| 105203 | GN-24707 | WebUI | Administration > Nodes > Status and Filters > Actions > Problem with not outputting results when moving the node list | 5.0.33 |

continues on next page

Table 25 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 105203 | GN-24701 | Windows Agent | An issue where the authentication integration does not work when using the BASE64 encryption method when using the external authentication function | 5.0.0, 6.0.0 |
| 105203 | GN-24665 | Backup | A problem where securing free space on a local disk does not work when performing a backup via an external storage device | 4.0.19 |
| 105203 | GN-24652 | WebUI | An issue where the execution date label on the dashboard agent installation status is not displayed | 6.0.0 |
| 105203 | GN-24649 | Center, Windows Agent | If multiple permission objects are registered in the control policy, blocking malfunction caused by the Windows firewall control plug-in | 5.0.28, 6.0.0 |
| 105203 | GN-24645 | WebUI | An issue where management view edits are not reflected on the Status Filter tag screen | 5.0.9 |
| 105203 | GN-24637 | WebUI | An error occurred when changing the infrastructure from System > Site to Cloud -> Converged | 6.0.0 |
| 105203 | GN-24630 | WebUI | Fixed an issue where the control policy column tooltips for nodes registered in the center were displayed incorrectly | 5.0.27 |
| 105203 | GN-24628 | macOS Agent | An issue where the integrity check function does not work properly on macOS Agent | 5.0.27, 6.0.0 |
| 105203 | GN-24626 | WebUI | An error log is output when clicking the close list button on the node detail screen | 5.0.38 |
| 105203 | GN-24620 | WebUI | A problem where the node list is not displayed when viewing the filter and status menu after clicking on the node basket in the node management tree | 5.0.42, 6.0.0 |
| 105203 | GN-24592 | WebUI | A problem where related data does not appear on the page moved to the button created when system log collection is completed | 5.0.40 |
| 105203 | GN-24568 | Windows Agent | A problem where APs allowed by wireless LAN control are blocked | |
| 105203 | GN-24560 | Windows Agent | Files in the "%Program Files%" path "C:Program Files (x86)" cannot be executed when using the Run option in the Agent Authentication window. | 5.0.0, 6.0.0 |
| 105203 | GN-24554 | WebUI | An issue where the paging output option is restored when conditions are deleted from the old node group detail screen (changed to 50 when 255 is set) | 5.0.12 |
| 105203 | GN-24523 | WebUI | Certain columns are missing when exporting users (Excel format) | 4.0.7 |
| 105203 | GN-24502 | WebUI | An issue where the value of an unchanged option is modified when the policy is modified after copying the node policy | 5.0.44 |
| 105203 | GN-24449 | Windows Agent | The 'Select Delete' button is unresponsive in the program removal plugin | 5.0.42, 6.0.0 |
| 105203 | GN-24192 | WebUI | Symptoms that when assigning user tags, the tag is displayed in the user list as the number of authenticated nodes | 4.0.138,<br>5.0.35 |
| 105203 | GN-21894 | Center | Node type: An issue where unclassified nodes are not deleted when IP/MAC usage time expires | 5.0.31 |
| 103937 | GN-24685 | WebUI | An issue where a blocked IP set to be used is assigned when using the Allow Blocked IP option | 4.0.12 |

### 23.4.37 Genian ZTNA 6.0.3 Release Notes (2022-04-12)

Last Updated: 2022-06-10

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 104957 | GN-24908 | WebUI | Tomcat version upgrade (8.5.78) | | 8.6 |
| 104926 | GN-24917 | Center, macOS Agent, Sensor, Windows Agent | Upgrading to the latest version of OpenSSL (OpenSSL 1.1.1o) | | 9.8 |
| 104654 | GN-24851 | Center | Apache HTTP Server 2.4.53 upgrade | | 9.8 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 104355 | GN-24852 | WebUI | Improved node group tree output query in the node management screen | |
| 103851 | GN-24546 | WebUI | Improved so that blocked IPs can be assigned when the IP to be assigned is allowed to be assigned in IP management in the management console | |
| 103851 | GN-24493 | macOS Agent | Add ESET Endpoint Security information to the macOS antivirus data collection plug-in | |
| 103851 | GN-24469 | Center | Improved so that the sensor DHCP node IP update function can be applied when registering a node via a switch | |
| 103851 | GN-24458 | Windows Agent | Fix the wireless connection manager so that the wireless connection manager is not displayed if there is no AP that can be connected | |
| 103851 | GN-24367 | WebUI | [CC] Handling the center/sensor reboot command hidden in the management console | |
| 103851 | GN-24319 | Linux Agent | Linux Agent adds the ability to handle re-registration events when deleting a node | |
| 103851 | GN-24316 | Windows Agent | Modified so that the DNS control plug-in can remove the setting value that matches the IP address and host. | |
| 103851 | GN-24312 | syslog | Modify syslog-ng settings to not use TLS 1.0 when using syslog TLS | |
| 103851 | GN-24281 | WebUI | Node command REST API improvements | |
| 103851 | GN-24278 | WebUI | Improved so that when the "Node Action" plug-in is assigned in the status group, the plug-in can be changed in the node action | |
| 103851 | GN-24272 | WebUI | Cloud Security Group Policy screen improvements | |
| 103851 | GN-24267 | Center | Agentless AD SSO - Improved to be able to set up 3 or more servers | |
| 103851 | GN-24263 | Center | Improved to display the authentication user ID including the domain during SMTP authentication, and added an authentication source to the authentication audit log | |
| 103851 | GN-24262 | IPMGMT, WebUI | Fixed an issue where emails are sent to all users according to the Forward All option if no approver is set when filling out an IP application | |
| 103851 | GN-24243 | WebUI | Enable limited IPSec and ZTNA Client features in the case of a centralized hub in site management | |
| 103851 | GN-24229 | WebUI | Remove the node detail page flowData tab | |
| 103851 | GN-24212 | WebUI | Improved the dashboard ZTNA Client Session Status and IPSec Tunnel Status BigNumber widgets to allow site settings | |
| 103851 | GN-24204 | WebUI | NHN CLOUD support | |
| 103851 | GN-24178 | Linux Agent | [CC] Linux Agent Clam antivirus information collection function added | |
| 103851 | GN-24044 | Center | An issue where passwords are stored in plain text when setting up sftp for backup | |
| 103851 | GN-24000 | WebUI | Site administration screen - monitoring function added | |
| 103851 | GN-23766 | WebUI | CONF settings UX improvements | |
| 103851 | GN-23716 | WebUI | REST API Event Integration Service (Java version) development | |
| 103851 | GN-17595 | macOS Agent | Creating a macOS agent device control plug-in | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 105188 | GN-24989 | Sensor | A problem where sensor daemon memory increases when a sensor receives non-DHCP packets on the DHCP server port (UDP/destination port 67) | 4.0.11 |
| 105167 | GN-24956 | WebUI | A problem where the related UI does not work properly when the NAT IP of the sensor connected from ztna-client in site management is not set | 6.0.0 |
| 104926 | GN-24941 | Windows Agent | Installation fails due to large number of file copies when updating agents from 4.0 to 5.0 on certain PCs | 4.1.2, 5.0.0, 6.0.0 |
| 104904 | GN-24789 | Sensor | A problem where FQDN information on the agent installation terminal is changed due to sensor NETBIOS scans | 4.0.146 |
| 104778 | GN-24920 | WebUI | Error page displayed when entering "%" in the information synchronization condition statement | 5.0.42, 5.0.45, 6.0.2 |
| 104597 | GN-24829 | WebUI | An issue where an XSS discovery audit log is left even though it is normal policy application data | 5.0.42, 5.0.45, 6.0.2 |
| 104576 | GN-24838 | macOS Agent | GNPlugin process does not run when using the 'Monitor Information Collection' plug-in in the macOS monterey environment | 5.0.17 |
| 104567 | GN-24837 | macOS Agent | The pkg installation file cannot be executed when running the 'file distribution' action in the macOS monterey environment | 5.0.45 |
| 104270 | GN-24696 | macOS Agent | An issue where the ZTNA connection status in the macOS Agent tray menu is displayed incorrectly in an unspecified manner | 6.0.0 |
| 104208 | GN-24819 | Windows Agent | The action policy was not executed due to an unspecified action policy integrity check failure. | 5.0.0, 6.0.0 |
| 104208 | GN-24695 | Windows Agent | An issue where the ZTNA connection status in the agent tray menu is displayed incorrectly in an unspecified manner | 6.0.0 |
| 104160 | GN-24661 | WebUI | An error where group conditions cannot be corrected immediately due to missing values for vaccine-related node groups required | 5.0.23 |
| 104125 | GN-24806 | Center | An issue where the Account packet request destination IP and response origin IP are different in RADIUS redundancy configurations | 6.0.3, 5.0.46, 4.0.149 |
| 104017 | GN-24673 | VRRPD | [General-purpose OS] An issue where the interface MAC address changes when switching between M->S in an HA environment | 5.0.42, 6.0.0 |
| 103976 | GN-24430 | Center | IP management message first: An issue where the CWP design template set in the node policy is not applied when On is set | 5.0.14 |
| 103851 | GN-24668 | Center | A problem where the UP/DOWN state of a node registered through a manually registered switch is not synchronized with the sensor | 5.0.36 |
| 103851 | GN-24660 | Center | An issue where the node's platform information changes from Microsoft Windows to Unknown Platform | 5.0.42, 5.0.45, 6.0.2 |
| 103851 | GN-24631 | WebUI | A problem where when approving new IP applications in batches, it appears that there are no assigned IPs even though there are unassigned IPs | 6.0.3, 5.0.46 |
| 103851 | GN-24577 | macOS Agent | A problem where some plug-ins that always perform the cycle work even when the macOS action conditions are unsatisfactory | 5.0.0, 6.0.0 |

continues on next page

Table 26 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 103851 | GN-24563 | Windows Agent | A problem where some plug-ins whose cycle is always executed even when the action conditions are unsatisfied | 5.0.0, 6.0.0 |
| 103851 | GN-24496 | Center | A problem where the node information host name (NL_FQDN) changes after checking sensor node information | 4.0.25 |
| 103851 | GN-24434 | WebUI | A problem where the content is not saved even though the check box for specifying the node type is selected on the node details screen | 5.0.44, 6.0.1 |
| 103851 | GN-24424 | WebUI | A malfunction issue with the return button after moving from the target node list tab on the node group detail screen to the node detail screen | 5.0.31 |
| 103851 | GN-24418 | Windows Agent | A problem that can be terminated by an external program while the authentication window is prohibited from being closed | 4.1.0, 5.0.0, 6.0.0 |
| 103851 | GN-24410 | CWP | When using the CWP template, an error does not work properly if the IP management message is set first and then the user authentication component is used | 4.0.143, 5.0.40 |
| 103851 | GN-24407 | IPMGMT, WebUI | When approving new IP applications in batches, the problem is that they are approved in batches with the same IP address even if there are not enough IP addresses that can be assigned | 4.1.4 |
| 103851 | GN-24406 | IPMGMT, WebUI | Automatic approval does not work when applying for a new IP through the REST API | 5.0.8 |
| 103851 | GN-24360 | Windows Agent | An issue where the agent installation node continues to exist in the center management band even after installing the agent sensor | 5.0.40, 6.0.0 |
| 103851 | GN-24338 | Windows Agent | Fixed an issue that left repeated debug logs for Windows security settings actions | 4.0.109, 5.0.6, 6.0.0 |
| 103851 | GN-24329 | Windows Agent | <br>Tag display error when displaying notifications and announcements | 5.0.42, 6.0.0 |
| 103851 | GN-24327 | WebUI | An error page occurred when adding a dashboard widget audit log filter | 4.0.13 |
| 103851 | GN-24318 | Docker | A problem where the host machine's network interface disappears when DKNS is installed | 6.0.1 |
| 103851 | GN-24314 | WebUI | My information IP display error when viewing the connection authentication page (CWP) of the target node task | 5.0.40 |
| 103851 | GN-24307 | Center, Sensor | A symptom occurs where the node role is not delivered to the sensor when the IPs of a node group composed only of IP are changed | 5.0.11, 6.0.0 |
| 103851 | GN-24303 | WebUI | An error where a condition item is output in the item when setting the node group IP/MAC information CSV batch | 5.0.43, 6.0.0 |
| 103851 | GN-24301 | Center | An issue where LOG cannot be transferred to SFTP when backing up SFTP | 5.0.45, 6.0.2 |
| 103851 | GN-24300 | Windows Agent | "Run after authentication" option in agent authentication window is not working | 5.0.0, 6.0.0 |
| 103851 | GN-24290 | GenianOS | Warning occurs when running NAC check script (sysinspect) 'Check Setup Config' | 4.0.120, 5.0.17 |
| 103851 | GN-24245 | Windows Agent | A problem displayed as an internal network when communication with the policy server is not possible | 5.0.43, 6.0.0 |
| 103851 | GN-24244 | Center | An error message is displayed on the screen when backing up on devices with redundancy settings | 4.0.119, 5.0.16 |

continues on next page

Table 26 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 103851 | GN-24241 | Center | A problem where the node type and platform are registered as normal nodes when there are multiple sensors in the same band | 6.0.0 |
| 103851 | GN-24200 | WebUI | The problem of not being able to display the 2nd band list when assigning in the IP application form after setting the sensor subnet to 23 bits | 5.0.13 |
| 103851 | GN-24187 | Windows Agent | An issue where the "Hide when using a wired connection" option in the wireless connection manager does not work | 5.0.0 |
| 103851 | GN-24181 | macOS Agent | An issue where the macOS Agent 'Agent Removal Method' is not applied | 5.0.41, 6.0.0 |
| 103851 | GN-23710 | macOS Agent | An issue where authentication cannot be disabled when using the authentication restriction function in the macOS agent authentication window | 5.0.17, 6.0.1 |
| 103851 | GN-23285 | Windows Agent | An issue where the agent does not work when the Windows shell is not an explorer | 4.0.0, 5.0.0, 6.0.0 |
| 103851 | GN-22689 | WebUI | A problem where the device name (System Name) does not change in System Management > System List when changing the hostname in CLI (conf terminal) | 5.0.33 |

## 23.4.38 Genian ZTNA 6.0.2 Release Notes (2022-02-09)

Last Updated: 2022-04-12

### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 103842 | GN-24689 | WebUI | Issues where XSS is possible in Audit > Logs > Log Search | | 4.3 |
| 103670 | GN-24651 | Center, macOS Agent, Windows Agent | Upgrading to the latest version of OpenSSL (OpenSSL 1.1.1n) | 4.0.0, 5.0.0, 6.0.0 | 7.5 |
| 103638 | GN-24687 | WebUI | An issue where files can be accessed by relative paths on the debug log screen | | 3.83 |
| 102685 | GN-24535 | WebUI | Remove logstash | | 5.9 |

### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 103413 | GN-24648 | WebUI | Fixed an issue where search results were slow when there was an IP owner column in the node list | |

continues on next page

Table 27 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 103066 | GN-24302 | Center | Add macros and provide a response message capture function to enable MD5 (MD5B64), an encryption method linked to webhook authentication | |
| 103058 | GN-24257 | Center | Improved so that a server connection timeout can be set when linking LDAP authentication | |
| 103053 | GN-24198 | WebUI | A problem where a specific domain is not registered in the network address of a network object | |
| 102920 | GN-24557 | Center, RADIUSD | Provides a node registration function as an optional setting function during RADIUS authentication | |
| 102892 | GN-24151 | WebUI | Added an API for setting and querying sensors that can be used for each purpose of the IP application system | |
| 102436 | GN-24246 | macOS Agent | Implementing features related to secondary authentication in macOS ZTNA Connection Manager | 6.0.2 |
| 102436 | GN-24172 | WebUI | Fixed so that Tomcat version information is not output when Bad Request (400) occurs | |
| 102436 | GN-24165 | WebUI | Fixed so that html tags are not converted when entering instance message content | |
| 102436 | GN-24130 | macOS Agent | Structural improvements for multiple VPN connections to the macOS ZTNA connection manager | 6.0.2 |
| 102436 | GN-24082 | WebUI | Improved so that additional tags other than node tags can be queried through the /nodes/ {nodeID} /tags API | |
| 102436 | GN-24077 | WebUI | Modified to enable web access even if the MySQL authentication plugin is changed to sha256_password | |
| 102436 | GN-24068 | WebUI | Improved to be able to specify the date format displayed in the new dashboard chart widget tooltip | |
| 102436 | GN-24059 | WebUI | Added a reverse assignment function when applying for IP | |
| 102436 | GN-24045 | DKNS | Improved so that DHCP Pool can be set when setting up ZTNA Client | |
| 102436 | GN-24029 | Center | Ability to send authentication codes through Google OTP secondary authentication and webhooks during agent authentication and RADIUS authentication | |
| 102436 | GN-24020 | WebUI | Adding parameters for functions added to the Applications REST API | |
| 102436 | GN-24010 | WebUI | Modified so that when the sensor name is changed, the sensor names of the nodes belonging to the sensor are changed immediately | |
| 102436 | GN-23980 | Center | Improved so that emails are sent to multiple email accounts when sending query report emails | |
| 102436 | GN-23964 | WebUI, Windows Agent | Node Information - Show virtual type for connection method in interface information | |
| 102436 | GN-23953 | WebUI | Self-signed certificate regeneration and externally generated SSL certificate registration function | |
| 102436 | GN-23943 | Center | Improved the part where Hangul is displayed when generating an English audit log | |
| 102436 | GN-23930 | WebUI | Support for custom encryption algorithm methods | |

continues on next page

Table 27 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 102436 | GN-23918 | WebUI | A problem where two or more of the same standalone plug-in actions can be included in a node policy | |
| 102436 | GN-23896 | WebUI | Performance improvements such as removing JOIN queries when querying a list query on the node detail screen | |
| 102436 | GN-23895 | Authsync | Improved so that it can be linked up to Oracle Database 19c | |
| 102436 | GN-23880 | Linux Agent | Linux Agent, an issue where the agent works abnormally when changing the OS login user or logging out Linux Agent, re-logging in | |
| 102436 | GN-23869 | Windows Agent | Adding a 5.0 Version "Http URL Authentication" Custom Plug-in | |
| 102436 | GN-23865 | Windows Agent | Added a custom plugin for hostname authentication in version 5.0 | |
| 102436 | GN-23861 | WebUI | Improved Cloud Sensor registration function | |
| 102436 | GN-23852 | WebUI | Improved to enable Google OTP second authentication in CWP | |
| 102436 | GN-23833 | WebUI | Template modification function added to Security Group detail screen | |
| 102436 | GN-23831 | WebUI | Modify the time period setting in the flow log widget to output a subtitle | |
| 102436 | GN-23825 | Linux Agent | Linux Agent adds a function to operate with the previous policy when the center connection is not possible | |
| 102436 | GN-23817 | IPMGMT, WebUI | Improvement of the IP application system email step-by-step approval method | |
| 102436 | GN-23802 | WebUI | Improved software update guidance - provides separate patch and upgrade | |
| 102436 | GN-23752 | Linux Agent | Linux Agent, new distribution and version information added | |
| 102436 | GN-23749 | Linux Agent | Linux Agent develops a function to check the latest TmaxOS updates | |
| 102436 | GN-23731 | WebUI | Security Group Terraform tf file download function | |
| 102436 | GN-23724 | WebUI | Added a CONF_OPTIONS item that reflects the default initial value according to the CONF engine's choices | |
| 102436 | GN-23722 | Linux Agent | Linux Agent, interface control action development | |
| 102436 | GN-23698 | WebUI | Add relevant content to the widget schema to set link targets | |
| 102436 | GN-23644 | GenianOS | Added some missing file system checks at boot time | |
| 102436 | GN-23468 | Center | Improved so that other webhook APIs can be called using the Webhook API call results | |
| 102436 | GN-23221 | Windows Agent | Chrome and Edge option controls added to IE security option control plug-in | |
| 102436 | GN-23212 | Ubuntu(Debian) | [General-purpose OS] Repository separation work for installing each genian-nac version | |
| 102436 | GN-23210 | macOS Agent | macOS ZTNA connection manager plugin added | |

continues on next page

Table 27 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 102436 | GN-23189 | macOS Agent | macOS Agent appearance and personalization plug-in - adds screensavers and desktop controls | |
| 102436 | GN-22690 | WebUI | Audit log limit function - An issue where all logs are displayed in the audit log even when the node management scope is limited | |
| 102436 | GN-22074 | WebUI | Improved SAML authentication integration to support 2 or more IdPs (Authentication Information Providers) | |
| 102436 | GN-21279 | CLOUD | Improved so that files can be attached when sending emails via AWS SES | |

### Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 103817 | GN-24691 | Center | A problem where a log is generated when a node registered through a switch is registered by a sensor | 5.0.43, 6.0.0 |
| 103760 | GN-24683 | Sensor | An issue where the sensor daemon abnormally terminates due to an incorrect memory reference after starting a DHCP scan | 4.0.2 |
| 103726 | GN-24724 | Windows Agent | An issue where agent action policies are applied late after transitioning from an external to an internal network state | 5.0.40, 6.0.0 |
| 103639 | GN-24284 | WebUI | When assigning directly from the IP application approval screen, an error occurs when approval is performed after changing the management sensor | 5.0.13 |
| 103620 | GN-24682 | WebUI | A problem where IPs are not assigned in reverse order when the approval method for each IP use is automatic approval | 5.0.44, 6.0.2 |
| 103614 | GN-24684 | WebUI | An unresponsive issue when logging in to an account (genians.com) on the license screen | 5.0.20 |
| 103517 | GN-24617 | WebUI | An issue where the added node type (virtual sensor, agent sensor) is missing from the node group settings list and the search field conditions in the node list | 5.0.40 |
| 103488 | GN-24597 | Center | An issue where node groups cannot be included due to agent version comparison conditions | 5.0.16, 6.0.0 |
| 103432 | GN-24485 | macOS Agent | An issue where macOS Agent memory continues to grow | 4.0.0, 5.0.0, 6.0.1 |
| 103404 | GN-24644 | Center | An issue where the center daemon dies intermittently when updating ARP management plug-in information | 5.0.43, 6.0.0, 4.0.146 |
| 103399 | GN-24658 | OpenVPN | An issue where the authenticated user is incorrectly displayed when connecting to ZTNA Client with an ID of 9 or more digits | 6.0.0 |
| 103384 | GN-24678 | Sensor | An issue where some information is missing when collecting SNMP v3 switch information | 5.0.44, 6.0.1 |
| 103342 | GN-23923 | Windows Agent | A problem where the information collection plug-in collects empty information and deletes node information | 5.0.0 |
| 103247 | GN-24619 | Center | A problem where the node type of a manual registration switch is changed to a network device due to a node information scan | 5.0.14 |
| 103224 | GN-24582 | Center | Symptoms that an authorized object does not work when copying a control policy from a mirror sensor | 4.0.116, 5.0.13 |

continues on next page

Table 28 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 103213 | GN-24622 | Enforcer | An issue where the Enforcer kernel module panics due to incorrect garbage values during the node information update process | 6.0.1 |
| 103093 | GN-24586 | Windows Agent | Some SW were not collected due to the software information collection plug-in and a DB error occurred | 5.0.43, 6.0.0 |
| 103048 | GN-24603 | Center | The problem of not updating the control policy permission cache when adding a new control policy or changing the control policy using/not using the control policy | 4.0.M2 |
| 102987 | GN-24593 | Enforcer | A problem where the node status changes to down by performing a healthcheck on a node registered to the virtual sensor | 5.0.32 |
| 102950 | GN-24358 | Center | A problem where a normal node other than a virtual sensor is set as an agent sensor if the virtual sensor and IP are the same | 5.0.40 |
| 102867 | GN-24544 | Sensor | An issue where WOL packets are sent to the wrong interface | 5.0.40 |
| 102836 | GN-24375 | | The problem of not being able to organize ES backups (Snapshots) | 5.0.42 |
| 102798 | GN-24350 | WebUI | A problem where the settings UI is not displayed properly when changing the settings of the node action being used | 5.0.45, 6.0.2 |
| 102557 | GN-24364 | WebUI | IP collision protection - the problem of not being able to set multiple MACs | 5.0.42, 6.0.0 |
| 102509 | GN-24467 | WebUI | A problem where the list is not output when adding a rank column from the node management list | 5.0.33 |
| 102500 | GN-24479 | WebUI | An issue where the NAC license text may be output even though the license has not been exceeded | 4.1.M3 |
| 102436 | GN-24598 | Enforcer, Sensor | Fixed abnormal earlyrole behavior when setting “if not a member” AND “if not a member” in node group conditions | 4.0.114, 5.0.11 |
| 102436 | GN-24415 | Authsync | Library path error when synchronizing Cloud NAC Oracle information | 5.0.45, 6.0.2 |
| 102436 | GN-24346 | Authsync | [CLOUD] An issue where information synchronization takes a long time to complete | 5.0.23 |
| 102436 | GN-24307 | Center, Sensor | A symptom occurs where the node role is not delivered to the sensor when the IPs of a node group composed only of IP are changed | 5.0.11, 6.0.0 |
| 102436 | GN-24273 | | A problem where users are not authenticated when connecting to ZTNA Client | 6.0.1 |
| 102436 | GN-24268 | WebUI | An issue where automatic node snapshot report generation fails | 6.0.0 |
| 102436 | GN-24261 | Center | An issue where the HA VIP node's Device Type is registered as a NODE | 5.0.40 |
| 102436 | GN-24254 | RADIUSD | When the RADIUS daemon is stopped, the winbindd daemon does not stop and remains a problem | 5.0.35 |
| 102436 | GN-24194 | Center | An issue where user groups cannot be reapplied when updating user passwords | 5.0.44 |
| 102436 | GN-24188 | WebUI | An issue where the screen does not move after processing priority use approval of the application form for items awaiting email approval | 5.0.13 |
| 102436 | GN-24153 | WebUI | IP Management > There are matrices that are not properly output in Matrix View | 4.0.12 |
| 102436 | GN-24147 | WebUI | <br>Fixed a tag display issue in the audit log description column tooltip | 5.0.22 |

continues on next page

Table 28 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 102436 | GN-24139 | Windows Agent | A problem where the total storage capacity is incorrectly collected when collecting storage device information | 4.1.0, 5.0.0, 6.0.0 |
| 102436 | GN-24136 | WebUI | A problem where the image path is displayed in the node group setting value when (comma) is present in the node action name | 5.0.14 |
| 102436 | GN-24120 | WebUI | Management role management screen > An error occurred when creating a service role | 5.0.42 |
| 102436 | GN-24113 | WebUI | An error where menu restriction settings cannot be disabled when modifying a management role | 5.0.0 |
| 102436 | GN-24110 | Windows Agent | An issue where incorrect authentication values are linked to the Smart NAC alternate authentication plug-in | 5.0.41 |
| 102436 | GN-24092 | WebUI | A problem where input items do not change depending on the selected item when setting node group conditions | 5.0.20 |
| 102436 | GN-24085 | WebUI | A problem where a password cannot be entered when importing users from the user management screen | 5.0.40 |
| 102436 | GN-24071 | WebUI | An issue where the identity verification item is not displayed on the CWP new user registration screen | 5.0.42, 6.0.0 |
| 102436 | GN-24011 | RADIUSD | A problem where RADIUS authentication fails when the number of RADIUS attributes is high | 5.0.24 |
| 102436 | GN-24005 | Center | The problem of not being able to download when using the file distribution plug-in https URL | 4.0.0, 5.0.0 |
| 102436 | GN-24002 | Linux Agent | Linux Agent, the issue where the tray icon is not displayed | 5.0.42, 6.0.0 |
| 102436 | GN-23997 | WebUI | A problem where an error message is output when clicking the edit button for the object in the permission object's condition settings | 5.0.25 |
| 102436 | GN-23962 | WebUI | An issue where special characters are not assigned to a control policy if the permission object ID contains special characters | 4.0.M8 |
| 102436 | GN-23952 | IPMGMT | The problem of not being able to automatically log in and log in to the IP application system when using http | 5.0.27 |
| 102436 | GN-23950 | Authsync | The problem of not being synchronized when synchronizing csv information using https | 4.0.5 |
| 102436 | GN-23949 | CWP | An issue where when registering a new user, an approval request email is sent even if the visitor's email approval is disabled | 4.0.M8 |
| 102436 | GN-23925 | Sensor | An issue where local network packets for an interface added as an Alias IP are forwarded to the Default Gateway | 5.0.42 |
| 102436 | GN-23917 | Sensor | An issue where virtual IPs are not registered when adding virtual IPs manually | 5.0.41, 6.0.0 |
| 102436 | GN-23891 | | A problem where authentication is attempted even if the connection fails from the primary server when linking LDAP authentication | 5.0.15, 4.0.137 |
| 102436 | GN-23855 | Center | Improved so that when the switch is manually registered, the sensor tree switch information is updated when the same switch exists with an IP in a different network band | 4.0.117, 5.0.14 |
| 102436 | GN-23836 | | Changes in how IP Mobility duplicate node registrations are prevented | 6.0.1 |
| 102436 | GN-23835 | Center | An issue where node group conditions cannot be set related to the Equipment Lifecycle Management Additional Field (NI_CUSTOM) | 4.0.129, 5.0.26 |

continues on next page

Table 28 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 102436 | GN-23819 | WebUI | Error where custom web application cannot be set because the link to the tomcat webapps folder does not exist | 5.0.40 |
| 102436 | GN-23760 | Enforcer, Sensor | Redundant poisoning issues during VXLAN tunneling | 6.0.1 |

### 23.4.39 Genian ZTNA 6.0.1 Release Notes (2021-12-08)

Last Updated: 2022-02-10

#### Security Vulnerability

| Revision | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 101693 | GN-24305 | GNOS | 2.4.52 version upgrade for Apache vulnerability measures | | 9.8 |
| 101614 | GN-24253 | WebUI | log4j vulnerability improvements | | 9.8 |
| 100944 | GN-23714 | Center | Complementing agent-related APIs with poor authentication | | 4.6 |
| 100944 | GN-23461 | WebUI | [SaaS] Saas security authentication source code inspection result measures | | 9.1 |
| 100944 | GN-23446 | gnlogin, WebUI | Handle passwords so that specific words cannot be used | | 8.7 |

#### New Features and Improvements

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 99155 | GN-23327 | Center, Sensor | Improved to work with site management K8s | |
| 104132 | GN-23367 | Center, RADIUSD | Add RADIUS Secondary SMS Authentication and Attributes (Axgate-Auth-Type) | |
| 102166 | GN-24251 | WebUI | Change how to reissue OTP authentication keys when lost | |
| 102130 | GN-24279 | WebUI | [gndbcp] Modified so that garbage values can be removed and decrypted when decrypting DB passwords stored in local.conf | |
| 101774 | GN-24304 | WebUI | Fixed an issue where the IP application system was slow to apply for approval | |
| 101542 | GN-24315 | Documents | 5.0.44 Global Release | |
| 101503 | GN-24265 | macOS Agent | Add BSSID information for wireless LAN connected to macOS Agent network information | 5.0.0 |
| 101486 | GN-24149 | GnBrowser | Problems where some functions, such as deleting nodes, do not work in gnBrowser | |

continues on next page

Table 29 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 101418 | GN-24190 | Center, MySQL | Change conf settings and use jemalloc memory allocators to reduce MYSQL/CENTERD memory usage | |
| 100944 | GN-24132 | macOS Agent | Protocol information added to macOS Agent wireless LAN control plug-in information | |
| 100944 | GN-23982 | Windows Agent | OpenVPN-based secondary authentication function added to ZTNA connection manager (SMS) | |
| 100944 | GN-23809 | Windows Agent | Added the ability to change the logo image and print help to ZTNA Connection Manager | |
| 100944 | GN-23791 | WebUI | System > Fixed an issue where Cloud Providers used on the site could be deleted from the Cloud Provider menu | |
| 100944 | GN-23771 | | Make it possible to restart the system even when KeepAlive is down | |
| 100944 | GN-23746 | WebUI | [JSF/component] Add pattern input component | |
| 100944 | GN-23735 | | Change the size of the dashboard widget settings pop-up window | |
| 100944 | GN-23723 | Sensor | Juniper Switch MAC information is collected when SNMP Switch information is collected | |
| 100944 | GN-23672 | -Unknown/None- | [Geumoh University of Technology] Oracle Binary Development for Synchronization | |
| 100944 | GN-23658 | Sensor | Improved host name detection with MDNS | |
| 100944 | GN-23642 | | Add missing C30G_R1 and C50G_R1 product installation scripts | |
| 100944 | GN-23635 | WebUI | Built-in management role editing function | |
| 100944 | GN-23626 | | Support for BASE64_DECODE (UNHEX (HASH)) HASH values in the password encryption method SHA256 | |
| 100944 | GN-23622 | | Improved debug log processing method to solve the problem that takes a long time to run syslog at boot time | |
| 100944 | GN-23618 | WebUI | Enhanced description of the hardware (hardwareinfo) search column in node management | |
| 100944 | GN-23602 | gnlogin | Display DB migration progress in an easier to understand manner | |
| 100944 | GN-23583 | WebUI | Improved so that the department name step is displayed when adding the department name of user information to the management view from the node management list | 5.0.41 |
| 100944 | GN-23570 | WebUI | Added a feature to enable multiple selection/deselection in the IP matrix view | |
| 100944 | GN-23568 | WebUI | An issue where an XSS detection log is left in the audit log when reporting a false positive in Administration > Node Details | |
| 100944 | GN-23561 | | VXLAN over IPSEC structure operation support | |
| 100944 | GN-23537 | WebUI | Flow log column sorting function added | |
| 100944 | GN-23536 | WebUI | Add a Top 10 traffic source widget based on Flow logs | |

continues on next page

Table 29 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 100944 | GN-23524 | WebUI | Add a pattern input component | |
| 100944 | GN-23516 | Windows Agent | Added an option to shut down the application when shutting down in the system shutdown plug-in | |
| 100944 | GN-23507 | WebUI | Improved settings related to Http Header Security distributed within the code to be in Tomcat | |
| 100944 | GN-23495 | WebUI | WebUI-related modifications due to the change to create a password for the ZTNA client server from the center | |
| 100944 | GN-23490 | Center, DKNS | IPsecVPN connection status collection function | |
| 100944 | GN-23487 | Sensor | IPSEC-related module equipped with OnPrem sensor | |
| 100944 | GN-23482 | Center, DKNS | Change ZTNA client server password generation to center | |
| 100944 | GN-23474 | Enforcer, ulogd | When creating a flow log, add additional information such as http header/sni. | |
| 100944 | GN-23459 | Enforcer | An issue where individual sessions occur for icmp echo and reply | |
| 100944 | GN-23453 | Center, Sensor | Improved ZTNA Client sensor mode to follow Bind Interface mode | |
| 100944 | GN-23450 | WebUI | Improved site management IPSEC settings | |
| 100944 | GN-23447 | Center, Enforcer, Sensor | Improved transfer of permissions to nodegroup settings | |
| 100944 | GN-23424 | WebUI | Dashboard UI improvements | |
| 100944 | GN-23423 | WebUI | Policy > Objects > Permissions > Add the ability to assign state groups to network objects | |
| 100944 | GN-23406 | WebUI | Added a sensor selection option for site management routing settings | |
| 100944 | GN-23401 | Center | Platform detection function (GDPI API) for nodes created by the Cloud Collector | |
| 100944 | GN-23391 | GNOS | Kernel version upgrade to support the latest drivers (5.10) | |
| 100944 | GN-23366 | WebUI | Separate Agentless AD SSO settings from LDAP authentication integration | |
| 100944 | GN-23360 | Center | Improved to work with multiple sensors in site management | |
| 100944 | GN-23332 | Center, DKNS | Send ZTNA IPSec log files to Policy Server | |
| 100944 | GN-23331 | WebUI | Added the ability to export new dashboard PDF and DOC reports | |
| 100944 | GN-23182 | WebUI | IPsec Status UI added | |
| 100944 | GN-23113 | WebUI | Added developer mode to the web management console | |

continues on next page

Table 29 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 100944 | GN-23075 | Center | Added syslog VPN audit records and improved the operation of uppercase and lowercase character conversion and node information log filters when converting filter macros | |
| 100944 | GN-22673 | WebUI | Added an OS-specific tab category feature when adding a node action to a node policy in the management console | |
| 100944 | GN-22626 | Containerization | Adding Terraform to the Cloud NAC Policy Server image | |
| 100944 | GN-22606 | Sensor | Implementation of a destination-based dynamic access control function (Host - Host: VXLAN) | |
| 100944 | GN-22594 | WebUI | Improved query for Admin > Nodes > Group Tree and list of nodes belonging to a nodegroup | |
| 100944 | GN-20083 | WebUI | UI improvements for related processes when selecting all nodes from the node list and running batch jobs | |

## Issues Fixed

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 102413 | GN-24428 | WebUI | An error occurs when there is no code for the department name of the user information in the management view in the node management list | 5.0.44 |
| 102311 | GN-24400 | Windows Agent | Agent update issues in a closed network environment due to changes in electronic signature certificates | 5.0.0, 6.0.0 |
| 102262 | GN-24239 | WebUI | Problem with not being able to search by tag name in node management search | 4.0.144, 5.0.41 |
| 102104 | GN-24365 | WebUI | When modifying an action, the same multi-plug-in action is not modified when an action is assigned to a policy | 5.0.43, 6.0.0 |
| 102091 | GN-24341 | Center | A problem where an agent sensor in the same network band is re-registered while the agent sensor is registered in the network band | 5.0.40 |
| 102039 | GN-24176 | WebUI | A problem where items changed on the node detail screen do not appear to be reflected if there is no screen update | 5.0.22 |
| 102032 | GN-24417 | WebUI | A problem where a node is not recognized when the MAC address is in lower case in node group conditions | 5.0.31 |
| 101846 | GN-24293 | WebUI | Node Management > Task Selection > Node Group Assign/Unassign Command Problem Not Working | 5.0.44, 6.0.1 |
| 101778 | GN-24264 | | Abnormal behavior when controlled by the network control plug-in with 'automatic rule setting' | 5.0.28 |
| 101737 | GN-23675 | Genian Syncer | The problem of not being able to register a license file on Genius Sinker | 4.0.144, 5.0.41 |
| 101702 | GN-24167 | Center, Sensor | A problem where the sensor interface information is empty in the sensor managed node information and the sensor cannot manage the node | 5.0.36 |
| 101528 | GN-24310 | macOS Agent, Windows Agent | An issue where the agent is re-executed indefinitely when updating the 5.0.43 or higher version of the agent | 5.0.43, 6.0.0 |

continues on next page

Table 30 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 101332 | GN-24259 | WebUI | An issue where the software update UI shows a lower version than the current version (when revisions are 100000 or more) as being upgradeable | 5.0.20 |
| 101278 | GN-24260 | Center | A problem where the center daemon terminates abnormally due to the generation of an abnormal event frame when sending an agent-specified action event | 3.3.1.1009 |
| 101263 | GN-24202 | Center | A problem where node group matching works abnormally when a node group condition belongs to a node group (if it doesn't) and the node group that matches the condition is disabled or missing | 5.0.35 |
| 101141 | GN-24015 | procmond, RADIUSD | An issue where the radius daemon is constantly restarted in Policy Server Redundancy Configurations | 4.0.143, 5.0.40 |
| 101018 | GN-24078 | Center | A problem where the operating state of the switch is incorrectly set to DOWN | 5.0.35 |
| 101005 | GN-24124 | WebUI | A phenomenon where policy application time is slow when IP-related conditions are added by OR calculation from a node group to group conditions | 5.0.11 |
| 100944 | GN-24161 | WebUI | An issue where the number of licenses has not been exceeded, but a message stating that the license quantity has been exceeded is displayed on the node management screen | 5.0.3 |
| 100944 | GN-24122 | WebUI | A problem where the contents of the set column are not output when adding a management view in node management | 5.0.42 |
| 100944 | GN-24118 | macOS Agent | Some missing issues with the macOS Agent software information collection plug-in | 5.0.0 |
| 100944 | GN-24114 | WebUI | Fixed an issue with tag output from the user list | 5.0.34, 5.0.39 |
| 100944 | GN-24075 | | 외부인증 연동시 사용자패스워드에 특수문자(')를 사용하는 경우 인증실패 발생하는 문제 | 4.0.145, 5.0.42, 6.0.1 |
| 100944 | GN-24074 | | An issue where the update fails because an agent (4.x) information update (updateinfo) request is detected using the SQL Injection syntax | 4.0.145, 5.0.42 |
| 100944 | GN-24072 | WebUI | An issue where Tomcat Context.xml cannot use the db password registered in local.conf | 4.0.146, 5.0.44, 6.0.1 |
| 100944 | GN-24066 | Authsync | A problem where CSV information fails to be synchronized due to reading failure even when the file is normal | 4.0.146, 5.0.44, 6.0.1 |
| 100944 | GN-24025 | WebUI | A problem where the add to the task selection node basket function does not work | 5.0.44, 6.0.1 |
| 100944 | GN-23948 | Sensor | SNMP v3 switch SNMP information collection abnormal issue | 5.0.41 |
| 100944 | GN-23845 | WebUI | An error message is displayed when the widget displayed as an audit log > analysis chart is filtered by a log filter | 4.0.14 |
| 100944 | GN-23807 | Center | In a proxy environment (operating system update proxy service settings), the update fails because the WSUS server IP is not included in the PAC | 4.0.115, 5.0.12 |
| 100944 | GN-23804 | WebUI | Fix the error message output format when the switch port manager is down | 4.0.106 |
| 100944 | GN-23788 | WebUI | A problem where data cannot be retrieved when sorting usage locations on the IP usage application results search screen | 4.1.0, 4.0.23 |

continues on next page

Table 30 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 100944 | GN-23773 | WebUI | Improved import of file and folder lists in the debug log screen | |
| 100944 | GN-23761 | WebUI | File distribution actions cannot be assigned when creating a node policy | 5.0.36 |
| 100944 | GN-23755 | WebUI | [4.0.1] Problem with adding/deleting Syslog audit log filters in Settings > Preferences > Audit History not working properly | 4.0.145 |
| 100944 | GN-23751 | CLOUD | A problem where backup files are created because secondary backups for cloud site backup continue to accumulate in object storage | 6.0.0 |
| 100944 | GN-23703 | | Site Administration > An issue where the sensor's vxlan cannot be reset when changing IPSEC network settings | 6.0.1 |
| 100944 | GN-23691 | Authsync | A problem where information synchronization fails because the CLOUD Policy Server (NAC6) AUTHSYNC > gndbserver setting is set to dbserver | 6.0.0 |
| 100944 | GN-23689 | WebUI | Improved dashboard-related data generated at login time to be generated when an administrator is created | 6.0.0 |
| 100944 | GN-23664 | WebUI | A problem where log2migration does not work properly | 5.0.41 |
| 100944 | GN-23656 | WebUI | An issue where v3 settings are not possible when setting SNMP switches in batches | 5.0.17 |
| 100944 | GN-23648 | | VXLAN interface disappearance issue | 6.0.1 |
| 100944 | GN-23625 | WebUI | An error occurred on the login page when the management console administrator account allowIp setting was set to X.X.X.X/0 | 5.0.41 |
| 100944 | GN-23621 | | An issue where the httpd daemon does not run due to an SSL certificate generation error when upgrading from 4.0.112 or 5.0.9 or earlier | 4.0.112,<br>5.0.9 |
| 100944 | GN-23612 | WebUI | An issue where paging does not work after moving from quick search to the node list | 5.0.38 |
| 100944 | GN-23609 | WebUI | Modify the minimum value of the node status check minimum cycle option | 5.0.38 |
| 100944 | GN-23601 | | Unable to boot when upgrading a device with gntarget=s_i686 set in grub.conf | 4.0.12 |
| 100944 | GN-23599 | WebUI | A problem where tags are assigned on the node detail screen and then deleted without updating the screen, they are not deleted | 5.0.22 |
| 100944 | GN-23590 | | A problem where the management console does not work when upgrading to 4.0 | 4.1.M5 |
| 100944 | GN-23571 | WebUI | A problem where an error is displayed as a required input value when the user clicks the Edit button after deleting the upload file on the custom button, but the file is deleted | 4.0.106 |
| 100944 | GN-23553 | CWP | An issue where html tags are output when a file upload error is output from the CWP user registration page | 4.0.106 |
| 100944 | GN-23534 | Center | Symptoms of the DPI link for the node being registered not being displayed due to the agent | 5.0.39 |
| 100944 | GN-23528 | WebUI | A problem where password verification fails when performing an agent action (file distribution) on a node | 4.0.4 |

continues on next page

Table 30 – continued from previous page

| Revision | Key | Components | Description | Affects Versions |
|---|---|---|---|---|
| 100944 | GN-23519 | WebUI | A problem where the quantity of software status does not match the number of nodes in node management | 5.0.38 |
| 100944 | GN-23440 | Windows Agent | A problem where a network drive is included when testing the entire vaccine through the vaccine information collection plug-in | 4.1.0, 5.0.0 |
| 100944 | GN-23275 | WebUI | Problems showing UTC time in node report charts | 5.0.22 |
| 100944 | GN-23217 | Authsync | A problem where all users can be deleted if a csv read error occurs when synchronizing csv user information | 4.0.1 |
| 100944 | GN-23026 | IPMGMT | IPMGMT file upload additional field function error | 5.0.36 |

## 23.5 Security Advisories

### 23.5.1 Genian ZTNA Security Advisories

Last Updated: 2025-10-01

#### Security Vulnerability

| Fixed Versions | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 6.0.9 | GN-25753 | WebUI | Improved so that CWP does not redirect to an illegal path via the PAGEFW parameter | | 4.2 |
| 6.0.9 | GN-25746 | Center, Sensor | Secure coding inspection results vulnerability patch | | |
| 6.0.9 | GN-25438 | Center, Sensor | Improved the _filelist.html file to be generated differently for each center | | 3.0 |
| 6.0.8 | GN-25561 | WebUI | Blind SQL Injection vulnerability in node search bar | | 5.3 |
| 6.0.8 | GN-25184 | Sensor | Modified Dnsmasq to not cache query results in order to prevent DNS Cache Attacks | | 3.7 |
| 6.0.8 | GN-23677 | Center, Sensor | Administrator approval system to enhance security when registering sensor policy servers | | 7.9 |
| 6.0.7 | GN-25387 | Database, WebUI | Issues where management roles are not applied to Policy > Cloud Security Group Policy | | 3.5 |
| 6.0.7 | GN-25309 | Center, Sensor | CSAP (SaaS) Security Certification Audit Source Code Vulnerability Measures - C/C++ | | 7.5 |
| 6.0.7 | GN-25250 | WebUI | Possible problems with XSS when/is appended after the HTML Tag string | | 4.9 |
| 6.0.7 | GN-25239 | WebUI | Tomcat version upgrade (8.5.78 -> 9.0.65) | | 7.5 |
| 6.0.7 | GN-25237 | WebUI | CSAP (SaaS) security certification audit source code vulnerability measures | | 0.0 |

continues on next page

Table 31 – continued from previous page

| Fixed Versions | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 6.0.7 | GN-25193 | WebUI | [Universal OS Ubuntu] Management Console > An issue where the 'X-Frame-Options' header on the CWP Design Template list page is displayed as allowall | | 6.5 |
| 6.0.7 | GN-25119 | macOS Agent | Upgrade to the latest versions of macOS Agent, OpenVPN (2.5.7), and OpenSSL (1.1.1q) | | 5.3 |
| 6.0.6 | GN-25306 | WebUI | A problem where usable method information is output through an unused HTTP-method | | 5.3 |
| 6.0.6 | GN-25110 | Linux Agent | Upgrading Linux Agent, OpenVPN (2.5.7), and OpenSSL (1.1.1q) to the latest versions | | 5.3 |
| 6.0.5 | GN-25104 | Center, macOS Agent, Sensor, Windows Agent | Upgrading to the latest version of OpenSSL (OpenSSL 1.1.1q) | | 5.3 |
| 6.0.5 | GN-24782 | WebUI | Library upgrades based on vulnerability checks | | 9.8 |
| 6.0.4 | GN-25064 | WebUI | Web service vulnerability improved so that Apache WAS information is not exposed | 4.0.119, 5.0.16 | 2.5 |
| 6.0.4 | GN-24583 | WebUI | A lib upgrade where a vulnerability was discovered in the Java lib used by WebUI | | 9.8 |
| 6.0.4 | GN-23947 | Windows Agent | 윈도우 에이전트 Secure coding inspection results vulnerability patch | 5.0.0, 6.0.0 | |
| 6.0.39, 6.0.35 (LTS), 6.0.26 (LTS) | GN-30800 | WebUI | Tomcat version upgrade (9.0.108 -> 9.0.111) | 5.0.65 (LTS), 6.0.26 (LTS), 6.0.35 (LTS), 5.0.75 (LTS), 6.0.36, 5.0.76 | 2.2 |
| 6.0.39 | GN-30004 | WebUI | Lib version update/removal work with critical vulnerabilities | | 0.0 |
| 6.0.37, 6.0.35 (LTS), 6.0.26 (LTS) | GN-30382 | WebUI | Improved so that files that can execute scripts are not uploaded | | 3.1 |
| 6.0.37, 6.0.35 (LTS), 6.0.26 (LTS) | GN-30205 | WebUI | Improve issues where node and user management policies can be modified and policies can be applied with limited rights through web browser control | | 3.1 |
| 6.0.32 | GN-26504 | WebUI | Vulnerability where internal network information can be queried through CWP | 5.0.0, 6.0.0 | 4.3 |

continues on next page

Table 31 – continued from previous page

| Fixed Versions | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 6.0.3 | GN-24917 | Center, macOS Agent, Sensor, Windows Agent | Upgrading to the latest version of OpenSSL (OpenSSL 1.1.1o) | | 9.8 |
| 6.0.3 | GN-24908 | WebUI | Tomcat version upgrade (8.5.78) | | 8.6 |
| 6.0.3 | GN-24851 | Center | Apache HTTP Server 2.4.53 upgrade | | 9.8 |
| 6.0.28 | GN-26452 | WebUI | A vulnerability that can modify a user's immutable information | 5.0.0, 6.0.0 | 2.2 |
| 6.0.27 | GN-23501 | | Change REST API calls to be made only through the management console port (8443) | | |
| 6.0.22 | GN-26723 | WebUI | Vulnerability fixes that are not immediately reflected when the administrator's rights are changed | | 3.3 |
| 6.0.21, 6.0.16 | GN-28063 | WebUI | A problem where blind injection is possible in the node management search bar | | 2.2 |
| 6.0.20, 6.0.16 | GN-27107 | WebUI | Service disabled by executing a Tomcat restart command by an unauthorized administrator | 5.0.41 | 2.7 |
| 6.0.2 | GN-24689 | WebUI | Issues where XSS is possible in Audit > Logs > Log Search | | 4.3 |
| 6.0.2 | GN-24687 | WebUI | An issue where files can be accessed by relative paths on the debug log screen | | 3.83 |
| 6.0.2 | GN-24651 | Center, macOS Agent, Windows Agent | Upgrading to the latest version of OpenSSL (OpenSSL 1.1.1n) | 4.0.0, 5.0.0, 6.0.0 | 7.5 |
| 6.0.2 | GN-24535 | WebUI | Remove logstash | | 5.9 |
| 6.0.18, 6.0.16 | GN-26393 | WebUI | Vulnerability where information can be modified by directly entering a URL to an unauthorised page | | 3.1 |
| 6.0.18, 6.0.16 | GN-26390 | WebUI | File export permission bypass vulnerability for unauthorized administrators through the Audit Log REST API | | 3.1 |
| 6.0.17, 6.0.16 | GN-27492 | WebUI | Tomcat version upgrade (8.5.94 -> 8.5.96/9.0.81 -> 9.0.83) | | 7.5 |
| 6.0.17, 6.0.16 | GN-27278 | WebUI | Tomcat version upgrade (8.5.94/9.0.81) | | 7.5 |
| 6.0.17, 6.0.16 | GN-26315 | WebUI | Improved two-step verification to limit the number of times the verification code can be entered and the time limit | | 4.3 |
| 6.0.17 | GN-26600 | WebUI | The problem of not being able to log in after an abnormal API call | 5.0.42, 5.0.49, 6.0.7, 4.0.156, 5.0.56 | 5.3 |

continues on next page

Table 31 – continued from previous page

| Fixed Versions | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 6.0.16 | GN-27014 | WebUI | A problem where Passkey can be registered using the Passkey re-registration function without permission | | 3.9 |
| 6.0.16 | GN-26935 | WebUI | Vulnerability where an html tag output as a department name is executed in a tree | 5.0.0 | 1.2 |
| 6.0.16 | GN-26835 | Center | Command Injection vulnerability via SQL used to update data | | 6.6 |
| 6.0.16 | GN-26833 | Sensor | nmap script tampering vulnerability during sensor NMDB update | | 4.1 |
| 6.0.16 | GN-26696 | Sensor | Insufficient validation of incoming sensor events | | 6.3 |
| 6.0.16 | GN-26694 | Center | Parameter injection vulnerability due to insufficient verification of download URLs | | 6.6 |
| 6.0.16 | GN-26383 | WebUI | Vulnerability where html/script code can be injected | | 5.3 |
| 6.0.15 | GN-26814 | Center | Code improvements to Bufferoverflow | | 2.0 |
| 6.0.15 | GN-26725 | Linux Agent, macOS Agent, Windows Agent | [Agent] Added validation for events sent from the Center and sensors | | 6.3 |
| 6.0.15 | GN-26392 | WebUI | Vulnerability that allows unprivileged administrators to download debug logs | | 2.9 |
| 6.0.15 | GN-26368 | WebUI | Vulnerability where an administrator's API key is exposed to other administrators | | 5.3 |
| 6.0.15 | GN-26222 | WebUI | A problem where redirection can be performed by modulating the returnURL parameter used when moving pages in the management console | | 1.9 |
| 6.0.14 | GN-26460 | Windows Agent | A vulnerability that allows an ordinary user to obtain PC administrator rights via an agent | 5.0.0, 6.0.0 | 4.6 |
| 6.0.14 | GN-26391 | WebUI | Vulnerability where an unauthorized administrator can view debug logs in real time | 5.0.0, 6.0.0 | 2.9 |
| 6.0.13 | GN-26286 | WebUI | An issue where Google OTP 2-step verification can pass 2-step verification by receiving a new security key | | 6.5 |
| 6.0.12 | GN-26205 | Database | MySQL version upgrade 5.7.40 -> 5.7.41 | | |
| 6.0.12 | GN-26150 | WebUI | Tomcat version upgrade (9.0.68 -> 9.0.72, 8.5.78 -> 8.5.86) | | |
| 6.0.12 | GN-26062 | Center, macOS Agent, Sensor, Windows Agent | OpenSSL 1.1.1t upgrade - Passing random pointers to memcmp calls can read memory contents or cause denial of service | | 7.4 |
| 6.0.12 | GN-26000 | MySQL | MySQL version upgrade 5.7.33 -> 5.7.40 | | |

continues on next page

Table 31 – continued from previous page

| Fixed Versions | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 6.0.12 | GN-25869 | CWP | A problem where only an account (ID) is authenticated when CWP is authenticated using the agent user authentication menu when the IP management message is first on | 6.0.3, 5.0.46 | 3.4 |
| 6.0.11 | GN-25982 | WebUI | CSP and HSTS headers added to WebUI Response Headers | | |
| 6.0.11 | GN-25875 | Windows Agent | A problem where agents have high privileges when running a web browser | 4.0.0, 5.0.0, 6.0.0 | 3.3 |
| 6.0.11 | GN-25849 | WebUI | WebUI lib vulnerability check | | |
| 6.0.11 | GN-25811 | IPMGMT | A problem where you can log in with only a user ID via frontpage in the IP application system | | 4.9 |
| 6.0.10 | GN-25925 | IPMGMT, WebUI | IP Application System > IP Application Screen XSS Possible Problems | | 5.4 |
| 6.0.10 | GN-25847 | WebUI | Added a re-authentication procedure when accessing the user information modification page on the CWP screen | | 4.2 |
| 6.0.10 | GN-25740 | WebUI | Issues where XSS is possible in Audit > Logs > Log search bar | | 5.6 |
| 6.0.1 | GN-24305 | GNOS | 2.4.52 version upgrade for Apache vulnerability measures | | 9.8 |
| 6.0.1 | GN-24253 | WebUI | log4j vulnerability improvements | | 9.8 |
| 6.0.1 | GN-23714 | Center | Complementing agent-related APIs with poor authentication | | 4.6 |
| 6.0.1 | GN-23461 | WebUI | [SaaS] Saas security authentication source code inspection result measures | | 9.1 |
| 6.0.1 | GN-23446 | gnlogin, WebUI | Handle passwords so that specific words cannot be used | | 8.7 |
| 6.0.0 | GN-24030 | GNOS | Removing the reverse shell feature from the netcat (nc) command included with the product | | |
| 6.0.0 | GN-24014 | Center | SOAP/REST restrictions that can be called via HTTP | | 2.5 |
| 6.0.0 | GN-23981 | macOS Agent, Windows Agent | An abnormal termination issue due to packet manipulation of UDP events to the agent | | 3.4 |
| 6.0.0 | GN-23977 | macOS Agent, Windows Agent | Fixed an XSS vulnerability when the agent displayed instant messages | | 6.8 |
| 6.0.0 | GN-23972 | Center, Sensor | A problem where the daemon may terminate abnormally when processing UDP event packets | 5.0.36 | 6.4 |
| 6.0.0 | GN-23970 | WebUI | Administrator login bypass vulnerability using mobile apps | | 6.1 |
| 6.0.0 | GN-23967 | WebUI | REST API Command Injection | | 6.7 |

continues on next page

Table 31 – continued from previous page

| Fixed Versions | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 6.0.0 | GN-23966 | WebUI | XSS attack vulnerability when applying as an Excel file when applying as a CWP user | | 6.8 |
| 6.0.0 | GN-23965 | WebUI | Internal file download vulnerability via a relative path on the Agent Download page | 5.0.37 | 5.2 |
| 6.0.0 | GN-23794 | WebUI | A problem where the REST API can be called even if there is no valid authentication base when calling the REST API | | 4.9 |
| 6.0.0 | GN-23743 | Center | Improving Denial of Service (DoS) vulnerabilities through APIs | | 6.4 |
| 6.0.0 | GN-23708 | Center | Complementing sensor-related APIs with poor authentication | | 4.6 |
| 6.0.0 | GN-23706 | Center | Internally used SOAP API vulnerability exposed externally via RPC | | |
| 6.0.0 | GN-23705 | WebUI | (KVE-2021-1062) Enhanced name validity check for the file upload component in Conf Engine | | 6.7 |
| 6.0.0 | GN-23702 | WebUI | (KVE-2021-1062) SSTI vulnerability in CWP Design Template | | |
| 6.0.0 | GN-23701 | Windows Agent | (KVE-2021-1062) Vulnerability where relative paths can be used when generating agent files | | 6.1 |
| 6.0.0 | GN-23700 | Center | (KVE-2021-1061) A vulnerability where passwords can be changed without being an authenticated user on a node | | 8.7 |
| 6.0.0 | GN-23699 | Center, Sensor | (KVE-2021-1061) Vulnerability where information from all nodes can be obtained without sensor information | | |
| 6.0.0 | GN-23663 | macOS Agent, Windows Agent | Agent OpenSSL 1.1.1l update | | 9.8 |
| 6.0.0 | GN-23662 | GNOS | Upgraded to openSSL version 1.1.1l | 4.0.146, 5.0.44, 6.0.1 | 9.8 |
| 6.0.0 | GN-23563 | Center | Fixes to defend against command injection attacks | | 8.0 |
| 6.0.0 | GN-23533 | Center | Improved so that unusable plug-ins are not delivered to agents | | 7.6 |
| 6.0.0 | GN-23500 | Center | Improved SQL Injection defense processing method | | 8.7 |
| 6.0.0 | GN-23499 | GNOS | Remove the vulnerable LD_LIBRARY_PATH environment variable within GNOS | | |
| 6.0.0 | GN-23488 | WebUI | [SaaS] SaaS security authentication WAS (Tomcat) vulnerability improvements | | 7.5 |
| 6.0.0 | GN-23377 | GNOS | Upgrading openssh to version 8.6p1 | | |
| 6.0.0 | GN-23358 | WebUI | [CC] Web vulnerability check results security | | 6.5 |
| 6.0.0 | GN-23237 | GenianOS | Apache httpd (2.4.48)/tomcat (8.5.63) upgrade | | 7.5 |

continues on next page

Table 31 – continued from previous page

| Fixed Versions | Key | Components | Description | Affects Versions | CVSS Score |
|---|---|---|---|---|---|
| 6.0.0 | GN-23233 | Elastic-Search | [CC] Elasticsearch upgraded to version 5.6.16 | | 8.8 |

CHAPTER

# TWENTYFOUR

# SECURITY ADVISORIES

## 24.1 GZ-SA-2023-001: Genian ZTNA - Multiple Vulnerabilities

### 24.1.1 Date

- Aug 15, 2023

### 24.1.2 Serverity

- High

### 24.1.3 Summary

The following vulnerabilities were discovered on the Genie Update Server and measures were taken, and additional security updates were released to enhance product security. Users using the affected version are recommended to update to the latest version.

- Plaintext exposure vulnerability (CVE-2023-40251)
- Unauthorized Script Execution Vulnerability (CVE-2023-40252)
- Improper Authentication Vulnerability (CVE-2023-40253)
- Integrity Verification Insufficient Vulnerability (CVE-2023-40254)

### 24.1.4 Affected Products

- Genian ZTNA 6.0.15 or lower

### 24.1.5 Resolution

The vulnerabilities contained in this advisory can be addressed by upgrading to version listed below:

- Genian ZTNA 6.0.16 or later

### 24.1.6 Workaround

- Plaintext exposure vulnerabilities can be temporarily addressed by changing the event port.

**Note:** To address vulnerabilities, you must upgrade the policy server, network sensor, and agent.

## 24.2 GZ-SA-2024-001: Genian ZTNA - Blind SQL Injection Vulnerability

### 24.2.1 Date

- April 26, 2024

### 24.2.2 CVSS score

- 2.2

### 24.2.3 Influence

- low

### 24.2.4 Details

We have discovered a problem that could lead to Blind SQL Injection attacks due to insufficient validation of input values for search conditions when searching for nodes in the Genie NAC management console. We have taken action and announced a security update to enhance product security.

Users using this version are recommended to update to the latest version.

- Genian ZTNA SQL Injection (CVE-2024-23843)

### 24.2.5 Influence version

- Genian ZTNA 6.0.20 and below
- Genian ZTNA 6.0.16 LTS (Revision 125554 or earlier)

### 24.2.6 How to solve

The vulnerabilities included in this advisory can be addressed by updating to the versions below.

- Genian ZTNA 6.0.21 or later
- Genian ZTNA 6.0.16 LTS (Revision 12555 or later)

### 24.2.7 Temporary measures

- doesn't exist

CHAPTER

TWENTYFIVE

# SERVICE LEVEL AGREEMENT

This document outlines the service levels for Genians Next-Gen ZTNA solution, which includes the Genian ZTNA Software with the valid maintenance, Cloud-managed ZTNA Subscription and Genian ZTNA Appliances with the valid extended coverage.

## 25.1 Software Upgrade & Patch

Genians will provide software upgrade and patches to customers who purchase valid maintenance service or subscribe to the cloud services.

- At least 2 updates per year are provided to improve the function. (Including Major version upgrades)
- At least 4 updates per year are provided to fix errors.

## 25.2 Technical Support Services

### 25.2.1 Standard Online Support Service

The service will be provided by Genians via Email, Slack, and Online forum at Genians.com. The following services are included in the subscription fee.

- **Public Channel**
  - Answers (Online forum) on genians.com
  - Slack Channel (#qna)
- **Private Channel**
  - Email
  - Dedicated Slack Channel
  - Remote control (if needed)
- **Support hours**
  - 24x5 (Monday~Friday)
- **Initial Response Time**
  - Level 1 (Critical Business Impact): Within 4 Hours
  - Level 2 (Significant Business Impact): Within 8 Hours
  - Level 3 (Minimal Business Impact): Within the next business day

### 25.2.2 Advanced Support Services

Advanced or additional services like on-site visit, 24x7 can be provided by Genians certified partners. Learn more https://www.genians.com/with-partners/

## 25.3 Service Availability (Cloud-managed only)

### 25.3.1 Service Uptime

Genians will guarantee to manage Genians Cloud-based Services (Policy Server, Device Platform Intelligence) 99.9% uptime during the subscription period. If Genians fails the service uptime, Service Credit (See the table below) will be applied to the following subscription month/year (or any subsequent month/year)

| Service Availability Level | Service Credit |
|---|---|
| 99.8% - 99.0% | 10% of total subscription fees applicable to month/year in which failure occurred |
| 98.9% - 98.0% | 20% of total subscription fees applicable to month/year in which failure occurred |
| 98.9% - 98.0% | 30% of total subscription fees applicable to month/year in which failure occurred |
| Below 96.0% | 50% of total subscription fees applicable to month/year in which failure occurred |

Customer must inform any issues related to the service uptime immediately to Genians online support team via Slack or Email. Customer must inform Genians online support team within thirty (30) days from the time Customer becomes eligible to receive a Service Credit. Failure to comply with these service credit request terms will forfeit Customer's right to receive a Service Credit.

### 25.3.2 Software Upgrade & Maintenance

Genians will inform customers via Slack or Email in advance for the purpose of the following reasons:

- Upgrading the software on a regular or irregular basis
- Maintaining the system for the purpose of improving functionality and providing stable service.

## 25.4 Genians Appliance

Customer can use either their own hardware or Genian ZTNA Appliances. The following services are provided only to the customer who purchases Genian ZTNA Appliances.

### 25.4.1 Warranty

Genians provides 90 days warranty. Once the failed appliance is received by Genians, the repaired device will be shipped within two days.

### 25.4.2 Extended Coverage

- Basic Care (BC)
  - Once the failed appliance is received by Genians, the repaired device will be shipped within two days.
- Instant Replacement (IR)
  - Basic Care Included
  - Genians will ship replacement appliances in advance once the appliance fault is confirmed by Genians.
  - If the customer purchases an IR program for four consecutive years from the time of appliance purchase, Genians provides new appliance.