Genian NAC

Release 5.0.61

GENIANS, INC.

Apr 26, 2024

DEPLOYMENT GUIDE

1 Deployment Overview 3

2 Phase 1 - Network Surveillance / Visibility 5

3 Phase 2 - Plan / Design 7

4 Phase 3 - Configure 9

5 Phase 4 - Test / Validate 11

6 Phase 5 - Expand Deployment 13

7 Understanding Network Access Control 15

8 Deploying Genian NAC 21

9 Installing Genian NAC 47

10 Monitoring Network Assets 71

11 Controlling Network Access 109

12 Managing On-boarding Process 165

13 Managing User Authentication 177

14 Controlling Endpoints with Agent 213

15 Detecting Anomalies 295

16 Managing Logs and Events 311

17 Managing Systems 325

18 API Guide 371

19 Log Format 373

20 Node Group Templates 375

21 Frequently Asked Questions 377

22 Troubleshooting 381

23 Release Notes 421

24 Security Advisories 501

25 Service Level Agreement 507

DOWNLOAD PDF

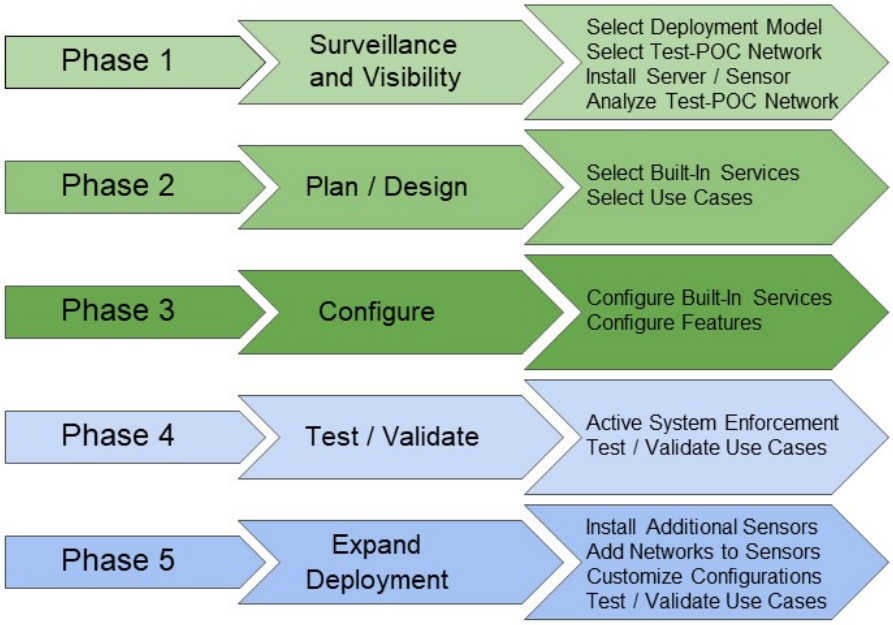
CHAPTER

ONE

DEPLOYMENT OVERVIEW

There are 5 recommended phases for Network Access Control (NAC) 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 NAC to successfully deploy the Genian NAC 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 NAC.

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*
- *Installing Genian NAC*

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 Genian NAC*

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 NAC 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 NAC?

Network Access Control (NAC) 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. NAC 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 NAC 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 NAC 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 NAC policy server is notified and network access can be controlled if a violation has occurred.

7.2 The Evolution of NAC:

First Generation

The earliest generation of NAC 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 NAC 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 NAC 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 NAC provides the ability to quarantine malicious devices from the rest of the LAN. A NAC 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 NAC 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 NAC

Entry By Unauthorized Devices

Networks that do not implement NAC 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. NAC 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. NAC 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, NAC 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, NAC 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. NAC 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. NAC 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. NAC 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 NAC and Firewall

Users who are not familiar with NAC 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 NAC controls communiniation between endpoints within a network. For example, NAC 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 NAC, 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. NAC acts on the endpoints themselves to control traffic between devices within the network in a more flexible fashion.

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

7.5 Steps to Implement NAC

Gain Visibility

The ultimate goal of NAC 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 NAC

- **4th Generation NAC**
  Genian NAC is the flagship product of 4th Generation NAC, 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 NAC 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 NAC provides the broadest set of access control methods compared to other NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC

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

8.1 Understanding Components

To operate Genian NAC, 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 NAC. 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 NAC 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.

If a sensor is deployed in-line, prohibited traffic will be blocked from passing through the 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 NAC deployment with Genian NAC

Establishing network access control can lead to changes in the network environment. To avoid distruption to end-users, Genian NAC uses a phased approach to deployment. Based on the experience gained by deploying NAC 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.

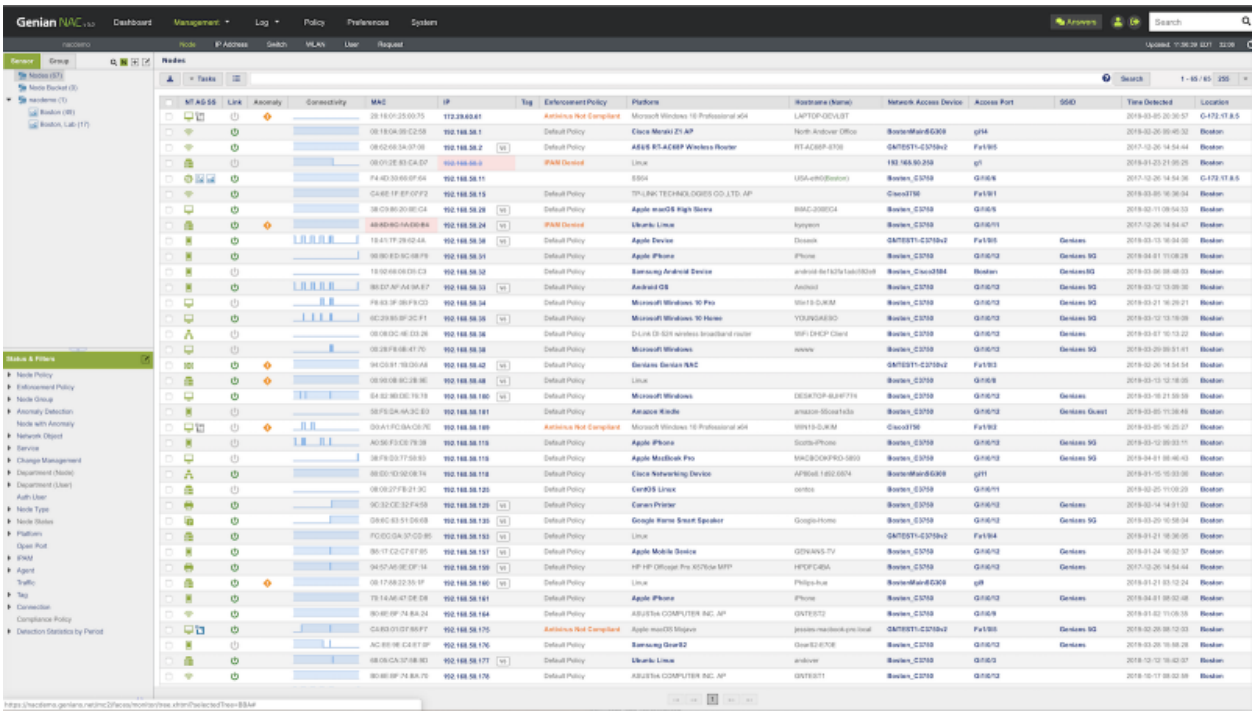
Having visibility into the network and the user device means that the following information can be monitored in real time:

- 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.

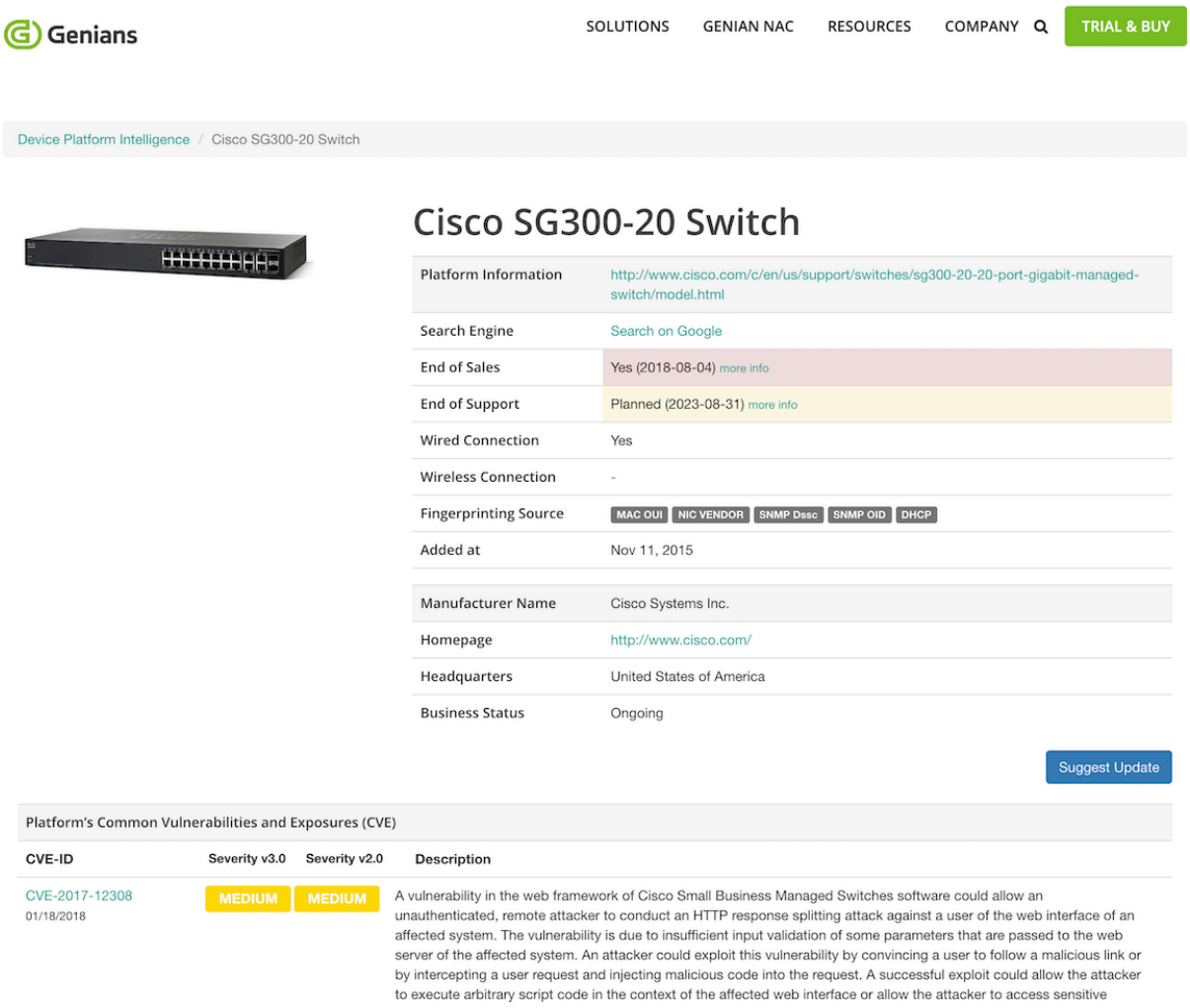


Genian NAC also provides **Agent** software for greater visibility into Windows and MacOS operating systems. It can be installed on the user's system to collect information (operating system / hardware / software / update, etc.) desired by the administrator.

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 NAC 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 NAC's Device Platform Intelligence.



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 NAC 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 NAC 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, Tap Device, 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 (WNIC on Sensor)	Monitoring (SNMP with Controller)	No	No	Monitoring / Control (WPA2-Enterprise)	Monitoring / Control (SSID Whitelist)
Layer 2 Security	Detect MAC Spoofing, Detect Rogue DHCP, Managing IP Conflict	No	No	No	No	No

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

8.2.3 Management Considerations

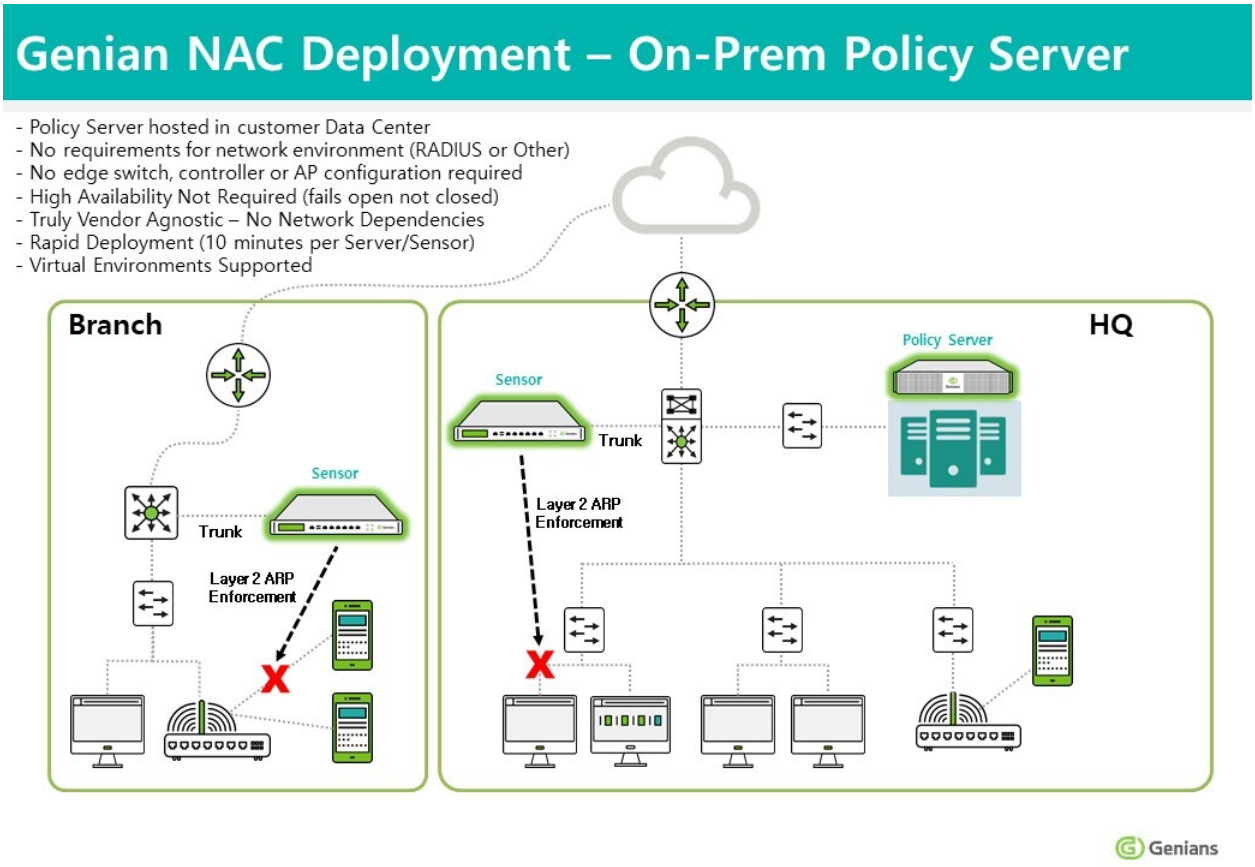
Topic	Layer 2 Sensor/Enforcer	SNMP/CLI	Port Mirror (SPAN)	Inline	802.1x	Agent
Network Config Change	Trunk port (optional)	Switch Config, VLAN/ACL	Tap Device, SPAN Port	Gateway Change	Switch Config, VLAN/ACL, Endpoint Config	No
Compatibility Issue	No	Vendor-dependent SNMP MIB/CLI	No	No	RADIUS Vendor Attribute,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

8.2.4 Deployment Models

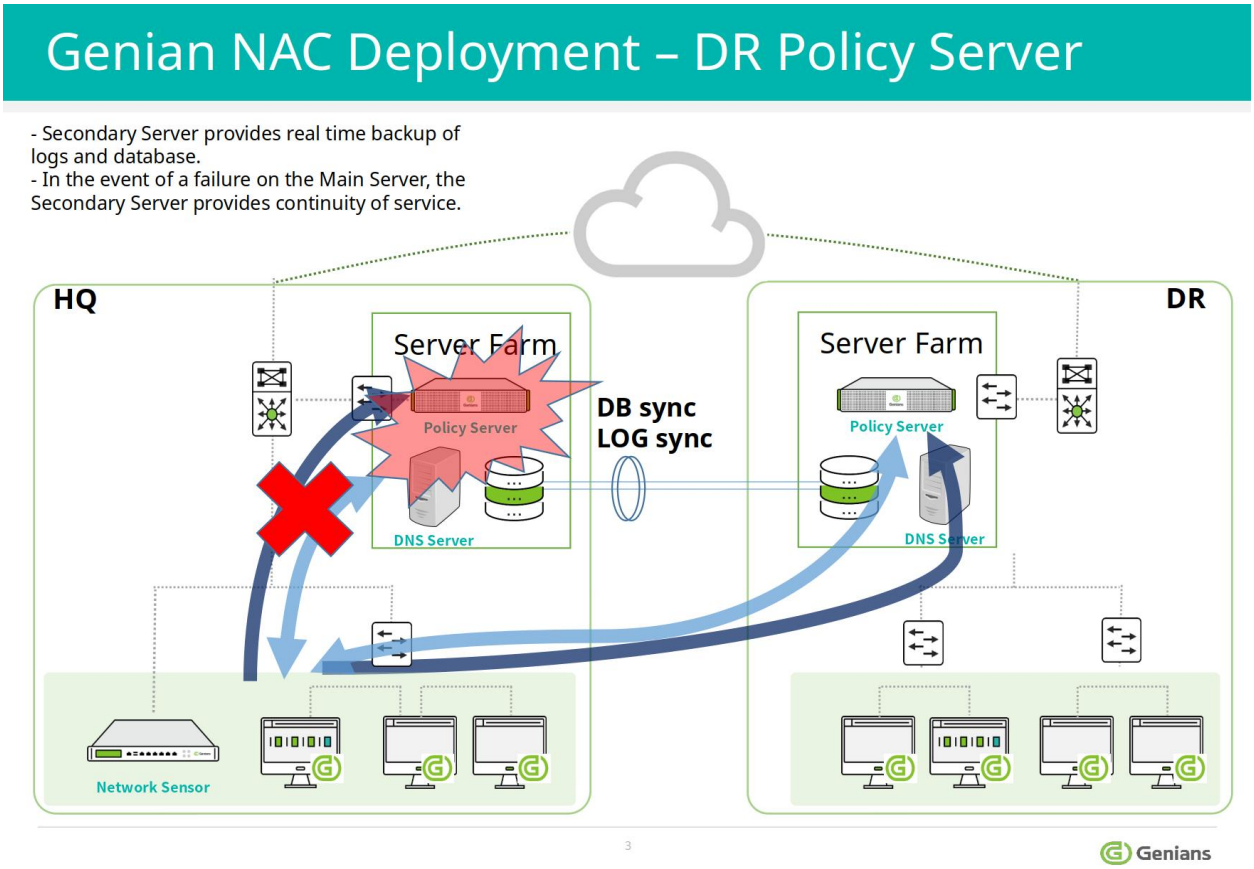
On-Premises

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*



Configuring High Availability

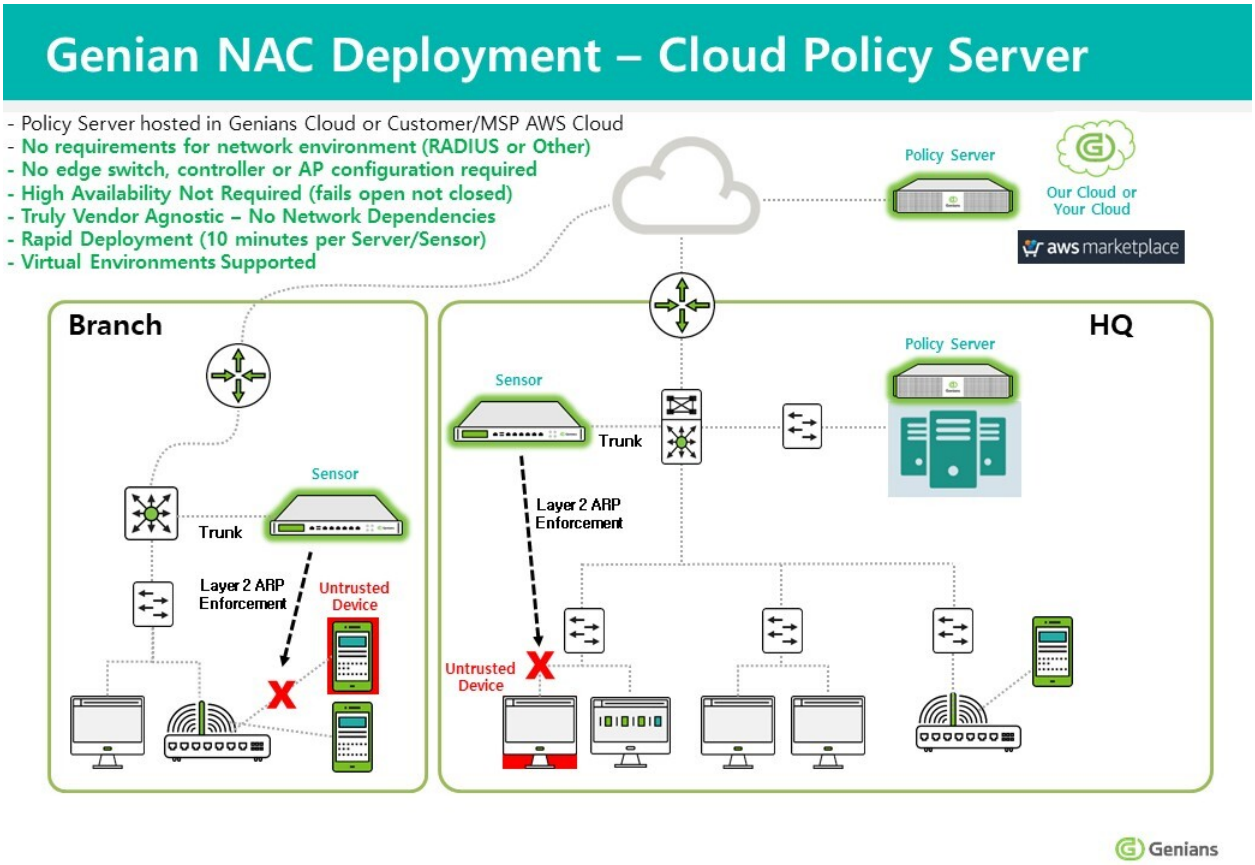


Your Cloud

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 NAC 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.



NAC 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 NAC Components:

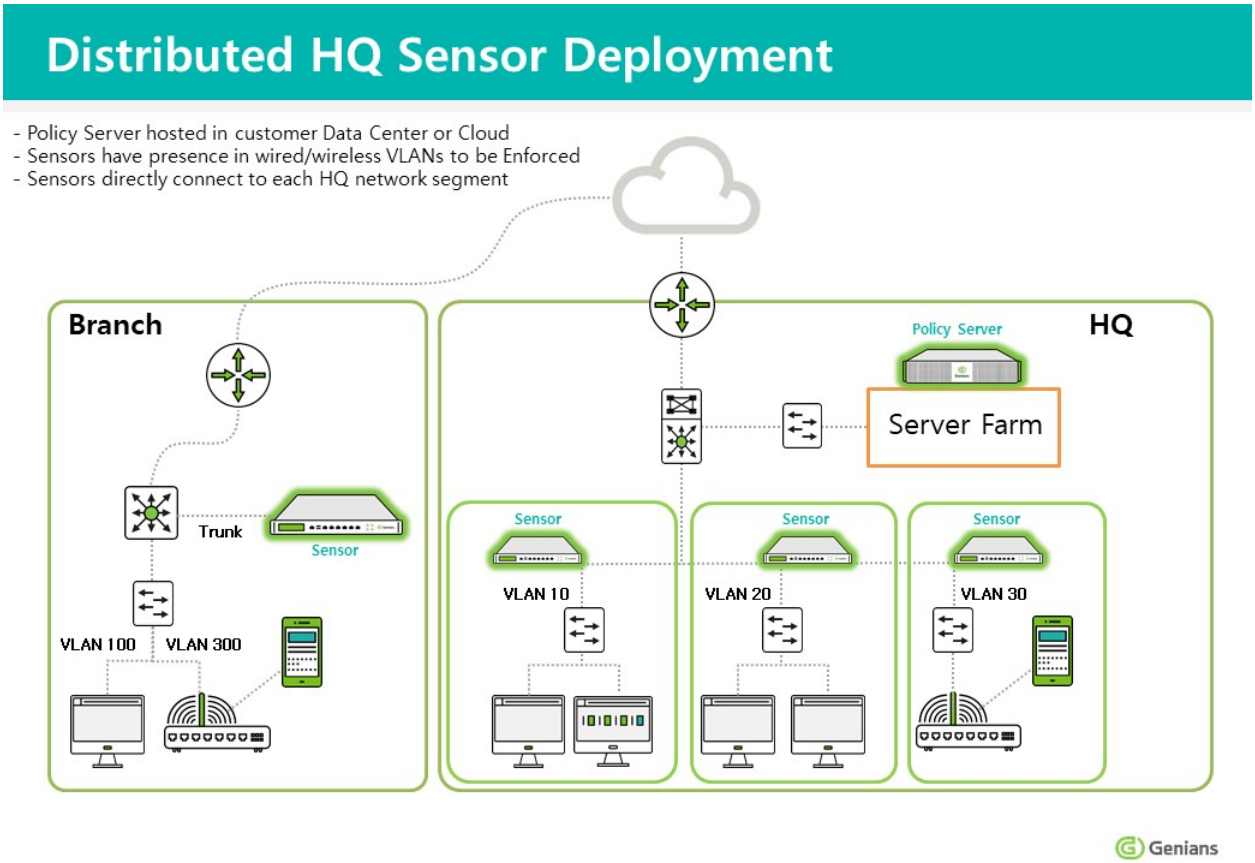
- Policy Server: Supports multi-tenancy (Docker container)
- Network Sensor: Support Universal customer premises equipment (uCPE)
- Agent: Multi functional features and customization

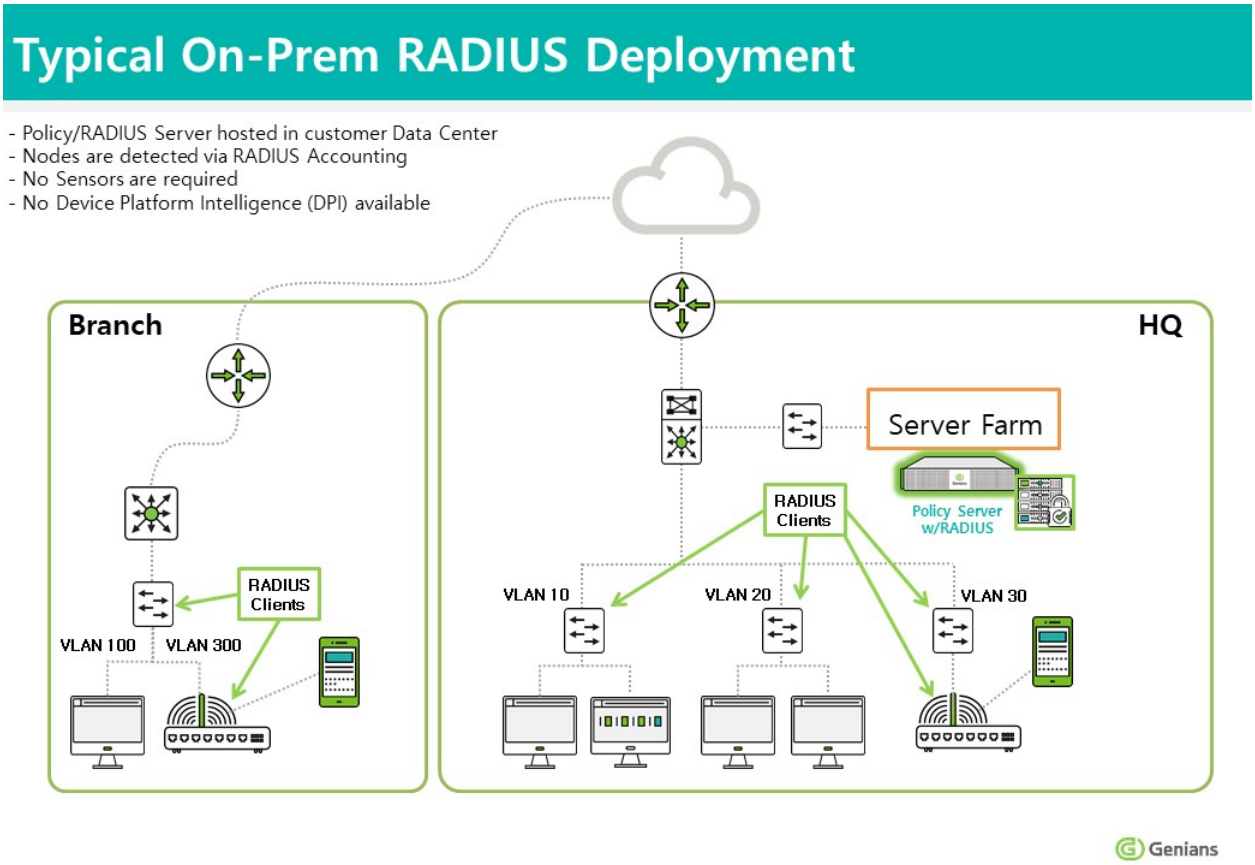
Management:

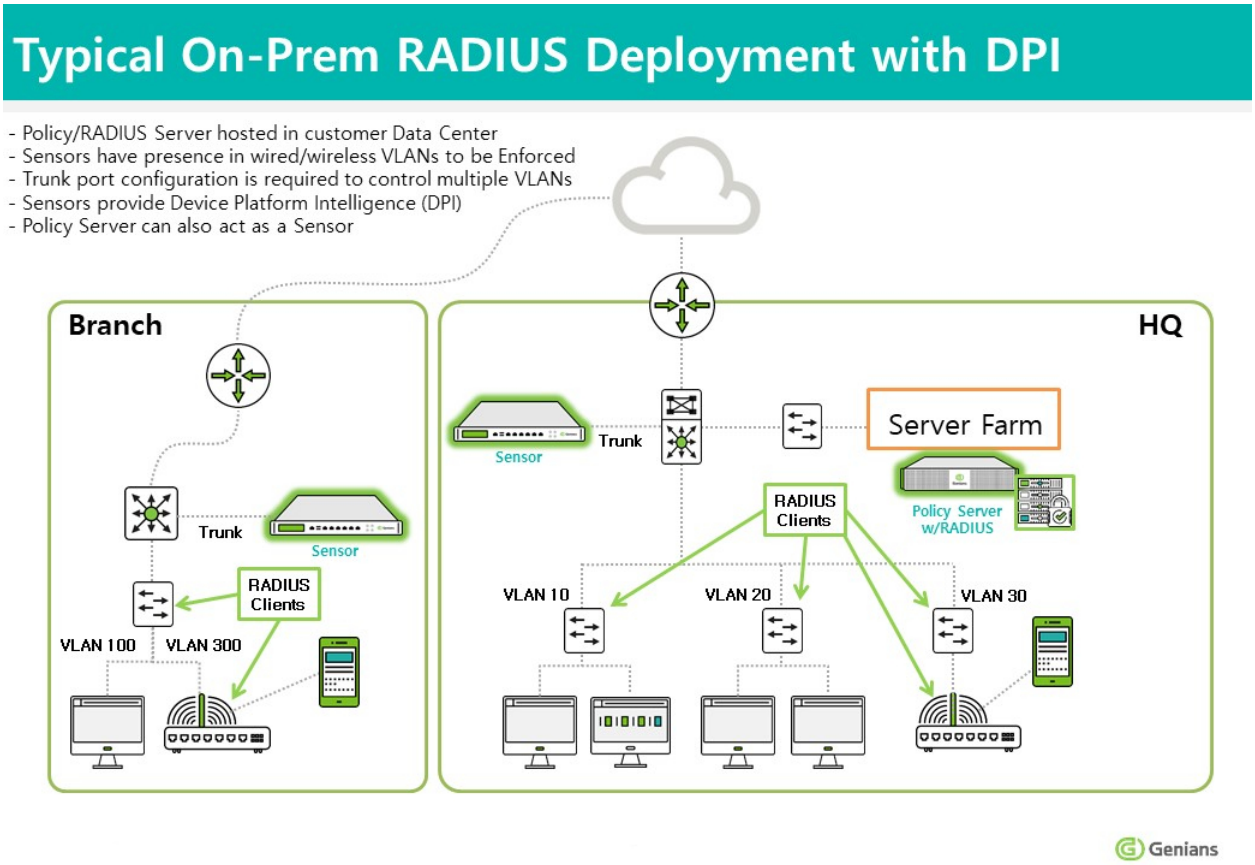
- One-stop service (sites, users, licenses, subscriptions, billing)
- Virtual domain support
- Centralized dashboard/reports
- Zero Config Provisioning
- White label service

Additional Deployment Models

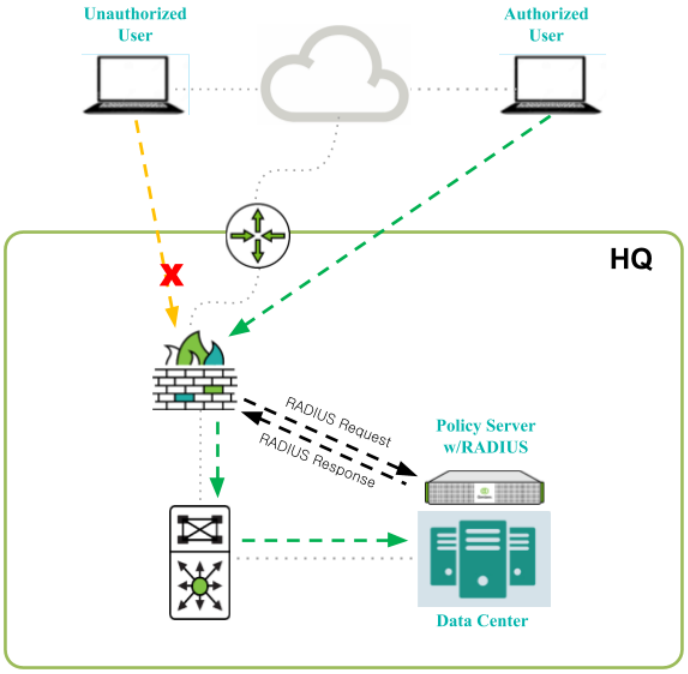
On-Premise


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
Branch
Trunk
Sensor
VLAN 100
VLAN 300
HQ
Policy Server
Server Farm
Sensor
VLAN 10
Sensor
VLAN 20
Sensor
VLAN 30
Genians


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
Branch
HQ
Server Farm
RADIUS Clients
Policy Server w/RADIUS
RADIUS Clients
VLAN 100
VLAN 300
VLAN 10
VLAN 20
VLAN 30
Genians


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
Branch
HQ
Trunk
Sensor
RADIUS Clients
VLAN 100
VLAN 300
Sensor
Trunk
Server Farm
Policy Server w/RADIUS
RADIUS Clients
VLAN 10
VLAN 20
VLAN 30
Genians

Genians VPN Enforcement – Unauthorized User



Highlights:

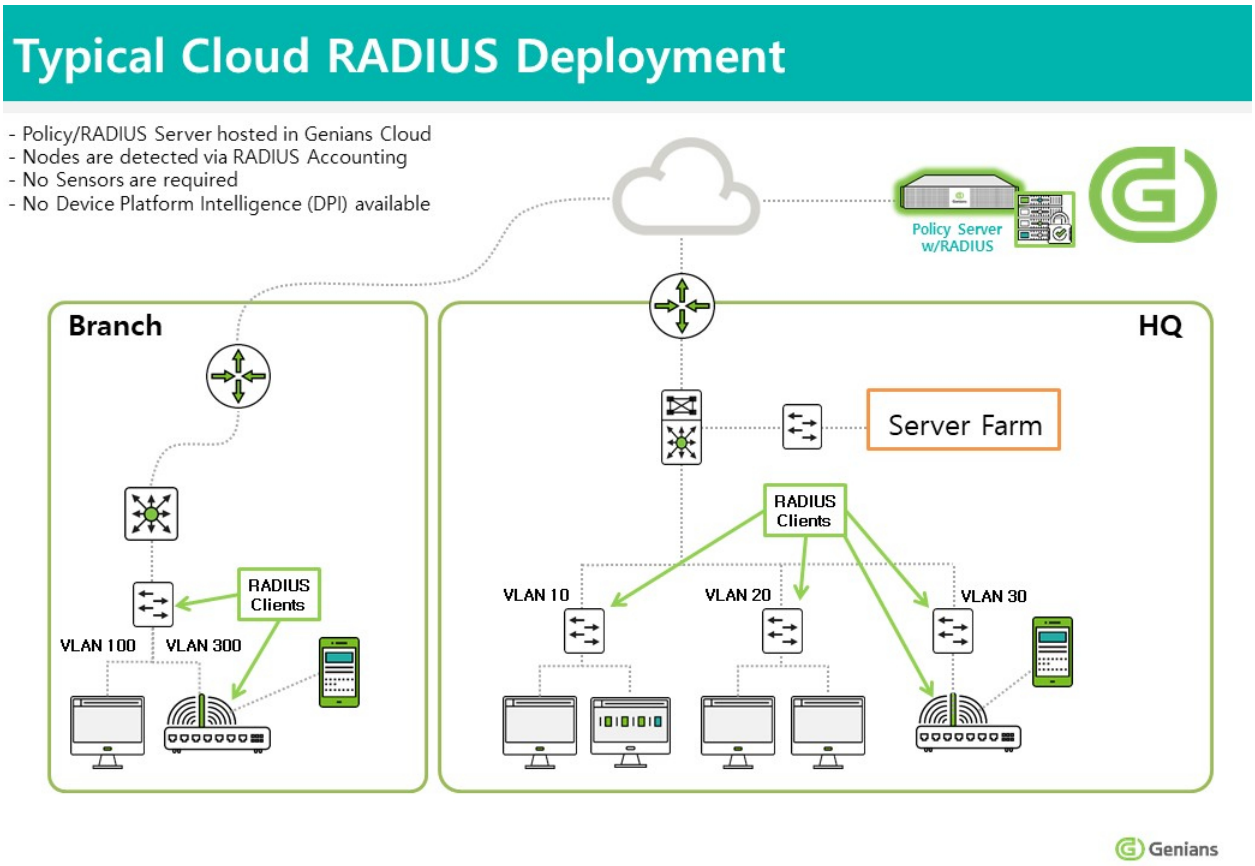
No Agent Required
AD/Local User Accounts
No RADIUS CoA Required

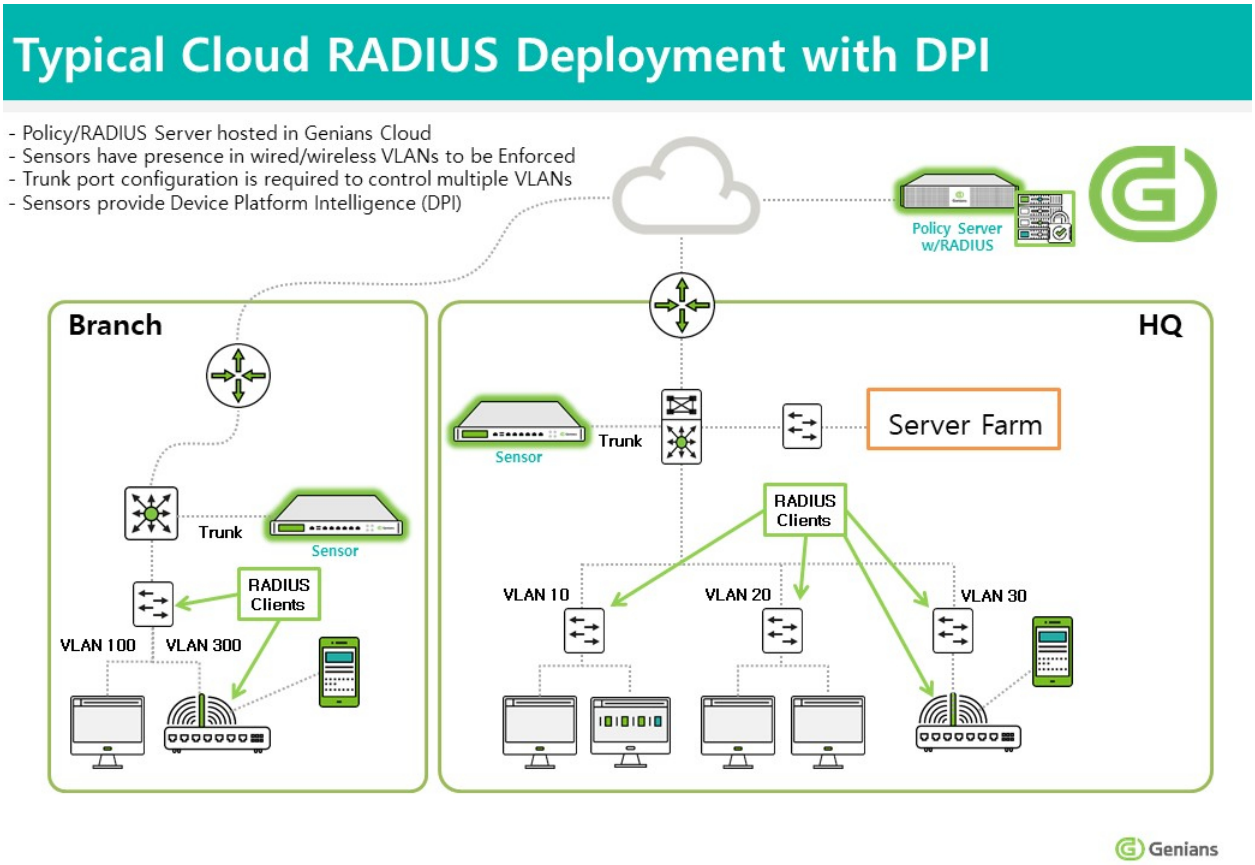
RADIUS Enforcement

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

Genians

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
Policy Server w/RADIUS
Branch
HQ
Server Farm
RADIUS Clients
VLAN 100
VLAN 300
RADIUS Clients
VLAN 10
VLAN 20
VLAN 30
Genians



8.3 Compare Editions

Genian NAC is available in three editions: Basic, Professional, and Enterprise.

Each edition has the following purpose.

Basic
: Provides visibility into network and IT assets.

Professional
: Provides network access control according to IT security policy.

Enterprise
: Provides advanced and automated IT security.

Your deployment can be built and upgraded step by step using each edition, making it easier to build gradually with less cost.

Please refer to the function comparison table for each edition below to select the product that suits you.

Category	Feature	Basic	Professional	Enterprise
Visibility	Detect/Monitor IP-enabled Device	Yes	Yes	Yes
	Device Platform Intelligence (Name, Type, Picture, EOL, Connection, CVE)	Yes	Yes	Yes

continues on next page

Table 2 – continued from previous page

Category	Feature	Basic	Professional	Enterprise
	Switch Port Information	Yes	Yes	Yes
	WLAN Monitoring / Security (Rogue/Misconfigured AP)	Yes	Yes	Yes
	Basic Endpoint Information (OS, HW, Software) by Windows/macOS Agent	Yes	Yes	Yes
	Condition based Dynamic Node Group	Yes	Yes	Yes
	Customizable Dashboards (Over 100 Widgets)	Yes	Yes	Yes
	Track Changes / Audit Logs	Yes	Yes	Yes
	Network Anomaly Detection (MAC Spoofing, Rogue Gateway, Ad-hoc)	Yes	Yes	Yes
	Basic Reports (Node, WLAN, Log)	Yes	Yes	Yes
	Notification (Email/Text Message)	Yes	Yes	Yes
	Custom Reports		Yes	Yes
User Authentication	Captive Portal Login (Web login)		Yes	Yes
	Active Directory SSO		Agent Based	Agentless
	External User Directory Integration (LDAP/RADIUS/SMTP/POP3/IMAP/SAML2)			Yes
	Multifactor Authentication (Text Message/Email/Google OTP)		Admin Only	Yes
Network Access Control	802.1X based Control (RADIUS Server, EAP, MAB, VLAN Assign, CoA)		Yes	Yes
	ARP based Layer 2 Enforcement		Yes	Yes
	Port Mirroring (SPAN) based Enforcement		Yes	Yes
	In-line Enforcement (Dual-homed Gateway)		Yes	Yes
	Switch integration (SNMP) based Enforcement		Yes	Yes
	DHCP based Enforcement (DHCP Server)		Yes	Yes
	Role based Access Control		Yes	Yes
	IP Address Management(IPAM)		Yes	Yes
	Tag-Based Control of Users, Wlans and Devices/Nodes (E.g., Guest devices, temporary privileges, policy exemptions)		Yes	Yes
Desktop Management	Compliance Check (Antivirus, OS Update, Required SW, OS Settings)		Yes	Yes
	OS Configiguration (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
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

continues on next page

Table 2 – continued from previous page

Category	Feature	Basic	Professional	Enterprise
	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
Scalability and Availability	High Availability (Policy Server / Network Sensor)			Yes
	Interface Channel Bonding			Yes
	Disaster Recovery (DB Replication, Redundant Policy Server)			Yes

- Added in Genian ZTNA 6.0

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 NAC 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.

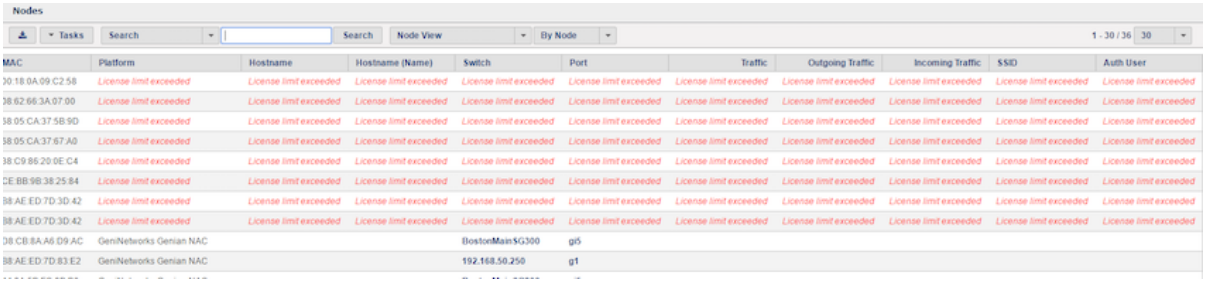
8.4.2 Step 1. Identify the Total Active Devices Number for Software License

The license of Genian NAC 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 NAC 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 NAC 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.)



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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 Firewall Requirements

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

On-Premise

SRC IP	DST IP	Service	Note
Policy Server IP	54.81.159.137 d1s536j2uzv1h7.cloudfront.net (IP may vary) Log-Server DB-Server Network Sensor IP, PC IP(Agent) https://alarm.geninetworks.com https://alarm2.geninetworks.com https://geniupdate.geninetworks.com https://cmupdate.geninetworks.com https://techlab.geninetworks.com https://pi-api.genians.com https://api.genians.com	TCP/443 TCP/443 TCP/9200~9300, TCP/9300~9400 TCP/3306 UDP/3871 TCP/443 TCP/443 TCP/443 TCP/443 TCP/80, TCP/443 TCP/443 TCP/443	Sign-in to www.genians.com (*On-Prem Only*) Download Updated Software Image (*On-Prem Only*) Log-Server Database KeepAlive, Send Event Alarm Service Alarm Service GenianData Update **GENIAN Data** Update (*On-Prem Only*) GenianData Update(Global) Platform false positive report/non-detection report Genian DPI Join Us Login Feature
Network Sensor IP	Policy Server IP/FQDN	Various services on unique ports	See UI under System > Services > Port
PC IP (Agent)	Policy Server IP/FQDN	UDP/3870 TCP/80, TCP/443 TCP/8000	Keep Alive Update Information/Policy Windows Update
Management PC	Policy Server IP, Network Sensor IP Policy Server IP	TCP/3910 TCP/8443	SSH Console WEB Console

Note: **GENIAN Data**: It required to allow the On-Premise Policy Server to get weekly/monthly updates for the Platform Detection DB, CVE and NIC Vendors.

Cloud Managed

SRC IP	DST IP	Service	Note
Policy Server IP	3.34.24.101 Network Sensor IP, PC IP(Agent)	TCP/80, TCP/443 UDP/**UNIQUE PORT**	Platform false positive report/non-detection report KeepAlive, Send Event
Network Sensor IP	Policy Server IP/FQDN	UDP/**UNIQUE PORT** TCP/80, TCP/443	Keep Alive Update Information/Policy
PC IP (Agent)	Policy Server IP/FQDN	UDP/**UNIQUE PORT** TCP/80, TCP/443 TCP/8000	Keep Alive Update Information/Policy Windows Update
Management PC	Network Sensor IP	TCP/22	SSH Console

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 NAC

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

9.1 Installing Genian NAC

Note: All installation methods require a Genian NAC iso image. This image contains both the Policy Server and Network Sensor.

9.1.1 Choose Policy Server Deployment

Cloud-managed

A Genians Cloud deployment option is available that does not require users to manually install and manage Policy Servers. Additionally, a Private Cloud option is available through an AWS Marketplace AMI. A Network Sensor appliance is still required on your network in order to access most features of Genian NAC. Continue reading for network sensor installation instructions.

Learn more about Cloud-Managed NAC

On-Premise

In an On-Premise deployment, both the Policy Server and Network Sensor(s) are both installed on the users physical or virtual appliances.

9.1.2 Choose Appliance Installation Type

All-in-One (Policy Server + Network Sensor)

This option is for On-Premise deployments only. In a small network, a system can function as a policy server and network sensor. Sensor may be disabled if only Policy Server is desired (see next section).

Note:

All in one configuration does not support:
- High Availability

- CWP domain
All-in-One is more resource intensive, because both Policy Server and Sensor processes are performed.

Standalone Policy Server

Complete the same steps as shown in **All-in-One** configuration. After installation, disable the network sensor component.

1. Go to **System** in the top panel
2. Select the Policy Server **IP Address**
3. Click the **Sensor** tab
4. Find the **Interface** of the sensor, and select **Sensor** under **Settings**.
5. For **Sensor Mode**, select **Inactive**
6. Click **Update**

Network Sensor Only

Network Sensor only installations are used along with the Cloud-Managed Policy Server, as well as in larger distributed Networks for performance and reliability. At least two systems are required for this deployment type.

> #curl -s https://docs.genians.com/install/ztna-sensor.sh | sudo BRANCH= bash -s - POLICY-SERVER.DOMAIN or IP

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

It is recommended that the Wireless Network Adapter be installed (unavailable in virtual installation) in order for the network sensor to collect Wireless LAN information. See wireless-adapter-compatibility

Physical Machine

You can use generic intel server like HP, Dell or Mini PC for testing and small deployment. If you have any hardware comparability issue, please contact us

Minimum Hardware Requirements

- Processor: Intel or AMD Dual core
- Memory: 4GB (8GB Recommended)
- Storage: 120GB
- NIC: 1+ Wired Network Interface, Wireless Interface (Optional)

Virtual Machine

You can install Policy Server on virtual machine. We support various hypervisors like VMWare, VirtualBox, XenServer.

Configure the Virtual Machine to Run as System Type: `Linux`, Version: `Other 64-Bit`.

Note: If installing to a Virtual Machine:

- you must enable Promiscuous mode.
- 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 be detected, even if the host machine uses a wireless network interface.Genian NAC 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*
- You must set your adapter to Bridge Mode if connecting to an access port, or enable VGT mode (or equivalent settings) if connecting to a trunk port. For more info see the page below:

Configuring Trunking in Virtual Environments

If you are deploying a sensor using a hypervisor and plan to monitor multiple VLAN through a trunk port, special configuration is needed.

- Configure your physical switch port and Genian NAC as described in *Installing Genian NAC*.
- Special settings will be configured within the virtual network to allow Genian NAC to communicate with the physical trunk port.
- For all hypervisors, ensure the NIC assigned to Genian NAC supports VLANs and is placed in `promiscuous mode`.
- The virtual sensor host must be linked to the physical switch using a virtual switch.

ESXi

Different configurations are possible depending on which switching technology is being used in ESXi.

vSwitch

- On the Virtual Switch, edit the port group:
- Enable `VGT Mode`
- Set the VLAN ID to `4095`.

  This will allow traffic from all VLANs to travel through the virtual switch, between your Physical switch port and Genian NAC.

Distributed vSwitch

- Under **Home > Inventory > Networking**, **Edit Settings** for the desired dvPortGroup.
- Go to **Policies > VLAN**:
- Set VLAN type to VLAN `Trunking`
- Set range or list of VLANs.

  This will allow traffic from all specified VLANs to travel through the virtual switch, between all virtual machines and physical NICs assigned to to the vSwitch.

Hyper-V

> **Warning:** Hyper-V does not support trunk configuration in the GUI, Powershell is required.
>
> Please be warned trunking configurations will **not be visible** in the GUI after they have been configured.
>
> Because Hyper V names all interfaces "Network Adapter" by default, we strongly advise renaming, removing + recreating, or using a script to select target interface by MAC address.In the example below, we will demonstrate deleting a single interface and recreating it, before configuring trunking.
>
> These changes will result in temporary disconnection, and are best performed with the guest system is powered down.

- In Powershell, enter the following commands with the bracketed values changed to match your environment:
- List the interfaces connected to the VM:
- `Get-VMNetworkAdaptervlan -VMName [vmname]`
- Delete the existing interfaces that were output by the above command. Repeat as needed.
- `Remove-VMNetworkAdapter -VMName [vmname] -Name "[Network Adapter]"`
- Add back interfaces using the command below. Assign unique interface names if adding multiple interfaces. (Single interface recomended)
- `Add-VMNetworkadapter -VMName [vmname] -Name "[Eth0]"`
- Lastly configure the interface(s) to a trunk port. Be sure to not include the native vlan within the allowed vlan scope.
- `set-VMNetworkAdapterVlan -VMName [name] -VMNetworkAdapterName "[Eth0]"-Trunk -AllowedVlanIdList "[allowed vlans]" -NativeVlanId [native vlan]`
- Check your interfaces
- – `Get-VMNetworkAdaptervlan -VMName [vmname]`

Real world syntax examples:

- `Get-VMNetworkAdaptervlan -VMName GenianNAC`
- `Remove-VMNetworkAdapter -VMName GenianNAC -Name "Network Adapter"`
- `Add-VMNetworkadapter -VMName GenianNAC -Name "Eth0"`

- `set-VMNetworkAdapterVlan -VMName GenianNAC -VMNetworkAdapterName "Eth0"-Trunk -AllowedVlanIdList "10,20,30" -NativeVlanId 1`
- `Get-VMNetworkAdaptervlan -VMName GenianNAC`

Citrix Hypervisor (Xenserver)

- In the host Network Tab in Xencenter:
- Add an `external network` for each VLAN, and assign each entry to the NIC that is connected to the switch trunk port.

For more information about hardware requirements, See *Sizing Software and Hardware*.

9.1.3 Prepare Network Connection

Genian NAC requires a network connection with at least one static IP address for management. If you are installing in an All-in-One configuration, you can use the management interface with an interface for network sensors.

Genian NAC needs to monitor network broadcast packets (ARP, DHCP, uPNP...), **it must be connected to all the segments (broadcast domains)** that you want to manage.

If you have a switch configured with VLANs, you can set up an 802.1Q trunk port to monitor multiple networks with one physical interface.

If you are installing Genian NAC in a virtual environment, the VM (Sensor) must have direct communication to and from all segments you wish to monitor and control. This may be accomplished in a variety of ways depending on your available hardware, and the capabilities of your virtualization platform.

Access Port

No additional configuration is required to monitor a single network over a switch access port. If you are installing to a machine with more than one NIC, you can still monitor multiple LANs, or VLANs through access ports.

Trunk Port

To monitor multiple VLANs on a single interface, your switch port must be set to trunk mode with 802.1Q encapsulation. 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
```

9.1.4 Download Software

Download the Policy Server ISO file from the download page and create a CD-ROM or bootable USB for **physical machine** installation

Create a Bootable USB Drive

> **Caution:** All files in the USB drive will be deleted during the process so back up your files from the USB Drive to move forward.

To install Genian NAC Policy Server to a physical machine, first create a USB drive using UNETbootin.

Getting UNETbootin

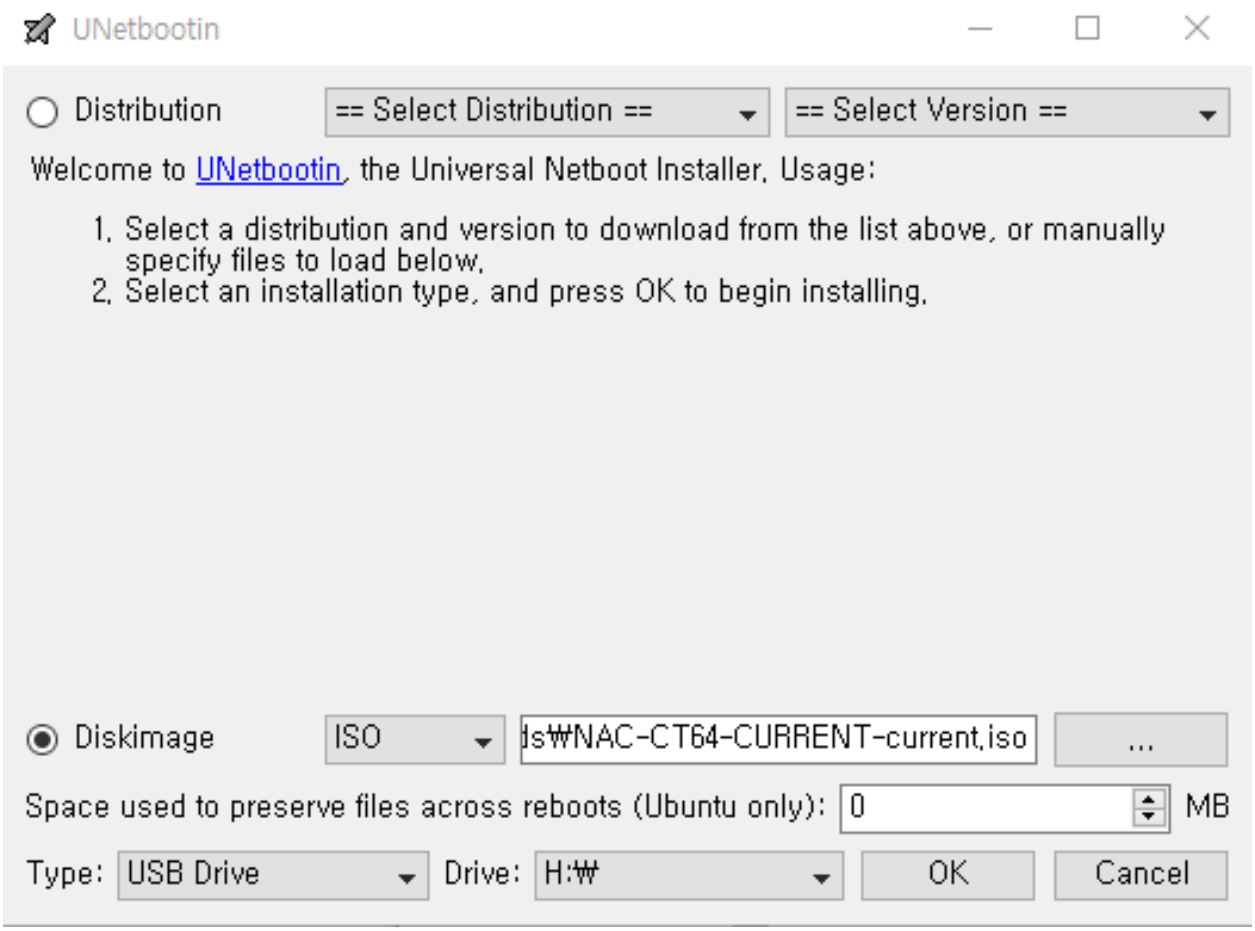
Genians recommends UNETbootin which allows you to create a USB flash drives for Genian NAC installation without burning a CD. Choose your Operating System to download UNETbootin.

Create a USB Drive

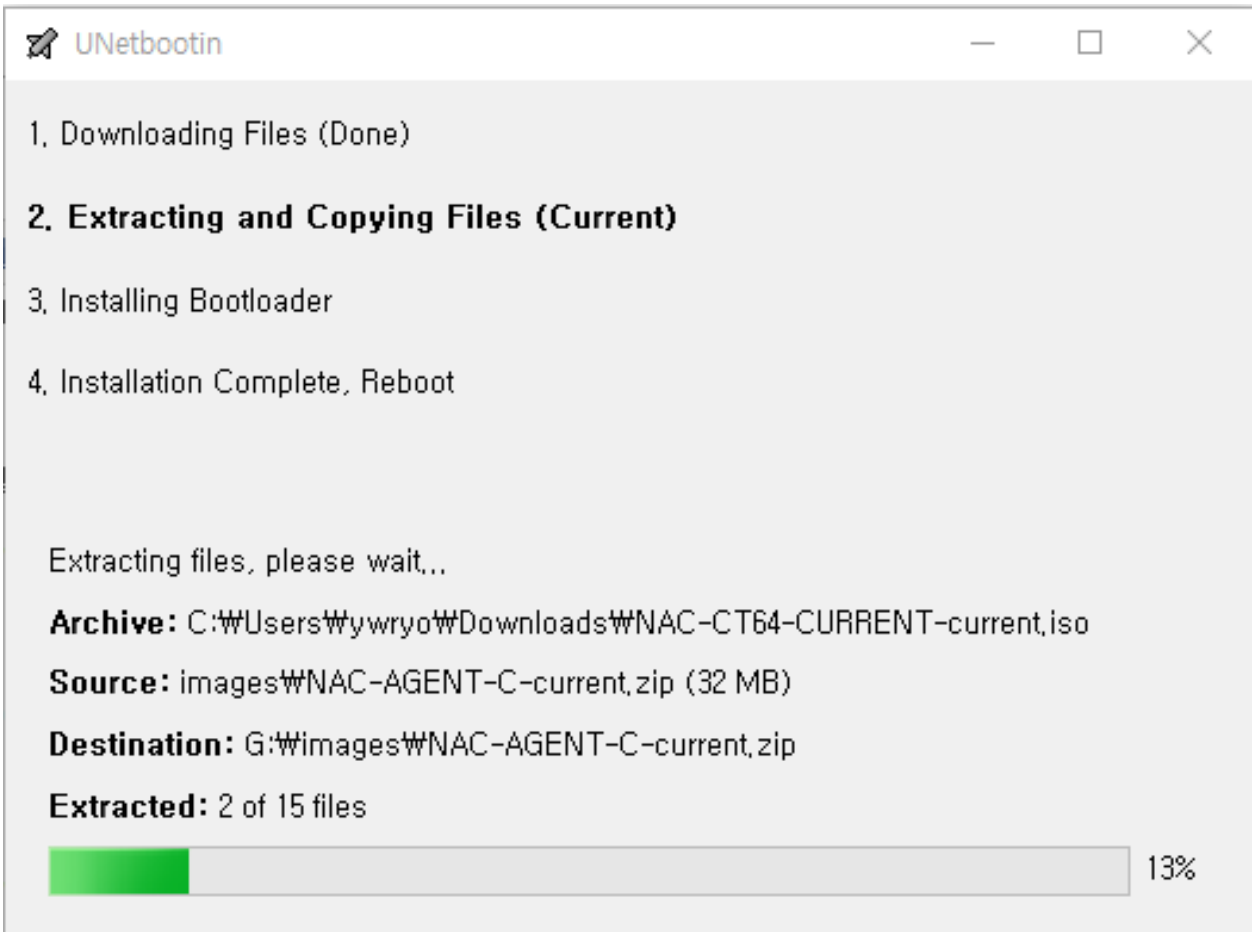
Ensure that your USB drive is formated FAT32. Other file systems may not be supported.

Once UNETbootin is installed, follow the steps below.

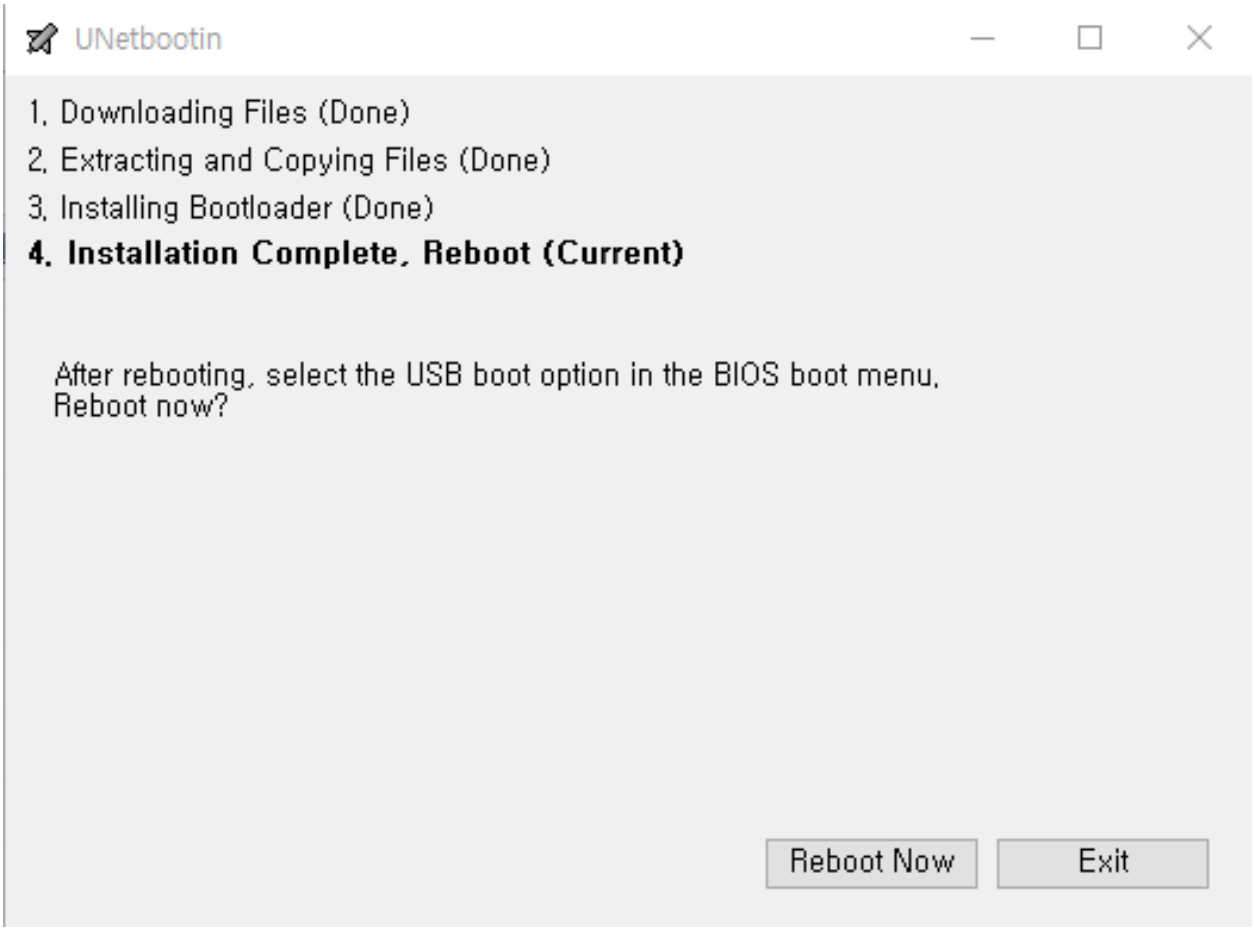
1. Load the Disk image



2. Click OK and move on.


UNetbootin
1. Downloading Files (Done)
2. Extracting and Copying Files (Current)
3. Installing Bootloader
4. Installation Complete, Reboot
Extracting files, please wait...
Archive: C:₩Users₩ywryo₩Downloads₩NAC-CT64-CURRENT-current.iso
Source: images₩NAC-AGENT-C-current.zip (32 MB)
Destination: G:₩images₩NAC-AGENT-C-current.zip
Extracted: 2 of 15 files
13%

3. Click Exit



Now, you have the USB drive to install Genian NAC into your desired machine. Congrats!

Troubleshooting

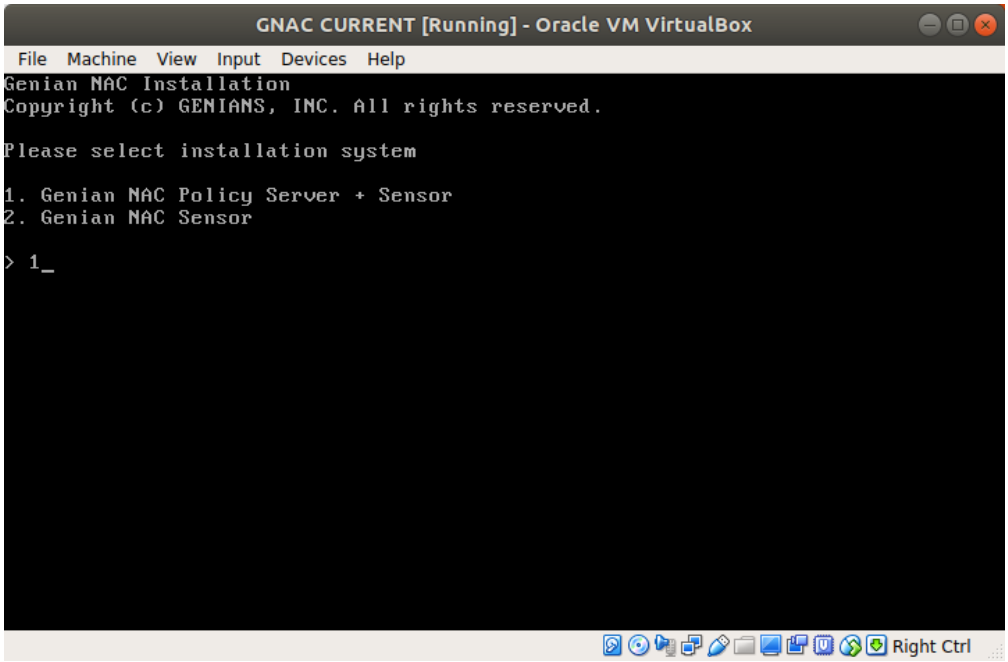
- Error message: "BOOTMGR is missing" indicative of improperly formatted USB drive.

Note: The Genian NAC installation contains the linux operating system. You do not need to install a separate OS.

9.1.5 Installing Genian NAC

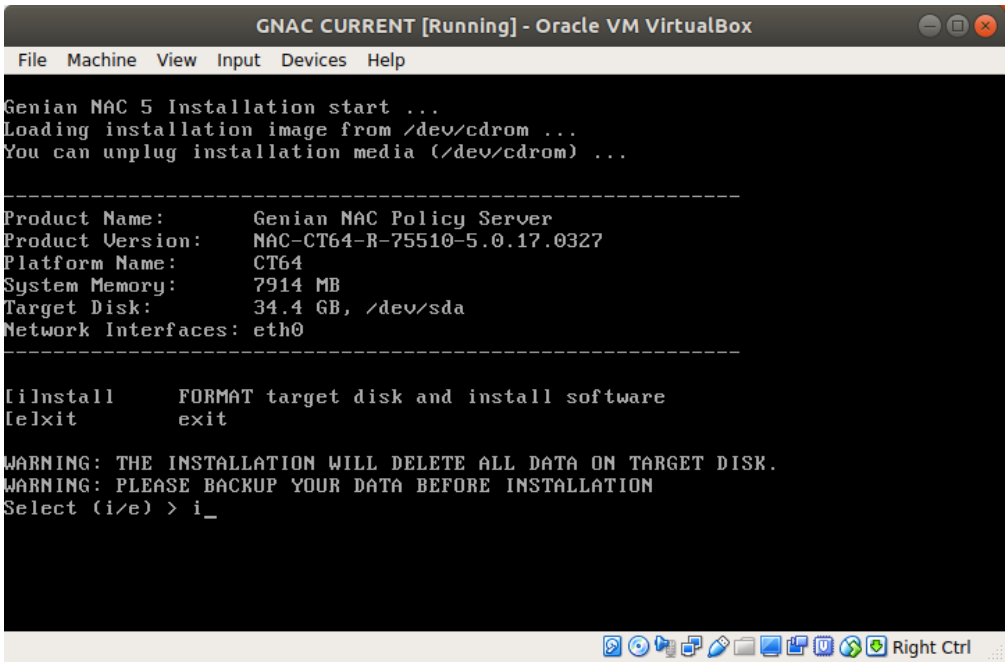
Follow these steps to install a Policy Server, Sensor, or combined system on a device.

1. Boot up your machine
   - Insert the CD-ROM or bootable USB flash drive into your physical machine
   - Change the boot sequence to boot from the CD-ROM or USB drive
   - On virtual machine, select ISO file for installation media.
2. Type “1” for **Genian NAC Policy Server + Sensor** (or type "2" for install additional network sensor)

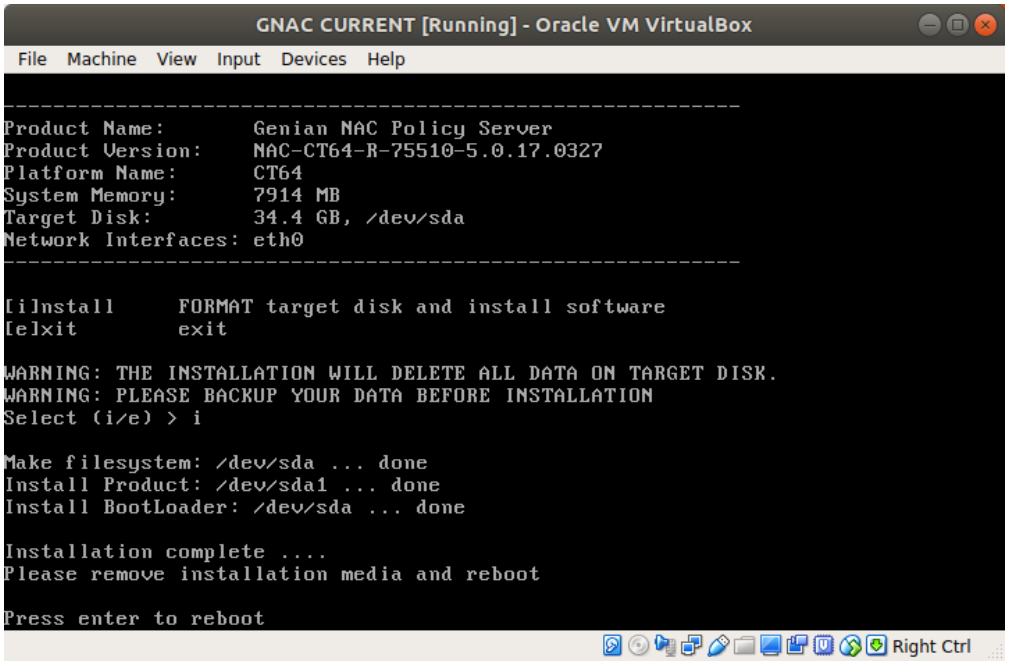


Warning: This will erase all files on the target disk. Data lost will not be recoverable.

3. Type "i" to proceed



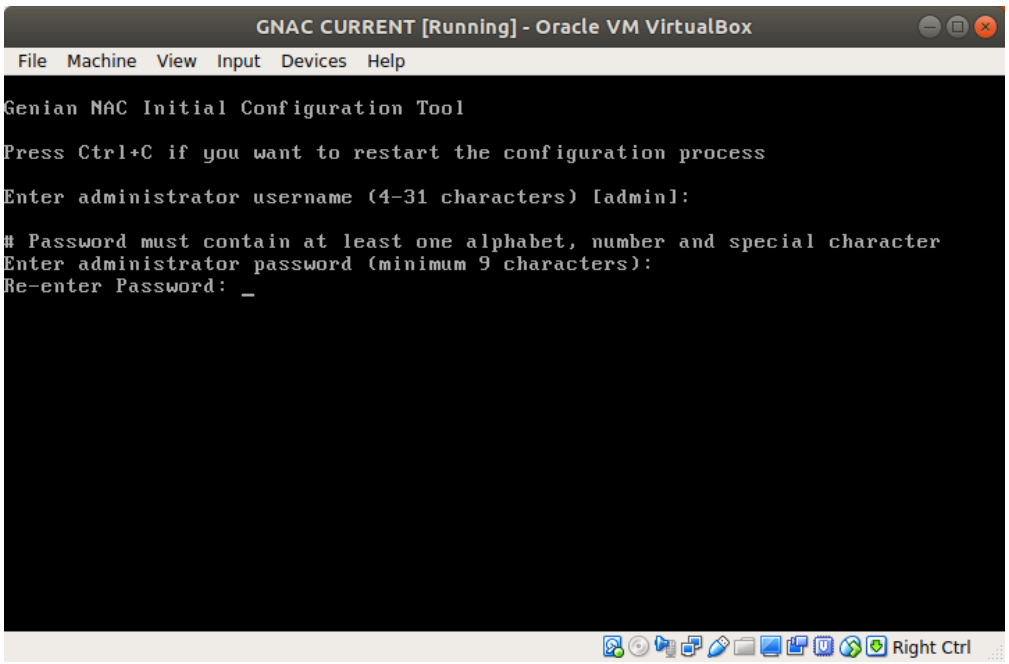
4. Reboot your system
   - Remove the installation media (*e.g. USB*)
   - Press Enter to reboot



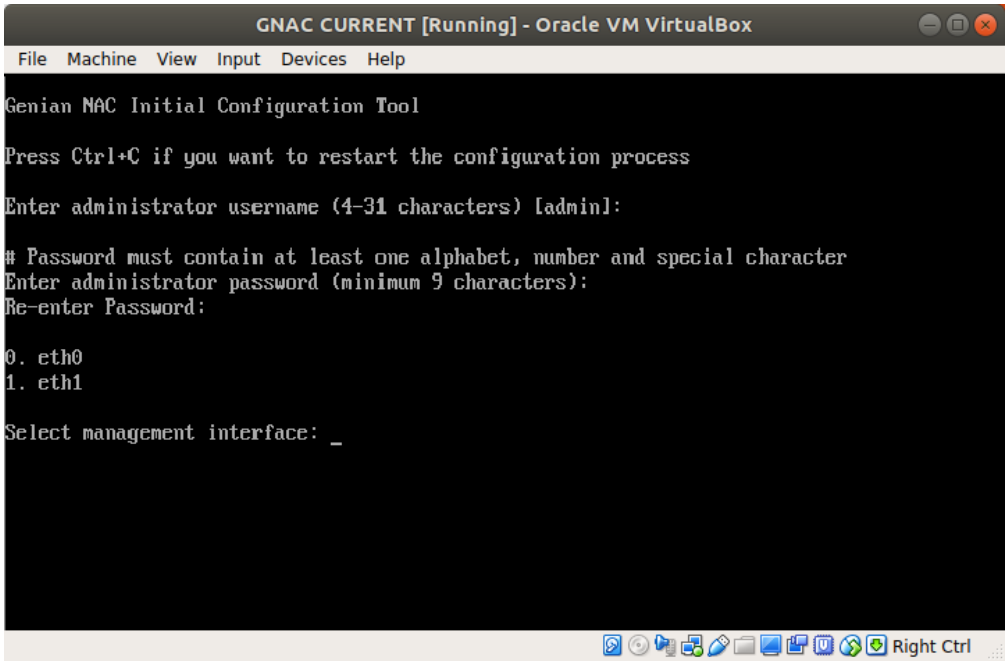
9.1.6 Initial Configuration

After the system reboots, you need to do the initial setup.

1. Create admin account for Web UI and SSH connection
   - Enter superadmin account name. (default is *admin*)
   - Enter superadmin password



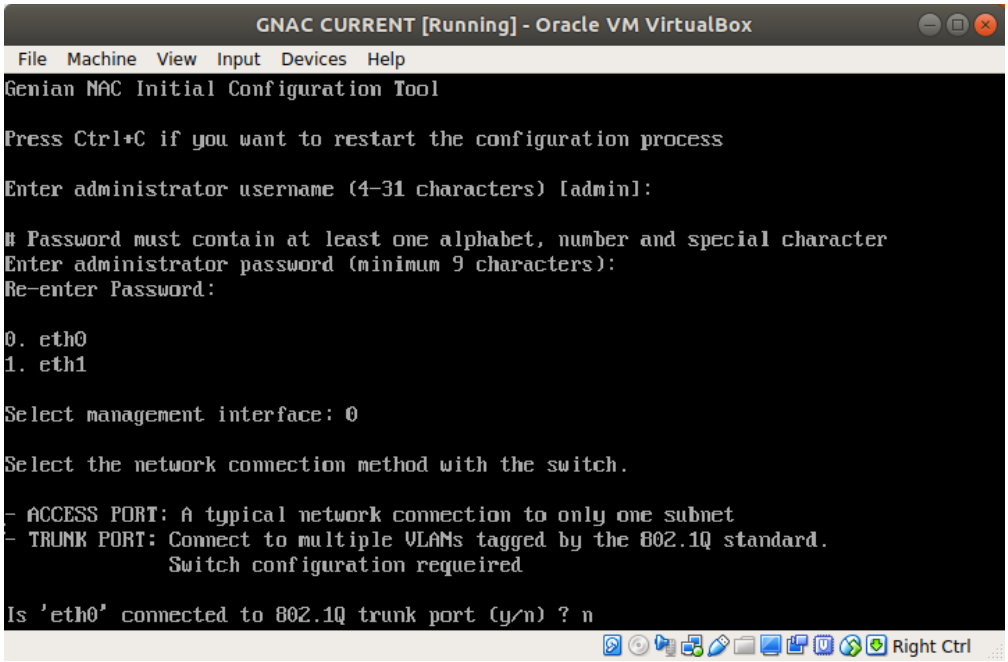
2. Select interface & connection type



Note:

Please make sure that the network connection is connected to the first interface (eth0) of the system.

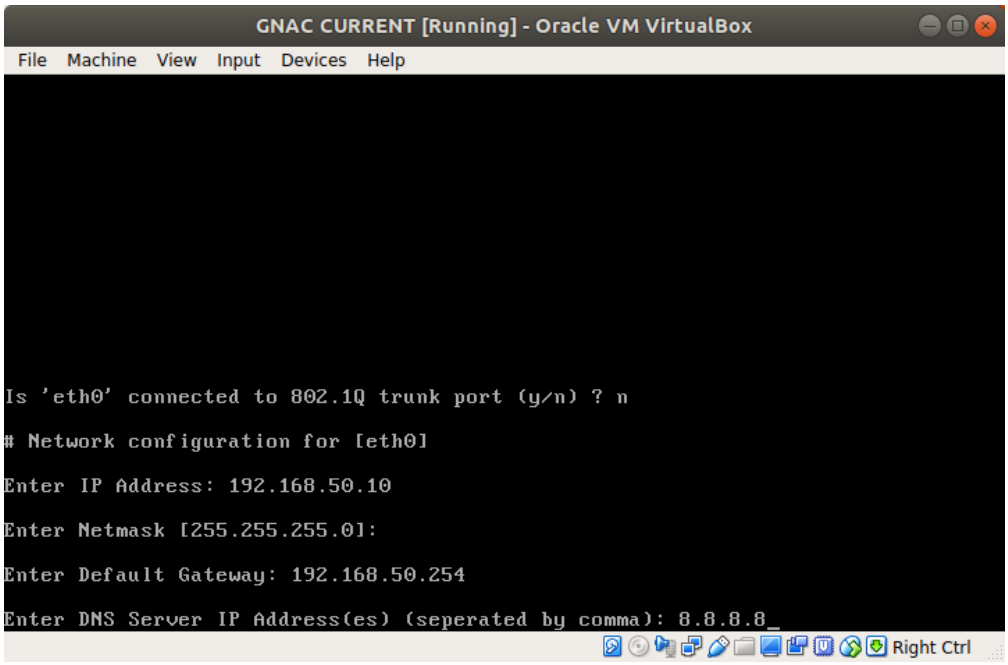
- In case the interface eth0 is connected **access port** (regular port)
  - Type "n"
- In case the interface eth0 is connected to 802.1Q **trunk port**
  - Type "y"
  - Enter VLAN IDs for activate NAC service (*Concatenated by comma or A-B for range. e.g: 10,20-30*)
  - Enter VLAN ID for management interface
  - Select Y / N to set VLAN Sensor interfaces as DHCP Clients.
  - To define static IP's for VLAN interfaces after the initial installation, see: *Configuring Interface IP Addresses*.



3. Network configuration

   This step is to set the interface IP address for management.

   - Enter IP address
   - Enter netmask
   - Enter default gateway
   - Enter DNS IP addresses (*Concatenated by comma*)



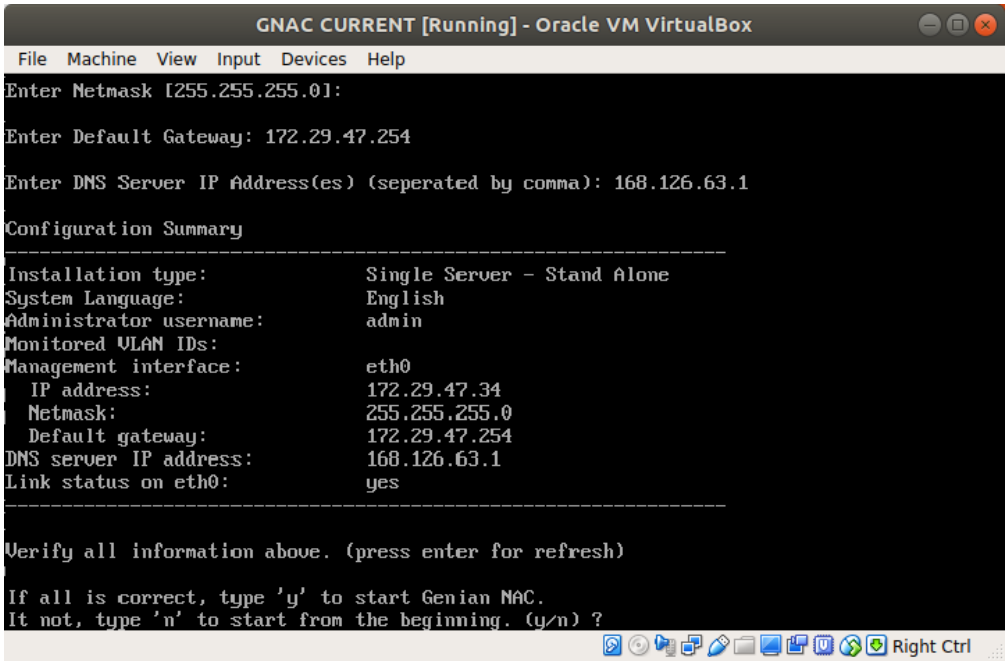
4. Enter Policy Server IP or FQDN.

Note:

This step appears only if you selected Network Sensor during ISO installation step 2.

- IP Address (e.g. 192.168.50.10)
- Cloud Site Name (e.g. *sitename*.genians.net)

5. Verify all information
   - Everythings correct. Type “y” to start
   - Something wrong. Type "n" to restart configuration



6. Login to Genian NAC management UI on the Policy Server. See *Administration Console*

Important: Review **Firewall Requirements** in *Preparing Network* to ensure that communications between the Policy Server and Sensors/Agents is allowed.

9.1.7 Unsupported Hardware

If you find any device driver unsupported problems. please report to us.

Note: If the storage device or network interface is not recognized when installing the virtual machine, please change the storage type to SATA or change the network interface driver to Intel series such as E1000.

Reporting unsupported hardware

If you have unsupported hardware, such as storage devices, Ethernet adapters, or wireless LAN adapters, during the Genian NAC 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

9.2 Administration Console

Genian NAC 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.

9.2.1 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/)
```

9.2.2 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 NAC 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*

9.3 Installing License

When Genian NAC 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

9.3.1 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**

9.3.2 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*)

9.3.3 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**

9.4 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.

9.4.1 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*
- *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 NAC 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 NAC 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

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*

9.4.2 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*

9.4.3 Installing Linux agent

Installing the Linux Agent over CWP

There are several ways to install agents in Genian NAC.

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 installation script in the download directory as follows:**
    - cd ~/Download
    - chmod 755 lnxagent_*Serveraddress*.sh
    - sudo ./lnxagent_*Serveraddress*.sh
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 installation script may vary.
- The installer cannot run if the user does not have permission to install the file, so it must be run as an administrator. The process will automatically run when the script ends.
- This Script 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.

Find agent logs on Linux

- **Open Terminal in your Linux distribution to view the log files below.**
    - Installation path: /usr/local/Geni
    - Log path: /var/log/genians
    - Setup file path: /usr/share/genias/GenianDB
    - PID file path: /var/run/genians

Installation Specifications

Disk	Memory
20~30MB	20~30MB

Linux Agent Supported OS List

See: *Supported Operating Systems and Plugins*

9.4.4 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 NAC 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

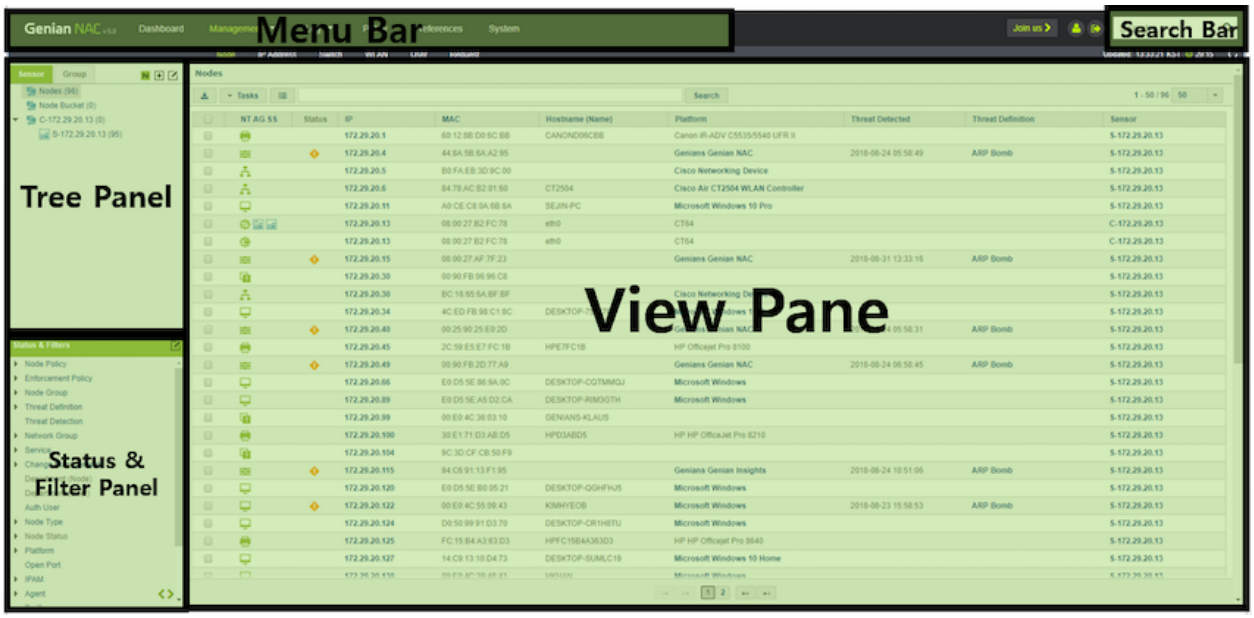
Genian NAC collects information of various network assets through network sensors and agents and provides real time visibility to network and endpoints including:

- 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.



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 NAC, 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 NAC log collection method*
- *Genian NAC 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 NAC 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 NAC 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 NAC 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 /system/gathering-options

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 NAC 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 NAC can identify the IT devices in the network and show their CVEs to make network management easier.

How to Detect Device Platform

Genian NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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. For **Status**, **Enabled**
5. 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*)

6. Click **Add**
7. Click **Save**
8. 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**

Import / Export Node Group in JSON Format

Genian NAC 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 NAC 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, 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)

10.3 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 NAC 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 NAC 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 SNMP-WALK.

---

1. Login to your **Switch** and verify it's SNMP Community strings
2. Verify **Genian NAC** 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**.

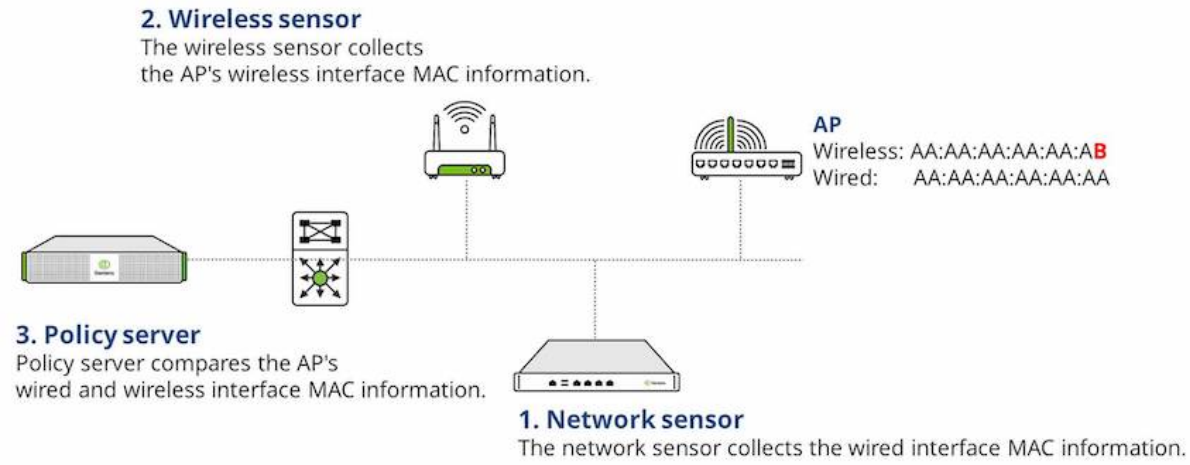
Show Internal SSIDs

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

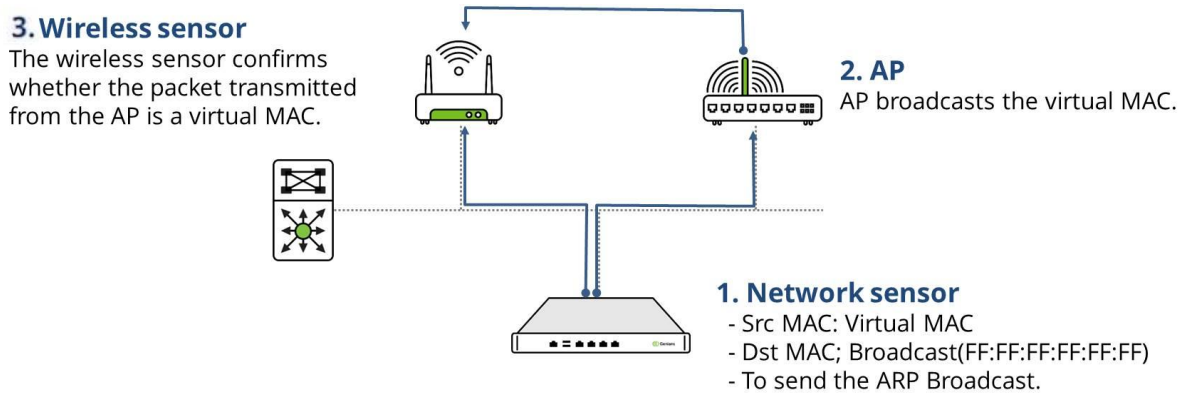
The AP detected by the Genian NAC Agent and the wireless sensor can be distinguished as an internally connected AP by several criteria. The Internal AP detection method is as follows:

MAC Similarity Check



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



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 NAC 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 **Dashboard** in the top panel.
2. Click **Tools > Create Dashboard**.
3. Find **Name** in Create Dashboard window. Enter in Unique Name.
4. Set **Share** to **ON** or **Off** to make the dashboard available to other Administrators.
5. Select **Type**, and **Layout** in Create Dashboard window.
6. Click **Save**.

10.6.2 Edit Dashboards

1. Click **Dashboard** in the top panel.
2. Select the **Dashboard** you wish to edit.
3. Click **Tools > Edit Dashboard**.
4. Find **Name** in Create Dashboard window. Enter in Unique Name.
5. Set **Share** to **ON** or **Off** to make the dashboard available to other Administrators.
6. Select **Type**, and **Layout** in Create Dashboard window.
7. Click **Save**.

10.6.3 Import Dashboards

1. Click **Dashboard** in the top panel.
2. Click **Tools > Import Dashboard**.
3. Move the desired **Dashboards** into the selected column.
4. Click **Save**.

10.6.4 Remove Dashboards

1. Click **Dashboard** in the top panel.
2. Click desired **Dashboard** tab.
3. Go to **Tools > Delete Dashboard**.
4. Click **Ok**.

10.6.5 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**.

10.6.6 Arrange Widgets

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

10.6.7 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.

10.6.8 Creating a Custom widget

The widget that is generated based on code is set based on HTML Code values. Enter a page source created in HTML to allow the page to act as a widget.

1. Go to **Dashboard** in the top panel.
2. Click `Tools` > Add Widget.
3. In the Add Widgets window, browse to the Custom widget category item.
4. In the Add Widgets window, click the `Create` button at the bottom.
5. In the Add Widgets window, select the Classification item as **Content**.
6. Make the following widget settings:

- Title
- Description
- Image URL(Option)
- Content

```
<html>
<body>Hello, world!</body>
</html>
```

7. Click the `Save` button.

10.6.9 Creating a URL-based custom widget

Sets the widget based on the Uniform Resource Locator (URL) value. Enter the URL you want to represent as a widget to bring up and display the page as a widget.

1. Go to **Dashboard** in the top panel.
2. Click `Tools` > Add Widget.
3. In the Add Widgets window, browse to the Custom widget category item.
4. In the Add Widgets window, click the `Create`` button at the bottom.
5. In the Add Widgets window, select the Classification item as **Content**.
6. Make the following widget settings:
   - Title
   - Description
   - Image URL(Option)
   - Content

```
https://www.genians.com
```

7. Click the `Save` button.

10.6.10 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 **Ok**.

10.6.11 Creating a Sensor Map

To monitor and customize Sensor Placement globally using Google Maps.

1. Go to **Dashboard** in the top panel.
2. Click **Tools > Create Dashboard**.
3. Find **Name** in Create Dashboard window. Enter in **Unique Name**.
4. Find **Type** in Create Dashboard window. Select **Sensor Map**.
5. Click **Sensor Map** tab that was just created.
6. Find **Settings Icon** in the right corner. Click **Assign Node Group**.
7. Find **Node Group** in Node Group window. Double-click Node Group to add.
8. Click **Save**.

10.6.12 Place a Sensor on Sensor Map

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

10.6.13 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** and select the format

10.6.14 Creating Custom Widget

Administrators can customize widgets and add them to the dashboard. Genian NAC provides Content and Link features for custom widgets. Administrators can personalize widgets by using an HTML page and URL and monitor the external Web pages.

Creating Custom Widget by HTML Code

Genian NAC provides Content features for create custom widgets using HTML code.

1. Go to **Dashboard** in the top panel.
2. Click **Tools > Create Dashboard**.
3. Find **Custom** in Categories list.
4. Click **create** button on the bottom.
5. Choose **Content** button.

6. Enter widget name on **Title**.
7. Enter a description on **Description**.
8. Uplaod image on **Image URL** (optional).
9. Enter Height on **Height** (optional).
10. Insert Html source code on **Content**.

```
<html>
<body>Hello, world!</body>
</html>
```

11. Click **Save**.

Creating Custom Widget by URL

Genian NAC provides Link features for create custom widgets using URL(Uniform Resource Locator).

1. Go to **Dashboard** in the top panel.
2. Click **Tools > Create Dashboard**.
3. Find **Custom** in Categories list.
4. Click **create** button on the bottom.
5. Choose **Link** button.
6. Enter widget name on **Title**.
7. Enter a description on **Description**.
8. Uplaod image on **Image URL** (optional).
9. Enter Height on **Height** (optional).
10. Insert URL on **URL**.
11. Insert URL Parameter on **Parameter**

```
https://www.genians.com
```

12. Click **Save**.

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 Criteria, Value Font Size, Lable Font Size, Time Graph, Name, Update Interval, Height.
8. Click **Save**.

10.7 Genian NAC Monitor(for Mobile)

Genian NAC can check the status on Mobile through **Genian NAC 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 NAC 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 NAC monitor" app on mobile device (Android and IOS support)

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 NAC 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 NAC, 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 Policies** are mainly used for collecting information from Nodes, **Enforcement Policies** are typically used to block the endpoint from accessing the network and potentially take additional action. This additional action may involve redirection to a **Captive Web Portal** for compliance instructions, or control of the endpoint through an agent.

Once **Node Groups** are created, (*Managing Node Groups*) controls can be defined by creating **Enforcement Policies**. These policies can then be applied to the **Node Group** to enforce those conditions upon the Nodes within the Group.

Creating Permissions

Understanding Permissions

Permissions allow you to define Node Access based off of a combination of Network, Service, and Time 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 and Time 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.

(*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 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, and Time 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 Troubleshooting

- *Genian NAC log collection method*
- *Genian NAC diagnosis Method*
- *Running Genian Agent is not Detected in WebUI*
- *Agent is Installed but not Running*
- *A problem in which the node is assigned the wrong policy due to platform false positives*
- *Compliant Node is Blocked*

11.2 Policy Enforcement Methods

You need a way to control devices that violate network policies defined by your organization. Genian NAC 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.

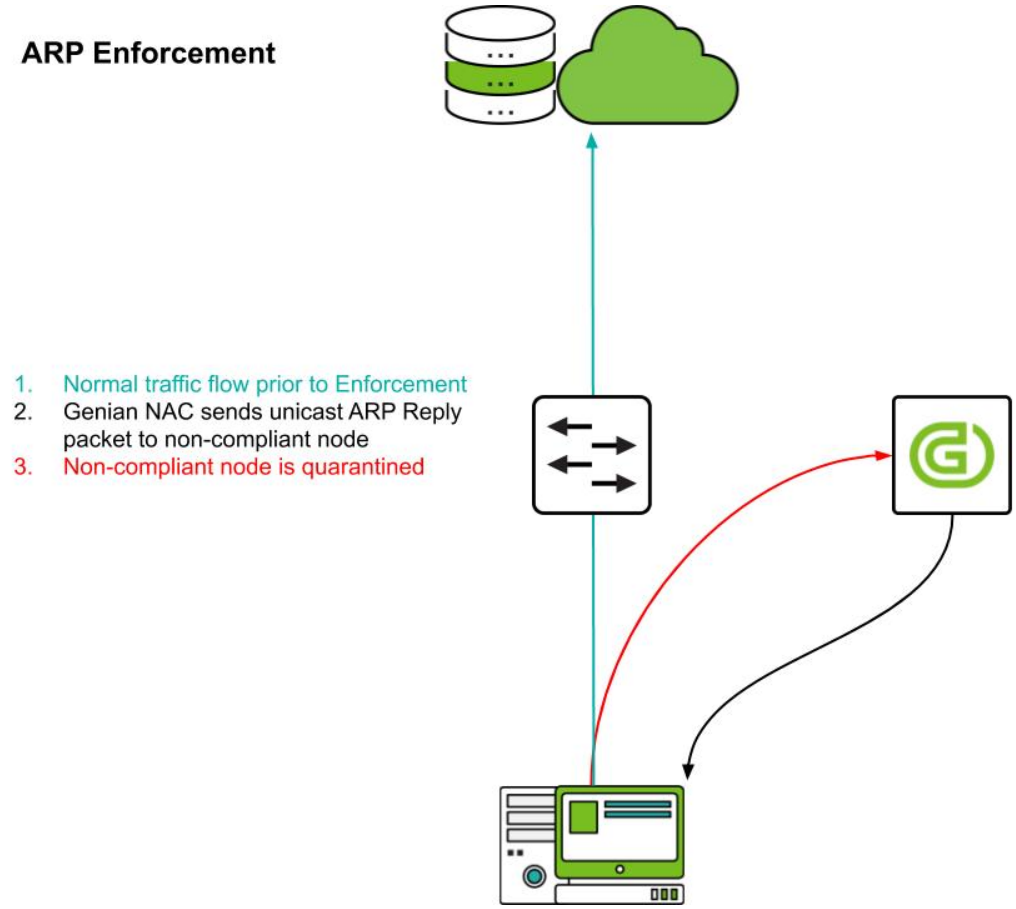
Another option is to use network access control with ARP Enforcement. ARP Enforcement uses the characteristics of the ARP protocol to perform access control. The device conducting the enforcement impersonates other network endpoints in order to intercept traffic.

Genian NAC 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.

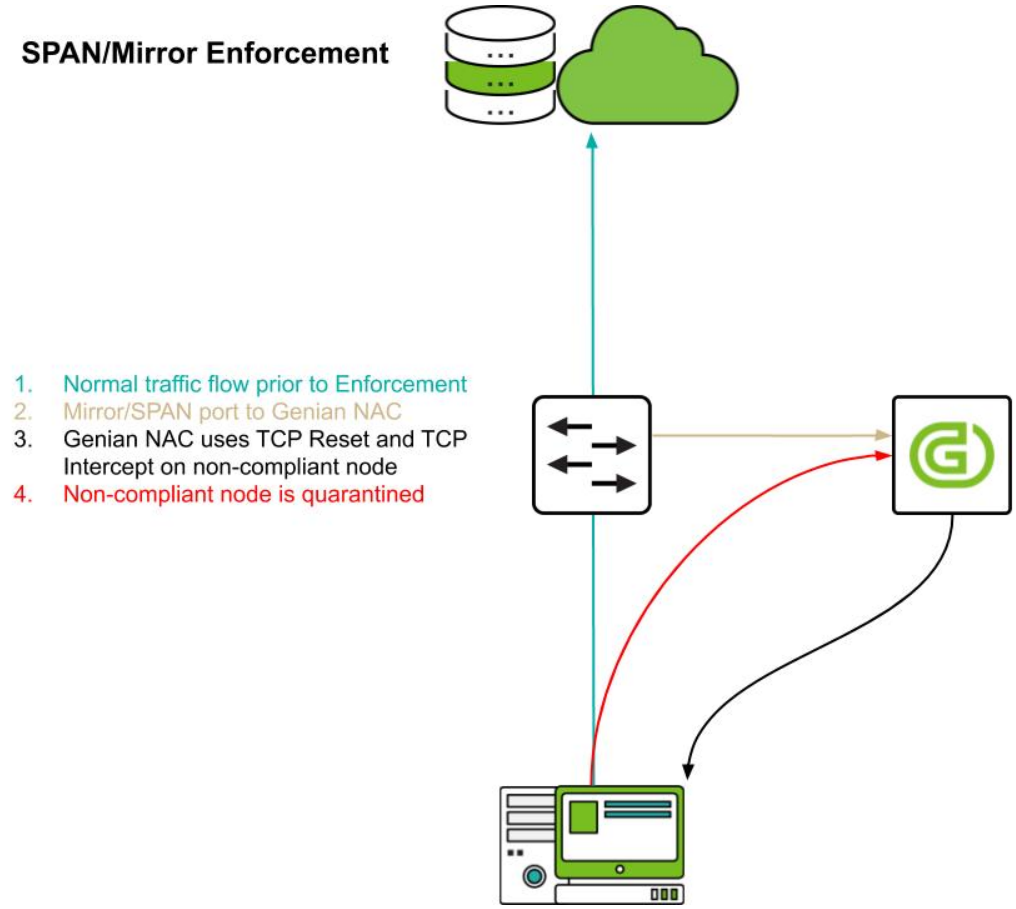
Genian NAC has a built-in RADIUS server for 802.1x and ARP Enforcement via network sensor, so users can select the option best for their network environment.



11.2.2 Port Mirroring (SPAN)

Genian NAC 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 NAC using a Port Mirroring supported switch or a Network TAP device.



Genian NAC 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.

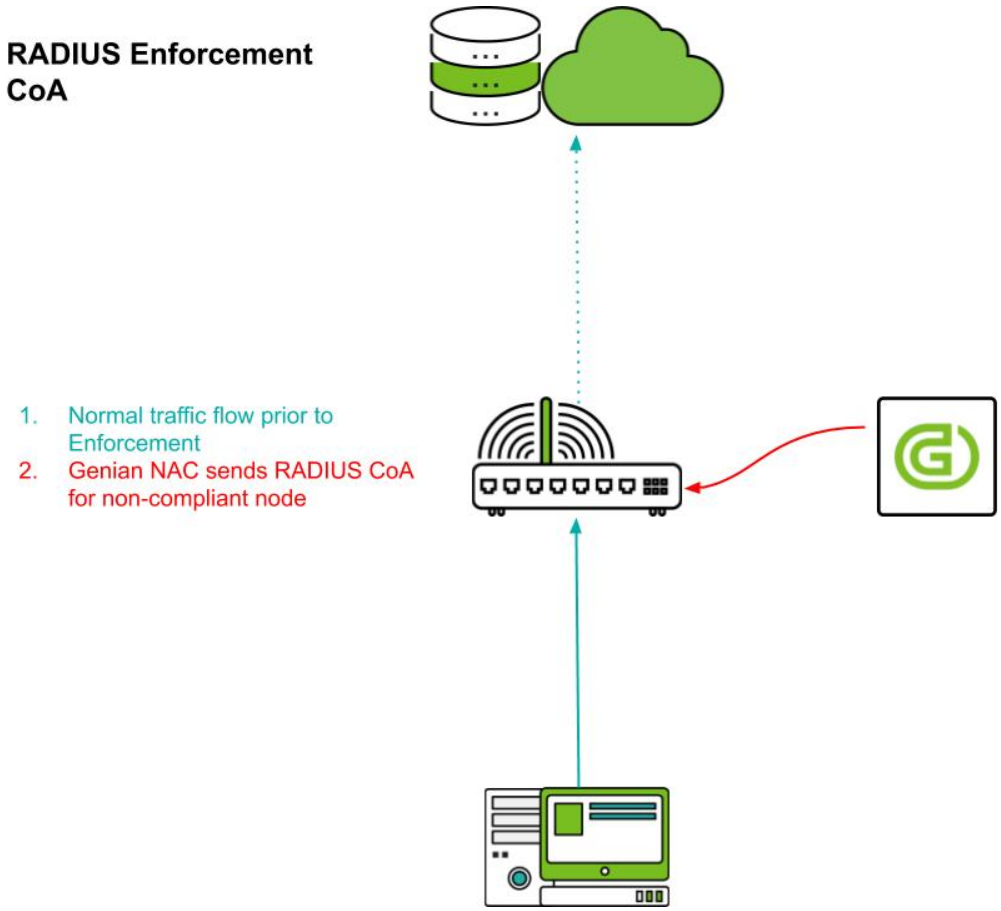
This requires a user device that supports 802.1x, a network access device such as an 802.1x-capable access point or switch, and a RADIUS server. Genian NAC provides a built-in RADIUS server and provides the following access control functions.

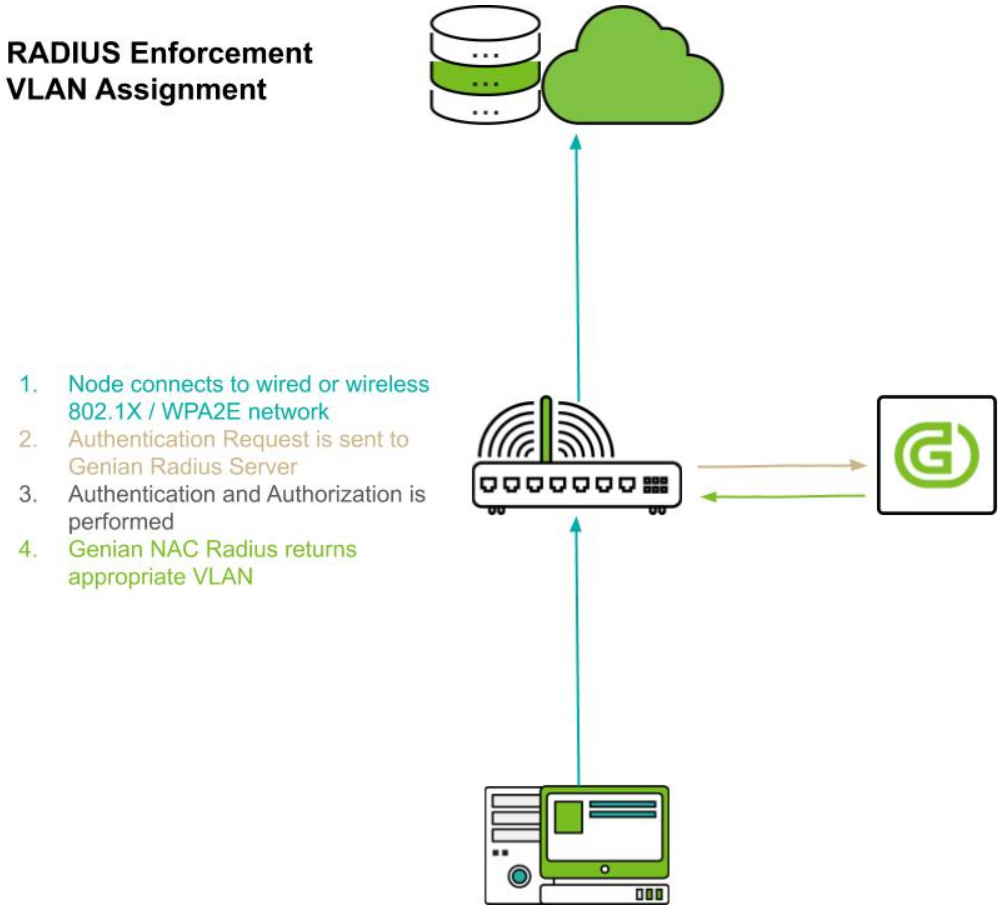
User Authentication

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.



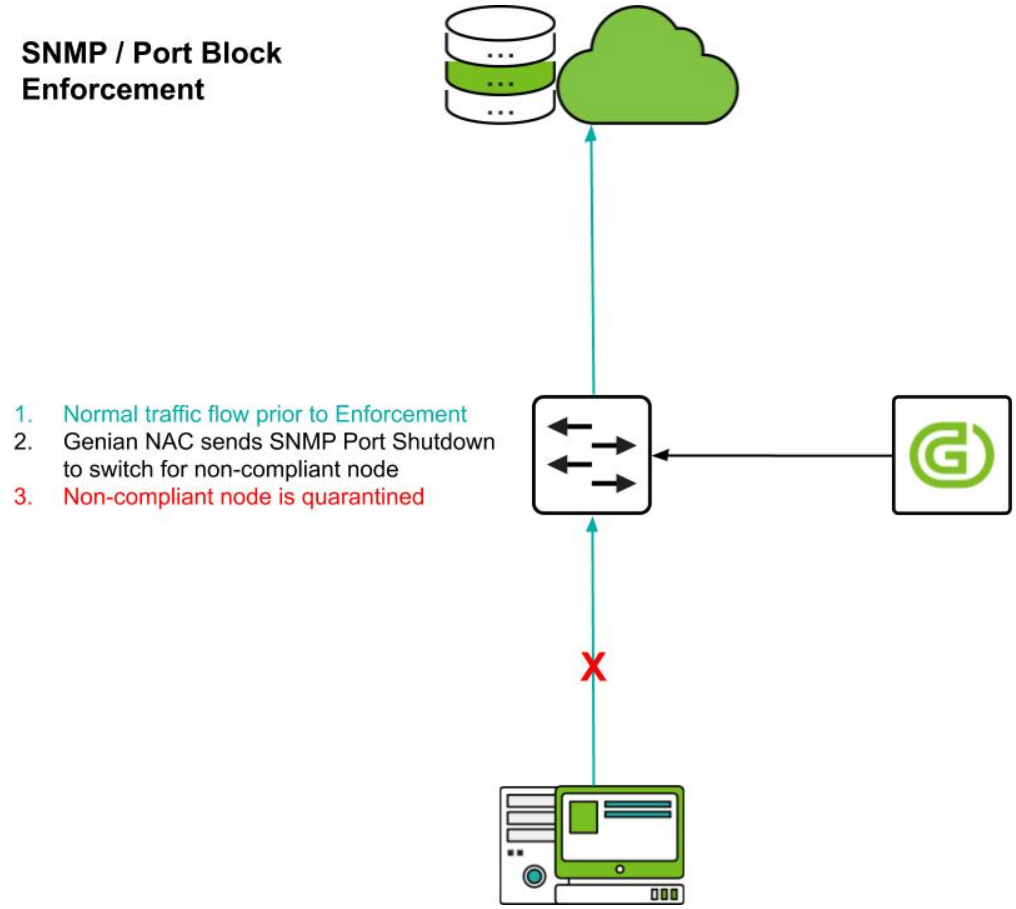


11.2.4 DHCP

Genian NAC 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 NAC 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.

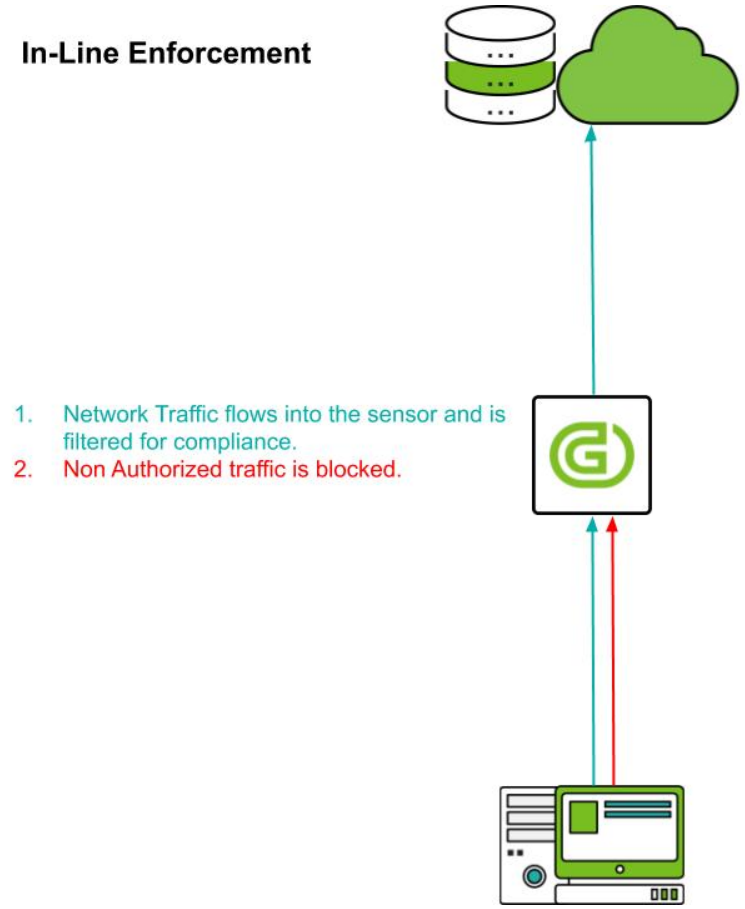


11.2.6 Inline packet filtering

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.

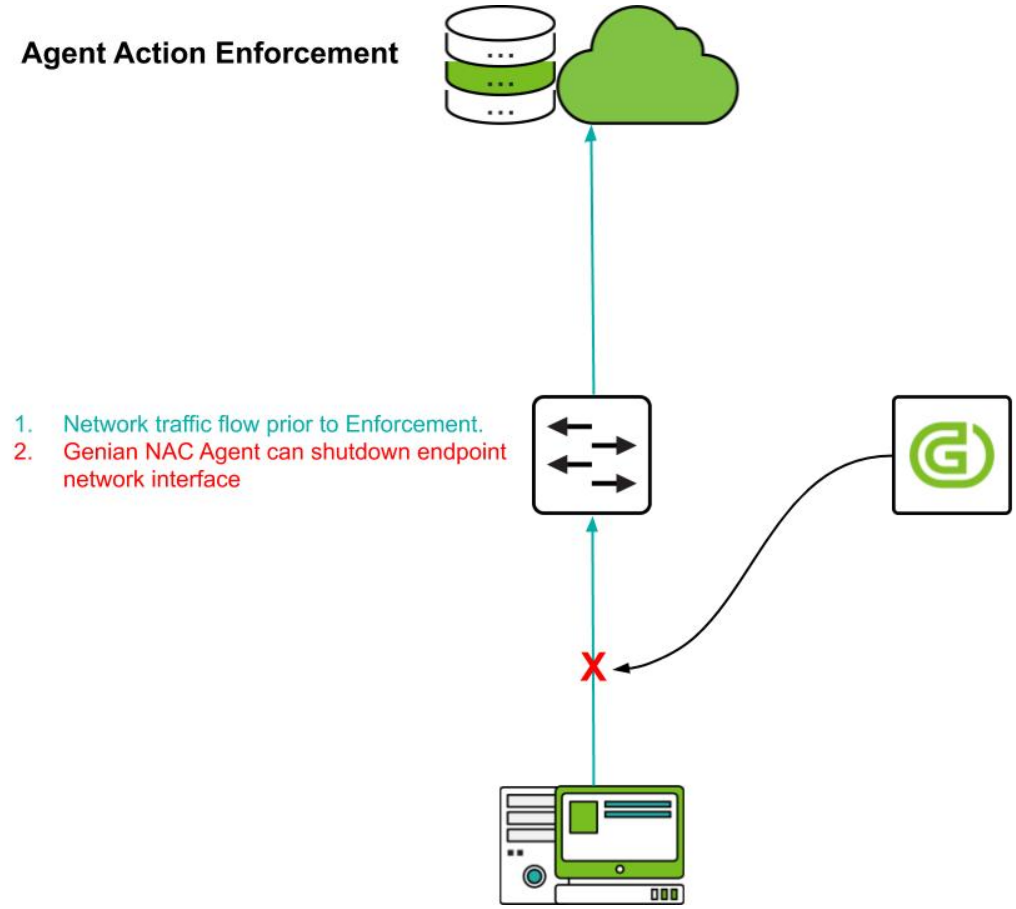


11.2.7 Agent Action

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.



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 NAC 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 NAC 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 NAC 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 NAC 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 NAC RADIUS Server supports authorization in the form of initial VLAN assignment. Additional access controls are available with Genian NAC 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 NAC 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.

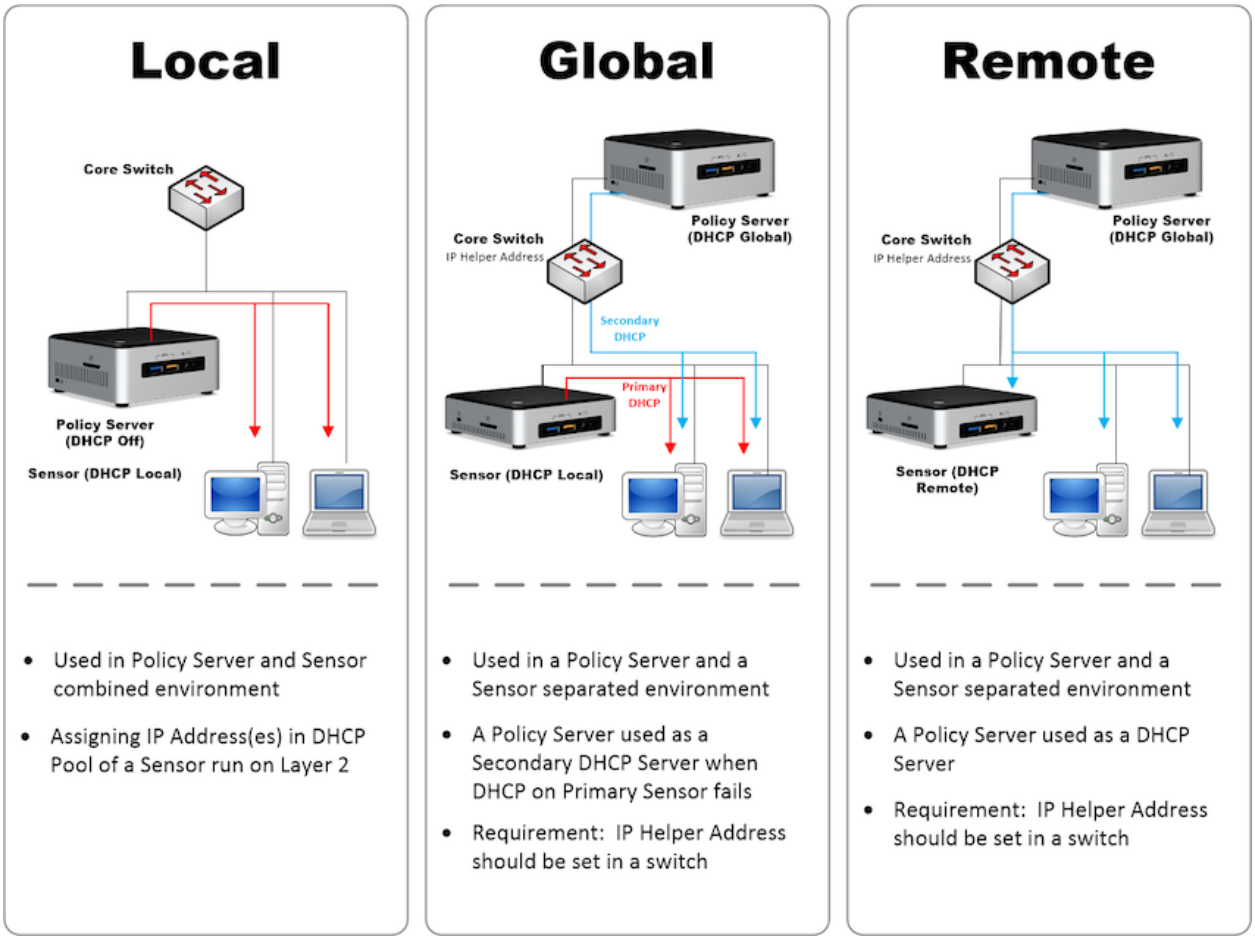
1. Go to **Policy** in the top panel.
2. Go to **Policy > Enforcement Policy** in the left panel.
3. Click name of enforcement policy to disconnect connection.
4. Under **Enforcement Options > RADIUS Control**.
5. For **RADIUS CoA**, select **On**.
6. For **CoA Commands**, select **Terminate Session** 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**)



11.6.1 Configuring DHCP Services

- dhcp-networks-sensor

11.6.2 Assign fixed IPs to devices

Genian NAC 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 NAC 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 Integrating External Systems

Note: This feature requires Enterprise Edition

Genan NAC can integrate with a variety of security vendors to establish security intelligence.

11.9.1 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 NAC 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 NAC engineers and enterprise operators can send information of user authentication to PAN firewall.

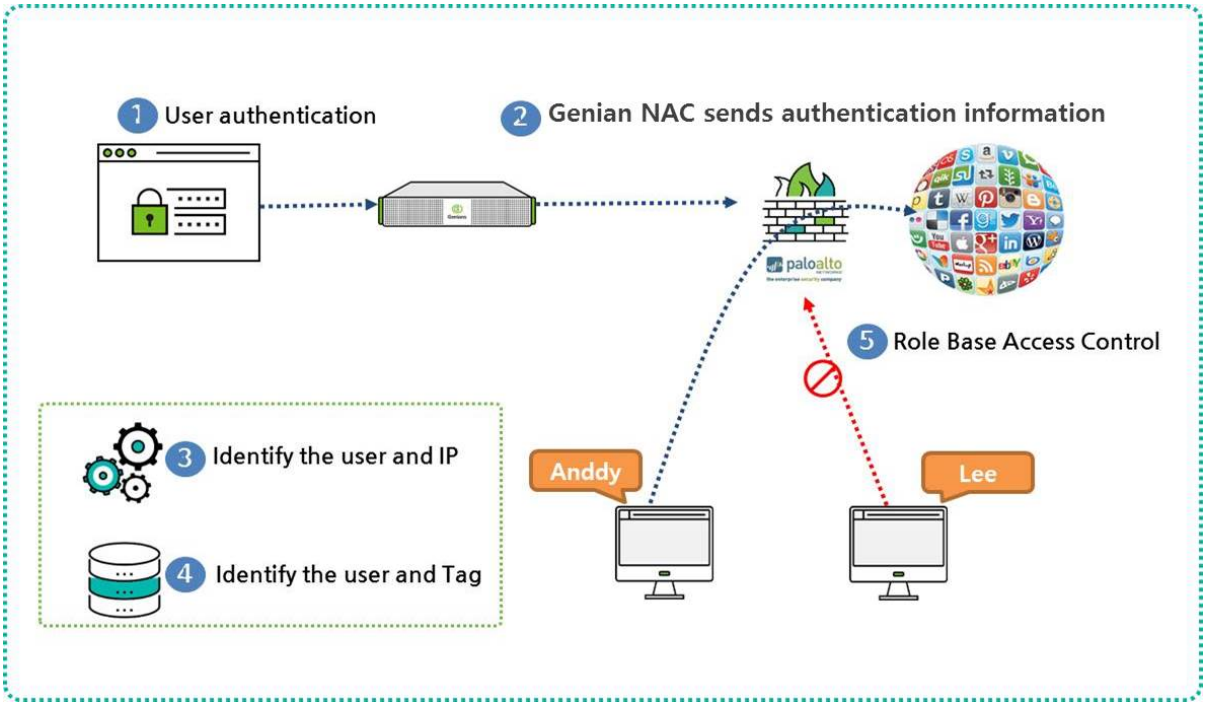
PAN Firewall generally requires that when a user changes a department or location, the IP information changes and the assigned permissions are modified accordingly. IP-based firewall policies do not know who is using an IP, but they can work with Genian NAC to get user information about an IP.

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 NAC using PAN Firewall

Genian NAC provides the integration of authentication. The PAN firewall refers to the IP and user authentication information provided by Genian NAC, and performs USER-ID mapping to enable access control by user role in the PAN Firewall.

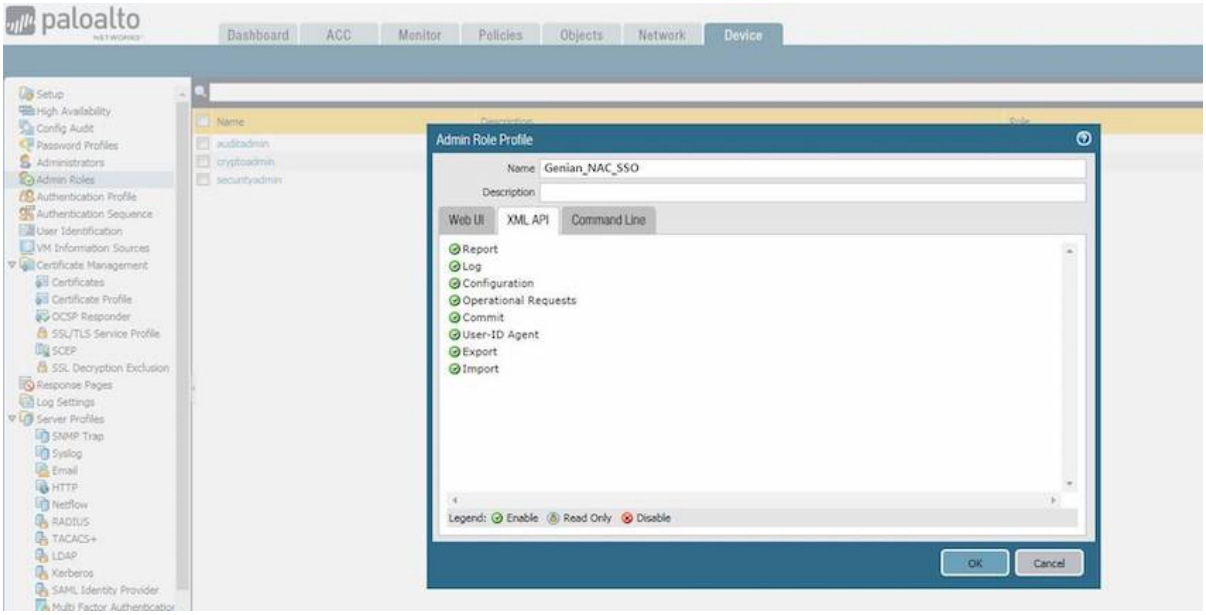


The authentication process is described below:

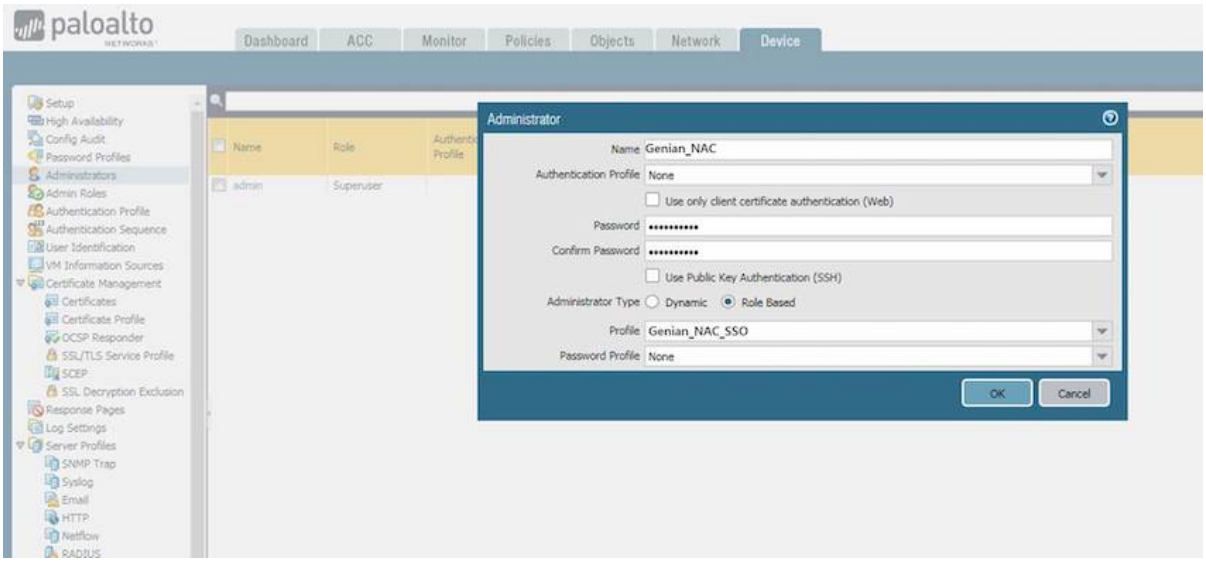
1. User Authentication in Genian NAC
2. Genian NAC sends authentication user and IP information to PAN firewall
3. The PAN firewall compares the authentication user and IP information it receives from Genian NAC with its own user ID table.
4. PAN confirms tag assigned to User-ID
5. Establish role-specific 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_NAC_SSO, under the **XML API** tab - Enable everything and validate it with **OK**



3.2 Create an account for Genian NAC. Assign the SSO role to the account. - Enter a **Name**: Genian_NAC - Select the **Administrator Type**: Role Based - Select the **Profile**: Genian_NAC_SSO



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 NAC for sending SYSLOG. Genian NAC 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

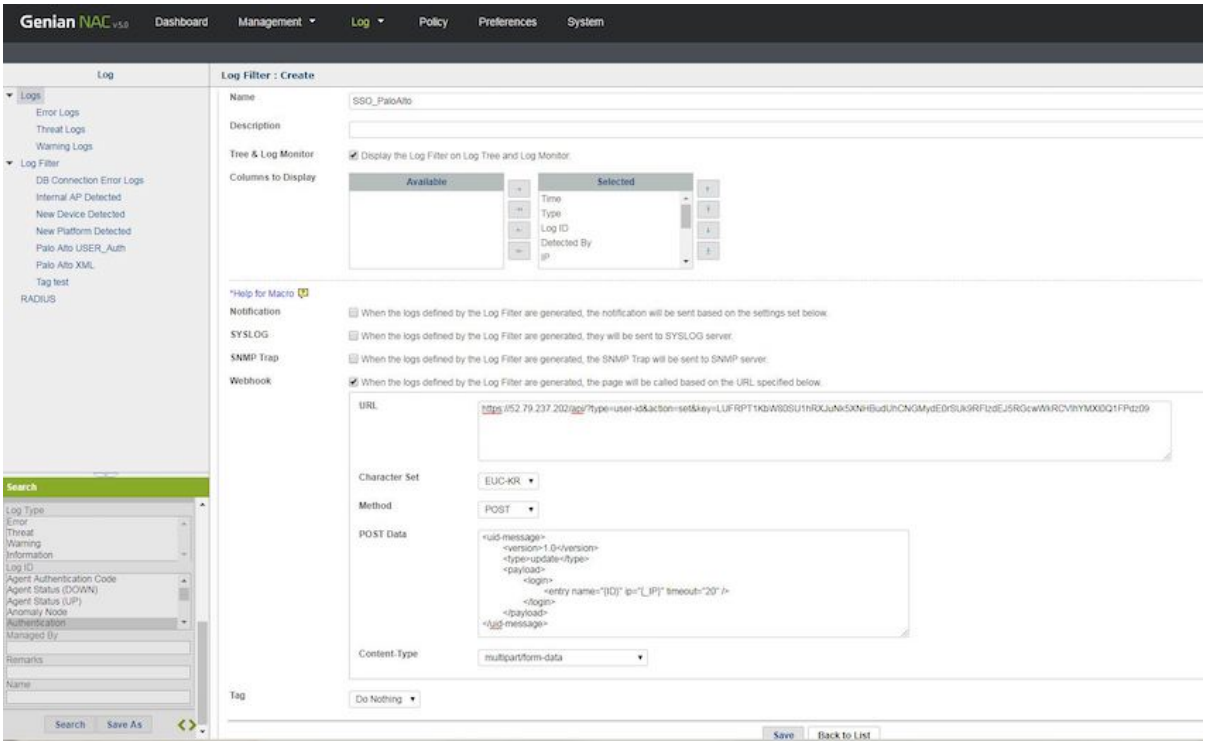
Enter a **Name**: SSO_PaloAlto Set the **Webhook URL:**

```
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



3.5 Configuring User Identification on Security Zones. PAN firewall policy rules use security zones to identify the Data

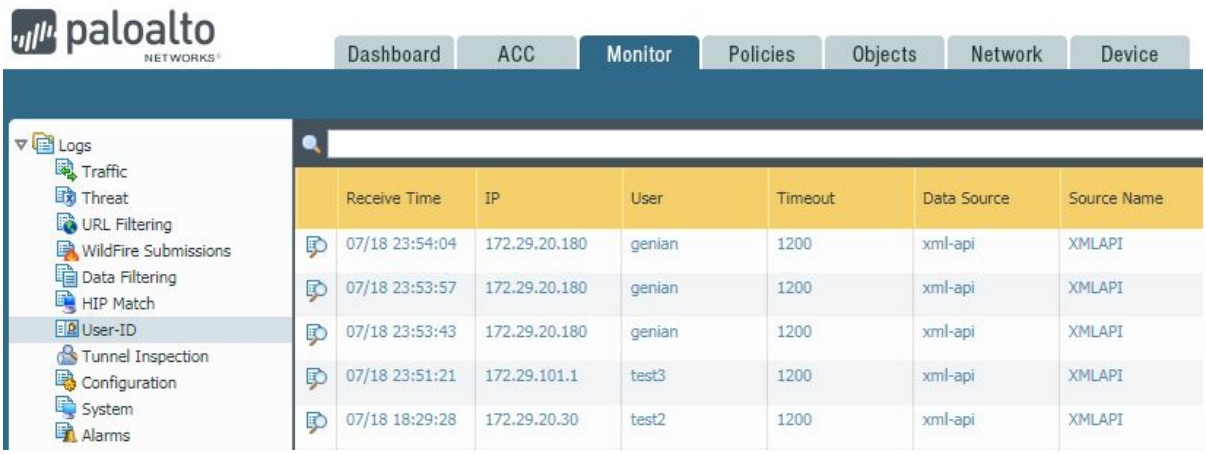
traffic which flows freely within the zone, not flowing freely between the different zones until you define the allowed security policy rules. To enable enforcement of user identity, you must enable user identification in both the inbound and outbound zones that are passed by end-user traffic.

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 NAC

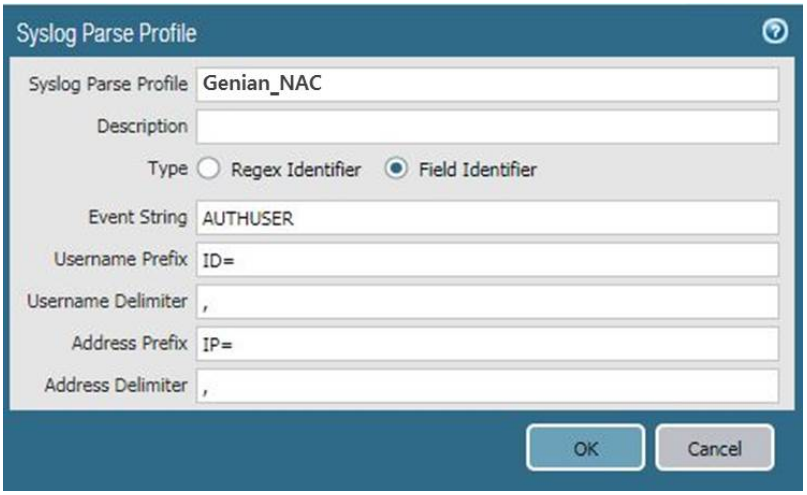


4. Configuring PAN Firewall for Integration via SYSLOG

4.1 Create a filter. The Palo Alto Firewall creates a log filter to distinguish authentication-related messages when receiving Syslog messages from Genian NAC.

- 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_NAC
Enter a Event String: AUTHUSER
Enter a Username Prefix: ID=
Enter a Username Delimiter: ,
Enter a Address Prefix: IP=
Enter a Address Delimiter: ,
```



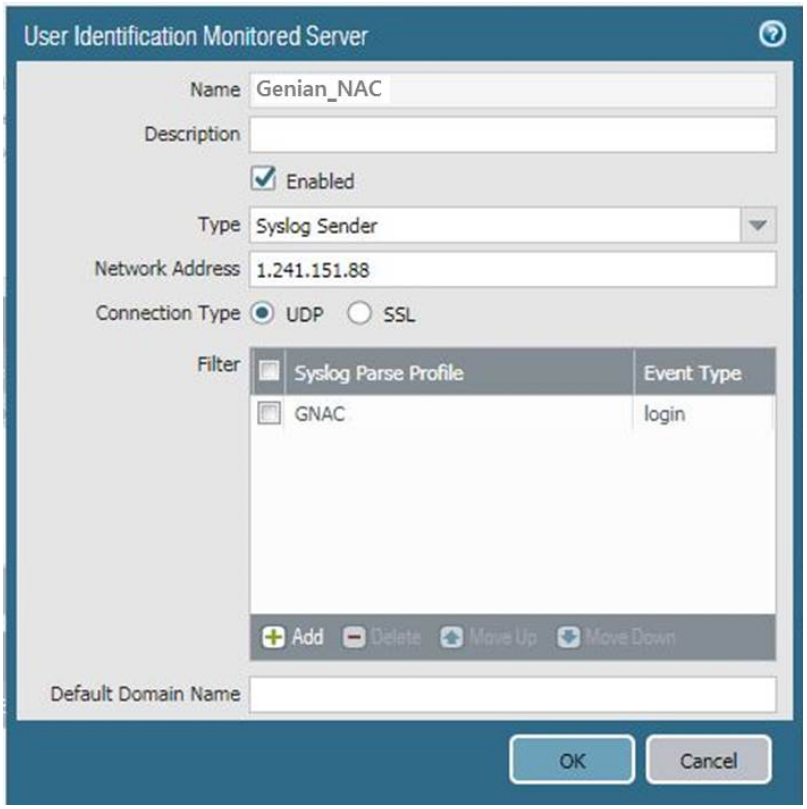
4.2 Specify the SYSLOG sender that the PAN firewall monitor.

- 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 NAC 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)



4.3 Enable SYSLOG listener services. It is able to listen to the SYSLOG from Genian NAC.

- Go to **Network > Network Profiles > Interface Mgmt > ADD** a new profile

```
Enter values
Enter a Name to identify the Network Profile: Allow Genian NAC
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 NAC** > Click **Ok**
- **Commit**

4.5 Configure the Genian NAC for sending SYSLOG. Genian NAC uses filters in the audit log to integrate with SYSLOG.

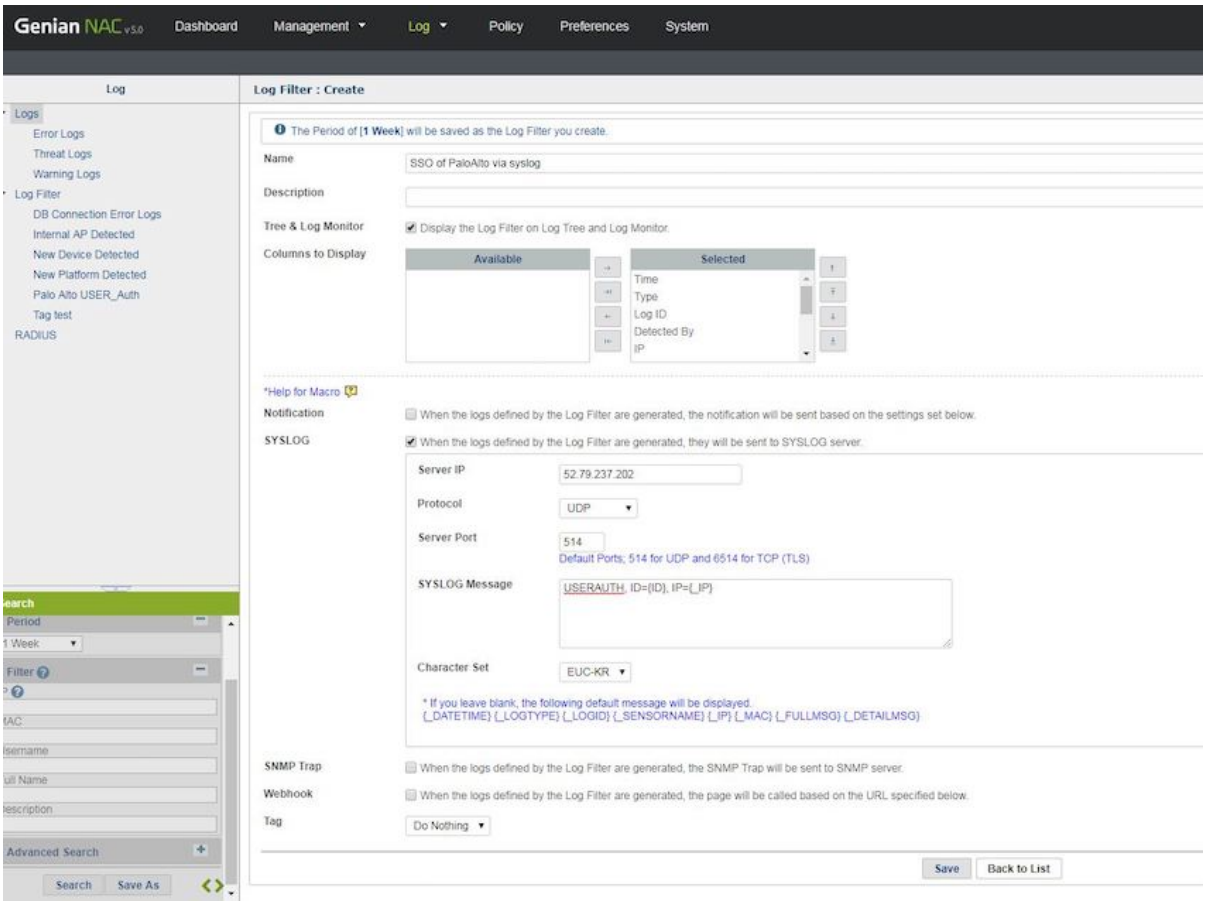
- Go to **Log** in the top panel
- Go to **Log > Search > Advanced Search > Log ID** > Check Authentication > Click **Search** button in the left Log panel
- You will see the Log of Authentication user and then you click the "**save as**" button

```
Enter values
Enter a Name
Enter a Server IP address[ Palo Alto IP]
Select the Protocol either UDP or TCP(TLS)
Set a Server port(UDP for 514, TCP(TLS) for 6514)
```

(continues on next page)

(continued from previous page)

```
Enter the SYSLOG Message: USERAUTH, ID={ID}, IP={_IP}
Click the Save
```



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
```

11.9.2 Integrating FireEye

This guide provides an overview of integration with FireEye. It includes the following information:

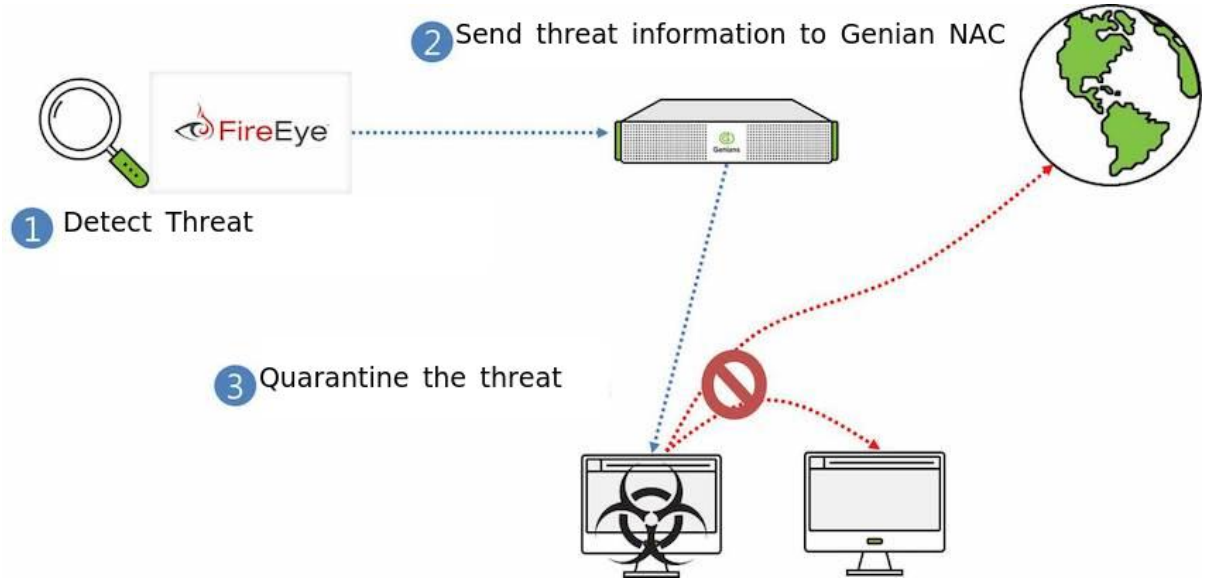
- *1. About This Guide*
- *2. Deployment of Genian NAC using FireEye*
- *3. Configuring FireEye for integration via SYSLOG*
- *4. Apply Genian NAC Policy based on FireEye Data*

1. About this Guide

The guide describes how to integrate Genian NAC and FireEye.

When a specific anomaly is detected by FireEye, FireEye sends anomaly information detected to Genian NAC through SYSLOG Genian NAC will be able to prevent the spread of anomalies by quarantine the anomaly target.

2. Deployment of Genian NAC using FireEye



1. FireEye detects the threatening device.
2. FireEye sends the anomaly information to Genian NAC via SYSLOG.
3. Genian NAC 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 NAC

For Genian NAC 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 NAC 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

Name	FireEye
Filter | host	
Filter Value|[IP address of FireEye]	
IP Prefix	src=
MAC Prefix	smac=

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 NAC 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 NAC > Click on **Add Rsyslog Server** button
8. Enter the IP address of the Genian NAC in the IP Address field
9. Click the **Update** button below

3.3 Verification

1. Go to **Log** on the top panel of Genian NAC.
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.

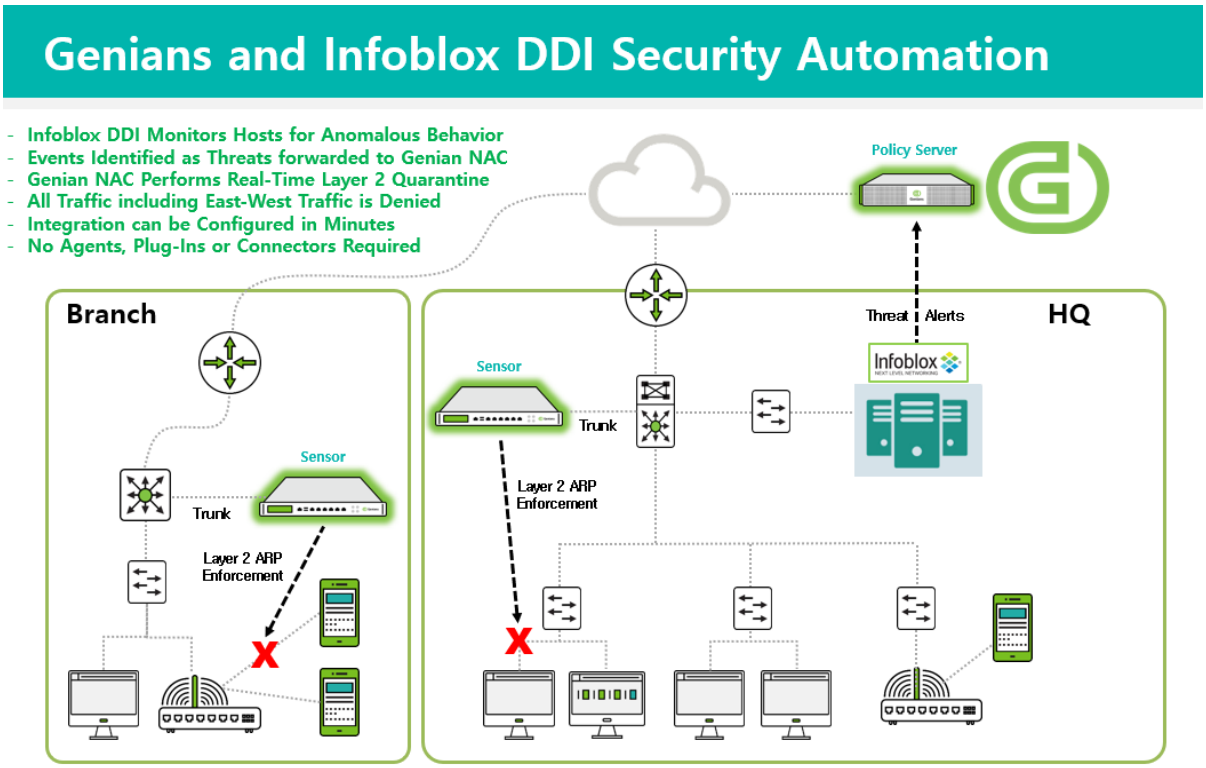
4. Apply Genian NAC Policy based on FireEye Data

Once Genian NAC 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*

11.9.3 Integrating Infoblox DDI

This document describes how to integrate Infoblox with Genian NAC using syslog. This integration provides the ability to extend the Infoblox DDI Response Policy Zone (RPZ) feature into the Enforcement capabilities of Genians NAC. A full video Webinar covering this integration along with a demo is available on the Genians YouTube Channel.



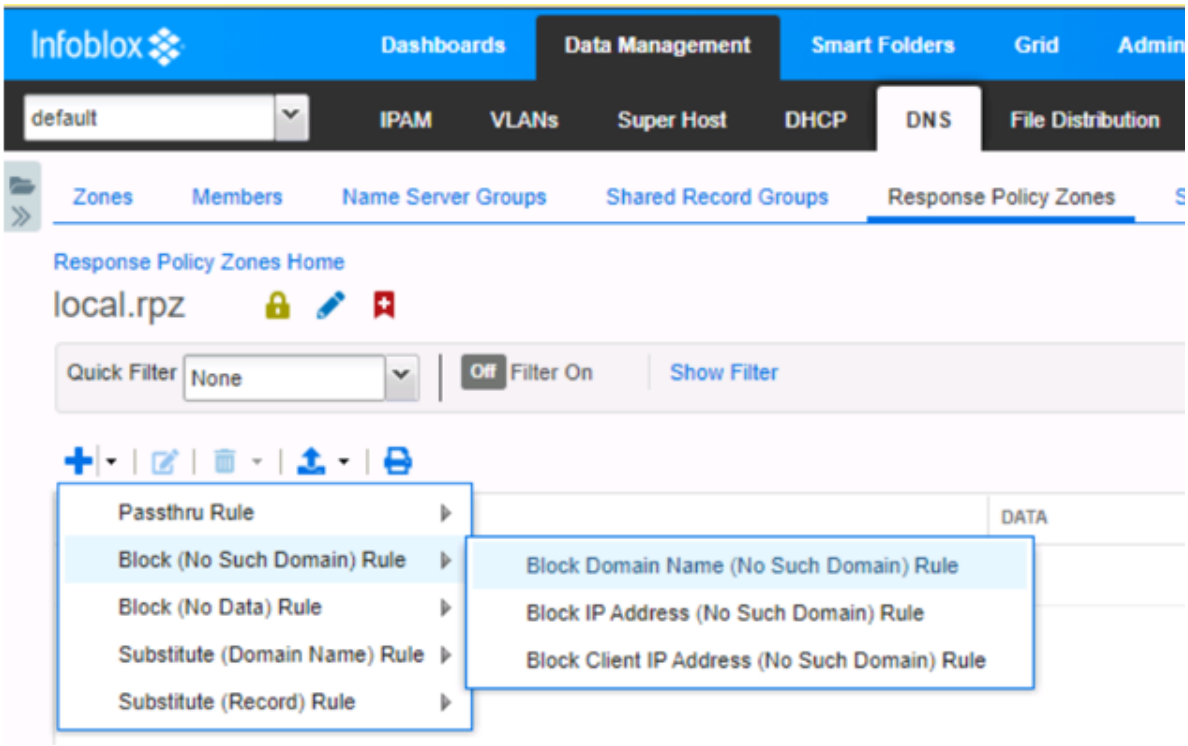
The main steps of this integration are as follows:

- Configure a domain to be blocked in Infoblox
- Export this blocking event to Genian NAC via syslog
- Configure Genian NAC to interpret this event, and apply enforcement to the impacted node.

Infoblox Domain Blocking Configuration

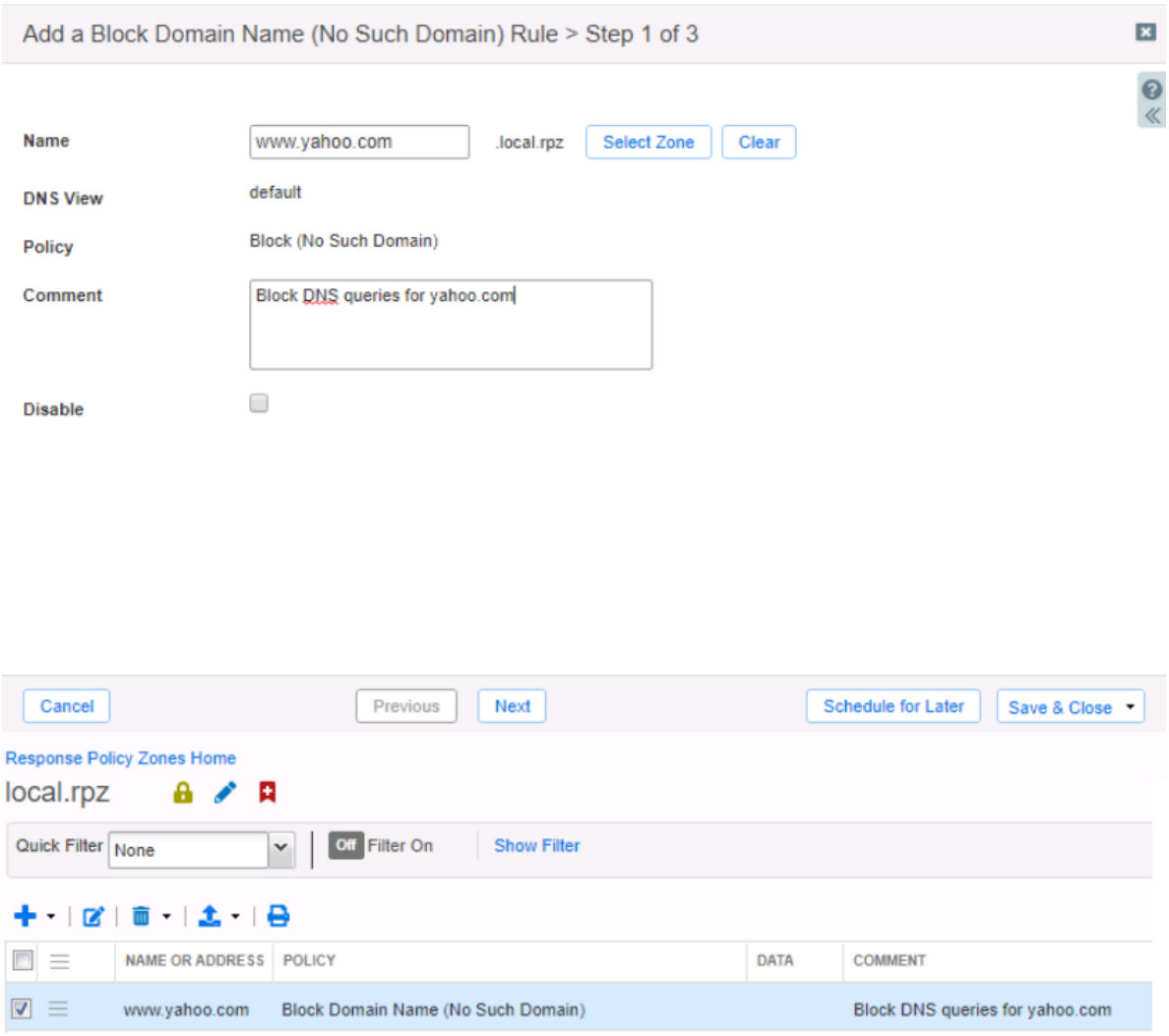
The steps below demonstrate how to configure and export critical RPZ events from Infoblox DDI to Genians via Syslog.

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.

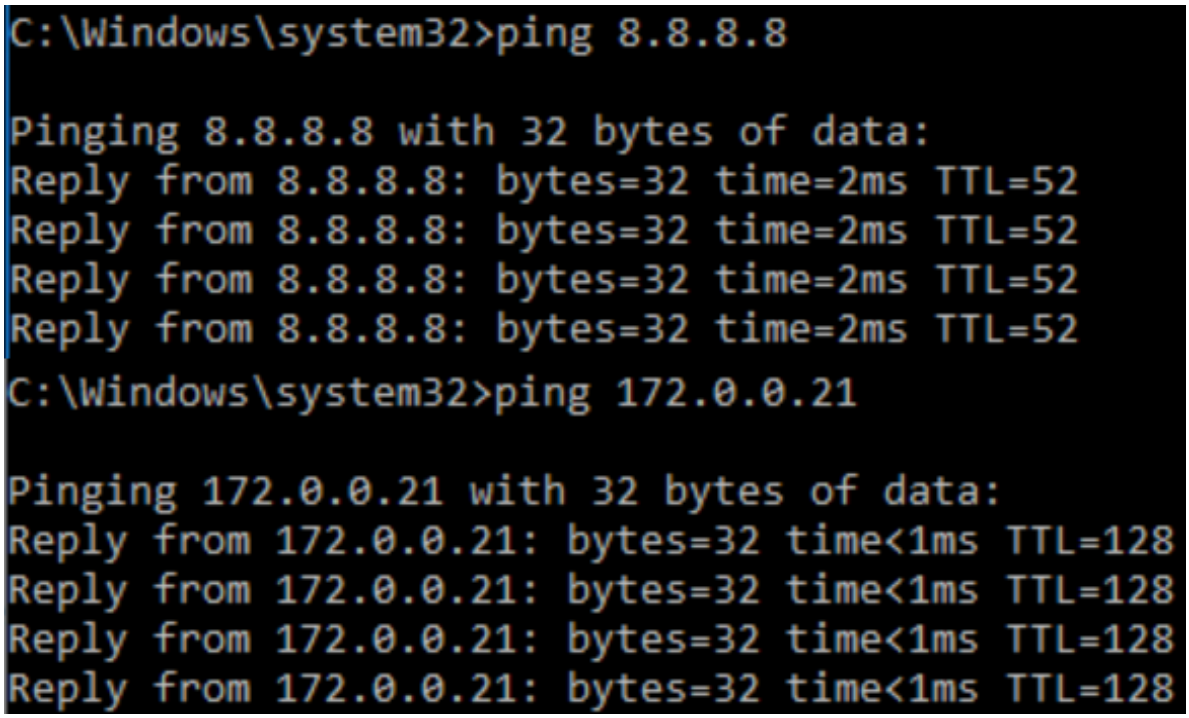


4. On a test machine subject to the previously configured Response Policy Zone, perform an nslookup on authorized domain (infoblox.com) and then perform an nslookup on unauthorized domain simulating malware site (www.yahoo.com).

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
```

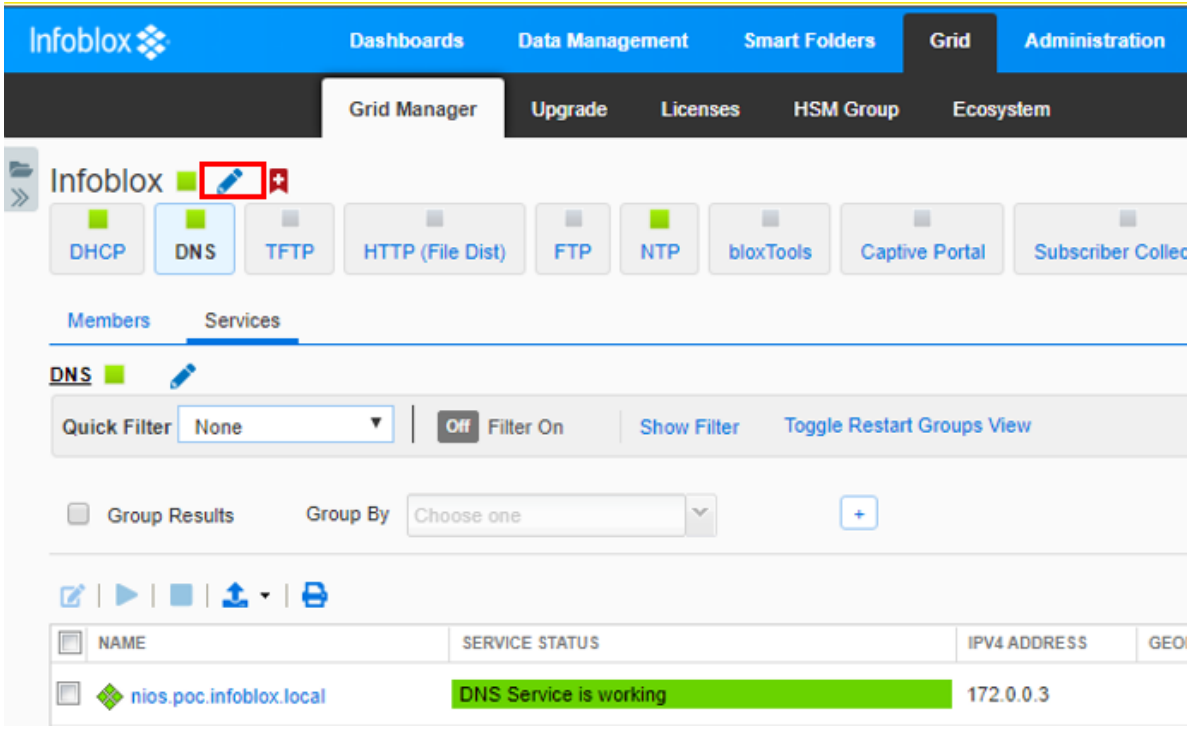
6. On the test machine, generate continuous pings to both an internal and external host. Note that even though Infoblox DDI has denied the domain from being resolved, the device still has network access, both to external and internal hosts:



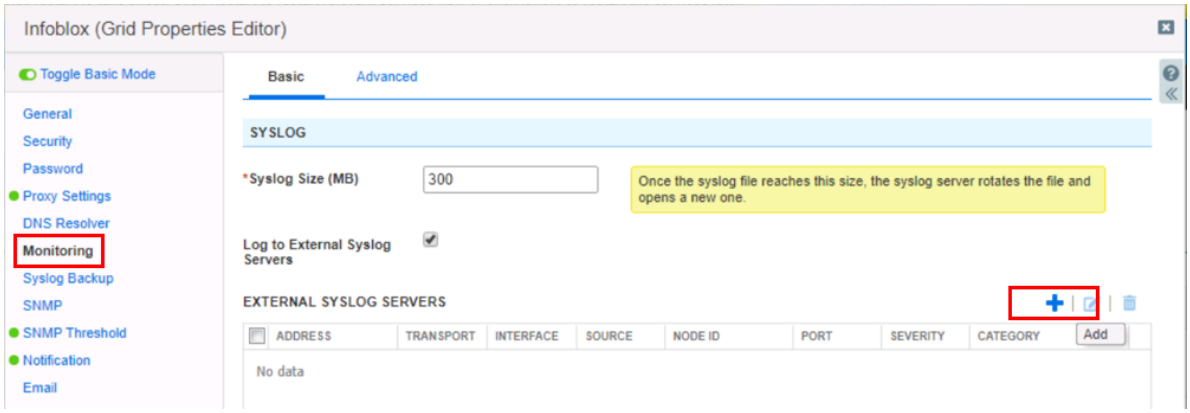
7. Once the test above has been validated, perform the steps below to export Non-existent domain events to the Genian NAC Policy Server.

Infoblox Event Export Configuration

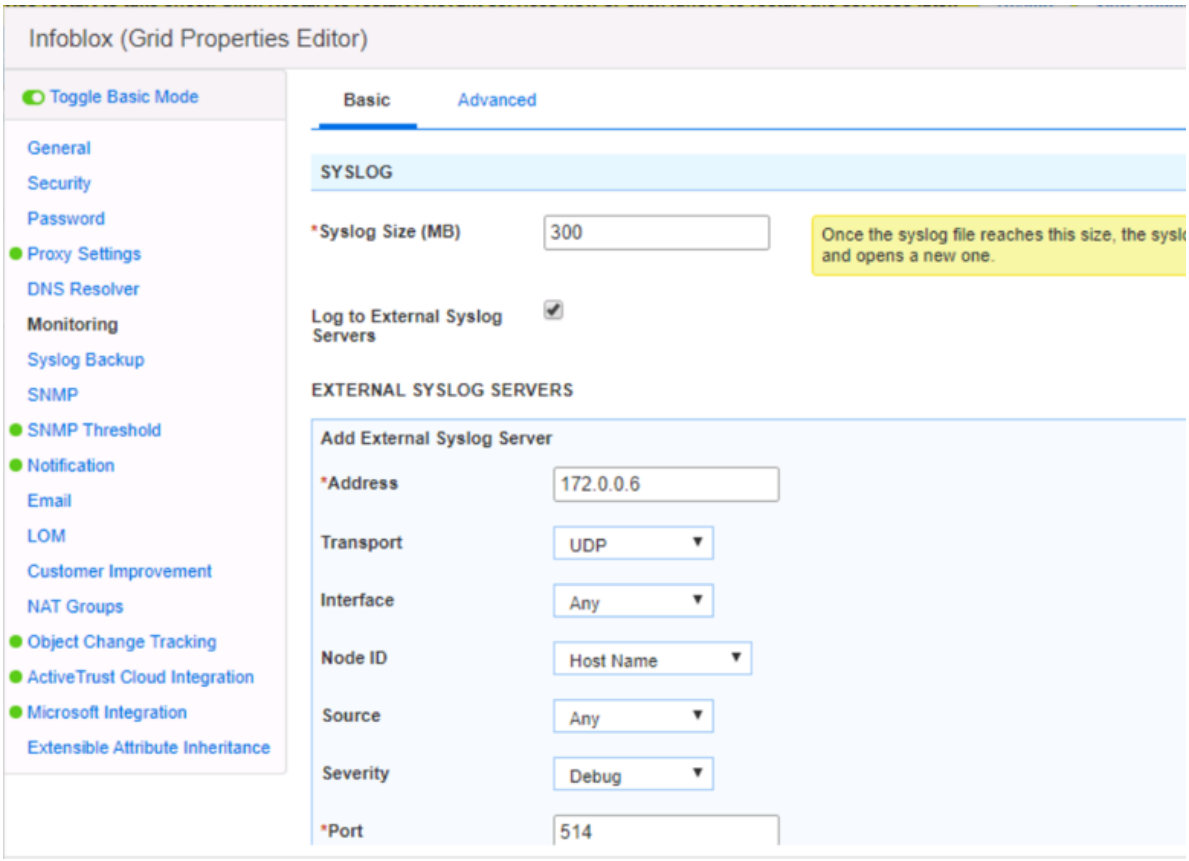
1. Navigate to **Grid > Grid Manager** and click on the **edit** button next to Infoblox.



2. Click on **Monitoring** and then click the **+** button to add a new Syslog server.



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 NAC 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.



Genian NAC 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.

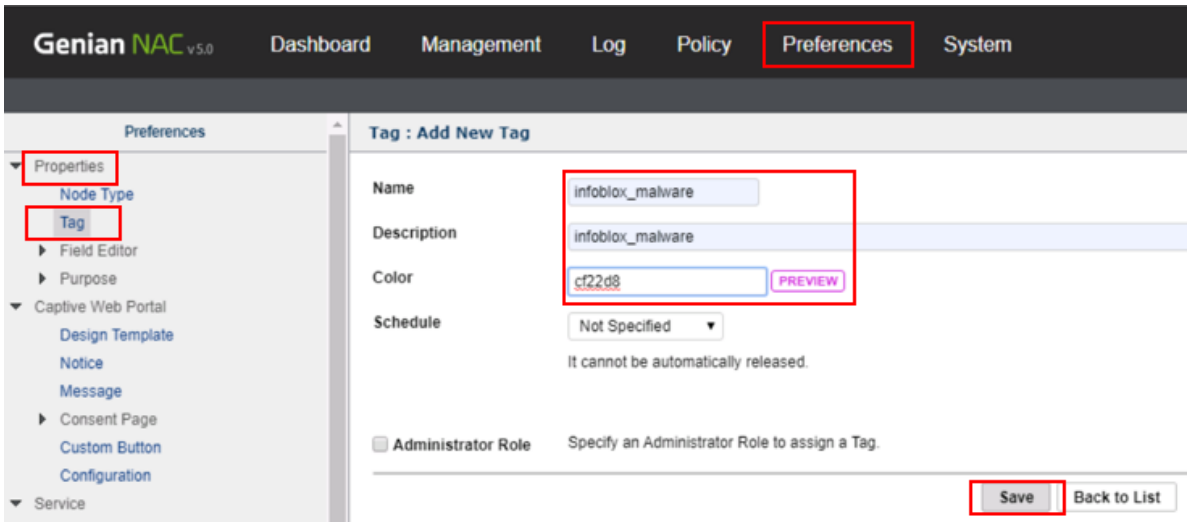
These options may be found under **General > Log** in the **Preferences** section.

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 NAC 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.

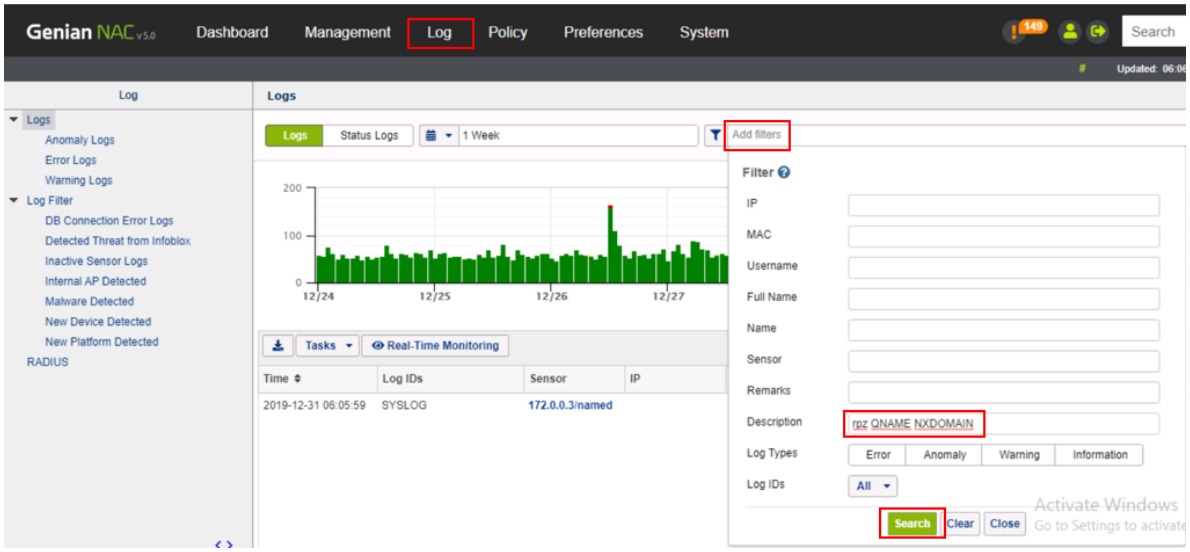
Now the message from the Infoblox system will be correllated with the nodes detected by Genian NAC.

Genian NAC 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.

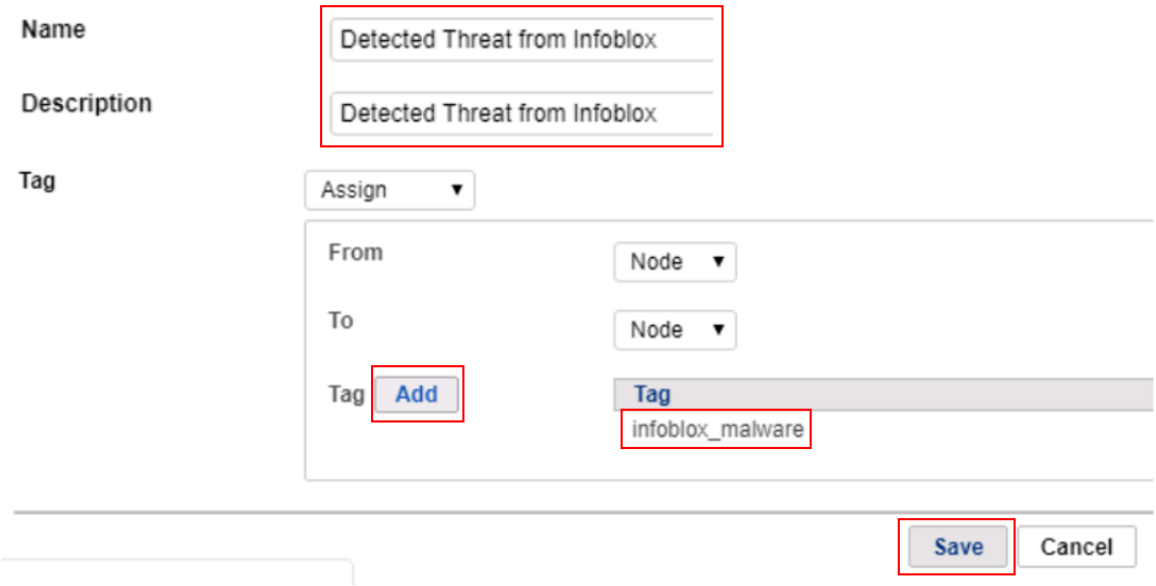


2. Click on **Log** and then **Add filters**. Critical RPZ syslog alerts from Infoblox DDI include the key words "rpz QNAME NXDOMAIN". Type these words into the Description field of the log filter and click **Search**.



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.



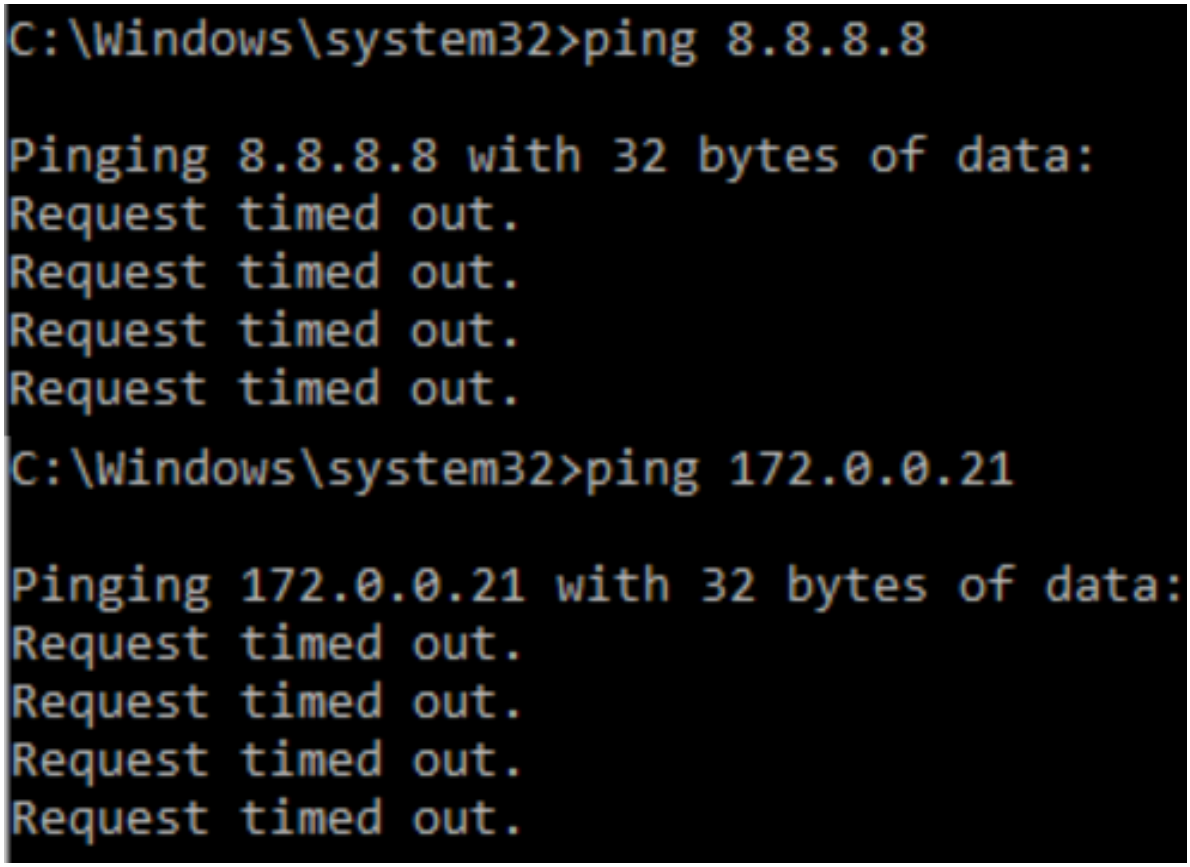
5. Navigate to **Policy > Group** then click **Tasks > Create** to create a new Node Group. Under General enter an ID and Description and set the Status to Enabled. Under Condition, click **Add** to add the previously created "Infoblox_malware" tag then click **Save**.

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.

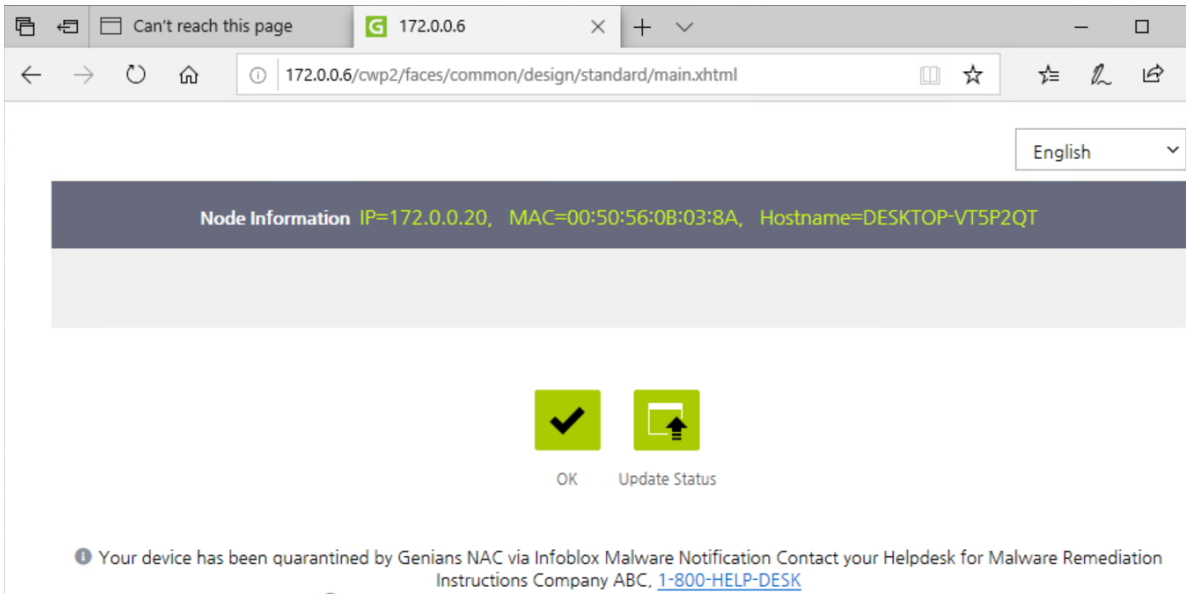
7. With all configurations now in place, the Genians Network Sensor must be switched from Passive to Active mode to facilitate the Layer 2 quarantine of non-compliant nodes on the network. Navigate to **System > Sensor > Edit Sensor Settings** and set the Sensor Operating Mode to Active then click Update 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.



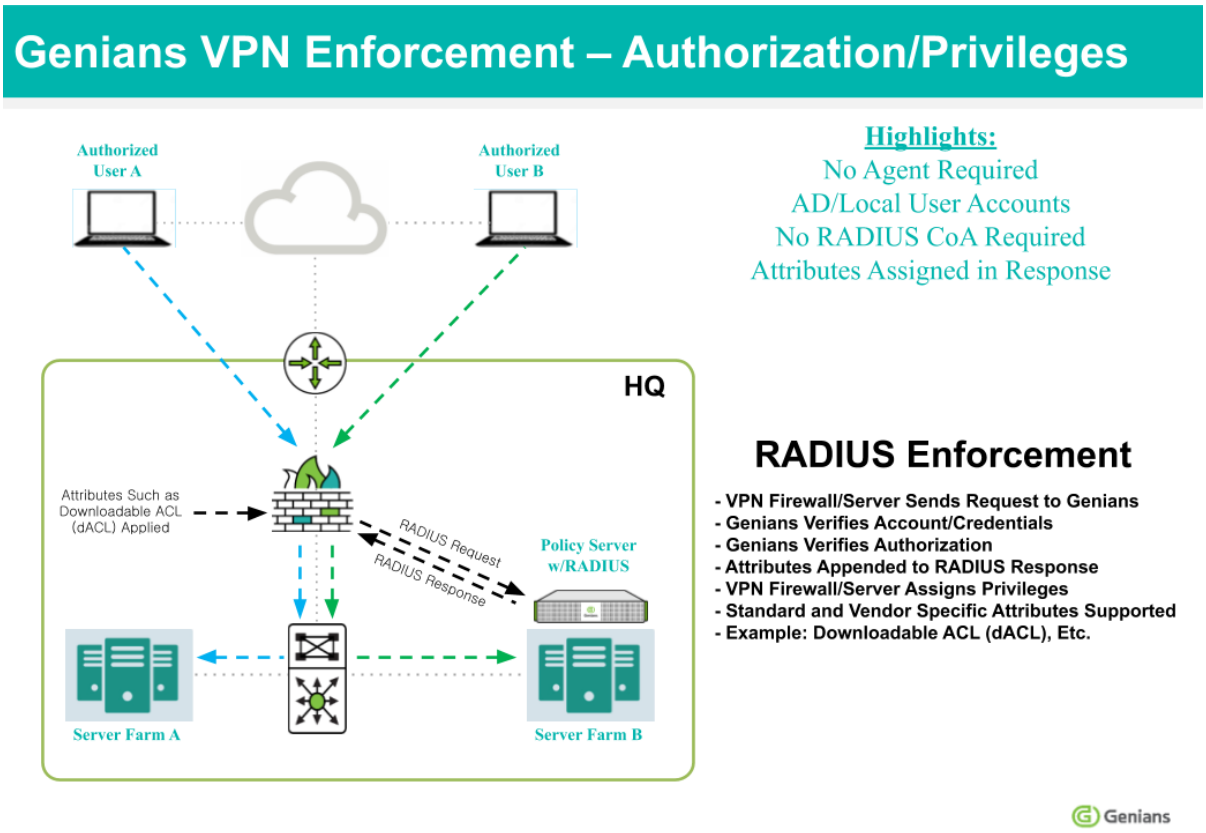
9. In the browser of the test machine, navigate to Infoblox.com and the Genians Captive Portal will be displayed with your message. Both the page design and contents may be customized, this is just a generic template.



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.

11.9.4 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.

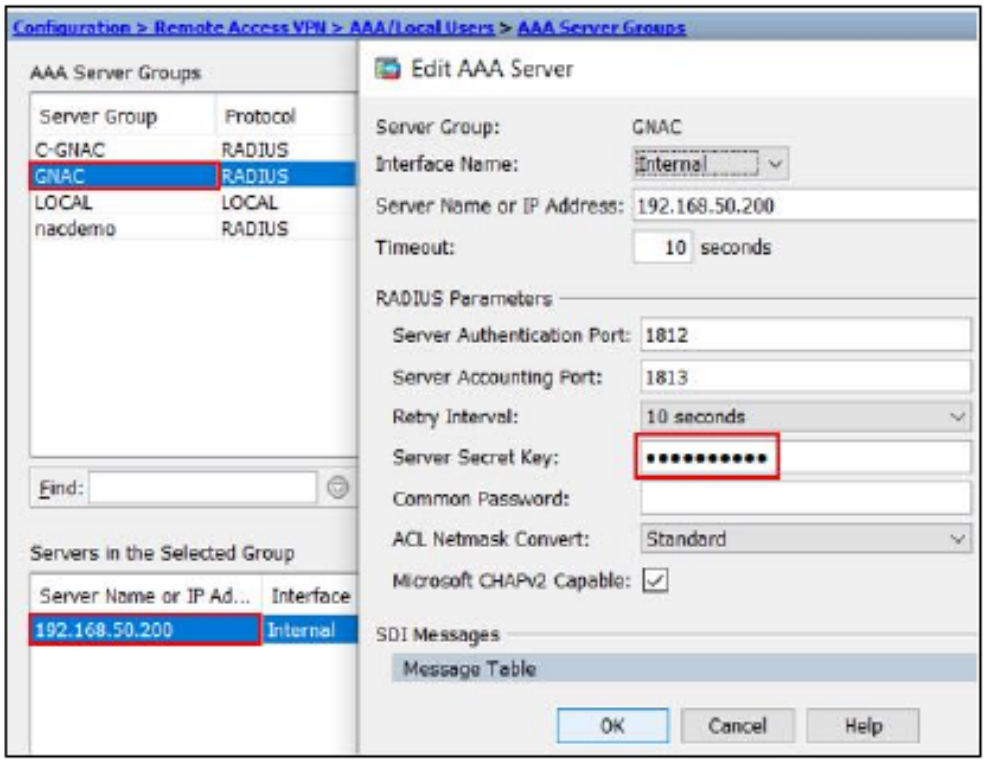


Integrating the Radius Server

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 NAC 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:



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
```

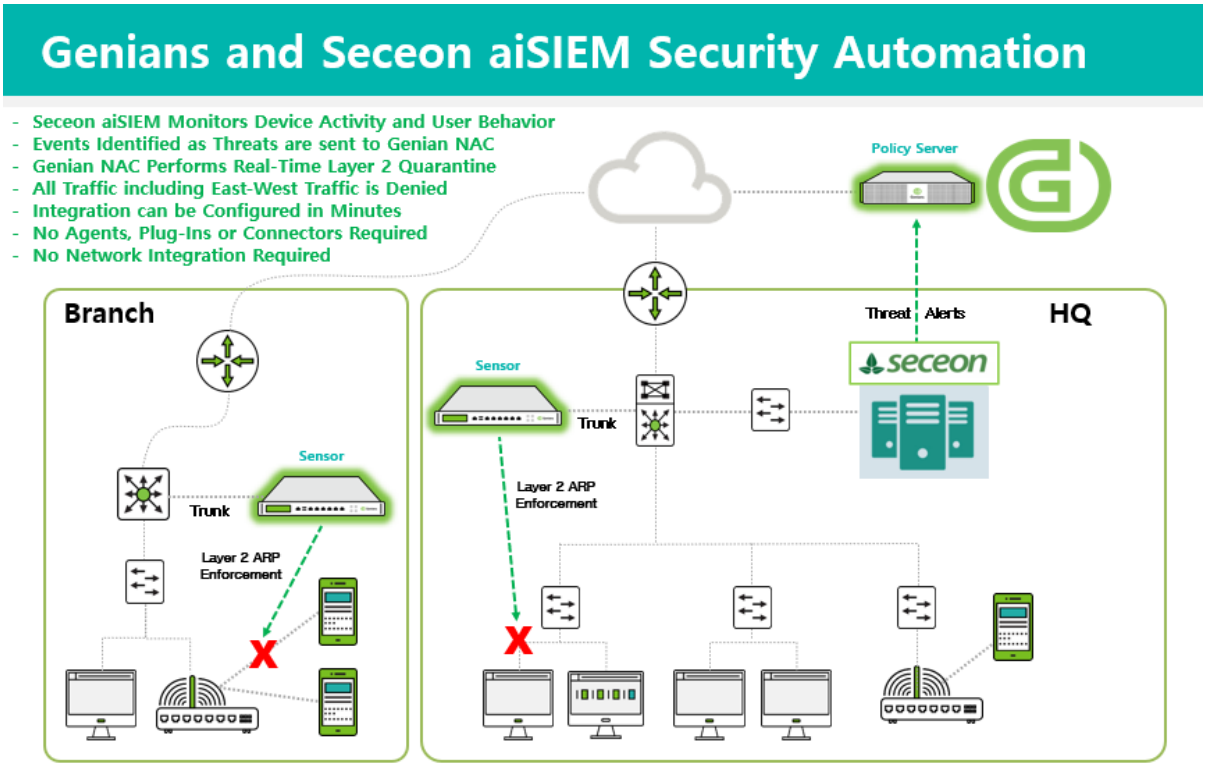
10. Click **Add** button.
11. Click **Create** button.

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*

11.9.5 Integrating Seceon aiSIEM

This document describes how to integrate Seceon aiSIEM with Genian NAC using syslog. This integration provides the ability to extend Seceon aiSIEM threat detection capabilities into the Enforcement capabilities of Genians NAC. A full video Webinar covering this integration along with a demo is available on the Genians website under **Resources > Videos.**



The main steps of this integration are as follows:

1. Configure a Remediator in the Seceon APE
2. Configure Genian NAC 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 NAC as the Device, Firewall as the Device Type and enter the IP of your Genian NAC 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 NAC 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 NAC.

Genian NAC 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**.

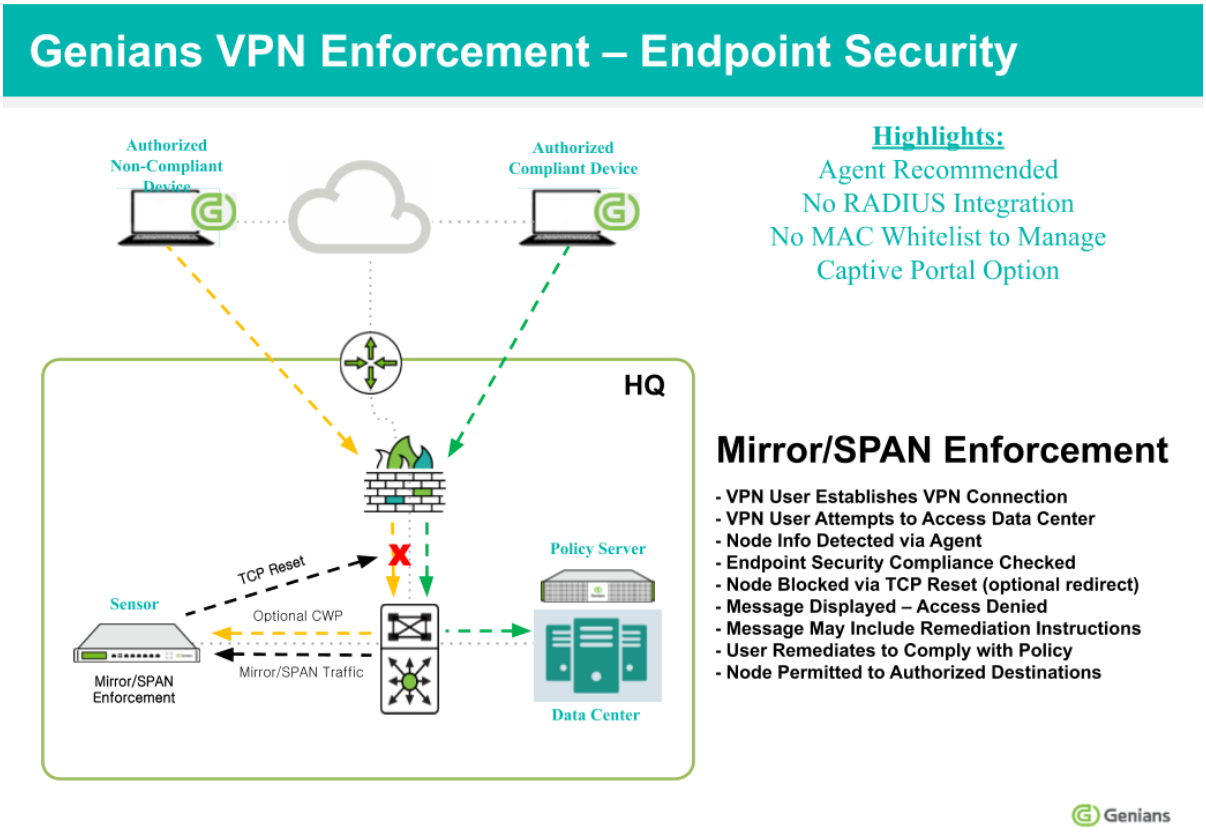
With all configurations now in place, the Genians Network Sensor must be switched from Monitoring to Enforcement mode to facilitate the Layer 2 quarantine of non-compliant nodes on the network. Navigate to **System > Sensor > Edit Sensor Settings** and set the Sensor Operating Mode to Enforcement then 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 NAC 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 NAC.
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 NAC. 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.

11.10 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 NAC can block these unapproved devices at Layer 3 using a Network Sensor deployed in Mirror Mode.



11.10.1 Cofigure Sensor

To configure a Sensor in Mirror Mode, see: *Configuring Mirror Mode*

11.10.2 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*

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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 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.

13.1.1 Authentication using Captive Web Portal

Genian NAC 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 NAC 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 NAC 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 NAC 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 NAC 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). NAC 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 netbios, 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

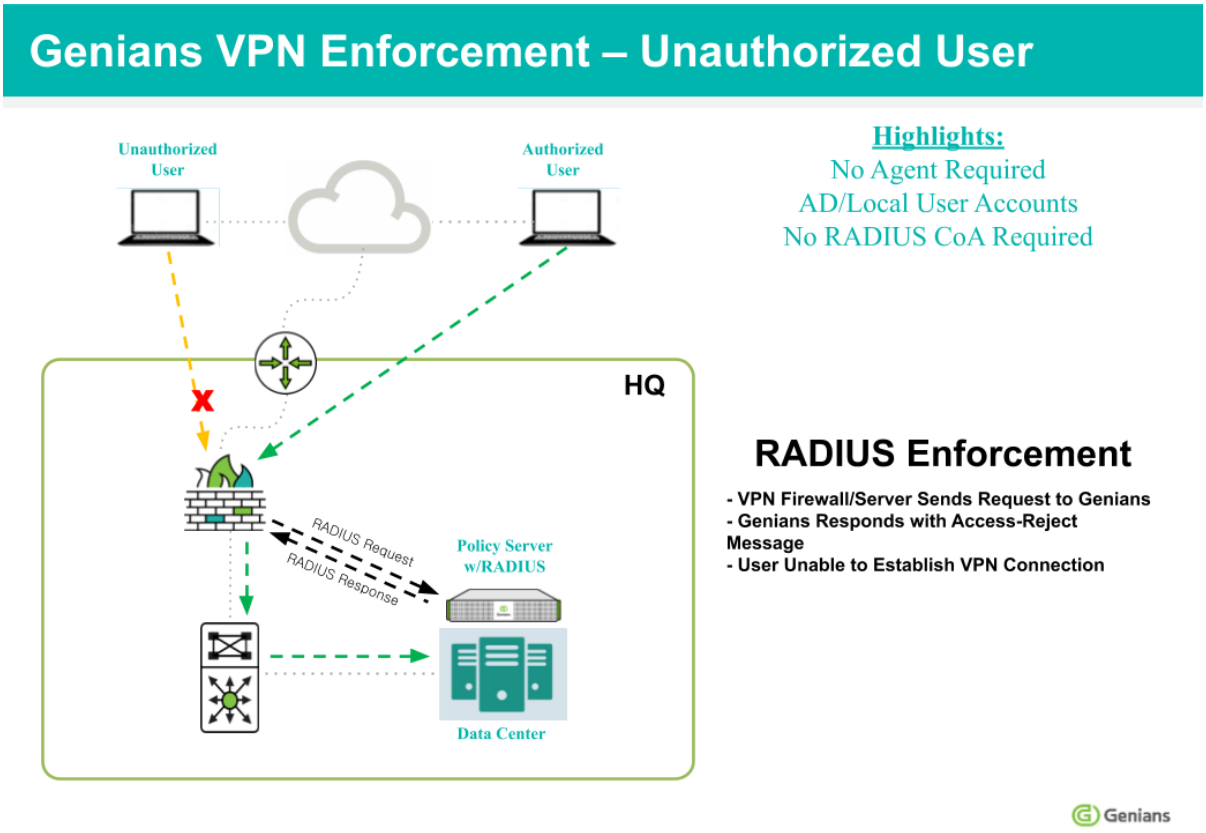
Assign the following permissions to each of the namespaces:

- 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.

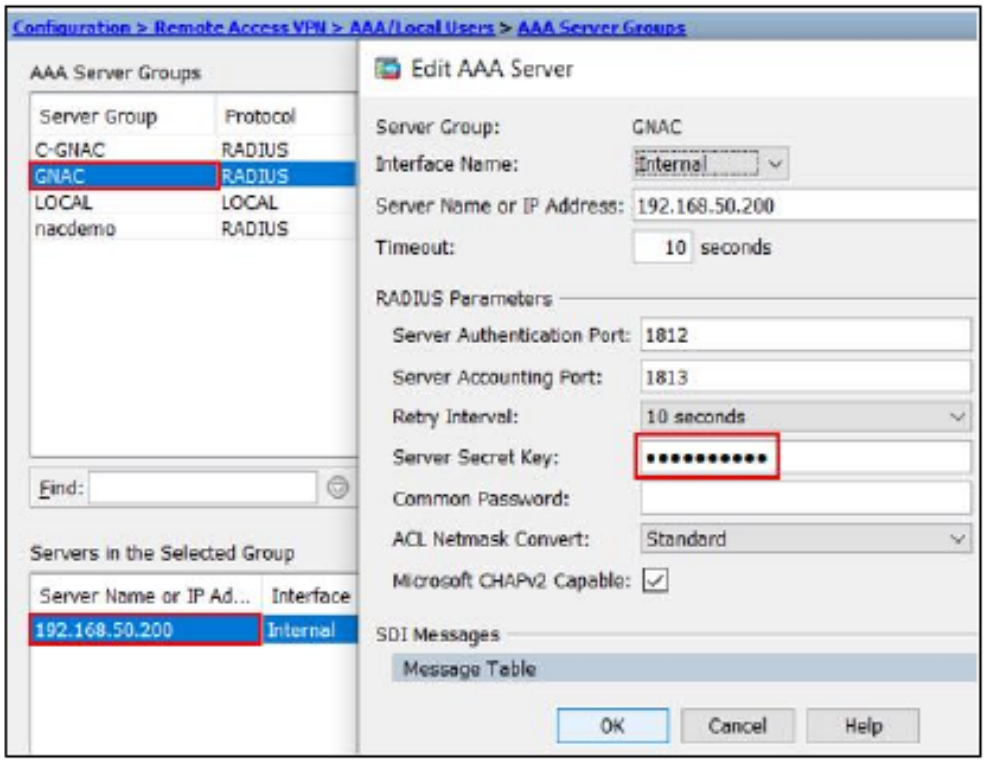


Integrating the Radius Server

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 NAC 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:



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.

13.2 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 NAC.

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 NAC 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.

13.3 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 NAC 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 NAC is integrated with Google through SAML, Genian NAC 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 NAC 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 NAC (Service Provider), and Okta (Identity Provider).

This enables user authentication through Okta without having to manage users in Genian NAC.

SSO is achieved by invoking Okta authentication using the SAML2.0 protocol on the Genian NAC CWP(Captive Web Portal) page and checking Okta for user authentication.

Recommended Version

Product	Version
Genian NAC PolicyServer	V5.0.31 +
Okta APP	SAML2.0

Supported features

The Okta SAML integration currently supports the following features:

- SP-initiated SSO
- IdP-initiated SSO

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.

4. Add OTP for Okta Admin console connections.

   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

General tab (enter SP information for Genian NAC in Okta APP)

1. In the menu, navigate to **Applications > Applications**.
2. Click the blue **Create App Integration** button among the buttons on the screen.
3. In the pop-up screen, select **SAML 2.0** and click the **Next** button.
4. Type the name and logo of the APP to be used for integration with NAC and click the **Next** button.
5. In the **Single sign-on URL** entry, enter a value for the Genian NAC **Web Console > Preferences > User Authentication > Authentication Integration > SAML2 > SP ACS URL**.
6. In the **Audience URI (SP Entity ID)** entry, enter a value for the Genian NAC **Web Console > Preferences > User Authentication > Authentication Integration > SAML2 > SP Entity ID** and click the **Next** button.
7. In the **Feedback** tab, the **Are you a customer or partner?** item checks **i'm an Okta customer adding an internal app**.
8. Click the **Finish** button.

- The following SAML attributes are supported:

Name	Value
firstName	user.firstName
lastName	user.lastName
email	user.email

Sign On tab (enter IDP information in Genian NAC)

1. Click the **Sign on methods > SAML 2.0 > More details** button in the middle of the screen to view IdP information.
2. Copy and paste the following details into the Genian NAC **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.
3. In **Sign in button text**, enter the text that will appear on the SAML authentication button in the NAC Web Console Authentication page.
4. Click the **Update** button at the bottom of the Genian NAC Web Console Settings screen.

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 NAC SAML App.

How to test on Genian NAC 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 NAC CWP page (SP-initiated SSO)

1. Prepare the device (node) to which the Genian NAC Node Policy is assigned the Authentication Method password policy.
2. Access the Genian NAC 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.

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 NAC (Service Provider), and Okta (Identity Provider).

SSO is achieved by invoking Okta authentication using the SAML2.0 protocol on the Genian NAC web console page and checking Okta for administrator authentication.

Recommended Version

Product	Version
Genian NAC PolicyServer	V6.0
Okta APP	SAML2.0

Prerequisites

The current version does not support JIT provisioning, so you cannot authenticate without a administrator created in Genian NAC (SP). Please create a administrator in NAC first.

Supported features

The Okta SAML integration currently supports the following features:

- SP-initiated SSO
- IdP-initiated SSO

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

General tab (enter SP information for Genian NAC in Okta APP)

1. In the menu, navigate to **Applications > Applications**.
2. Click the blue **Create App Integration** button among the buttons on the screen.
3. In the pop-up screen, select **SAML 2.0** and click the **Next** button.
4. Type the name and logo of the APP to be used for integration with NAC and click the **Next** button.
5. In the **Single sign-on URL** entry, enter a value for the Genian NAC **Web Console > Preferences > General > Console > SAML2 Authentication > Identity Provider (IdP) > SP ACS URL**.
6. In the **Audience URI (SP Entity ID)** entry, enter a value for the Genian NAC **Web Console > Preferences > General > Console > SAML2 Authentication > Identity Provider (IdP) > SP Entity ID** and click the **Next** button.
7. In the **Feedback** tab, the **Are you a customer or partner?** item checks **i'm an Okta customer adding an internal app** .
8. Click the **Finish** button.

Sign On tab (enter IDP information in Genian NAC)

1. Click the **Sign on methods > SAML 2.0 > More details** button in the middle of the screen to view IdP information.
2. Copy and paste the following details into the Genian NAC **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.
3. In **Sign in button text**, enter the text that will appear on the SAML authentication button in the NAC Web Console Authentication page.

4. Click the **Update** button at the bottom of the Genian NAC Web Console Settings screen.

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 NAC SAML App.

How to test on the Genian NAC Admin Web Console page (SP-initiated SSO)

1. Connect to the Genian NAC 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.

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
```

Google G suite(SAML2.0)

This document guides you through how to set up the G suite and Genian NAC authentication integration functions.

Summary

You can work with Genian NAC and Google G Suite to authenticate users with Google G Suite without having to manage Genian NAC's own user DB. For user authentication, normal SSO is performed by calling G suite authentication using SAML2.0 protocol on the Genian NAC CWP page and verifying user authentication.

Step 1: How to set up Google workspace

1. Log in to https://admin.google.com . (**Log in with your Workspace Administrator account.**)
2. In the left console menu bar, **click Apps -> Web and Mobile Apps** .
3. Click Add App -> Add a Custom SAML App.
4. Set the app name, description, and app icon.
5. After accessing the Genian NAC web console, click **Preferences -> User Authentication -> Authentication Intergration -> SAML2 Identity Provider -> Add** .
6. Enter the values created in the Google Administration Console in the Genian NAC SAML2 Certification Integration window.
   - **SSO URL, Entity ID , x.509 Certificate -> IdP SSO URL, IdP Entity ID, x509 Certificate**
7. Conversely, enter the values you created in the Genian NAC SAML2 authentication integration screen in the Google Admin console window.
   - **SP Entity ID, SP ACS URL -> ACS URL, Entity ID**
8. **policy -> Node Policy -> Authentication Method -> Assign** click to add SAML2 authentication.

Step 2: Add Users for Google Workspace Integration

1. On the Google Administration Console main screen, click Users
2. Click Add user.
3. Set the user's name and mail, then click **Add New User** .
4. Click Main Screen - Users - Reset Password, then reset your password.

Note: The Password entry selects whether the administrator creates the password by specifying it or if you want to change it when you log in for the first time.

Step 3: Google SAML Authentication Integration Test

1. **Preferences -> User Authentication -> Authentication Integration -> Authentication Test** click Test.
2. Change Repository to SAML
3. Click the SAML authentication login button that you set on the screen that is displayed -> Login progress
4. If it is set normally, the Google login window will be printed and authentication will be successful.
5. You can check the ID of the logged-in account and the logged-in authentication method (SAML) in the audit log.

Note: After setting up the Authentication Integration, you must add the IdP domain to the enforcement policy permission when applying the policy to display the authentication linkage window even in the blocking state.

```
1. To add permissions
2. Policy -> Object -> Network
3. Tasks -> Create
4. Enter basic information
5. Condition -> Select FQDN -> Enter the IDP domain (e.g. accounts.google.com)
6. Click Create
7. Go to the Permissions menu
8. Create permissions using created network objects
9. Assign permissions that you create to a control policy that controls the device␣
↪network
```

13.3.7 Webhook Authentication Integration

When a user attempts to log in to the Webhook authentication integration, a Webhook event occurs and Genian NAC invokes the Webhook URL.

This is an authentication method in which a user logs in when a successful return value from the called URL is returned to the Genian NAC.

Here's how to set up to use the Webhook authentication integration.

1. Policy -> Node Policy , Select the node policy for which you want to enable Webhook authentication.
2. Advanced -> Authentication Policy -> Authentication Method -> Assign SAML after clicking ASSIGN
   - **The authentication method located at the top of the authentication method list is used for authentication.**
3. Preferences -> User Authentication -> Authentication Integration -> Webhook
4. Set the URL and call method to call when the event occurs. (Get, select the call method during POST.)

```
ex) content-type - json
Get Method : https://called URL/?id={_USERID}&pwd={_USERPASSWORD}
Post Method : https://called URL
```

5. For POST method, select **content-type** and enter the appropriate POST data for the data format.

```
ex)
content-type - application/json
Post Data : id={_USERID}&pwd={_USERPASSWORD}
```

6. Enter Regex for Authentication. (**Creates a return success value.**)

7. Enter Regex for Result Message
8. Enter Charset for Result Message

Note: To enable SSL-based encrypted communication, modify the Webhook URL to https.

13.3.8 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

13.3.9 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 NAC 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. Set **Synchronization Interval** and **Action**
6. Find **Advanced > External DB** section in main window. Select **RDBMS**
7. Find **Advanced > User, Department, Job Title, Node, and LifeCycle Information** sections in main window. Add in information as needed.
8. Click **Tasks > Synchronize Now**

13.4.2 Synchronizing User Directories

Note: This feature required Enterprise Edition

Genian NAC 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.

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. Set **Update Interval**.
6. Find **Advanced> DB Type** and select **CSV**.
7. In the **Data Synchronization** list, click the **checkbox** in the desired synchronization list.
8. Click **Tasks> Synchronize now**.

13.4.4 Google G Suite

Note: This feature required Enterprise Edition.

Genian NAC 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.

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 NAC 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 NAC, 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. **ID** : Select a Name for the synchronization
2. **Update Interval** : Configure when to synchronize the information.
3. **Policy Apply** : Enable to reflect changes after synchronization.

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 NAC

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-xxxxxxxxxxxx-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 NAC 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.

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 NAC 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)

14.2 Supported Operating Systems and Plugins

14.2.1 Supported Windows

- Windows XP
- Windows XP x64
- Windows Vista
- Windows Vista x64
- Windows 7
- Windows 7 x64
- Windows 8
- Windows 8 x64
- Windows 8.1
- Windows 8.1 x64
- Windows 10
- Windows 10 x64
- Windows 11 x64
- Windows Server 2012

- Windows Server 2016
- Windows Server 2019

14.2.2 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.
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.
ScriptCtrl	Runs VB script or batch script.
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.

14.2.3 Supported macOS

- OS X Mavericks
- OS X Yosemite
- OS X El Capitan
- macOS Sierra
- macOS High Sierra
- macOS Mojave
- macOS Catalina
- macOS Big Sur
- macOS Monterey
- macOS Ventura
- macOS Sonoma

14.2.4 Supported macOS Plugins

Plugin Name	Description	Agent Version
InfoOS	Collects information about OS installed on the computer.	5.0.11~
InfoHW	Collects information about hardware of motherboard, memory and disk space.	5.0.11~
InfoSW	Collects information about all installed applications on the system to display Applications in Software of Node Management.	5.0.11~
InfoNet	Collects information about all network interfaces and the open ports detected to display in Node information.	5.0.11~
InfoVaccine	Collects information about Antivirus software installed on the system.	5.0.11~
MacUpdate	Checks for macOS updates and executes an action on a scheduled basis.	5.0.11~
ProcessCtrl	Terminates a specific process defined in Condition Settings.	5.0.28~
Blank	Checks Condition Settings configured in Agent Action.	5.0.14~
GeniAuth	Uses Genian Agent Authentication and customizes the display options.	5.0.15~
SaverCtrl	Collects information about the lock screen configured and controls the configuration settings.	5.0.15~
InfoPrinter	Collects information about all printers currently installed on the computer.	5.0.16~
InfoMonitor	Collects information about all monitors currently connected to the computer.	5.0.17~
PowerCtrl	Controls the power options of the system.	5.0.17~
CheckSoftware	Collects information about all installed applications on the system to display Applications in Software of Node Management.	5.0.21~
UserMsg	Changes slide-out notification settings to notify users.	5.0.27~
FileCtrl	Runs, deletes, copies, moves and renames the files on the computer.	5.0.28~
WirelessCtrl	Provides information about wireless APs detected on wireless network interfaces and restricts disallowed AP connections.	5.0.38~
ARPCtrl	Perform administrative tasks on ARP tables on your PC.	5.0.31~
DeployCtrl	Run the file or download it to a specific location.	5.0.31~
HostNameCtrl	Change the host name of the computer.	5.0.34~
DeviceCtrl	Controls external device settings to	5.0.46~

14.2.5 Supported Linux

- Ubuntu 18 ~ 22
- Gooroom 2 ~ 3
- HamoniKR 3.0 ~ 4.0
- Tmax Gooroom 2, 21
- Hancom Gooroom 2 ~ 3

14.2.6 Supported Linux Plugins

Plugin Name	Description	Agent Version
Blank	Checks Condition Settings configured in Agent Action.	5.0.42~
InfoHW	Collects hardware information such as motherboard, memory and disk space to display in Node Information.	5.0.42~
InfoSW	Collects information about all installed software on the system.	5.0.42~
InfoNet	Collects information about all network interfaces and the open ports detected to display in Node information.	5.0.42~
InfoOS	Collects information about OS installed on the computer.	5.0.42~
NetIfCtrl	Disables a network interface when an anomaly is detected.	5.0.45~
UpdateOS	Checks for linux updates and report.	5.0.45~
InfoAV	Collects information about Antivirus software installed on the system.	5.0.46~
ProcessCtrl	Terminates a specific process defined in the action.	5.0.48~
ARPCtrl	Manages ARP table to prevent from ARP spoofing.	5.0.49~
DeployCtrl	Executes files or downloads files into a specific location.	5.0.50~

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 NAC 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
ESTSecurity	Alyac Enterprise	5.0.3
ESTSecurity	Estsecurity AIYak V2 V3	3.5.0
Hauri	ViRobot	5.0.3
Hauri	Virobot Desktop	5.0.3
Hauri	ViRobot Security 1.0	5.0.59
INCA	nProtect Anti-Virus/Spyware	5.0.3
SGA Solution	VirusChaser	5.0.3
Avira	Internet Security Suite	5.0.3
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

continues on next page

Table 2 – continued from previous page

Vendor	Product	Genian Version
F-Secure	F-Secure Anti-Virus	5.0.15
Kaspersky	Antivirus	5.0.3
Kaspersky	Kaspersky Endpoint Security	3.5.0
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
Trend Micro	APex One	5.0.42
Check Point	Endpoint Security	5.0.42

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_VideoController
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 /onboarding/apply-ap-profile

Creating Client Profile

For Creating AP Profile, please refer to /onboarding/apply-client-profile

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.

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 **Authentication Policy:**

1. For **Authentication Methods**, Select a method to authenticate a user.
2. For **2-Step Authentication**, Select a 2-Step Authentication method.

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 color.
4. For **Font Color**, Specify a font color.
5. For **HTML Help Message**, Specify a HTML Help Message.
6. For **URL Button**, Specify a link to embed in the authentication window, and a button caption.

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.
3. Click **Update.**

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

You can control wired and wireless network interfaces on end users Windows devices by disabling wired, wireless, bridged, and promiscuous mode. You can also send interface disabled event notifications with custom messages that appear as pop-ups.

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.
4. Enter in **Conditions**, optional settings.

Under **Disabling Network:**

1. For **Network Type**, specify the Network type to be disabled. (*Wired, Wireless, or both*)
2. For **Exceptions**, turn on to enable the exclusion of specified Network Devices.
3. For **Disabling Network Bridge**, turn on to disable any Network Bridge Interface regardless of the exclusion above.
4. For **Disabling Promiscuous**, turn on to disable any Promiscuous Interfaces regardless of the exclusion above.
5. For **Interface Disabled Event Notification**, optional messages sent to user from Interface Disabled Events.

Under **Enforcing Network Device Properties:**

1. For **Internet Connection Sharing**, select to disable the shared Internet Connection.
2. For **IPv6**, select to disable the IPv6 Interface Connection.
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.**

14.4.23 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**.

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.	internal-ssid

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 or to enter DNS manually.
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) • 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) • 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 NAC 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 Manage Files

You can manage files on the Windows devices by copying, deleting, moving, and renaming files. You can also run specific files.

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 Files** 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 **Source Path**, specify a source file to be managed.
2. For **Management Action**, specify action to take on source file. (*Run, Delete, Copy, Move, Rename*)
   - **CLI Parameter**, specify a command line parameter.
3. For **Account Options**, specify a account to manage file from drop-down.

4. For **Restart Options**, specify whether to Prompt or 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 **Manage Files** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**
12. Click **Update.**

14.4.34 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.**

14.4.35 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.**

14.4.36 Run Script

You can setup Batch or VB scripts to run 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 **Run Script** 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 **Script Format**, specify a script format to run. (*VB Script, Batch Script*)
2. For **Script**, type and enter script to be run.
3. For **Account Options**, specify an account to run a script from drop-down.
4. For **Restart Options**, specify whether to Prompt or 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 **Run Script** in the **Available** section. Select and drag it into the *Selected* section.
11. Click **Add.**
12. Click **Update.**

14.4.37 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.**

14.4.38 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.**

14.4.39 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

continues on next page

Table 3 – continued from previous page

Vendor	Product Name	Product Version
AVG Technologies CZ, s.r.o.	AVG AntiVirus Free	18.x
AVG Technologies CZ, s.r.o.	AVG Internet Security	18.x
Kaspersky Lab	Kaspersky Total Security	19.x
Kaspersky Lab	Kaspersky Total Security	20.x
Kaspersky Lab	Kaspersky Internet Security	19.x
Kaspersky Lab	Kaspersky Internet Security	20.x
Kaspersky Lab	Kaspersky Anti-Virus	19.x
Kaspersky Lab	Kaspersky Anti-Virus	20.x
Kaspersky Lab	Kaspersky Free	19.x
Kaspersky Lab	Kaspersky Free	20.x
Kaspersky Lab	Kaspersky Small Office Security	19.x
Kaspersky Lab	Kaspersky Small Office Security	20.x
Kaspersky Lab	Kaspersky Security Cloud	19.x
Kaspersky Lab	Kaspersky Endpoint Security	11.x
Kaspersky Lab	Kaspersky Security for Windows Servers	10.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
Kaspersky Lab	Kaspersky Total Security	19.x
Kaspersky Lab	Kaspersky Small Office Security	19.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
Kaspersky Lab	Kaspersky Small Office Security	19.x
F-Secure Corporation	F-Secure PSB Workstation Security	12.x

14.4.40 Deploy Files

You can deploy files in Windows by uploading a file to the Policy Server, or providing a download link. Additionally, this agent action allows for actions to be taken after the file is deployed.

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 **Deploy Files** 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. Set **Time Object**, **Retry Interval** and **Retry Attempts**
3. Select **Upload** or **URL** for the **File Deployment Method**.
   - If **Upload**: Use the prompt to upload the desired file to the Policy Server.
   - If **URL**: Use the prompt to specify a web address to download the file from.
4. For **Verifying Digital Signature**, select **On** or **Off**.
5. For **Post Deployment Action**, select **Run File** or **Download**.

   Files are deployed to **C:\Program Files\Geni\Genian\Patch** by default.
   - If **Run File**: Use the prompt to select an **Execution Path** + optional file name and a **Command Line Parameter** for the distributed file. For **Execution Account** select **Root** or **Logon Account**. For **Restart Options** select **Do Nothing**, **Prompt**, or **Restart**.
   - If **Download**: Use the prompt to specify a **Destination Path** and optional file name for the distributed file.
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 Network Information** in the **Available** section. Select and drag it into the **Selected** section.
11. Click **Add.**

12. 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.

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 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.**

14.5.8 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.**

14.5.9 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.**

14.5.10 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 NAC.

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
Kaspersky	Kaspersky Internet Security	5.0.9
Sophos	Sophos Endpoint	5.0.17
Sophos	Sophos Home	5.0.17
Symantec	Norton Antivirus	5.0.9

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.**

14.5.11 Deploy Files

You can deploy files in macOS by uploading a file to the Policy Server, or providing a download link. Additionally, this agent action allows for actions to be taken after the file is deployed.

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 **Deploy Files** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

Deploy Files

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Find and click **Deploy Files** in the Agent Action window.

Under **Settings** section:

1. Select **Upload** or **URL** for the **File Deployment Method**.
   - If **Upload**: Use the prompt to upload the desired file to the Policy Server.
   - If **URL**: Use the prompt to specify a web address to download the file from.
2. For **Verifying Digital Signature**, select **On** or **Off**.
3. For **Post Deployment Action**, select **Run App**, **Run File**, **Download** or **Install Package**.

   Files are deployed to **/Users/Shared/Genians/Resources** by default.

   - If **Run App**: Use the prompt to select an **Execution Path** + optional file name and a **Command Line Parameter** for the distributed file. For **Restart Options** select **Do Nothing**, **Prompt**, or **Restart**

- If **Run File**: Use the prompt to select an **Execution Path** + optional file name and a **Command Line Parameter** for the distributed file. For **Execution Account** select **Root** or **Logon Account**. For **Restart Options** select **Do Nothing**, **Prompt**, or **Restart**.
- If **Download**: Use the prompt to specify a **Destination Path** and optional file name for the distributed file.
- If **Install Package**: Use the prompt to select an **Execution Path** For **Restart Options** select **Do Nothing**, **Prompt**, or **Restart**.
- Leave forms blank to leave the file in the default location.

4. For **Excution Interval**, select a time to execute and if applicable, adjust Periodic Interval.(Seconds - Months).
5. Click **Update**

14.5.12 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.**

14.5.13 Controlling WLAN

Policy Server communicates with the Agent to collect SSID 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 **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.
     - **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. 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 WLAN** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

14.5.14 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.

NAC provides a plugin to manage ARP tables to solve these problems. Delete static ARP to prevent vulnerabilities bypassing NAC.

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.**

14.5.15 Manage Files

You can manage files in macOS by copying, deleting, moving, and renaming files. You can also run specific files.

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 **Manage File** in the **Available** section. Select and drag it into the **Selected** section.
6. Click **Add.**
7. Click **Update.**

Manage Files

1. Go to **Policy** in the top panel.
2. Go to **Policy > Node Policy** in the left Policy panel.
3. Find and click **Manage File** in the Agent Action window.

Under **General** section:

1. For **Manage Files**, 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" filed.

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. Select a **Management Action** for the source file: **Run App**, **Run File**, **Delete**, **Copy**, **Move**, **Rename**
2. For all Actions, define a **Source Path** , specifying the **source file** to manage.
3. Configure Action Specific options:
   - If **Run App**: Use the prompt to select a **Command Line Parameter**. For **Restart Options** select **Do Nothing**, **Prompt**, or **Restart**
   - If **Run File**: Use the prompt to select a **Command Line Parameter**. For **Execution Account** select **Root** or **Logon Account**. For **Restart Options** select **Do Nothing**, **Prompt**, or **Restart**.
   - If **Delete**: Proceed to the next step.
   - If **Copy**, **Move** or **Rename**: Define a **Destination Path**.
4. For **Excution Interval**, adjust Periodic Interval.(Seconds - Months)
5. 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.
    - **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 :

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.**

14.6 Controlling Linux

You can control Linux devices with the Agent installed using these plugins:

14.6.1 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.**

14.6.2 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.**

14.6.3 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.**

14.6.4 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.**

14.6.5 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.**

14.6.6 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.**

14.6.7 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.**

14.6.8 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 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.**

14.6.10 Manage ARP Table

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 **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:**

1. For **Deleting Static ARP Entries**, turn **On** to delete static ARP entries.
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 **Manage ARP Table** in the **Available** section. Select and drag it into the **Selected** section.
8. Click **Add.**
9. Click **Update.**

14.6.11 Deploy Files

You can deploy files in Linux by uploading a file to the Policy Server, or providing a download link. Additionally, this agent action allows for actions to be taken after the file is deployed.

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 **Deploy Files** 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 **Upload** or **URL** for the **File Deployment Method**.
   - **Upload**: Use the prompt to upload the desired file to the Policy Server.
   - **URL**: Use the prompt to specify a web address to download the file from.
2. For **Post Deployment Action**, select **Run File**, **Download** or **Install Package**.

   Files are deployed to **/usr/share/genians/resource** by default.
   - **Run File**: Use the prompt to select an **Execution Path +** optional file name and a **Command Line Parameter** for the distributed file. For **Execution Account** select **Root** or **Logon Account**.
   - **Download**: Use the prompt to specify a **Destination Path** and optional file name for the distributed file.
   - **Install Package**: Use the prompt to select an **Installation Path**

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 Network Information** in the **Available** section. Select and drag it into the **Selected** section.
9. Click **Add.**
10. Click **Update.**

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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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

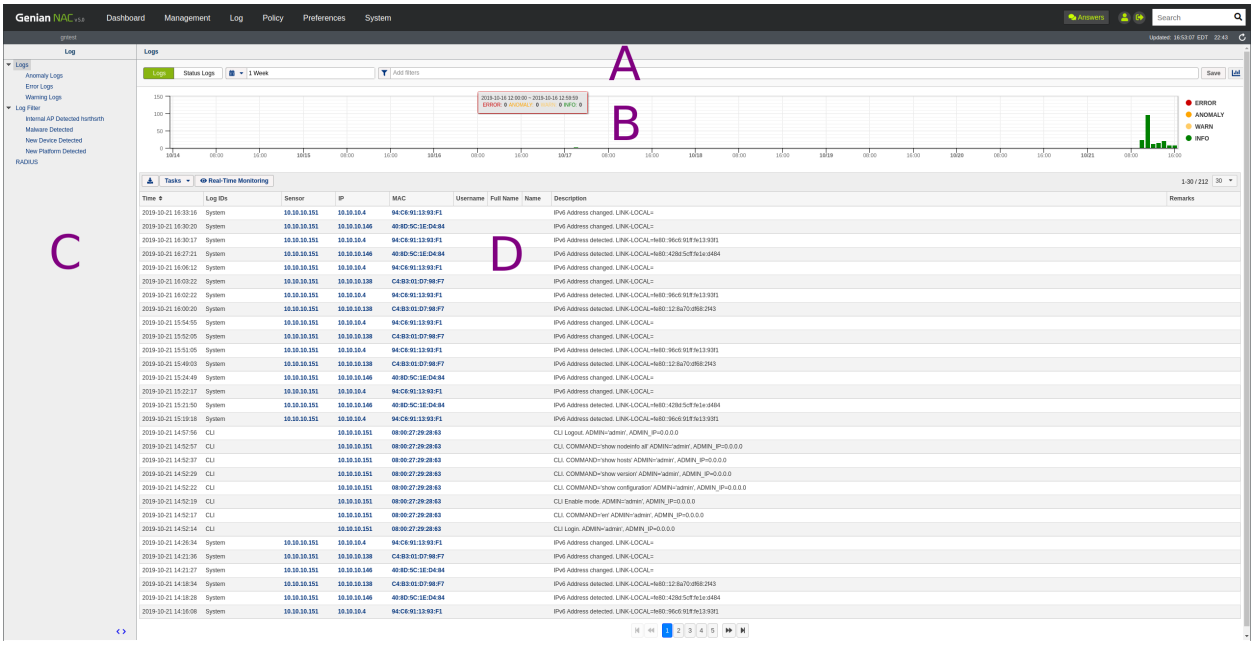
MANAGING LOGS AND EVENTS

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.



16.1 Managing Logs

You can find specific data by searching, filtering, tagging, and visualizing in real time. By default, Genian NAC 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 NAC 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 NAC 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 **Log** in the top panel.
6. Go to **Log Filter** in the left **Log** panel.
7. Find and click **Log Filter 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.

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 (2009/11/27 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)

16.2.2 Sending Logs

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*.

---

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 NAC, 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 NAC.
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 NAC with Slack using webhook. This integration provides the ability to send notifications for any Genian NAC 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 NAC log filter to send Posts to Slack

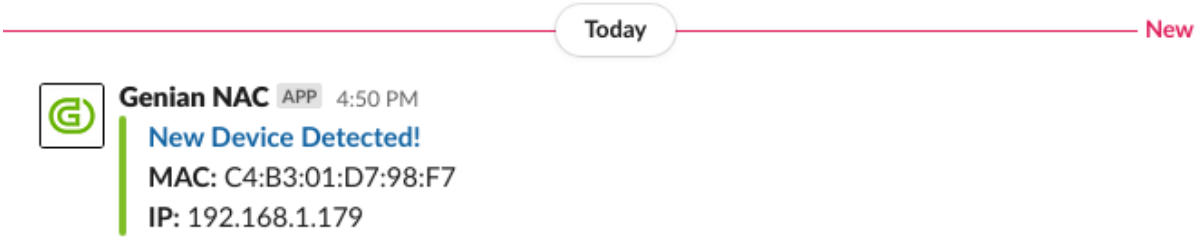
Slack App Configuration

The steps below demonstrate how to configure Slack to accept webhook Posts from Genian NAC.

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 NAC 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



These steps will select logs from Genian NAC, 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.

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 Shutdown and Restart System

Warning: To avoid system corruption, never remove device power source, or manually power off device before properly shutting down Genian NAC.

17.1.1 Control Power Through Web console

1. Click **System** in the Menu Bar.
2. Select the IP address of the desired device from the view pane.
3. Click the **Power** tab.
4. Click **Restart** or **Shutdown**

17.1.2 Control Power Through Command Line Interface

See: *Command Line Interface*

1. Connect to policy server or network sensor through command line.
2. Enter Global configuration mode.
3. To:
   - Restart: Enter command **restart system** or **reboot**
   - Shutdown: Enter command **shutdown service** or **halt**

Note: Device will remained powered on, but will now be safe to power off manually.

17.2 Managing Administrators

To manage administrative users, you can define administrative roles and assign a role to users.

By default, administrative roles are provided:

- **superAdmin**, Full Administrative Privileges
- **ipAppManager**, IP Address provisioning (The Enterprise Edition only)
- **Auditor**, Log and event analysis

17.2.1 Administrator Accounts

You can manage your Administrators by adding, deleting, and adding various restrictions

To Add Administrator

1. Go to **Management > User** in the top panel
2. Click **Tasks > Add User**

General

1. For **Username**, type a username
2. For **Name**, type in full name
3. For **Administrator Role**, select a optional Role for Administrator
4. For **Description**, type optional description
5. For **Purpose**, select **Disabled**
6. For **Status**, select **Enabled** (*You can choose **Disable** to disable the account temporarily)
7. For **Expiry**, click **Checkbox** and choose date and time by clicking in empty space

Password Reset

1. For **Password**, type password
2. For **Password Confirmation**, re-type password

Authentication Restrictions

1. For **Number of Auth IPs**, specify the number of authorized IPs this account can use (*0-256 or leave blank*)
2. For **Number of Auth MACs**, specify the number of authorized MACs this account can use (*0-256 or leave blank*)
3. For **Number of Auth Devices**, specify the number of authorized devices this account can use (*0-256 or leave blank*)
4. For **Auth IPs**, specify IP Addresses separated by commas or leave blank to not restrict
5. For **Auth MACs**, specify MAC Addresses separated by commas or leave blank to not restrict

6. For **Auth Node Groups**, specify Node Groups separated by commas or leave blank to not restrict

Setting Login

1. For **Web Console IP1**, Specify comma-separated IP addresses or enter them in CIDR form
2. For **Web Console IP2**, Specify comma-separated IP addresses or enter them in CIDR form
3. For **2-step authentication**, Select Text message or Google Authentication (OTP) or Disable to disable it
4. For **Time Zone**, Select the time zone for that administrator.
5. For **API Key**, If you are using the REST API, click the Generate API KEY button to generate the API key.

Notification

1. For **Notification Option**, Check if you want to receive notifications about user registration request, IP request, or external device request. The Administrator can receive an New event occurrence alarm for selected item.
2. For **Mobile Phone**, If you want to receive notifications by SMS, enter your phone number with your country code.
3. For **Email**, Enter an email to receive email notifications. (Required)

Management Restrictions

The management restriction setting is an item that you set when you create a non-Superadmin administrator account to restrict the permissions of the administrator account.

- Restricted administrator role to Sensor Manager, IP Manager, User Manager, etc.
- *Restrict administrator privileges*

Trusted Connection Settings

Set up a trusted client that calls the REST API externally.

1. For **IP Pattern**, Sets the IP pattern of trusted clients calling the REST API.
2. For **URL Pattern**, Sets the trusted URL pattern for REST API calls.

User Information

1. For **Company**, type Company Name
2. For **Department**, select optional department (*To create Department go to Users > Departments > Tasks > Create*)
3. For **Email**, type in Email address
4. For **Mobile Phone**, type in phone number using format of your choice (*e.g. 123-456-7890, or 1234567890*)
5. For **Job Title**, select optional Job Title (*To create Job Title go to Users > Job Titles > Tasks > Create*)
6. For **Telephone**, type in phone number using format of your choice (*e.g. 123-456-7890, or 1234567890*)

Note:

The administrator can receive **Find ID/PWD authentication mail, User Acconut/IP/External Device/User Change request approve mail, Node list's bulk action Send Email** by User Information Email.

Remove Administrator

1. Go to **Management > User** in the top panel
2. Find and click **Checkbox** of user to delete
3. Click **Tasks > Remove User**
4. Click **Ok**

Configure Administrator Role Options

activate, edit, or add a predefined Administrator Role.

- assign the registered administrator role to users.
- restrict menus and restrict permissions with detailed settings.

1. Go to Preferences in the top management menu.
2. Select **Administrator Role** in the left panel.
3. From the right screen, select Administrator.

Create Administrator Role

1. Click the Tasks > Create button.
2. For **General**, Administrator role ID, description, landing page URL, status, menu restrictions.
3. For **Permission Setting**, Detailed permission settings for systems, policies, administration, logs, and subscription systems.
4. Click Save botton.

Administrator role settings

1. Go to **Management > User** in the top panel
2. Click the user ID to assign the administrator role.
3. In the General entry, select the Role you want to assign a value for the Administrator Role option.
4. Click the Update button at the bottom.

- Specify permissions within Management Console.

17.2.2 Administrator Roles

You can manage Administrator Roles by creating, assigning, and removing them depending on your requirements. By default, 3 administrative roles are provided:

Role ID	Role Name	Description / Access Level
auditor	Audit Administrator	Log and event analysis
ipAppManager	IP Request System administrator	IP Application Administrator (Web Console X) (The Enterprise Edition only)
ipManager	Administrator for managing IP usage	IP Application/Approval (Web Console)
logAuditor	Audit log administrator	Read only access to the Logs Tab
mediaManager	External device usage administrator	Access to external device requests
nodeAuditor	Node audit administrator	Node Management menu and Log menu only
superAdmin	Super Administrator	Full Administrative Privileges
userManager	User Account administrator	Administrator role with access to User Management menu only
insightsConnector	Integration service role for Insights	Administrator role to integrate with the Genian EDR product InsightsE

To Create an Administrator Role

1. Go to Preferences in the top panel
2. Go to User Authentication > Administrator Role in the left Policy panel
3. Click Tasks > Create
4. Configure basic permission options. (More precise permission controls available on account level)
5. Click Save

To Assign an Administrator Role

1. Go to Management > User in the top panel
2. Find User and click Username
3. Under General tab, select Administrator Role from the drop down menu.
4. Click Update

To Delete an Administrator Role

1. Go to Policy in the top panel
2. Go to Group > User in the left Policy panel
3. Find User and click Checkbox
4. Click Tasks > Delete
5. Click Ok

17.2.3 2-Step Authentication

Genian NAC uses 2-Step Authentication (AKA 2 Factor Authentication , 2fa , mfa) with OTP Google Authenticator to add a second level of authentication to an account log-in. Once Google Authenticator is installed a QR Code will display so you can scan it with your smartphone or tablet. A six digit code will then be presented to then enter as the final step in your 2-Step Authentication. (*Google Authenticator six-digit code is continuously changing so enter it in quickly*)

Step 1. Enable 2-Step Authentication For Administrator Account

1. Go to **Management > User** in the top panel
2. Go to **Administrators** in the left User Management panel
3. Find and click **Username** of Administrator account in the main Administrators window
4. Find and click **Administrator** tab
5. Find **General: 2-Step Authentication** section in the main window
6. Click **OTP (Google Authenticator)** in drop-down
7. Find **Notification Options** section. Enter the following:
   - **Mobile Phone** (*e.g. 123-456-7890*)
   - **Display Phone Number** (*This is an optional number you want visible to sender*)
   - **Email** (*Multiple Email Addresses separated by commas*)
8. Click **Update**

Step 2. Enable 2-Step Authentication For The Policy Server

1. Go to **Preferences** in the top panel
2. Go to **General > Console** in the left Preferences panel
3. Find **Web Console: 2-Step Verification Methods** section in the main Console window
4. Click **Checkbox** for **OTP (Google Authenticator)**
5. Click **Update**

Step 3. Setup Google Authenticator

1. On your **Mobile Phone** go to **App Store** to download **Google Authenticator**
2. Logout from Policy Server UI and Login again
3. 2-Step Authentication wizard appears to setup Google Authenticator
4. Click **Start**
5. Select **Mobile Phone** type, **Android** or **iPhone**
6. Select **Application Method** to Install via **QR Code** (*QR Code will appear as an example*)
7. Click **OK** then **Next** (*Make sure you have Google Authenticator installed on Mobile Phone and ready to scan QR Code*)
8. Select **QR Code** in drop-down and then click **Generate Security Key**
9. Using **Mobile Phone** scan the **QR Code** that was just generated

10. Mobile Phone will present a **6 digit code** that you will need to remember and quickly enter it into the **Google Authenticator Wizard**
11. Click **OK**

17.3 Command Line Interface

17.3.1 Connecting to Command Line Interface

Web Console

For On-Premise Policy Servers Only:

Genian NAC allows you to connect to the CLI for an appliance directly from the Web Console. To connect, navigate to the **System** tab, and select the **Terminal Icon** in the **IP** column of the appliance you want to access. Authenticate with your administrator username and password. If your appliance is using a different admininstrator credential set than your Web Console, you must authenticate in the terminal using the appliance admininstrator credentials.

External Terminal

> **Attention:** External SSH access only allowed from Approved IP. See: *Initializing the System* to add approved remote access sources.

You can connect to the Genians policy server or network sensor from a dedicated SSH client or any command line with SSH support. Any other inbound connection attempts will be denied.

1. Use standard procedure for your chosen utility to select SSH connection to your Genian policy server or network sensor IP Address.
2. Log in with Genian NAC Username and password.

17.3.2 CLI Commands

The first connection of the equipment is divided into console mode and shell mode. In console mode, you can check basic system status and support configuration. This document identifies and describes how to use commands in console mode.

Basic Commands

Command	Explanation
enable	Enables Global Congifuration mode
exit	Exits the current mode
help	Displays available commands
history	Displays a list of past commands used
quit	Exits console mode
configure terminal	Global mode to set configurations immediately
configure batch	Global mode to set configurations after system restarts
clear arp	Deletes the system arp entry
clear screen	Initializes the display screen
clock set	Sets system date and time
do backup	Performs a system backup
do cdbackup	Performs a system backup to the connected optical disk
do cdrestore	Restores the backup file from the connected optical disk
do initdisk	Initializes the disk
do restore	Restores from a backup file
do cert-reissuance	Reissue Certificate
geniup	If a Genians Update Server is specified, proceed with the upgrade to the latest Server file
halt	Prepare the system power shutdown mode
kill pid	Terminates process based on pid
kill pname	Terminates process based on the name
ping	Generates an ICMP request for IP test to a remote device
reboot	Reboots the system
restart system	Restarts the OS
shutdown service	Terminates the Insights OS service
traceroute	Displays the routing path for IP
show	Proceed to show command section

Show Commands

Command	Explanation
show arp	Displays the IP to MAC address mapping
show backup	Displays the list of backup files
show configuration	Displays the current system configuration
Show cpu	Displays the CPU information
show filesystem	Displays the file system of the appliance
show hosts	Displays a list of hosts
show interface	Displays the network interfaces of the appliance
show logging	Displays a list of system logging messages
show memory	Displays the memory statistics
show processes	Displays the current running processes
show route	Displays the current configured routes
show sensor	Displays a list of sensors. Options: all/active/passive/unknown
show superadmin	Displays a list of configured administrator accounts
show time	Displays the current system time
show uptime	Displays how long system has been up and running
show version	Displays the current running system version

Inspecting and Searching Commands

You can view available commands by entering the **?** character into a blank terminal.

Example:

```
genian> ?
 exit                  Exit from current mode
 help                  Show available commands
 history               Show a list of previously run commands
 quit                  Exit from the console
 configure             Enter configuration mode
 clear                 Clear Operation
 clock                 Manage system clock
 disable               Turn off privileged command.
 do                    Do system command
 geniup                Upgrade system software
 halt                  Prepare to Power Shutdown mode
 kill                  Kill
 ping                  Send ICMP echo request
 reboot                Halt and perform a cold restart
 restart               Restart service
 show                  Show system information
 shutdown              Shutdown
 traceroute            Trace route information to destination
```

You can view the function of a command by entering the **?** character after an entered command.

Example:

```
genian> show?
 show                  Show system information
```

You can view available command modifiers by entering the **?** character after an entered command and a blank space.

Example:

```
genian> show ?
 arp                   ARP table
 backup                Database backup list
 configuration         Display the system configuration
 cpu                   Display cpu information
 dataserver            Display database server status
 dhcp                  Display the DHCP server information
 enforcer              Enforcer status and information
 filesystem            Filesystem statistics
 ha                    High Availability status
 hosts                 Static host table
 interface             Network interface status and information
 logging               Display system local logging message
 memory                Memory statistics
 nodeinfo              Node status and information
 processes             Active process list
 route                 Display system routing table
 superadmin            Display super administrator
 time                  Display the system clock
 uptime                Display system uptime
 version               System hardware and software information
```

17.4 Configuring Network

You can connect through command line console change the interface IP address, or configure the interface for DHCP

17.4.1 Configuring Interface IP Addresses

Note: Many common issues can be resolved by rebooting the appliance, which reloads your configurations, and purges outdated settings. After verifying configurations, rebooting is a good next step in troubleshooting.

Checking Interface IP Address

Before making changes, check the configuration of the interface.

Enter "show configuration | grep interface [interface name]" as seen below:

```
genian# show configuration | grep interface eth1
interface eth1 address 192.168.50.43 255.255.255.0
interface eth1 gateway 192.168.50.1
genian# exit
```

If an interface has an IP/ Gateway and DHCP enabled, it will not function. One must be removed.

Configure the Interface as a Static IP

To define an IP address and gateway for an interface(eth0, eth1, etc.) or sub interface(eth0.10, eth0.20,etc.):

```
genian> enable
genian# configure terminal
genian(config)# interface eth1 address X.X.X.X X.X.X.X
genian(config)# interface eth1 gateway X.X.X.X
genian(config)# exit
```

To Remove a Static IP from an interface:

```
genian> enable
genian# configure terminal
genian(config)# no interface eth1 address X.X.X.X X.X.X.X
genian(config)# no interface eth1 gateway X.X.X.X
```

Configure the Interface as a DHCP Client

To configure the interface or sub interface as a DHCP Client:

```
genian> enable
genian# configure terminal
genian(config)# interface eth1 dhcp enable
genian(config)# exit
```

To Remove DHCP Client Status from an interface:

```
genian> enable
genian# configure terminal
genian(config)# no interface eth1 dhcp enable
```

17.4.2 Add Alias IP to Sensor Interface

If there is more than one logical subnet in a broadcast domain (VLAN), you need to configure Alias IP on the sensor's interface so that it can be recognized.

Add Alias IP

Alias IP can only be configured on the Web console.

1. Go to **System** in top panel
2. Go to **System > System** in the left panel
3. Click desired Network Sensor IP
4. Click **Sensor > IP Address** tab
5. Click desired interface name for adding alias IP
6. Click **Add an Alias IP** button beside of Sensor IP
7. Enter following information for alias IP
    - IP Address: Management IP for sensor
    - Subnet Mask
    - Gateway
    - Managed IP Range : let this value blank if you want restricts unused IP addresses in the managed network
8. Click **Update**

Delete Alias IP

1. Go to **System** in top panel
2. Go to **System > System** in the left panel
3. Click desired Network Sensor IP
4. Click **IP Address** tab
5. Click desired interface name for adding alias IP
6. Click **Delete** link on desired alias IP under **Sensor IP**

17.4.3 Add Virtual IP to Sensor Interface

Virtual IP addresses may be configured on each sensor to aid in anomaly detection. Virtual IP addresses may be automatically assigned from the pool of unused IP addresses or manually assigned.

Adding Virtual IP Manually - Administrator can manually specify and add virtual IPs

Adding Virtual IP automatically - Unused IP are randomly assigned as virtual IPs by the number of Virtual Honeypot IPs configuration. - If the Administrator change a virtual IP numbers, Genian NAC check the existing virtual IPs and assign additional virtual IPs.

Virtual IP Conflict Prevention - Adding Virtual IP Manually : If the IP of the new node and the virtual IP are the same, the virtual IP will be automatically changed to unused IP. - Adding Virtual IP automatically : If the IP of the new node and the virtual IP are the same, the new node will not be registered.

Viewing Virtual IP Addresses

1. Go to **System** in top panel.
2. Go to **System > System** in the left panel.
3. Click desired Network Sensor IP.
4. Click **Sensor > IP Address** tab.
5. Assigned Virtual IP addresses will be displayed on Virtual Honeypot IP.

Enable or Disable Automatic Virtual IP Assignment

1. Go to **System** in top panel.
2. Go to **System > System** in the left panel.
3. Click desired Network Sensor IP.
4. Click **Sensor > Sensor** tab.
5. Click desired interface name of Virtual IP.
6. Under **Virtual Honeypot IPs** , enter the number of Virtual IP Addresses to automatically assign from the unused IP pool. Enter `0` to disable.
7. Click Update.

Adding Virtual IP Manually

1. Go to **System** in top panel.
2. Go to **System > System** in the left panel.
3. Click desired Network Sensor IP.
4. Click **Sensor > IP Address** tab.
5. Click desired interface name for adding Virtual IP.
6. Click **Add** button beside of Virtual IP.
7. Define the Virtual IP, and choose to **enable** or **disable**.
8. Click Update.

9. If desired, repeat to add additional Virtual IP addresses.

Removing Virtual IP Manually

1. Go to **System** in top panel.
2. Go to **System > System** in the left panel.
3. Click desired Network Sensor IP.
4. Click **Sensor > IP Address** tab.
5. Click desired interface name for adding Virtual IP.
6. Click the **Delete** text beside of the Virtual IP interface to be removed.
7. If desired, repeat to remove additional Virtual IP addresses.

17.4.4 Adding And Deleting Network Sensors

Note: Many common issues can be resolved by rebooting the appliance, which reloads your configurations, and purges outdated settings. After verifying configurations, rebooting is a good next step in troubleshooting.

As your network changes, you may add or delete sensors.

- If you add additional remote locations you can add Network Sensor Appliances to the sites.
- To monitor additional broadcast domains with an existing sensor, you may use multiple wired interfaces on that appliance if supported.
- For an Appliance with a single wired interface, you can monitor multiple VLANS over a 802.1Q trunk port by configuring sub interfaces.

Add Network Sensor Hardware

If you have added a new remote location, here are the steps to adding an additional Network Sensor hardware to your Policy Server.

1. Go to *Installing Genian NAC*. (*During the Installation, you will be prompted to link the Sensor with a Policy server IP or FQDN*)
2. After Installation, you should see **Network Sensor** in the UI Management pane under **System > System > Sensor**.

Delete Network Sensor Hardware

Note:

If you delete the network sensor, the connected VLAN and all node information are deleted together.

---

1. Disconnect **Network Sensor** hardware from the network and power down.
2. Access **Policy Server Webconsole** to delete Network Sensor.
3. Go to **System** in the top panel.

4. Go to **System > System** in the System Management panel.
5. Find and click on the **Checkbox** of desired Network Sensor.
6. Go to **Tasks > Delete System**.
7. Click **OK** to confirm.

Add Interfaces on an Existing Sensor

This option allows you to monitor separate LANs or VLANs on a single sensor appliance without the use of a trunk port. **One wired interface is required for each network.**

Network Sensors cannot be added through Webconsole, Administrator must be configured through CLI by adding sub-interfaces to the existing eth0 or eth1 interface.

1. Connect through **SSH client** to Network Sensor. See: *Administration Console* .
2. Enter the following commands below for each Network Sensor to be added:

For this example, interface eth0 is already configured. The interface eth1 will be configured to monitor a separate LAN:

```
genian> enable
genian# configure terminal
genian(config)# interface eth1 address X.X.X.X X.X.X.X
genian(config)# interface eth1 gateway X.X.X.X
genian(config)# exit
```

Or setup the interface as a DHCP client:

```
genian> enable
genian# configure terminal
genian(config)# interface eth1 dhcp enable
genian(config)# exit
```

Delete A Specific Network Sensor Interface

Note:

This deletes a single Network Sensor and all Nodes and Node information

1. Connect through **SSH client** to Network Sensor: *Administration Console*
2. Enter the following commands below for each Network Sensor interface to be removed:

```
genian> enable
genian# configure terminal
genian(config)# no interface eth1 address X.X.X.X X.X.X.X
genian(config)# no interface eth1 gateway X.X.X.X
genian(config)# exit
```

If the interface is configured as a dhcp client , use the following method:

```
genian> enable
genian# configure terminal
genian(config)# no interface eth1 dhcp enable
genian(config)# exit
```

1. Go to **System** in the top panel
2. Go to **System > Sensor** in the System Management panel.
3. Find and click on the **IP Address** of desired Network Sensor.
4. Find and click **Delete** in General tab.
5. Click **OK** to confirm.

Add VLANs (Sub-Interfaces) to an Existing Interface

This option is used when the Network Sensor is installed in trunk port mode. By configuring sub interfaces off of the main physical interface,up to 128 VLANs(Recommended 64 VLANs)configured on that trunk port may be monitored through a single physical interface. When added, a sub interface will show up in the Genians Web Console as a separate sensor/node. This is because for every VLAN that is monitored, an IP address will be assigned to the sensor within that VLAN.

Note:

Up to 128 VLANs can be added to Genian NAC, and more than 128 VLANS cannot be set. Genians recommends to set 64 VLANs.

- Ensure the Genians Network Sensor is connected to a properly configured .1q trunk port. See *"VLANs" in Preparing Network*
- Connect through **SSH client** to Network Sensor. See: *Administration Console*.
- Enter **ALL** VLANs you wish to monitor using commas to separate values and hyphens to denote ranges. Note that each Vlan ID will determine the suffix after `eth0.` in the sub interface name.

```
genian> enable
genian# configure terminal
genian(config)# interface eth0 vlan 10,20,30-50
```

- Enter the following commands below for each Network Sensor to be added:

```
genian> enable
genian# configure terminal
genian(config)# interface eth0.30 address X.X.X.X X.X.X.X
genian(config)# interface eth0.30 gateway X.X.X.X
genian(config)# exit
```

- Or configure the interface as a DHCP client.

```
genian> enable
genian# configure terminal
genian(config)# interface eth0.30 dhcp enable
genian(config)# exit
```

Note: If you want to monitor an untagged vlan, including the Native VLAN on a trunk/dot1q port, this can only be done on interface eth0. Specific VLAN interfaces (eth0.x) only monitor tagged traffic.

Delete A Specific VLAN Network Sensor

Note:

This deletes a single VLAN Network Sensor and all Nodes and Node information.

- Connect through **SSH client** to Network Sensor. *Administration Console*.
- Enter ALL VLANs you wish to monitor, and exclude the Vlan to be deleted.

```
genian> enable
genian# configure terminal
genian(config)# interface eth0 vlan 10,20,40-50
```

- Enter the following commands below for the Vlan Sensor Interface to be removed:

```
genian> enable
genian# configure terminal
genian(config)# no interface eth0.30 address X.X.X.X X.X.X.X
genian(config)# no interface eth0.30 gateway X.X.X.X
genian(config)# exit
```

- If the interface is configured as a DHCP client , use the following method:

```
genian> enable
genian# configure terminal
genian(config)# no interface eth1 dhcp enable
genian(config)# exit
```

1. Go to **System** in the top panel.
2. Go to **System > Sensor** in the System Management panel.
3. Find and click on the **IP Address** of desired Network Sensor.
4. Find and click **Delete** in General tab.
5. Click **OK** to confirm.

17.4.5 Change Network Sensor Interface Type

Note: Many common issues can be resolved by rebooting the appliance, which reloads your configurations, and purges outdated settings. After verifying configurations, rebooting is a good next step in troubleshooting.

Changing the network configuration may change the interface type of the network sensor from the access port to the trunk port, or vice versa. This chapter describes how to change the sensor interface type.

Access Port to Trunk Port

First, ensure the Genians Network Sensor is connected to a properly configured .1q trunk port. See *"VLANs" in Preparing Network*

Check existing interface configuration and save existing config. If there are any settings other than IP or Gateway on the interface you want to change, you must transfer the settings to the new interface.

Note: This example assumes that the physical interface is eth0.

```
genian# show config
...
interface eth0 address 192.168.50.22 255.255.255.0
interface eth0 gateway 192.168.50.1
interface eth0 management-server enable
interface eth0 node-server enable
interface eth0 radius-server enable
...
```

Create VLAN interface on physical interface

```
genian(config)# interface eth0 vlan 10,20,30-35                    // Replace by your␣
↪VLAN IDs separated by comma or hyphen
```

If your trunk port has a native VLAN, eth0 will be the native VLAN. any other VLAN interface name will be **ethX.VLANID**. If you don't have the native VLAN, You should delete eth0 interface settings.

```
genian(config)# no interface eth0 address X.X.X.X X.X.X.X
genian(config)# no interface eth0 gateway X.X.X.X
genian(config)# no interface eth0 management-server enable       // Optional
genian(config)# no interface eth0 node-server enable             // Optional
genian(config)# no interface eth0 radius-server enable           // Optional
```

Setup static IP of VLAN interface and Gateway

```
genian(config)# interface eth0.10 address X.X.X.X X.X.X.X
genian(config)# interface eth0.10 gateway X.X.X.X
```

Or setup DHCP (In case not using static IP)

```
genian(config)# interface eth0.10 dhcp enable
```

Restore other config for Management interface (Optional)

```
genian(config)# interface eth0 management-server enable
genian(config)# interface eth0 node-server enable
genian(config)# interface eth0 radius-server enable
```

Make sure all VLAN interfaces are properly setup ether static IP or DHCP.

To configure running network sensor on VLAN interface:

1. Login to administrator Web UI and go to **System** menu
2. Click Network Sensor IP and go to **Sensor** tab
3. Click interface name

4. Change **Sensor Mode** from **Inactive** to **Host**
5. Click **Update** on bottom

When an interface is removed from the CLI settings, any sensors or nodes that were registered in the management console are not automatically deleted. To delete a sensor that no longer exists and the node it detects, follow these steps:

1. Goto **System** menu
2. Select **System > Sensor** on left panel
3. Click **IP** on desired sensor (You can identified by interface name on hostname column)
4. Click **Delete** on bottom

Trunk Port to Access Port

Delete VLAN

```
genian(config)# no interface eth0 vlan 10,20,30-35  // Replace by your VLAN IDs␣
↪separated by comma or hypen
```

Delete all VLAN interface settings

```
genian(config)# interface eth0.X address X.X.X.X
genian(config)# interface eth0.X gateway X.X.X.X
```

Setup eth0 address, gateway and other settings

17.5 Configuring High Availability

Genians can be set up using two Appliances in a active/standby configuration, one acting as a primary while the other as a secondary. These two Appliances communicate with each other to synchronize data and will failover from one to the other in the event of a system failure.

- **Group –** VRRP Group ID
- **Linkupdelay –** Time to wait until interface is activated
- **No-Virtual-Mac –** Does not convert MAC Address info to Virtual-MAC when switching to Master
- **Nopreempt –** Device as Master takes precedence regardless of priority
- **Priority –** Priority Value. Highest Value is Master
- **Timeout –** Wait time for VRRP packet loss
- **Virtual-IP –** Shared IP for devices and UI

Note:

All-in-One (Policy Server + Network Sensor) is not supported.

17.5.1 Serial Connection to Server if SSH is not established

- Protocol: **Serial**
- Port: **COM1**
- Baud Rate: **115200** (*9600 for Mini-PC*)
- Data Bits: **8**
- Parity: **None**
- Stop Bits: **1**

17.5.2 How to configure Servers for High Availability

1. Connect the prepared equipment to the network.
2. Connect to each Server by connecting to Command Line Interface
3. Run a show configuration to see current configuration. (*Record Master Server device-id as this needs to be the same on both Policy Servers*)
4. Enter Global Config mode: config terminal
5. On each Server enter the following configurations:

17.5.3 Master Policy Server

```
1. Interactive Wizard
2. Manual Configuration

Select installation type: 2

Enter administrator username (4-31 characters) [admin]: admin

# Password must contain at least one alphabet, number and special character
Enter administrator password (minimum 9 characters): *********
Re-enter Password:

Welcome to Genian NAC
Username: admin
Password:
The privileged EXEC mode password is the same as the console login password.
For security reasons please change your password.

Type 'enable'to access privileged EXEC mode for password change.
genian> enable
Password:

genian(config)# hostname PRIMARY
PRIMARY(config)# interface eth0 address [IP address] [Subnetmask]
PRIMARY(config)# interface eth0 gateway [Gateway IP]
PRIMARY(config)# ip default-gateway [Gateway IP]
PRIMARY(config)# ip name-server [DNS IP]
PRIMARY(config)# data-server username [username]
PRIMARY(config)# data-server enable
PRIMARY(config)# data-server password [password]
```

(continues on next page)

(continued from previous page)

```
PRIMARY(config)# data-server access-list [Secondary DB IP,Admin IP]
PRIMARY(config)# data-server replica serverid 1
PRIMARY(config)# data-server replica enable
PRIMARY(config)# log-server enable
PRIMARY(config)# log-server cluster-peers [Primary Policy Server real IP,Secondary
↪Log Server real IP]
PRIMARY(config)# log-server publish-port eth0
PRIMARY(config)# interface eth0 management-server enable
PRIMARY(config)# interface eth0 node-server enable
PRIMARY(config)# interface eth0 ha priority 200
PRIMARY(config)# interface eth0 ha group 20
PRIMARY(config)# interface eth0 ha linkupdelay 30
PRIMARY(config)# interface eth0 ha nopreempt enable
PRIMARY(config)# interface eth0 ha timeout 20
PRIMARY(config)# interface eth0 ha virtual-ip [Virtual IP]

PRIMARY(config)# show configuration
cli-pass change interval 0D
cli-pass history num 0
cli-pass minimum age 0D

data-server enable
data-server password ******
data-server replica enable
data-server replica serverid 1
data-server username root

device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (*Use same device-id for both Policy
↪Servers*)

hostname PRIMARY

interface eth0 address [IP address] [Subnetmask]
interface eth0 gateway [Gateway IP]
interface eth0 ha group 20
interface eth0 ha linkupdelay 30
interface eth0 ha nopreempt enable
interface eth0 ha priority 200
interface eth0 ha timeout 20
interface eth0 ha virtual-ip [Virtual IP]
interface eth0 management-server enable
interface eth0 node-server enable

ip default-gateway [Gateway IP]
ip name-server [DNS IP]

log-server enable
log-server cluster-name GENIAN
log-server cluster-peers [Primary Policy Server real IP,Secondary Log Server real IP]
log-server publish-port eth0
```

17.5.4 Secondary Policy Server

```
1. Interactive Wizard
2. Manual Configuration

Select installation type: 2

Enter administrator username (4-31 characters) [admin]: [Admin ID]
# Password must contain at least one alphabet, number and special character
Enter administrator password (minimum 9 characters):
Re-enter Password:

Welcome to Genian NAC
Username: [Admin ID]
Password:
The privileged EXEC mode password is the same as the console login password.
For security reasons please change your password.

Type 'enable'to access privileged EXEC mode for password change.
genian> en
Password:
genian# configure terminal

genian(config)# hostname SECONDARY
SECONDARY(config)# device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (From PRIMARY
↪server)
SECONDARY(config)# interface eth0 address [IP address] [Subnetmask]
SECONDARY(config)# interface eth0 gateway [Gateway]
SECONDARY(config)# ip default-gateway [Gateway]
SECONDARY(config)# ip name-server [DNS]
SECONDARY(config)# data-server username [username]
SECONDARY(config)# data-server enable
SECONDARY(config)# data-server password [password]
SECONDARY(config)# data-server access-list [Primary DB IP,Admin IP]
SECONDARY(config)# data-server replica serverid 2
SECONDARY(config)# data-server replica enable
SECONDARY(config)# data-server replica masterhost [PRIMARY DB IP]
SECONDARY(config)# data-server replica username [PRIMARY DB username]
SECONDARY(config)# data-server replica password [PRIMARY DB password]
SECONDARY(config)# log-server enable
SECONDARY(config)# log-server cluster-peers [Secondary Policy Server real IP,Primary
↪Log Server real IP]
SECONDARY(config)# log-server publish-port eth0
SECONDARY(config)# interface eth0 management-server enable
SECONDARY(config)# interface eth0 node-server enable
SECONDARY(config)# interface eth0 ha priority 100
SECONDARY(config)# interface eth0 ha group 20
SECONDARY(config)# interface eth0 ha linkupdelay 30
SECONDARY(config)# interface eth0 ha nopreempt enable
SECONDARY(config)# interface eth0 ha timeout 20
SECONDARY(config)# interface eth0 ha virtual-ip [Virtual IP]

SECONDARY(config)# show configuration
cli-pass change interval 0D
cli-pass history num 0
cli-pass minimum age 0D
```

(continues on next page)

(continued from previous page)

```
data-server enable
data-server access-list [Admin IP]
data-server password ******
data-server replica enable
data-server replica masterhost [PRIMARY DB IP]
data-server replica password ******
data-server replica serverid 2
data-server replica username [username]
data-server username [username]

device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

hostname SECONDARY

interface eth0 address [IP address] [Subnetmask]
interface eth0 gateway [Gateway]
interface eth0 ha group 20
interface eth0 ha linkupdelay 30
interface eth0 ha nopreempt enable
interface eth0 ha priority 100
interface eth0 ha timeout 20
interface eth0 ha virtual-ip [Virtual IP]
interface eth0 management-server enable
interface eth0 node-server enable

ip default-gateway [Gateway]

log-server enable
log-server cluster-name [Cluster name]
log-server cluster-peers [Secondary Policy Server real IP,Primary Log Server real IPP]
log-server publish-port eth0
```

17.5.5 Primary Sensor

```
device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

interface eth0 vlan 10,11,12
interface eth0.10 address [IP address] [Subnetmask]
interface eth0.10 gateway [Gateway]
interface eth0.10 ha group 100
interface eth0.10 ha priority 200
interface eth0.11 address [IP address] [Subnetmask]
interface eth0.11 gateway [Gateway]
interface eth0.12 address [IP address] [Subnetmask]
interface eth0.12 gateway [Gateway]

ip default-gateway [Gateway]
ip name-server [DNS]

node-server ip [Policy Server IP]
```

17.5.6 Secondary Sensor

```
device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

interface eth0 vlan 10,11,12
interface eth0.10 address [IP address] [Subnetmask]
interface eth0.10 gateway [Gateway]
interface eth0.10 ha group 100
interface eth0.10 ha priority 100
interface eth0.11 address [IP address] [Subnetmask]
interface eth0.11 gateway [Gateway]
interface eth0.12 address [IP address] [Subnetmask]
interface eth0.12 gateway [Gateway]

ip default-gateway [Gateway IP]
ip name-server [DNS IP]

node-server ip [Policy server IP]
```

Attention:

Network Sensor HA is available in the multi VLAN environment.
And the failover condition is as below.
- When the Network Sensor is down.
- When the link or interface between Network Sensor and Switch is down.
- If HA is enabled on all VLAN interfaces, failover proceeds if even one interface is down.

17.5.7 How to test HA

```
———————PRIMARY————————
PRIMARY# show ha Status

Status: MASTER
Priority: 200
Group: 50
LinkupDelay: 30
Timeout: 10
Preempt: 0
VirtualIP: [Virtual IP]

———————SECONDARY————————
SECONDARY# show ha Status

Status: SLAVE
Priority: 100
Group: 50
LinkupDelay: 30
Timeout: 10
Preempt: 0
VirtualIP: [Virtual IP]
```

17.5.8 How to test DB replication

```
------PRIMARY------
PRIMARY(config)# show dataserver replicastatus
Replication health is good. (Confirm left message is displayed)
==================== Primary Replication Status ====================
Host                      : [Master DB IP displayed]
File                      : mysqld.000009
**Position                  : 123456 (The log position value between the two servers
↪must increase equally.)

==================== Secondary Replication Status ====================
Host                      : [Slave DB IP displayed]
Slave_IO_Running          : Yes
Slave_IO_State            : Waiting for master to send event
Slave_SQL_Running         : Yes
Slave_SQL_Running_State   : Slave has read all relay log; waiting for the slave I/O
↪thread to update it
Master_Log_File           : mysqld.000009
Read_Master_Log_Pos       : 123456 (The log position value between the two servers
↪must increase equally.)
Relay_Master_Log_File     : mysqld.000009
Exec_Master_Log_Pos       : 123456
Last_Errno                : 0
Last_Error                :
Last_IO_Errno             : 0
Last_IO_Error             :
Last_SQL_Errno            : 0
Last_SQL_Error            :
Relay_Log_File            : mysqld-relay-bin.000026
Relay_Log_Pos             : 123456
 ------SECONDARY------
SECONDARY# show dataserver replicastatus
Replication health is good.(Confirm left message is displayed)

==================== Primary Replication Status ====================
Host                      : [Master DB IP displayed]
File                      : mysqld.000009 (Check Primary Replication Files)
Position                  : 123456 (Check Primary Replication Position)

==================== Secondary Replication Status ====================
Host                      : [Slave DB IP displayed]
Slave_IO_Running          : Yes (Must be marked as YES)
Slave_IO_State            : Waiting for master to send event
Slave_SQL_Running         : Yes (Must be marked as YES)
Slave_SQL_Running_State   : Slave has read all relay log; waiting for the slave I/O
↪thread to update it
Master_Log_File           : mysqld.000009 (Verify that it is the same as the primary
↪replication file)
Read_Master_Log_Pos       : 123456
Relay_Master_Log_File     : mysqld.000009
Exec_Master_Log_Pos       : 123456
Last_Errno                : 0
Last_Error                :
Last_IO_Errno             : 0
Last_IO_Error             :
Last_SQL_Errno            : 0
```

(continues on next page)

(continued from previous page)

```
Last_SQL_Error           :
Relay_Log_File           : mysqld-relay-bin.000026
Relay_Log_Pos            : 123456
```

Attention: Please run the Database Replication confirmation command at Primary and Secondary respectively.

17.5.9 Bonding Configuration

Bonding is a technology that logically combines multiple physical interfaces into one logical interface. Bonding is used to increase service availability in case that one physical interface fails.

Bonding settings

Policy Server & Network Sensor

```
genians(config)#interface bond0 slave eth0,eth1
genians(config)#interface bond0 address [PolicyServer IP] [Subnetmask]
genians(config)#interface bond0 gateway [gateway IP]
genians(config)#bonding parameters mode=1

#Bonding parameter#
#mode=0: for balance-rr
#mode=1: for active-backup (recommended)
```

Warning:

- No settings should exist on the interface prior to the Bonding setting.
- Equipment reboot is required to apply the Bonding parameters setting.
- In some environments (virtual appliances) using Bonded interfaces, the function of other non-bonded interfaces may be impaired.

Checking Bonding Interface Status

Bonding interfaces have statuses in the form of Active/Active, Active/Backup. Below is an example of how to check the current status, and an example output:

```
Genians$ cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: load balancing (round-robin)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth1
MII Status: up
```

(continues on next page)

(continued from previous page)

```
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:0c:29:21:be:a9
Slave queue ID: 0

Slave Interface: eth2
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:0c:29:21:be:b3
Slave queue ID: 0
```

17.6 Initializing the System

Genian NAC Appliances, and logical components such as Policy Servers, Network Sensors and Wireless Sensors may be configured individually. Settings include OS Update Proxy, SSH Access Restrictions, SNMP Agent, Hardware Usage Alerts, System Time and log management.

Default Settings are configured for both Network Appliances and Sensors, this allows configurations to be cloned onto other Network Appliances and Sensors when added onto the network. This eliminates the need for the Administrator to configure each one. As a Remote Site is added and a Network Sensor is installed it will inherit the configurations from the Network Appliance settings. If Additional VLANs are configured then these VLANs will inherit configurations from the Sensor settings. These settings are optional and can later be reconfigured on individual appliances.

17.6.1 Device Appliance Automatically

When Genian NAC Device is first registered, the administrator must change the appliance configuration for the device registered.

If you are in an environment where multiple network sensors are registered, you can specify the initial settings so that the preferences are automatically applied when registering new equipment.

1. Go to **System** in top panel
2. Go to **System Defaults > Network Appliance** in the left System Management panel

---

Note: The above settings are optional and will be the default settings for all additional policy servers.)

Configure Appliance Settings

1. Go to **System** in top panel
2. Find and click **Policy Server IP** in the main System window
3. Find and click **Appliance** tab in the main System window

Allow Remote Access via SSH

1. Find **Security** section and enter **Approved SSH Source IP**
   - Individual IP's may be allowed(*e.g. 192.168.1.10*).
   - Entire Subnets may also be allowed, regardless of individual IP. (*e.g. 192.168.1.0/24*).
   - Access from all sources may also be permitted (*e.g. 0.0.0.0/0*).

   Note: Be mindful of NAT when accessing an appliance across network segments. The external NAT address must be allowed.

2. Click **Update**

Proxy For Windows Updates

1. Find **Proxy** for **Windows Updates** section and select **On** in drop-down
2. Select **Network Group** for Proxy Service to use
3. Click **Update**

Setup SNMP Agent

1. Find **SNMP Agent** section and select **On** in drop-down
2. Enter the following:
   - **Username**
   - **Authentication Password** (*SHA, minimum length – 8 characters*)
   - **Privacy Password** for data encryption (*AES, minimum length – 8 characters*)
3. Click **Update**

Edit Asset Management Thresholds

1. Find **Asset Management** section
2. Enter the following:
   - **Data Disk Threshold** generates log if Data Disk is over this threshold (*Default is 90*)
   - **Memory Threshold** generates log if Memory is over this threshold (*Default is 90*)
   - **CPU Threshold** generates log if CPU is over this threshold (*Default is 95*)
3. Click **Update**

Edit System Date And Time

1. Find **Date** and **Time** section
2. Select **Country** and closest **City** from drop-downs for **System TimeZone**
3. Click **Update**

Change Character Set

1. Find **Miscellaneous** section
2. Select **Character Set** from drop-down
3. Click **Update**

Configure Sensor Log Settings

1. Go to **System** in the top panel
2. Select **Network Sensor IP** in the view pane.
3. Select the **Appliance** tab in the view pane.

Under: **Miscellaneous** Configure:

- Default Character Set
- Sensor Debug Logging
  - Log Location - (**Local**, **Policy Server**, **Local & Policy Server**)

Note: If logging is set to save to the Policy Server, individual log entries will be sent by Syslog over TLS using port 6514. If Syslog over TLS fails, standard syslog on port 514. For Cloud-Managed NAC, **Unique Ports** are used. You can check these port assignments under **System > Service > Port**

17.6.2 Network Sensor Settings Automatically

configure preferences for all network sensors that are added since the policy server is configured.

Initial settings are optional, and subsequently unique settings for individual network sensors can be changed on each sensor.

Configure Sensor Default Settings

This will be the initial sensor setting for the network sensor to be registered in the future.

1. Go to **System** in the top panel
2. Go to **System > System Defaults > Network Sensor** in the left System Management panel, and set the applicable options:
   - Sensor Operater

Specifies the mode in which the network sensor operates. Depending on your network environment, you can set it up as a combination of operation mode and operation mode as follows:

Sensor Mode	Sensor Operating Mode	Description
Inactive	Monitoring / Enforcement	Network sensors do not work regardless of operating mode when network sensor behavior mode is inactive setting
Host	Monitoring	Network Sensor Management Scope Perform only scans of the network; do not perform network control (recommended)
Host	Enforcement	Network Sensor Management Scope Perform scanning and network enforcement for the network (recommended)
Mirror(local)	Monitoring	Network Sensor Management Scope Perform traffic monitoring only for the network; do not perform network control
Mirror(local)	Enforcement	Network Sensor Management Scope Perform traffic monitoring and network control over the network
Mirror(Global)	Monitoring	Network Sensor Inoperative
Mirror(Global)	Enforcement	Perform network control over IP communications outside the network sensor's management scope

- **Traffic Monitoring:** *(Mirror Only)*
  - Collection Interval
  - Time for Average
  - Minimum Update Value
  - Update Fluctuation
  - Destination based Status Collection
- **Node Registration:**
  - Maximum Registration for a MAC
  - IP Utilization Alert
- **Node Information Scan:**
  - Port / Service Scan: Configure options for SNMP, WMI, and NMAP scanning
  - NetBIOS Name Queries
  - Scan Interval
- **Network Scan:**
  - DHCP Server Scan
  - UPNP Scan
  - HP SLP Scan
  - SIP Scan
- **Node Status Scan:**
  - MAC+IP Clone Detection
- **Subnet Node Scan:**

  - Execution Interval
  - Scans per Second
- **DHCP:**
  - DHCP Service
  - DHCP Node IP Update
- **Virtual Honeypot IP:**
  - Virtual Honeypot IPs
- **IPAM:**
  - New Node Policy
  - Sensor IP Conflict Prevention
- **Miscellaneous:**
  - MAC Exception

Configure Sensor Log Settings

1. Go to **System** in the top panel
2. Select **Network Sensor IP** in the view pane.
3. Select the **Appliance** tab in the view pane.

Under: **Miscellaneous** Configure:

- Default Character Set
- Sensor Debug Logging
  - Log Location - (**Local**, **Policy Server**, **Local & Policy Server**)

Note: If logging is set to save to the Policy Server, individual log entries will be sent by Syslog over TLS using port 6514. If Syslog over TLS fails, standard syslog on port 514. For Cloud-Managed NAC, **Unique Ports** are used. You can check these port assignments under **System > Service > Port**

17.7 Managing Backup And Restore

You can schedule backups to run automatically, and restore from backups in the event of system failure.

Note: This option is not available in Cloud Version

17.7.1 Configuring Backup

Schedule Recurring Backup Time

1. Go to **Preferences** in the top panel
2. Go to **General > Backup** in the left Preferences panel
3. Find **Backup** section in the Backup window. Click **On** for Scheduled Backup
4. Specify **Time** to have Backup recur
5. Specify **Threshold** for minimum disk volume
6. Click `Update`

Configure the Repository Type

1. Go to **Preferences** in the top panel
2. Go to **General > Backup** in the left Preferences panel
3. Find **Backup** section in the Backup window. Select proper **Type** from drop down
4. Click `Update`

Store Type	Description & Value
Local Disk	Save to Policy Server Local Disk
External Storage(External HDD, SSD, etc)	Save to an external USB-type attached disk on the policy server
CIFS Storage	Perform a CIFS-enabled backup using Windows Sharing.
NFS Storage	Mount directories on Unix or Linux file systems to perform backups.
FTP SERVER	Transfer backup files via File Transfer Protocol (FTP). (For security reasons, it is not recommended that passwords be passed in plain text)
SFTP SERVER	Transfer backup files via Secure File Transfer Protocol (SFTP) (recommended for secure encryption based on SSH)

Note: If you specify a storage device in a backup file as a type other than a local disk, you can respond to the loss of backup files when the Backup File Retention setting is set to ON.

17.7.2 Restoring From Existing Backup

Locate a Backup File and Restore

1. Click **Preferences** in the top panel
2. Go to **Configuration > Backup** in the left panel
3. Click **Download Backup File** button
4. Copy **Backup** file that you want to restore from the list and then exit out

5. Login to Policy Server through CLI Connecting Command Line Console
6. Type **enable** and **Admin Password** to get into **Global Mode**
7. Enter "do restore <filename> all" to restore backup

Restore from HA Configuration

If HA is configured, please contact Slack

17.8 Setting up Outbound Mail Server (SMTP)

This function supports Email alerts, and log alerts which are configurable under administrator profiles and log filters.

17.8.1 Setup Email Account

1. Go to **Preferences** in the top panel
2. Go to **General > Miscellaneous** in the left **Preferences** panel
3. Choose Mail Server type: **Not Used** (disabled) or **SMTP** or **Google Mail**

SMTP

1. **Server Address** : type server address (*e.g. smtp.gmail.com*)
2. **Server Port** : type port number (*e.g. SMTP = 25, SSL = 465, TLS / STARTTLS = 587*)
3. **Sender Address** : type address for sender (*Email Address to be displayed as from*)
4. **Sender Name** : type name of sender (*Name to be displayed as from*)
5. **Connection Security** : Choose same server port type with **Server Port** option.
6. **Username** : type username
7. **Password** : type and re-type password
8. **Default Country Code** : choose default country code for sending an SMS
9. Click **Update**
10. Click **Test** to test configuration settings and send e-mail

Google Mail

1. **Sender Address** : type address for sender (*Email Address to be displayed as from*)
2. **Sender Name** : type name of sender (*Name to be displayed as from*)
3. **Authorization** : Request Authorization Code
4. **Authorization Code** : Enter an Authorization Code you copied.
5. **Default Country Code** : choose default country code for send a SMS
6. Click **Update**

7. Click **Test** to test configuration settings and send e-mail

17.9 Managing Requests

Depending on the type of request provided by Genian NAC, different forms can be used. You can change the request input according to the purpose(request type) or change the administrator's approval method, so that the user can receive additional information or grant approval rights to non-administrators.

17.9.1 Setting Property Values for User Purposes

You can change the request inputs according to the purpose so that the user can receive additional information or change the request approval method to grant approval rights to non-administrators.

The items that can be set in user purpose are divided into request processing options, application information input in request, and account information input in request.

1. Go to **Preferences** in the top panel.
2. In the left **Properties** column, select **Purpose > User** .
3. Select **Create** in the **task** menu.

User Request Processing Options

The request processing option sets the approval method for the request.

You can select one approval method from the following:

Method	Explanation
Approval using the Approval menu	Only **Administrator Account** with approval authority can approve requests
Email Approval	Approval authority can be subdivided into **Administrator** and **Applicant** (objects with user accounts)
Instant Approval	No separate request approval, all requests are granted automatically.

Enter Request Field

Request Field can be set to use the items defined in Genian NAC. Through the Request Field item, the purpose of use and period of use can be received from the applicant, and the item to receive the request approval result can be specified.

Field	Usage
Description(Reason)	Request input the reason for applying for a user account.
Mobile Notification (AlarmMoblie)	Requests the applicants Mobile Phone #, which can be used for approval notification (SMS settings required)
Expiry(UserUsePeriodDate)	The applicant can set the validity period for the user account they are requesting.
Email(AlarmEmail)	Requests the applicants Email Address, which can be used for approval notification (Mail Server settings required)

Enter User Information Field

User Information Field can collect items defined as account information and values defined through custom fields as input from users.

For custom field related parts, please refer to extend-field-user.

17.9.2 Setting Property Values for IP Request Purposes

The IP Request System can be used for asset and user management in environments where IP's are statically assigned, or where additional oversight to IP assignment is need.

You can change the request input according to the purpose to receive additional information, or change the administrator's approval method to grant approval to non-administrators.

The items that can be set in the application are divided into the application approval method, processing option, and application information input.

The purpose of IP request can be set for IP request, IP Return, Device Change, and User Change, and each item provides the following functions.

1. Go to **Preferences** in the top panel.
2. Select **Purpose > Request** from the **Properties** column on the left.
3. Select one of **IP request, IP Return, Device Change, or User Change** according to the purpose of creation.
4. Select **Create** in the **task** item.

Item	Explanation
IP Request	Request to be assigned an IP and can be set for multiple purposes.
IP Return	Requesst to Return IP (remove association between the IP and the User/Device associated).
Device Change	Request to change which MAC is approved to use a specific IP.
User Change	Request to change user account is approved to use an IP.

Setting the Approval Method for IP Request Purposes

This is to set the approval method for IP request. **Approval authority is granted to non-administrators by setting the approval method.**

You can select one approval method from the following:

Method	Explanation
Instant Approval	No separate request approval, all requests are granted automatically.
Email Approval + Instant Approval	Approval occurs after the request email is answered.
Email Approval	After the request email is answered, additional administrator approval is required.

IP Request Approval Settings

You can specify the processing method according to the purpose in the IP request item.

Method	Explanation
IPAM Policy for Request	IPAM policy (Allow) is applied when request is apporved.
IP host number (Range Start)	Set the first IP number in the IP band that can be assigned an IP
IP host number (Range End)	Set the last IP number in the IP band that can be assigned an IP
Authentication for IP User	Set limits on which users can use the assigned IP
Hostname Rule	Set hostname requirements for which devices can use the IP
Updating Department IP Ownership	When applying for IP use on a department-based basis, change the ownership department assigned to the existing IP
IP Request with Denied MAC	Delete existing node registered with the same MAC when request is approved
Node Group	Specify which User Groups can use the IP
User Group	Specify which User Groups can use the IP

Request Field Options

Request Field Options allows you to set items created by Request in custom fields. It is possible to collect any value input from the user rather than the IP request input information defined through the custom field.

For custom field related parts, please refer to extend-field-ipm.

17.10 Editing System Messages

Genian NAC provides the ability to change multilingual (Korean, Japanese, English, Chinese) messages displayed in the Genian NAC system.

You can use the Change Message feature to insert or change words and phrases to suit your site.

1. Go to **Preferences** in the top panel.
2. Select **Message** in the **Captive Web Portal** item on the left.
3. Click on the **Message ID** you want to change.
4. Edit the **Message content** corresponding to the **Language** you want to change. (Korean, Japanese, English, Chinese)

5. Click the **Update** button.

17.10.1 Check Message Status

Message classification can be divided into system message and application mode (only on/off toggle is displayed) setting message, each of which can be used as follows.

Status*	Explanation
System Message	Always enabled, but the content of the message can be changed.
Application Mode	Can be disabled, and the content of the message can be changed.

17.10.2 Check Message Type

Messages are categorized by the following types:

Type	Explanation
Web Console	Requests and System Messages provided shown in the Web console.
CWP	Messages related to node status shown in the CWP page.
Agent	Messages shown in the agent pop-up notification window.
Log	Messages shown in the Policy Server audit record.
Message	Notification messages related to user authentication.

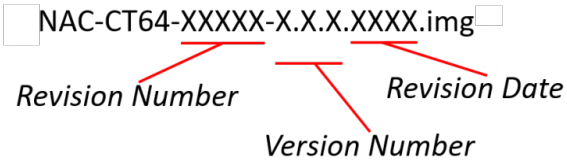
17.11 Managing System Software

> **Warning:** Updates are only available for licensed Policy Servers with an active Maintenance subscription.

17.11.1 Checking System Software Versions

Software packages are identified by four parts. Name, Revision Number, Version Number, and Revision Date.

- **NAC-CT** – Policy Server Software
- **NAC-SS** – Sensor Software
- **NAC-AGENT** – Agent Software



In addition to the software installed on the Policy Server or the Network Sensor, the Policy Server may also store a software image to be used for updating at a later time. For example, a Policy Server with version 5.0.19 installed may have a copy of Version 5.0.20 that can be used for updating the Policy Server, Network Sensors, or Agents at a later time.

System > Update > Genian Software will display the newest version of software stored on your Policy Server, even if it is not installed.

You can see the software version installed on individual Policy Servers and Sensors by navigating to **System** in the top panel. All appliances will be shown in the view pane along with the installed software.

Updating Policy Server and Network Sensor

You can update the Policy Server and Sensor through the WEBUI or CLI.

Note: For **Genians Cloud Managed Edition** the Policy Server, will update automatically. Network Sensor upgrades must be manually initiated.

Update the Policy Server and Sensor Automatically

1. Go to **System** in the top panel
2. Go to **Update > Genian Software** in the left System Management panel.
3. Find **Available Version** software in Genian Software window. Click **Update from Genian Cloud**
4. Select either **Download Only** retrieve the update and install manually, or **Download and Apply** to automate the installation to all eligible components.
    - If choosing **Download Only**: See steps 7-13 under "Update the Policy Server and Sensor Manually"

Update the Policy Server and Sensor Manually

This is done by obtaining Genian NAC Software from Genians and storing it locally on your machine to then upload onto the servers.

Prepare System Files for upload

1. Extract contents from the .iso file.
2. **Select desired software version from the /images directory in the .iso.**
    - For **Policy Server**, select file beginning with **NAC-CT** (*Includes network sensor files*)
    - For **Network Sensor**, select file beginning with **NAC-SS**

Update the Policy Server and Sensor by WEBUI

1. Go to **System** in the top panel
2. Find **Update** section in the left System Management panel. Go to **Genian Software**
3. Find and click **Upload File** button in Genian Software window
4. Click **Select File** in Upload window
5. Locate **Genian Software** in **File Upload** window. Double click on desired file
6. Click **Upload**
7. Go to **System** in the top panel
8. Go to **System > System** in the left System Management panel
9. Find **Policy Server/Sensor** in System window. Click **Checkbox**

10. Click **Tasks**
11. Click **Update Specific System Image** (*If you selected Policy Server and ALL sensors in Step 9, Click Update Latest System Images*)
12. **Enable** or **Disable** Database Backup before upgrade.
13. System will automatically update and reboot.

Update the Policy Server and Sensor by CLI(Command Line Interface)

Genian NAC provides updates to policy servers and network sensors through the CLI.

Genians highly recommends CLI upgrades for following case:

- Upgrade server separately, such a Policy server or DB server
- HA configuration

CLI update Command : `geniup`

Command Option

- `-h` : help
- `-f [image filename]` : Update software image from file
- `-u [URL]` : Specify image URL
- `-d` : Allow downgrade
- `-c` : Don't check image validation (Package, Owner)

1. Connect SSH with terminal emulator that supports Zmodem.
2. Use command `rz` and upload an image file on server.

```
Genians$ cd /tmp
Genians$ rz
```

3. Use `geniup` command and options to proceed with the upgrade.

```
Genians$ geniup -cf [image filename]
System software upgrade from
Current Version :
Target Version  :
Do you want to upgrade this target version ? (y/N):
Do you want to backup current database ? (Y/n):
Do you want to restart system after upgrade ? (Y/n):
```

For the details, please check the *Command Line Interface* documents.

Warning: Genians highly recommends a backup be completed prior to performing a CLI upgrade.

Upgrade methods by Configuration

How to upgrade Policy Server/Network Sensor

Different version of policy server and network sensor may cause abnormal operation. Please upgrade both server to the same version.

1. Access shell mode by typing `@shell`
2. Stop Policy server service.

```
Genians$ alder stop
```

3. Upgrade Policy server (Don't reboot policy server).
4. Upgrade Network sensor.
5. Reboot Policy server.

How to upgrade Individual Policy Server/DB Server

The DB Server should not be upgraded during the Policy server upgrade process.

1. Access to shell mode.
2. Stop Policy server service.

```
Genians$ alder stop
```

3. Upgrade DB server.
4. Reboot DBserver.
5. Upgrade Policy server.

Note:

The policy server and the DB server do not necessarily have to be the same version. Please refer to the release note and check the DB server revision before performing an upgrade.

How to upgrade HA configuration

The Master system should not be changed during the upgrade process.

1. Upgrade Slave server (Don't reboot policy server).
2. Stop Slave server service

```
Genians$ alder stop
```

3. Upgrade Master server
4. Reboot Master server
5. Reboot Slave server

Updating Agent

Note: For **Genians Cloud Managed Edition** the Policy Server, will distribute the agent update automatically.

You can update your Agent by uploading a updated zip file through the UI.

1. Go to **System** in the top panel
2. Go to **Update > Genian Software** in the left System Management panel
3. Find **Available Version** software for Agent in Genian Software window
4. Click **Download**
5. Navigate to **Preferences > Agent** and select an **Automatic Update Target** to determine which networks to distribute the agent updates to.

Updating Agent Plugins

Individual agent plug-in files can be uploaded and updated via the Web Console.

Note: For individual plug-in files, please contact Genians Technical Support.

1. Go to **System** in the top panel.
2. Select **Update > Genian Software > Agent Plugins** in the left System Management panel.
3. Click **Tasks** and select **Upload Plugins**.
4. Click the **Select File** button to select the plug-in file (extension: gpf) to be uploaded.
5. Click **Upload**.

checking Agent Plugin Versions

To check the plugin versions installed on the Policy Server:

1. Go to **System** in the top panel.
2. Select **Update > Genian Software > Agent Plugins** in the left System Management panel.
3. Check the information in the **Version** column of the Plugin of interest.

To check the plugin versions installed on an endpoint:

1. Go to **Management > Node** in the top panel.
2. Select the node you want to inspect and then navigate to the **Software** tab
3. Near the top right corner of the **Programs** table, toggle the **Include Agent** switch.
4. Check the information in the **Version** column of the Plugin of interest, which will be displayed as **Genian Agent Plugin - [Plugin Name]**.

Update Policy Server Plugin

Upload and update policy server plug-in files through the Web console.

The Policy Server Plug-in is used to apply features that are specific to the site, or features that require limited application, without including them in the product.

Note: It works in module form rather than Genian NAC product image and does not require a version upgrade when applying the feature.

---

1. Go to **System** in the top panel.
2. Go to **Update > Genian Software** in the left System Management panel
3. Click the Upload Plugins item in `Task` Selection.
4. Click the `Select File` button to select the plug-in file (file extention: .gwp) to upload.
5. Click the `Upload`

Define Separation by Plug-in Key

The plug-ins for policy servers supported by Genian NAC are as follows:

Module	Description	Example
Web Module	Plug-in for displaying separate pages, such as pop-up pages	OTP authtication utility
Wiget Module	Plug-in for widget purposes defined by the specified item	RSS Reader Wiget
Widget definition module	Plug-ins that allow administrators to define widgets based on data	
Report Module	Plug-in for report purposes defined by the specified item	Query reports, trend reports, node group reports
Report definition module	Plug-ins that allow administrators to define reports based on data	
Service Module	Plug-in intended to invoke the Rest	SSO Rest Service Module
External Integrate Module	Plug-in related to interlocking with other systems	CISCO ISE Integrate Module
Periodic Working Module	Feature-related plug-ins that require periodic operations	AWS Connector

17.11.2 NAC Operational Data Management

Download the latest data from the Genian Cloud Server.

- **CVE Update information**, Information about vulnerabilities in platforms.
- **Node information**, Data for gathering platform information
- **OS Update Information**, Information about updating your device operating system
- **PI Update Information**, Data for classifying platform information
- **Platform Information**, Data for detecting operating systems

17.11.3 Setting up automatic update of Genian data

automatically update the latest data with the Genian Cloud Server and periodic version checks.

1. Go to **Preferences** in the top panel.
2. Select **General > Miscellaneous** item on the left
3. Set the time and action in the Genian Data Settings topic

(*Genian Data updates are set to work by default.*) (*To update Genian data, the 'Internet Access' option must be enabled in Miscellaneous settings.*)

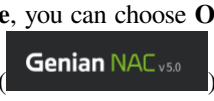
17.11.4 Manually update Genian data

1. Go to **System > Update > Genian Software** in the top panel.
2. Click the `Update` button at the top left.
3. If there is a new version, the update will be done automatically.

17.12 Preferences Settings for Admin Console

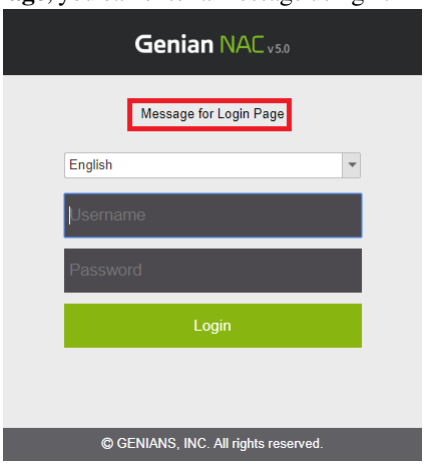
You can configure **Console** with your preferred settings

17.12.1 Web Console

1. Go to **Preferences** in the top panel
2. Go to **Preferences > General > Console** tab in left panel
   - **Console Name**, you can set a console name, that name appears on the left side of the sub menu bar and on the tooltip of the Agent icon in the tray menu (*Note: You must logout and login again to see the changes for the console name and must run an agent for the agent tooltip.*)
   - **Tree View Criteria**, you can choose either **Sensor** or **Group** displayed as a tab in **Tree View** in the left upper panel and will see the Nodes accordingly
   - **Management View Criteria**, you can choose either **By Node** or **By Device** (*This can be configued in* **View Criteria** *by clicking a menu button* ( ) *in Node Management page.*)
   - **Management View**, you can choose one of 10 Views (*This can be configued in* **Views** *by clicking a menu button* ( ) *in Node Management page.*)
   - **Sorting Tree**, you can decide how to sort the tree menu in the left panel of **Node Management**, **Switch Management** and **WLAN Management**
   - **Displaying IP Available**, you can specify whether to show an IP address not assigned yet
   - **Language, Date Format, Time Format**, you can set with preferred options
   - **Company Logo for Web Console**, you can choose **On** to see its options, **Background Color** and **Image** and the default logo in the left top (

) will be replaced with the one you configured

- **Number of Results**, you can specify how many rows are displayed in a single page of Node Management. (*This can be configued in right top drop-down menu with numbers* (

), *next to* **Search** *button, in Node Management page.*)
- **Session Timeout**, you can set the desired session timeout in seconds
- **Message for Login Page**, you can enter a message using html (*or plain text also possible option*), that message appears on login box 

- **2-Step Verification Methods**, you must tick the checkbox to enable **2-Step Authentication** (*Go to Management > User > Administrator tab > find General section*) for the administrator's authentication
- **Find Username / Reset Password**, you can decide whether to display **Find Username / Reset Password** for an administrator who forgot his or her username or password. If you choose **On**, more options, **Verification Methods** (Text message / Email), Find / **Reset Options** (Username / Password) and **Security Question** settings, will appear
- **Exported Dashboard Title**, you can set the display title for the document you would export a dashboard to. (*Go to Dashboa rd and click* **Export** *button on right top to export a dashboard as PDF, DOCX, PPTX*)

17.13 Download Mobile App

Genian NAC Monitor discovers all the Nodes, allows or denies IP or MAC, and manages an external device request. You can download the Genian NAC Mobile App for IOS and Android.

1. Go to **System** in the top panel
2. Go to **Update > Genian Software** in the left System Management panel
3. Find **Genian NAC Monitor for Mobile**, click **Checkbox** for either **iOS** or **Android**
4. Scan the **QR code** to download the software or click the link to go to GooglePlay to download
5. Click **Close**

17.14 Managing Policy Server With SNMP

You can download the Genian NAC MIB file to use in a Network Management System (NMS) type solution.

17.14.1 Download Genian NAC MIB File

1. Go to **Preferences** in the top panel
2. Go to **General > Log** in the left Preferences panel
3. Find **SNMP Trap Options** section in the main Log window
4. Select **On** from the drop-down
5. Enter **Community String**
6. Click **Download GENIAN MIB** (*Zip file will download to the local machine*)
7. Click **Update**
8. Unzip the **GENIAN-MIB.zip** file
9. Add the **GENIAN-MIB.mib** file to your desired **Network Management System**

17.15 Controlling Services

If there is an error or problem related to the service provided by the Policy Server, you can restart the services from the UI.

1. Go to **System** on the top panel.
2. Select **Service > Control** in the **System Management** item on the left.

17.15.1 Policy Application

If any Network Sensors in the envrionment are not operating according to the policy set on the Policy Server, you can force an application of all policies.

- Click the **Apply** button under **Apply Policy**

17.15.2 Stop / Start Services

You can manually Stop or Start all services provided by the Policy Server, Network Sensors, and Agents.

- Click the **Stop** or **Start** button under **The Service is [running / temporarily unavailable]**

17.15.3 Restart Web Application

If there is a problem with the web-related services provided by Genian NAC or a need to restart occurs, you can use the web application restart function.

1. Select **Web Console** (Policy Server Management interface) or **CWP** (Captive Web Portal) or **IP Request System** from the dropdown under **Restart Web Application**.
2. Click **Restart**.

17.16 Restrict administrator privileges

You can limit the privileges of administrators, to specific views, devices, and capabilities.

1. For **Node Management Scope**, Restriction by specifying node groups, network sensors, and node types
2. For **Node Management Task**, restrict the types of operations that can be performed on the Node Management screen
3. For **Node Management View**, restrict the selectable views on the Node Management screen
4. For **Node Management Tab**, restrict the selectable details tabs of a node
5. For **User Management Scope**, restrict departments that the admin can perform user management on
6. For **User Management Task**, Restrict the types of actions that can be performed on the User Management screen
7. For **Log Scope**, Limit available Log filters in the LOG menu
8. For **Disabling File Export**, Restrict File (Excel) Export Functions
9. For **Dashboard Widget**, Restrict Dashboard widget features

17.16.1 Create network sensor individual administrator accounts

Set permissions to manage only nodes under a specified network sensor by specifying the network sensor managed by the administrator.

- This setting is recommended for use with *Configure Administrator Role Options*.

1. Create an administrator account.
2. Select the administrator account you created.
3. Go to the Set Management Rstrictions topic.
4. **Node Management Scope** : Select Administration Sensor, click Assign button to assign Network Sensor
5. **Node Management View** : Select a Node View and drag it to the right
6. Click the Modify button at the bottom
7. Log in with the account you created to verify that only the nodes on the specified network sensor are visible on the Manage Nodes screen.

17.17 Troubleshooting

- *Genian NAC log collection method*
- *Genian NAC 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 NAC 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 NAC 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 NAC 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 product release cycle?

Genian NAC releases a new minor version every two months.

21.2 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.

21.3 Is the communication between each component encrypted?

Yes, communication between each component is encrypted through TLS.

21.4 What if I exceed the license amount?

See step 1 on *Sizing Software and Hardware*

21.5 How can I check Windows update of endpoints?

See step 1 on *Update Windows*

21.6 How come the blocked Nodes cannot open the CWP through Genian NAC?

See step 1 on *Blocked Nodes are not redirected to CWP page*

21.7 What Regex engine does Genian NAC utilize?

Genian NAC utilizes Perl Compatible Regular Expressions. For information including syntax reference the following resources:

- Perl Compatible Regular Expressions
- PCRE CheatSheet
- Regex Debugger

21.8 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*

21.9 Can Node info be imported from a wireless controller via SNMP?

No, this function is not supported.

21.10 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

21.11 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

21.12 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.

21.13 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.

21.14 How to set up RAID?

Genian NAC Appliances support RAID 0,1 by adding a separate RAID card (ASR-8405E v2). For more information, please contact our sales team.

21.15 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`.

21.16 How can I collect wireless LAN SSIDs?

Please refer to the following documents. *Controlling WLAN*

21.17 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*.

21.18 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.

21.19 How do you control unnecessary administrator web access?

Session management(session-control) allows unnecessary access sessions to be forcibly terminated.

CHAPTER

TWENTYTWO

TROUBLESHOOTING

This section describes common errors, their potential causes and how to resolve them.

22.1 Genian NAC log collection and diagnostic method

22.1.1 Genian NAC log collection method

Genian NAC 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 NAC

Genian NAC 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 NAC diagnosis Method

This section provides an overview of the major processes used by Genian NAC that can be examined to troubleshoot issues.

Genian NAC 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
httpd: 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 NAC, 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 NAC, 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.
```

httpd

```
Error_log: httpd 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 NAC 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 NAC 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 NAC.

Necessary processes by component:

```
Policy Server:
Mysqld, elasticsearch, java, centerd, sensord, httpd, 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 NAC may encounter the following problems.

- Genian NAC 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 NAC 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

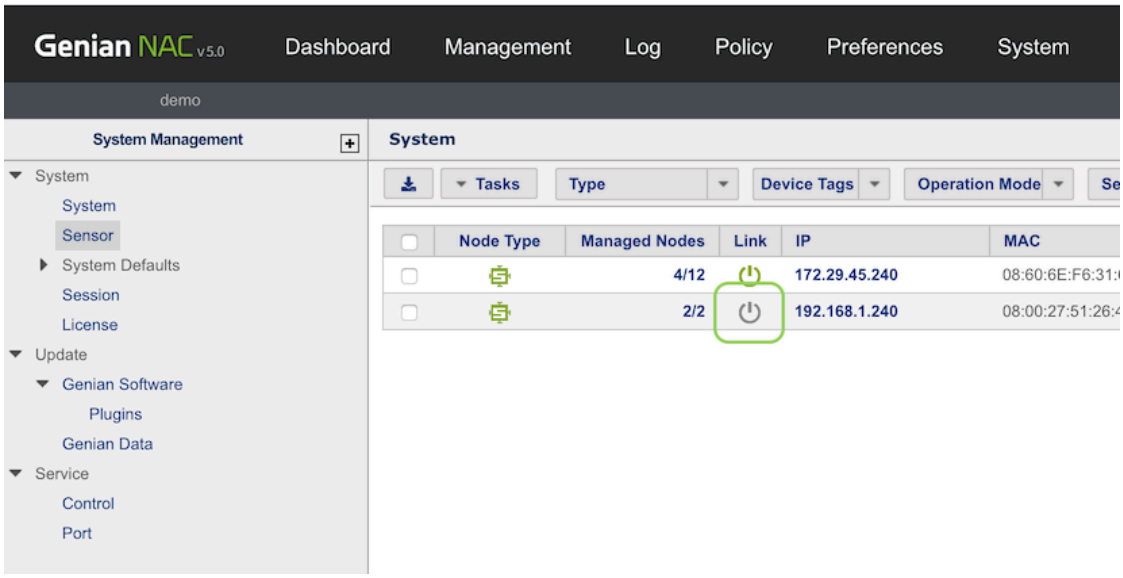
Check Connectivity

- 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.



Cause

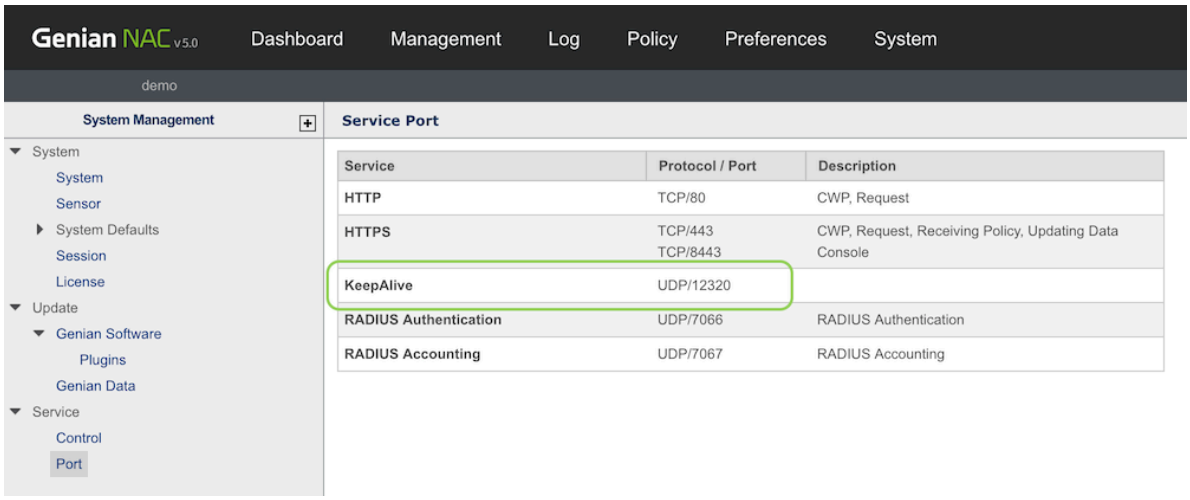
The network sensor periodically sends a keep-alive packet to the policy server to inform that it is operating normally. If this packet is not forwarded to the policy server, the link status is displayed as Down.

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



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 NAC 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 NAC 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

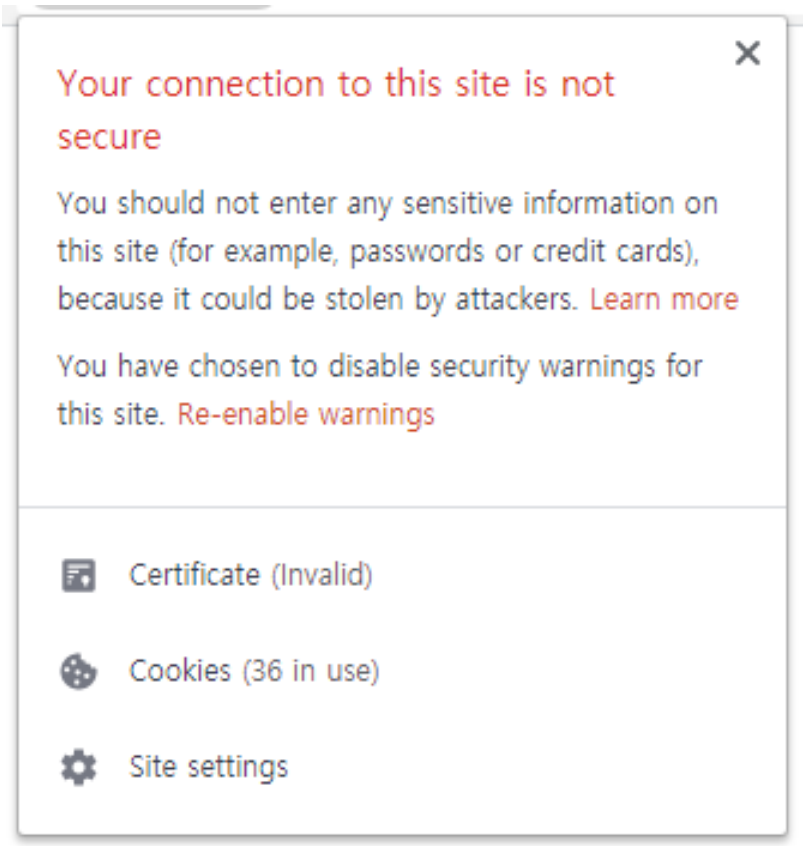
This feature can be disabled.

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



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 NAC 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 NAC 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 NAC 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 NAC 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 NAC.

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: *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.

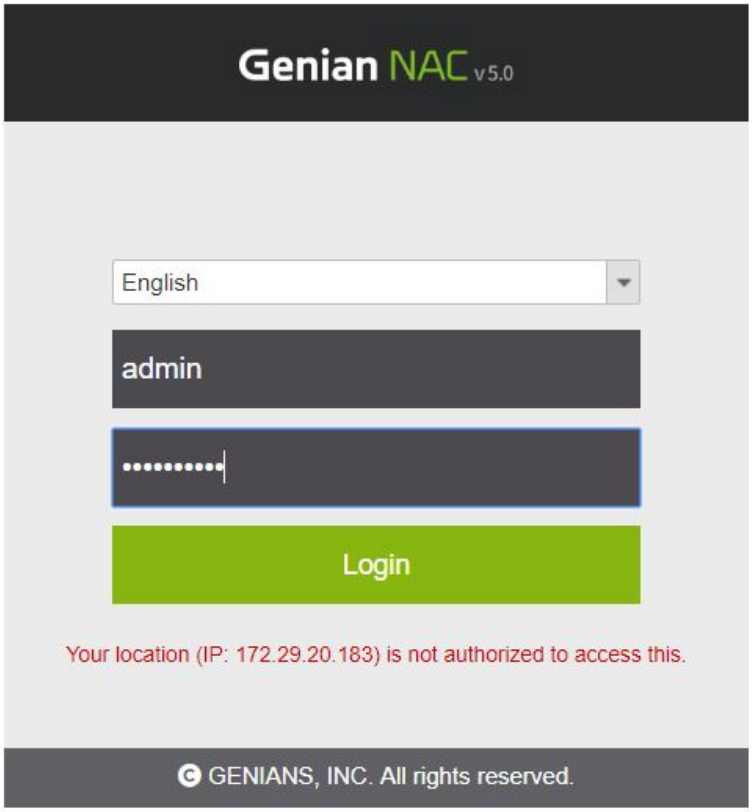
See:

- *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.



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 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
```

22.4.4 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

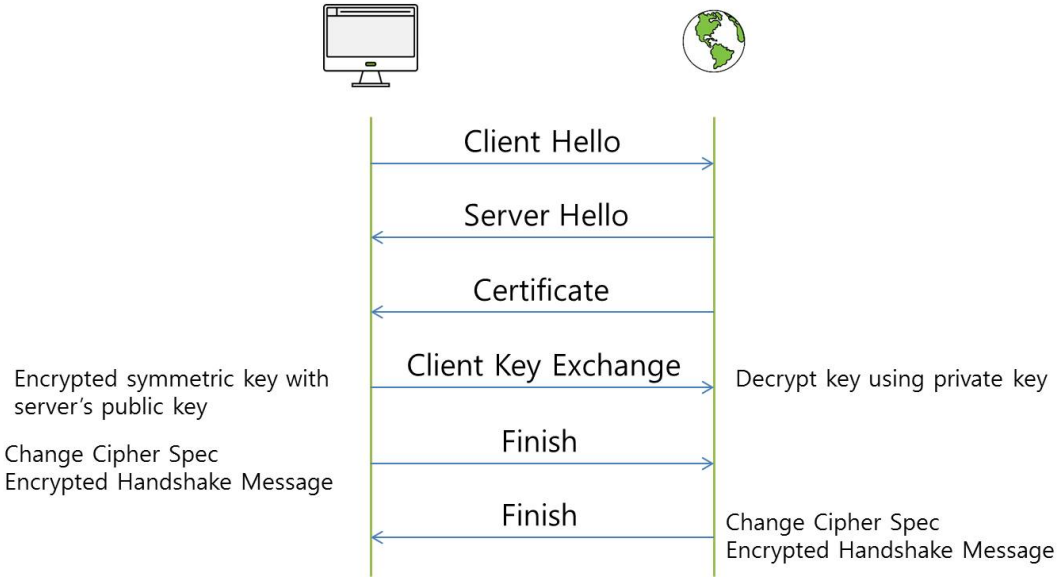
Certificate Warnings

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:

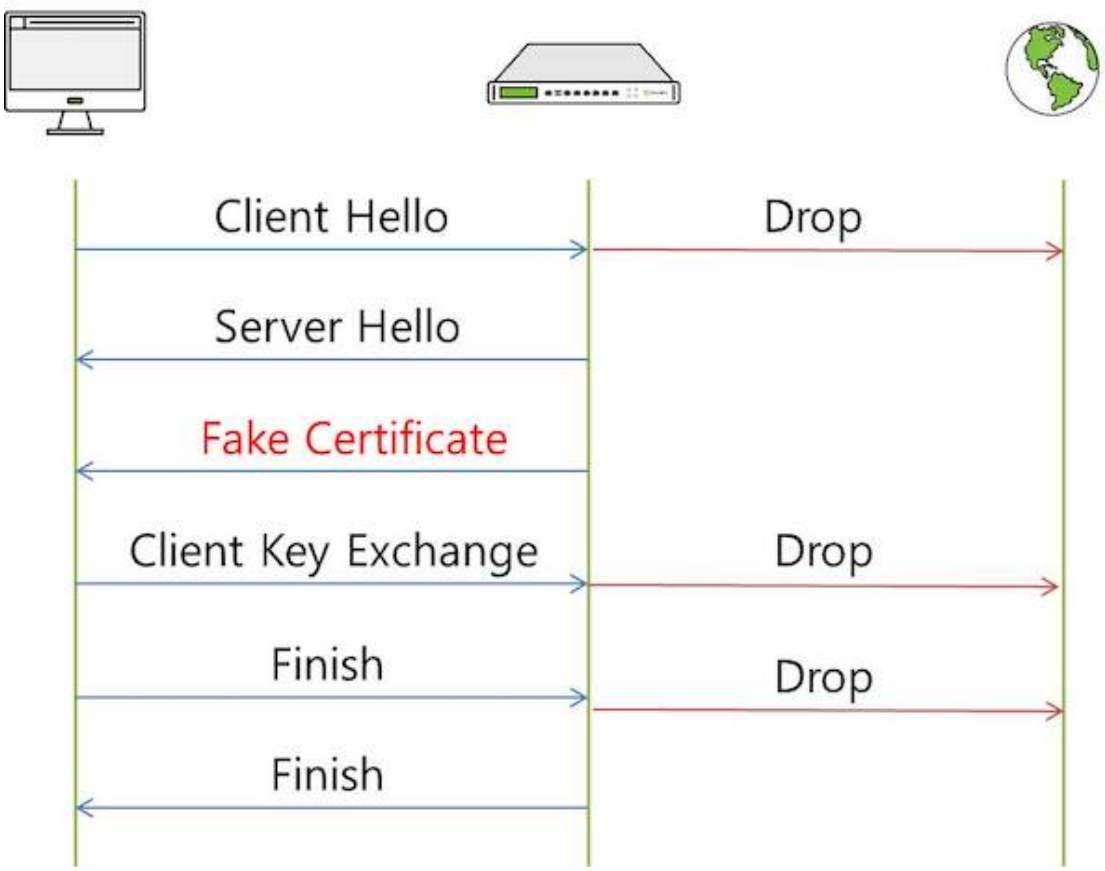


HTTPS communication requires intercommunication between the Web Server and the PC for encrypted communication before creating a cryptographic session.

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 NAC 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

Note: Starting with version 5.0.53 (LTS), CWP Redirect has been enhanced to operate even when connecting via Proxy.(#25704)

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.

22.4.5 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`

22.4.6 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 NAC 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:

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 NAC log collection method*

22.5.4 Recovering from database crashes

Every Genian NAC'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

GNAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC 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 NAC, Genian Proxy, or Microsoft Servers).
- Where the Windows downloads the updates from (Genian NAC, 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

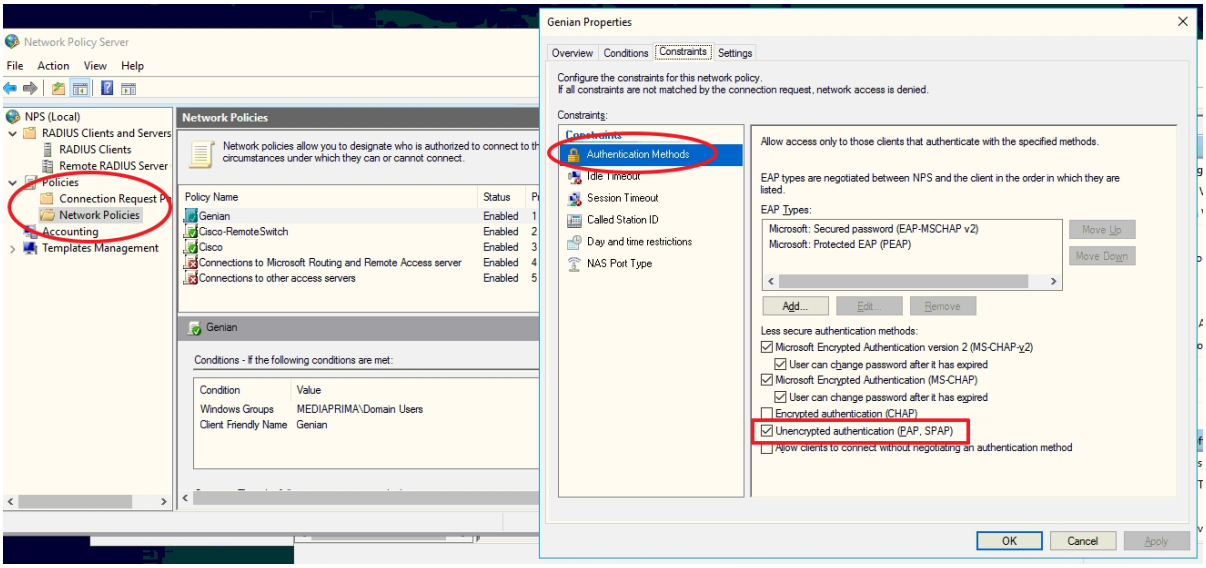
`secret key mismatched` error occurs when testing an integration of Genian NAC with an external RADIUS (Windows) server, using the built in test feature in the Web Console.

Cause

If the Genian NAC 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



CHAPTER

TWENTYTHREE

RELEASE NOTES

23.1 Current Version

23.1.1 Genian NAC v5.0.59 Release Notes (JAN 2024)

Release Date: 2024/1/5, Last Updated: 2024/1/16 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#26539	Improved UI of management details page by moving the Edit node details button to the bottom of the screen.
#26559	Improved processing of period settings on the user registration page so that they are set according to the administrator's time zone.
#26667	Added the ability to batch add node actions to multiple policies in the web console.
#26717	Added support for Ubuntu 22.04 version and upgraded to OpenSSL 3.0 version.
#27099	Improved to check active status of nodes when assigning DHCP IP in global DHCP environment.
#27133	Improved Dashboard sensor map, now color-coded to match the sensor operation status.
#27199	Improved quick search by adding more fields available for search criteria.
#27214	Changed the Timezone default in System Preferences to the administrator WebBrowser Timezone.
#27225	Improved support for Howry Virobot Security 1.0 products in the Antivirus Information Collection plugin.
#27229	Added a required field indicator to the Temporary User IP application password field.
#27315	Added device keepalive and sorting to the web console dashboard Center/Sensor device status widget.
#27348	Improved error page output to prevent providing unnecessary information.
#27357	Improved SAML IDP IP-Port output format for SAML authentication integration settings.
#27447	Improved Linux Agent software information collection to collect software installed via snap in addition to debian package format.
#27455	Updated Hauri ViRobot API used by the Windows Agent antivirus data collection plugin.
#27456	Added an approval reason column to the IP Application System application result.

Issues Fixed

Key	Description	Affects Version/s
#26253	Fixed an issue where when first logging in and using the Count by Platform Status widget the current location path would display null when navigating.	5.0.0
#26900	Fixed an issue that was causing errors when an IP that is being used by another MAC was assigned when the host made a DHCP DISCOVERY request.	4.0.158
#27064	Fixed an issue where if the device control plugin version changes after booting in safe mode, it was controlled only by the previous policy.	5.0.0
#27120	Fixed an issue where removing a registered item from the Node Policy Node Action Assignment screen would not display in the Assignable list.	5.0.57
#27173	Fixed an issue where the access device/access port information in the node list for a switch was not deleting in Web Console Switch Management.	4.0.158
#27205	Fixed an issue where if the web console session timeout exceeded 60 minutes the wrong remaining time was displayed.	5.0.0
#27236	Fixed an issue where the text on the CWP session expiration page was output to the system locale.	5.0.14
#27238	Fixed an issue where the cloud version ID/PASSWORD find phrase would display in the English ID/PASSWORD find phrase.	5.0.31
#27247	Fixed an issue where no results were displayed when moving the node list through the WMI collection information widget link.	5.0.33
#27371	Fixed an issue where the same standalone plugin with no coverage could be assigned to multiple policies.	5.0.43
#27396	Fixed an issue where the contents of the Last Operation Time column are displayed incorrectly when exporting the node list.	5.0.55(LTS)
#27405	Fixed an issue where the wireless LAN policy could not be modified after copying.	4.0.158
#27413	Fixed an issue where other language settings were not reflected when editing only local language items in the Multilingual Message component.	4.1.0 4.0.17 4.0.158
#27420	Fixed an issue where adding a sensor to a sensor group was not immediately reflected when the node management scope limit was set to sensor group.	5.0.31
#27429	Fixed an issue that prevented license information from being read when using OpenSSL 3.0.	5.0.0
#27442	Fixed an issue where sorting of the Last Operation Time column on the Web Console node management list screen did not work.	5.0.55(LTS)
#27443	Fixed an issue where the antivirus real-time monitoring status was reported as inactive after Windows Agent's PC was rebooted.	5.0.0
#27482	Fixed an issue where group copy failed when copying a wireless LAN group on the web console.	5.0.0

23.1.2 Genian NAC v5.0.50 (LTS) Release Notes (DEC 2022)

Release Date: 2022/12/07, Last Updated: 2022/12/07 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#23573	Improved Windows Agent's load balancing to be smooth when auto-updating agents on a large number of nodes.
#24820	Improved audit log screen to show log data usage.
#24841	Added feature to delete the contents set in sub-items when changing the setting a custom rule of the Windows Firewall Control Plug-in to All.
#25096	Improved RADIUS MAC authentication node group check so that it can be compared using Calling-Station-ID.
#25212	Improved so that the checkbox does not appear if the period item is set as a required item on the CWP new user registration screen.
#25231	Removed overlapping condition 'If MAC is the same' when adding a node group condition.
#25322	Added last deauthentication time column to the user management view to help distinguish dormant users.
#25388	Added help for the 'Allow SSID-Regular Expression' option to the 'Allow SSID' item in the WLAN Control Plug-in.
#25404	Improved so that the searched content displayed remains after clicking the apply change policy button in the node list.
#25416	Improved Linux Agent so if the agent and the policy server time zones are different, it is converted and displayed in the time zone of the administrator logged in to the management console.
#25446	Improved Sophos support of Linux Agent Vaccine Information Collection Plug-in.
#25457	Added ability to send messages to the node where the agent is installed using the REST API.
#25479	Improved to not display html syntax in device application processing notification message.
#25494	Improved Windows Agent password validation plug-in to check for change even when the password is changed directly in Windows instead of through the agent.
#25496	Improved macOS Agent's load balancing when auto-updating agents on a large number of nodes.

Issues Fixed

Key	Description	Affects Version/s
#25081	Fixed an issue where equipment change approvals were not being processed in the REST API.	4.0.110 5.0.7
#25117	Fixed an issue where there was a mismatch in the number of nodes on the management screen and in Status and Filter>Agent>Software status.	5.0.33
#25159	Fixed an issue where if a header list was deleted using Webhooks it was still showing up a Log search.	5.0.15
#25289	Fixed an issue with the macOS Agent Device Control plugin's network interface control option causing persistent block logs despite interfaces already being down.	5.0.46
#25317	Fixed an issue where node were still include in node groups even after time condition had expired.	4.1.3 4.0.152 5.0.50
#25340	Fixed an issue where installation date could not be collected by macOS Agent Operating system information collection plug-in.	5.0.47
#25350	Fixed an issue where the logged in admin UI session would terminate after an email approval/rejection of a new IP application.	4.1.0
#25390	Fixed an issue where a domain's IP would not renew when using an FQDN network object.	5.0.27
#25399	Fixed an issue where the number of nodes in Windows Update Status was displayed incorrectly when labeling the Windows Update Action.	4.0.113 5.0.10 4.0.152 5.0.50

continues on next page

Table 4 – continued from previous page

Key	Description	Affects Version/s
#25439	Fixed an issue where the platform of the node with an agent installed was changed to Unknown when updating GPDB manually with CLI command.	5.0.0 4.0.152 5.0.50
#25443	Fixed an issue where certificate expiration logs remain based on equipment certificates even when using a custom certificates.	5.0.0
#25462	Fixed an issue where a webpage error would occurr when clicking on details in the Genian Monitor window.	5.0.19
#25477	Fixed an issue where a large number of duplicate pop-up messages were displayed when waking from sleep mode while using the macOS Agent wireless LAN control plug-in.	5.0.49
#25498	Fixed an issue where the screen saver options in the macOS Agent, Appearance and Personalization plug-ins would not work properly with the input time.	5.0.15
#25559	Fixed an issue where the Wireless Connection Manager action would not recognize SSID if it was in Korean, and would registered it as the wrong SSID.	4.0.5 5.0.0 4.0.152 5.0.50
#25574	Fixed an issue where macOS Agent popup messages were not displaying correctly.	5.0.0
#25601	Fixed an issue where the administrator could not check documents registered when applying for IP because the detailed view page was disabled while awaiting approval.	
#25642	Fixed an issue where the node group condition setting UI were not displaying the new UI when upgrading to version 5.0.50 (LTS) or installing a new one.	5.0.49
#25652	Fixed an issue where an error page would be displayed on the CVE status widget in the dashboard if the bottom of the screen was clicked.	5.0.43
#25734	Fixed issue where hyperlink in Windows Agent notification message would launch Internet Explorer even when Edge was set as default browser.	5.0.47 6.0.4
#25745	Fixed an issue in the Linux agent file distribution plug-in where even when the distribution option was set to 'execute file' and the execution account to 'Root account' the file was not executed.	6.0.8

23.1.3 Genian NAC v5.0.42 (LTS) Release Notes (AUG 2021)

Long Term Support (LTS) version will be maintained with security and critical bug fixes for 2 years (until Jul 2023)

Security Advisories

- *GN-SA-2021-002: Genian NAC - Multiple Vulnerability*
- *GN-SA-2021-001: Genian NAC - SQL Injection Vulnerability*

New Features

Key	Description
#16843	Added a feature to display DHCP usage info in the IP management list.
#19733	Added an IP conflict log filter to be included by default.
#22123	Added the option to put a URL link button in the authentication plugin of the Windows Agent.
#22247	Added the option to fully display messages (rather than a preview) in the Windows Agent Pop up.
#22852	Added the ability to manually input a policy server IP if none is present when installing the macOS Agent.
#22891	Added a Linux Agent and node policy plugins.
#23003	Added the ability to customize the execution cycle of Linux Agent plugins.

Improvements

Key	Description
#21939	Windows Agent Software Uninstall Plugin can now remove software from the Microsoft Store.
#22698	Mail Server and SMS server integrations can now be disabled.
#22813	A log entry will now be generated when executing a network sensor image update command.
#22823	Windows Agent Software Detection Plugin can now detect software from the Microsoft Store.
#22956	Trend Micro APEX One is now supported in the Windows Agent Antivirus information plugin.
#22982	Check Point Endpoint Security is now supported in the Windows Agent Antivirus information plugin.
#23047	Notifications for authentication expiration can now be disabled.

Issues Fixed

Key	Description
#22395	Fixed an issue where macOS Agent installation failed.
#22464	fixed an issue where scheduled macOS Agent OS Update scans generated error logs.
#22481	Fixed an issue where the authentication window was duplicated while using 802.1x EAP GTC authentication on Windows.
#22749	Fixed an issue where active nodes displayed the current time in the 'last active' column of the node list.
#22909	Fixed an issue where equipment name / sensor name was not shown in exported node list spreadsheets.
#22932	Fixed an issue where nodes registered by virtual sensor cannot be blocked by mirror mode sensor.
#23024	Fixed an issue where the USER_CUSTOM macro did not function.

Cloud

Key	Type	Description
#23071	Problem	Fixed an issue where Network Sensor Debug files stored on the Policy Server do not correctly identify the sensor IP associated with the log entry.

23.2 Previous Version

23.2.1 Genian NAC v5.0.58 Release Notes (NOV 2023)

Release Date: 2023/11/14, Last Updated: 2023/11/14 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#25533	Added an option to clean cache information in Policy Server Agent Windows Update settings.
#26325	Improved the httpd startup script to check whether procmond is running and execute httpd.
#26482	Improved to now compress department codes with a hash function to prevent the column size from exceeding size limit when storing.
#26545	Upgraded to GNOS kernel version 5.15.0.
#26575	Added the ability to turn on/off the IP management system.

continues on next page

Table 9 – continued from previous page

Key	Description
#26907	Improved so you now have the ability to set multiple URLs for the search filter webhook setting URL in the web console audit log.
#26913	Added Exosphere support to Windows Agent antivirus data collection plugin.
#26921	Added external authentication integration plugin to replace Windows Agent GnExlib.
#26929	Improved logs to include USB information collected by the Windows Agent hardware information collection plugin.
#26942	Improved the logging in Tomcat debug when modifying device information in node details.
#26955	Improved to better retrieve and execute ES account information when executing the sysinspect script.
#27068	Added the ability to search items in the node group condition item list.
#27077	Improved the event socket not configured log when restarting the sensor.

Issues Fixed

Key	Description	Affects Version/s
#25805	Fixed an issue were the IP Change Prohibited (Designated IP range)-Single IP Violated icon was not displayed in the Web Console IP Matrix View.	4.0.8
#26742	Fixed an issue where the disable NMAP TCP SCAN setting in the Network Sensor node information scan setting was not being applied.	5.0.40
#26777	Fixed an issue where the policy last modified time was not updating when modifying the WebConsole node policy/control policy settings.	5.0.0
#26859	Fixed an issue where storage device information was not collected if the Linux Agent was not partitioned.	5.0.41
#26864	Fixed an issue where the Windows Agent's information collection plugin was intermittently not updating.	5.0.0
#26904	Fixed an issue where the Risk Detection icon was not displayed in the web console node list.	5.0.53
#26933	Fixed an issue where the calendar component used in the web console input field were displayed in only English.	5.0.20
#26951	Fixed an issue were the virus treatment log entries were not being recorded when using the antivirus information collection plugin.	4.0.144 5.0.41
#26965	Fixed an issue where an error message would appear when accessing the IP application page if there was no visitor usage setting in the application settings.	4.0.114 5.0.11
#26992	Fixed an issue where the agent plug-in was operating based on the time zone of the policy server instead of the local node time.	5.0.0
#27017	Fixed an issue in where the log was not saved when changing the log server credentials before the log server was started.	5.0.0
#27040	Fixed an issue where if the date information collected from the agent was ‘unknown’ or ‘no information’ it was displayed as ‘1970-01-01’.	5.0.0
#27048	Fixed an issue where the login screen and area would overlap when entering more than 3 lines for the web console login screen banner.	5.0.58
#27057	Fixed an issue where tomcat was displayed as tomcat9 in the log history when restarting tomcat, even though it was not tomcat9.	5.0.53
#27059	Fixed an issue where a tag name could be entered with a space when adding a tag in the web console.	4.0.M7
#27111	Fixed an issue where the job title synchronization failed if there was no job title information in the local DB when performing job title synchronization.	5.0.49
#27119	Fixed an issue where longer names used for the URL button of the Windows Agent authentication window were being cut off.	5.0.42

continues on next page

Table 10 – continued from previous page

Key	Description	Affects Version/s
#27148	Fixed an issue where the failure count was not resetting after a successful login when using 2FA for web console login.	4.0.10

23.2.2 Genian NAC v5.0.57 Release Notes (SEP 2023)

Release Date: 2023/9/18, Last Updated: 2023/9/18 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#25533	Added the option to delete cache data stored on the policy server under proxy service configuration.
#25714	Added option to set security pledge expiration date.
#26284	Improved self-signed certificates in products to auto-renew.
#26312	Improved node bulk registering process to better handle csv duplicate entires.
#26371	Added the ability to periodically check for deadlocks and restart the sensor daemon.
#26407	Improved the display of policy servers in the IP management matrix view.
#26410	Improved error messaging in case error occurred in SP after SAML authentication-linked Idp authentication.
#26412	Improved to switch to login screen when administrator session is forcibly terminated.
#26468	Improved the number of list output per page of the node-detailed software/history management list to be changeable.
#26473	Improved to validate input values when setting up SNMP Agent.
#26491	Improved to output the contents of the web console node management description column to match the column size.
#26544	Applied the latest GNOS kernel patch (5.10.181)
#26555	Added gnlogin command to be able to check IP information cached in sensor when using FQDN in network object.
#26640	Improved so when continuing to add node group conditions the previous item will be selected.
#26653	Improved so when changing the properties of a web console node, only one item in the same category can be selected.
#26665	Added 'Available OS Type' option when assigning agent action when creating policy.
#26668	Improved the Enable CWP SSL preference to be On by default.
#26734	Improved the error message displayed when an incorrect date is entered for the useful life start date/end date in the web console equipment properties.
#26753	Improved the error message displayed when entering a semicolon at the end of a query string in the web console query report.
#26801	Improved the output of the primefaces default system error in the web console.
#26803	Added audit logs for shared folder control via plugins.
#26827	Improved the popup message of the Start Backup Now button in the web console.
#26875	Improved message output to CWP when hostname restrictions are in effect.

Issues Fixed

Key	Description	Affects Version/s
#25759	Fixed an issue in Korean version were an English message would display when entering values that did not fit format in calendar.	
#25815	Fixed an issue where there was no response when approving and rejecting IP new/returning applications while the approval popup was enabled.	4.1.3
#26235	Fixed an issue were macOS Agent failed to get the motherboard information of new model (M2 series) macs.	5.0.41
#26369	Fixed an issue where the date display was incorrect when searching for the previous year in the Node/Log/Wireless LAN report.	5.0.34
#26447	Fixed an issue that caused web console to lag when performing the reapply node policy command for a specific node.	5.0.0
#26463	Fixed an issue where syscollect, a system information collection tool, might not work in a closed network environment.	5.0.0
#26464	Fixed an issue that caused images to appear broken when uploading and previewing images from the web console announcement creation screen.	5.0.0
#26487	Fixed an issue where an error page was displayed when there was no value in the CVE detail view.	5.0.24
#26529	Fixed an issue that caused an error page due to incorrect sensor's IP/MASK setting in the Network Sensor IP Utilization Top status widget.	4.1.4
#26558	Fixed an issue where the network address of a network object was not modified when only the TTL of the FQDN option was modified.	5.0.19
#26560	Fixed an issue where the search was not performed when AND was present in the search term in the node management screen.	5.0.38
#26566	Fixed an issue where the changed information was not updated or displayed when moving tabs after updating node information.	5.0.50
#26573	Fixed an issue with the RestAPI if import data in a language different from the session, the specified language setting parameter name is incorrect.	5.0.0
#26578	Fix an issue where the UserID and Department Name columns were blank in the IP Usage Application result search.	4.1.4
#26586	Fixed an issue where the Apply Change Policy button was not output when copying a node group and was applied immediately.	5.0.31
#26605	Fixed an issue where some information was missing from the audit log to the wireless LAN AP detection/wireless LAN AP information change log.	5.0.0
#26610	Fixed an issue where English was displayed on agent installation regardless of the user's default locale setting.	5.0.0
#26652	Fixed an issue where the IP start/end time of the data imported through node attribute import in the node management list was 9 hours different from the entered value.	4.1.M4
#26673	Fixed an issue where the MAC was blocked when the IP usage time expired for a node set to Do not change (designated IP subnet) if the new node policy MAC was blocked.	4.1.M5
#26680	Fixed an issue where the last line word of the password blacklist file was not restricted.	4.0.106
#26683	Fixed an issue where entering a value that does not match the form of the search criteria in the search bar of the web console node detail screen would result in an error.	5.0.22
#26689	Fixed an issue where the node IP was incorrectly recorded in the debug recorded when removing the Do Not Change setting.	5.0.43
#26692	Fixed an issue in the webconsole system management software where clicking the upload button without selecting a file would not end the process.	5.0.2
#26751	Fixed an issue where sensord deadlock was incorrectly checked.	5.0.0

continues on next page

Table 12 – continued from previous page

Key	Description	Affects Version/s
#26771	Fixed an issue where the center daemon process would not run normally when setting the policy server node-server enable through gnlogin.	5.0.42(LTS)
#26815	Fixed an issue where the contents were not displayed when selecting a node group in the web console node port.	5.0.24
#26836	Fixed an issue where a department information search error occurred in the node-group condition if a department name with the tag 'department' existed.	5.0.42(LTS)
#26843	Fixed an issue where the agent package was created twice during the initial startup of the center daemon, causing a delay in startup time.	5.0.0
#26845	Fixed an issue where the agent icon was retained when deleting an agent on a node assigned the Windows Update node action.	4.0.M1 5.0.0
#26889	Fixed an issue where self-sign certificates were not reissued.	5.0.45

23.2.3 Genian NAC v5.0.55 Release Notes (AUG 2023)

Release Date: 2023/8/7, Last Updated: 2023/8/7 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#22197	Added OAUTH 2.0 ROPC RADIUS integration for use in 802.1x environments.
#25072	Improved the tag assignment method for nodes to a table append method.
#25540	Changed the validity of Self-sign CA certificates distributed by agents to 10 years.
#25921	Improved Linux Agent to compress agent logs on the 10th of every month and delete compressed logs after one year.
#25940	Improved Linux Agent package authoring tool to allow agents to be installed in offline environments.
#26031	Added motherboard manufacturer, CPU name, and CPU manufacturer to the node group conditions.
#26037	Improved user application detail screen to include display pop-up showing the reason for rejection.
#26043	Improved SNMP settings to be able to select authentication and encryption methods.
#26105	Improved readability of node management operation state chart by adjusting the column width.
#26123	Improved the user account application approval email to display only the date and time/minute of the application time.
#26167	Improved synchronization of Postgres DB information by upgrading to PostgreSQL 10 version.
#26183	Improved to prevent the end of use date from defaulting to the same day when applying for IP.
#26186	Improved the audit log message *Event key mismatch* by adding *Authentication key validity log type* in the operating system update.
#26192	Added the ability to create SAML Service Provider Metadata.
#26329	Added the ability to force off the **Show Windows logon screen** setting when controlling the Windows Agent screensaver.
#26359	Added ability to force Windows Agent to disable the Wi-Fi random hardware address option in Windows.
#26462	Improved web console login screen browser *Title* bar to not expose customer information.
#26479	Improved to unblock blocked nodes when shutting down the device through the Network Sensor reboot/poweroff command.
#26563	Improved to allow the sensor to manage alias IP bands without setting the alias IP on the network sensor interface.
#26627	Improved to prevent CWP Web from re-displaying the authentication screen after agent authentication in the CWP Web page output state.
#26644	Changed the Install Center CA certificate option to Default ON and change how often it is performed.

continues on next page

Table 13 – continued from previous page

Key	Description
#26729	Added a setting to collect AhnLab V3 information when using the macOS Agent antivirus information collection plugin.
#26792	Improved validation for events received by Policy Server.
#26807	Improved the way Policy Server/Agent events are handled to Push Notification.

Issues Fixed

Key	Description	Affects Version/s
#25148	Fixed an issue where the web console smart help messages were not linking to the related page from some menus.	5.0.49
#26027	Fixed an issue where the Do Not Modify (IPM) icon was not displayed when registering as a new node after setting Do Not Modify to an unused IP.	4.0.8 5.0.0
#26097	Fixed an issue where export didn't not work if the Active value of a sensor was abnormal in the web console node management menu.	4.0.2
#26181	Fixed an issue where the tray icon would not display when switching the Linux Agent terminal to an already logged in user in a multi-user environment.	5.0.41
#26194	Fixed an issue where setting the HTTP/HTTPS port change in a multisensor environment would add an unnecessary IPTALBES rule.	4.0.17
#26204	Fixed an issue that caused a read failed error debug before running centerd when installing the policy server for the first time.	4.0.152 5.0.42(LTS)
#26250	Fixed an issue with the Linux Agent network information collection plugin that caused collections to be missed if an interface with no name or the same name exists.	5.0.51
#26272	Fixed an issue where authentication was not processed correctly if authenticating with account@domain in the SMTP authentication linking environment.	5.0.53
#26288	Fixed an issue where checkboxes were displayed in the list UI after modifying the web console custom field.	4.0.11
#26317	Fixed an issue that caused errors when adding the same field to the user information input field and the new application input field in the IP application form for visitors.	4.0.11
#26321	Fixed an issue where the OS type combo box in the Web Console Device Group screen was intermittently displayed as an empty value.	5.0.0
#26335	Fixed an issue where the tray icon was intermittently not displayed when switching Windows Agent logon users.	5.0.0
#26409	Fixed an issue in Linux Agent were Agent UI was not working due to failure to collect login user information.	5.0.55
#26444	Fixed an issue where the software settings window of the Web console node group condition could not search for Korean.	5.0.35
#26497	Fixed an issue in the Windows Agent Wireless Connection Manager where the wireless profile (EAP-TTLS) would not connect when server certificate verification was turned off.	5.0.49
#26551	Fixed an issue where only the result of the last condition were displayed when checking macOS Agent multiple action performance conditions.	5.0.21
#26566	Fixed an issue where after updating node information, the changed information was not updated or displayed when moving tabs.	5.0.50
#26606	Fixed an issue in the macOS authentication window where login was not performed when entering a single key.	5.0.15
#26643	Fixed an issue where the Windows Agent self-authentication window action policy was removed and the previously displayed authentication window was still displayed.	5.0.0

continues on next page

Table 14 – continued from previous page

Key	Description	Affects Version/s
#26687	Fixed an issue where the time in the Web Console Node Management Last Action Time column was not displaying in the administrator's time zone.	4.1.M4
#26901	Fixed an issue where building with an incorrect endianness prevented policy updates.	5.0.48
#26930	Fixed an issue where the search filter would not work when the audit log alarm transmission failure message was disabled.	5.0.39

23.2.4 Genian NAC v5.0.54 Release Notes (MAY 2023)

Release Date: 2023/5/16, Last Updated: 2023/6/12 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#26148	Improved so that node information can be updated immediately if the device is different from the existing node when the agent logs on.

Issues Fixed

Key	Description	Affects Version/s
#26118	Fixed an issue where when setting the exclusion of virtual printer some general printers were being incorrectly marked as virtual printers.	4.0.0 5.0.0
#26119	Fixed an issue were when registering the Windows Agent wireless LAN control plug-in as a CSV, the MAC address was case sensitive causing APs to be blocked even though it was allowed to connect.	4.0.0 5.0.0
#26259	Fixed an issue that was causing a display error in the Elasticsearch management tool on the Advance page of the web console.	5.0.17
#26267	Fixed an issue where today's audit log was not displayed before 9:00 KST in the web console audit log.	5.0.0
#26280	Fixed an issue where some sensors were registered as authorized in the re-registration process after deleting a multi-sensor device.	5.0.50(LTS)
#26296	Fixed an issue where other action policies malfunctioned when a large number of USB exception devices were used in the Windows Agent device control policy.	5.0.0
#26322	Fixed an issue where the message pop-up window after receiving a notification message in macOS Agent could increase CPU utilization.	5.0.27
#26353	Fixed an issue where synchronization failed when using fixed value settings when performing Google G Suite information synchronization.	5.0.0
#26357	Fixed an issue where the past detail screen was displayed when moving from the target node list to the default status.	5.0.35
#26414	Fixed an issue where the password verification window was periodically positioned in the center of the screen even when the fixed option was off.	5.0.53(LTS)
#26433	Fixed an issue where communication could fail due to an IP rule error generated when adding the gateway IP of a network sensor device.	5.0.42(LTS)
#26444	Fixed an issue where the software settings window of the web console node group condition could not search in Korean.	5.0.35
#26549	Fixed an issue where the dnsmasq daemon would restart intermittently.	5.0.53(LTS)

continues on next page

Table 16 – continued from previous page

Key	Description	Affects Version/s
#26587	Fixed an issue where the contents of the Web Console node management department name column were abnormally displayed.	5.0.50(LTS)
#26299	Fixed an issue where authentication-linked users were logged in even if they used a domain address other than the domain address used by the authentication-linked user.	5.0.53 (LTS)

23.2.5 Genian NAC v5.0.53 Release Notes (APR 2023)

Release Date: 2023/3/31, Last Updated: 2023/4/20 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#24094	Added detailed failure reason to the sensor upgrade log.
#24755	Added Genian NAC update notice to the web management console.
#24938	Improved so newly created node reports reflect the data at the time of creation.
#25269	Improved RADIUS policy to now be able to use username as an additional attribute value.
#25280	Added User creation wizard to more easily create or clone existing user profiles.
#25337	Added option to search only logs that occurred at a specific time to log search filters.
#25506	Improved macOS Agent operation when switching local user accounts.
#25517	Improved so you can now sort columns in the node list that you previously could not.
#25550	Added info popup to Agent Actions section that lists usage and also added ability to delete policy from the Agent Action page.
#25564	Added an option to renew or register a node when the Linux Agent and user's network interface information has changed.
#25567	Improved Linux Agent network information collection plugin to collect all multi-input IP and DNS settings information.
#25630	Improved Log search to allow bulk call to webhook.
#25639	When changing the ssh port in the CLI environment, it has been improved so that it is immediately reflected in the database.
#25704	Improved so CWP redirects are possible even when blocked devices are using a proxy.
#25710	Added the syslog-ng daemon to the monitoring list of procmond so that it can be restarted when shutting down.
#25739	Added option to add user management roles when registering users in bulk.
#25752	Improved Memory and Monitor widget output.
#25860	Improved so that when a tag is added the tag descriptions are also recorded in the log.
#25874	Changed the API Status logging cycle from 1 day to 10 minutes to more accurately analyze the policy server's usage status and timing.
#25891	Added option to the Windows Agent Network info Collection plug-in to collect only ports that are open for a certain period of time.
#25928	Improved Genian Syncer's patch collection to only display currently supported products.
#25990	Added support for User additions/updates through SAML Assertion Attribute.
#25994	Improved to collect USB device and Bluetooth information through macOS Agent hardware information collection plug-ins.
#26014	Improved Linux Agent by updating the installation path to better support GoormOS 3rd party app management.

Issues Fixed

Key	Description	Affects Version/s
#24674	Fixed an issue that was causing an error message to appear when assigning a department to a device in the CWP settings when using SSL.	5.0.42
#25604	Fixed an issue where the Agent installation icon was not displayed if CWP agent installation message was deleted.	3.0 4.0.153
#25760	Fixed an issue where a new node policy and IP policy were not applied when registering an IP reserved node through the API.	5.0.13
#25797	Fixed an issue where that once a node was moved to a node basket the Empty All Node Basket function was not working.	5.0.44
#25817	Fixed an issue where the Agent Version Status widget search was adding incorrect search conditions when moving the node list.	5.0.26
#25846	Fixed an issue where the 'Automatically include known gateways' setting was not being applied to Ad Hoc Network connection an flagging it as a risk.	5.0.21
#25936	Fixed an issue where the 'operate regardless of the management role permission' setting in the Restrict Node Management Commands section was not working.	5.0.44
#25944	Fixed an issue where software updates in the web console were displaying a version lower than the agent's current version.	5.0.20
#25978	Fixed an issue that was causing a password length error to display in the Switch details screen, even though the password has not been changed.	5.0.17
#25979	Fixed an issue where the existing Radius policy was not applied when creating a new policy.	5.0.23
#25998	Fixed an issue where the Windows Agent Password Validation plug-in was changing the password change time for some accounts every time it was checked and reported.	4.0 5.0.0
#26005	Fixed an issue where files with Korean paths were not uploading when using Genian Syncer.	4.0.0 5.0.0
#26008	Fixed an issue that prevented copying of policies from the node group details screen.	5.0.31
#26019	Fixed an issue where international SMS transmissions would fail if {_FULLMSG} was included in the search filter alarm.	6.0.0
#26020	Fixed an issue where Printer Info plugin was data without content resulting in empty fields and inaccurate quantities.	4.1.0 5.0.0
#26035	Fixed an issue where an error page would appear when clicking download image in the IP usage application details view.	5.0.42(LTS) 5.0.50(LTS)
#26040	Fixed an issue were an error message would appear in the Node Change Management page if all nodes were selected.	5.0.26
#26063	Fixed an issue where the CWP's automatic login function was not working correctly.	4.0.153 5.0.50(LTS)
#26106	Fixed an issue in the Windows Agent Network Shared Folder action would still be sharing after allotted time had expired.	5.0.42(LTS) 5.0.50(LTS)
#26130	Fixed an issue were the macOS Agent was crashing when the hardware information collection plug-in was used.	5.0.38
#26137	Fixed an issue that caused the page preview in the CWP design template detailed settings not to load.	5.0.42(LTS) 5.0.50(LTS)
#26160	Fixed an issue that would cause the integrity check to fail or not work correctly when downloading files using WGET.	5.0.0
#26170	Fixed an issue in the English CWP design template where using special characters in names would cause problems adding/deleting components.	5.0.48
#26219	Fixed an issue where and error would occur when copying a policy if a label was set as an action.	4.0.113 5.0.10

continues on next page

Table 18 – continued from previous page

Key	Description	Affects Version/s
#26242	Fixed an issue where Linux agents installed on Gooroom OS were displaying Windows icons in the node list in the WEB console.	5.0.50(LTS)
#34807	Fixed an issue where auto-generated dashboard reports would show a blank screen instead of downloading.	5.0.50(LTS)

23.2.6 Genian NAC v5.0.51 Release Notes (FEB 2023)

Release Date: 2023/2/16, Last Updated: 2023/2/16 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#25072	Improved assigning tags to nodes by adding a table.
#25269	Improved RADIUS policy to now be able to use username as an additional attribute value.
#25480	Improved storage information to be more accurate in the Storage section of the System information.
#25506	Improved macOS Agent operation when switching local user accounts.
#25564	Added function to update or newly register a node with the changed information when the Linux Agent and local network information are changed.
#25567	Improved Linux Agent network information collection plugin to collect all multi-input IP and DNS settings information.
#25579	Improved node audit records to be deleted together according to the time of audit record cleanup '3 years'.
#25625	Improved New user registration form to mark required fields.
#25639	Improved so when changing the ssh port in the CLI environment the DB reflects change immediately.
#25641	Improved loading times when adding columns related to services and IP policies in the node list.
#25656	Improved RADIUS logs to include reason for failure instead of just the generic 'user authentication failed'.
#25657	Improved IPAM Console temporary use section to allow you to add/delete the result item.
#25666	Improved RADIUS log to externally link through audit log filter.
#25735	Improved IPAM license status screen to include agent limit.

Issues Fixed

Key	Description	Affects Version/s
#25489	Fixed an issue where when deleting multiple nodes in node management, no matter the number selected the quantity displayed in the information message would be '1'.	5.0.44 5.0.51 6.0.0
#25543	Fixed an issue where the authentication user icon was not displaying in the node management list when authenticating a user with SAML2.	5.0.19 5.0.51 6.0.0
#25507	Fixed an issue where the tooltip explaining the condition in condition settings would not appear after initial save.	4.0.M1 5.0.0 5.0.51 6.0.0
#25553	Fixed an issue where the XSS-related text in the detailed information was broken when exporting the audit log to excel.	5.0.21 5.0.51
#25575	Fixed an issue where selecting a date through the calendar in the node report search bar would select a different date if the Policy Server timezone and the administrator account's timezone were different.	5.0.8 5.0.51
#25604	Fixed an issue that was disabling/deleting the agent installation message'SystemPlicy_K1' in CWP's message management and on the CWP page.	3.0.4.0.153 5.0.51

continues on next page

Table 20 – continued from previous page

Key	Description	Affects Version/s
#25608	Fixed an issue with Windows Agent and Wired Authentication Manager when using GTC authentication and reconnecting after reboot the authentication was automatically performed without a separate authentication request.	5.0.17 5.0.51
#25677	Fixed an issue where when moving to the CWP user information edit screen in the SAML authentication interlock environment, the SAML login button was not displayed.	5.0.45 6.0.2
#25686	Fixed an issue where wireless connection manager options where being displayed in agent tray menu even when the option was turned off.	5.0.0 5.0.51
#25694	Fixed an issue where the managing sensors on nodes was not able to set the sensor's Alias IP.	4.0.119 4.0.153 5.0.16 5.0.51
#25712	Fixed an issue where the DNS control plug-in would malfunction if Korean characters were included.	4.1.0 4.0.153 5.0.0 5.0.51 6.0.0

23.2.7 Genian NAC v5.0.49 Release Notes (OCT 2022)

Release Date: 2022/10/15, Last Updated: 2022/10/17 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#24662	Improved the node command execution REST API URL command so that it can be checked as a log.
#24693	Added the ability to add a lock screen background image when unauthenticated and using the lock screen option.
#24903	Added search feature to Node Group Condition settings section.
#24907	Added ability to resize columns in the node list.
#24950	Added feature to provide 'EAP-TTLS' profile through Wired Connection Manager.
#24966	Improved so that when moving the node list through a link on the policy management screen, the output is from the node point instead of the device point of view.
#24975	Improved loading speed when viewing Excel exported files.
#25001	Added ability to search for users by department name on the Users screen.
#25025	Added feature to provide 'EAP-TTLS' profile through Wireless Connection Manager.
#25046	Improved so the contents of the permission information can be output together with the Kernel debug function.
#25054	Added Agent full log compression for error reporting on Linux Agent.
#25058	Added a function to record parameter contents transmitted from interworking equipment in catalina.out when there is interworking through NAC and REST API.
#25059	Improved to display additional information in preview for uploaded certificate file.
#25078	Improved lock screen agent authentication window to lock the screen even when the monitor is extended.
#25089	Improved the manual link function so it can be provided according to the version and language.
#25093	Improved DHCP node IP renewal option help text.
#25100	Removed unnecessary port related warning logs when mysql client was running on a server where mysql was not enabled.
#25112	Added agent deletion options to Linux Agent.
#25137	Added ARP Management Actions Plugin feature to Linux Agent.
#25138	Added feature to provide result message of the Windows update action to GnPMS execution results.
#25160	Added Sophos Endpoint Agent antivirus information collection path.

continues on next page

Table 21 – continued from previous page

Key	Description
#25164	Improved audit log where if the owner is reset for every authentication to log only when the information is updated.

Issues Fixed

Key	Description	Affects Version/s
#24676	Fixed an issue where the administrator session was maintained when using the REST API and a duplicate login warning window was output when logging in from the management console.	5.0.14
#24914	Fixed an issue where Windows patch files uploaded via Genian Syncer could not be downloaded.	5.0.44
#24947	Fixed an issue where the password last changed time column was not modified when calling the user edit API.	5.0.43 4.0.151
#24998	Fixed an issue where synchronization of department information and job title information would not be synchronized if the data source classification value setting was changed.	4.0.0
#25016	Fixed an issue where the input text box and items that did not meet the conditions were displayed in the condition output of the vaccine information of the new node group.	5.0.31
#25029	Fixed an issue where the message did not pop up when blocking WLAN control in macOS Agent.	5.0.27
#25033	Fixed an issue where the private certificate was displayed on the client even after RADIUS EAP-TLS certificate enrollment and authentication failed on Windows 11.	5.0.42(LTS)
#25044	Fixed an issue that caused Genian Software file uploads to appear to hang when finished.	5.0.2
#25048	Fixed an issue where the tray icon was intermittently not displaying on the Linux Agent.	5.0.42(LTS)
#25074	Fixed an issue where the GPDB.info file was not updated when upgrading an image in a closed network causing the function did not work properly.	5.0.0
#25080	Fixed an issue where synchronization was not performed at the time of information synchronization execution cycle when changing settings in the management console.	4.0.151
#25091	Fixed an issue where the node list search filter did not work when clicking the audit log after assigning a specific management role.	4.0.151
#25115	Fixed an issue where the IP address column was not removed from the IP management application result list in the management console.	5.0.10
#25130	Fixed an issue where the dialog box created via the menu button in GnMonitor would not close, making it impossible to fix.	5.0.0
#25136	Fixed an issue where the count of the Satisfied/Dissatisfied column on the node management screen was output differently from the action execution result on the node information detail screen.	5.0.33
#25163	Fixed an issue where vaccine information was not immediately collected from nodes that were deleted and newly registered again.	5.0.0
#25218	Fixed an issue where a loading bar would be displayed when clicking on the right side of the Regulations and Permissions labels on the Control Policy screen.	5.0.46
#25222	Fixed an issue that caused intermittent Database Access errors when using the Linux Agent for a long time.	5.0.47

23.2.8 Genian NAC v5.0.48 Release Notes (AUG 2022)

Release Date: 2022/08/15, Last Updated: 2022/08/15 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#21428	Added an option to macOS Agent to apply policy application function according to the internal/external state.
#22808	Added node group condition function using extended node type.
#24183	Ported the NAC sensor module to the XGate UTM equipment, added a function that operates in the same way as the NAC sensor in UTM.
#24600	Added a function to specify the start time of user's account activation.
#24664	Added digital signature function to ensure the integrity of files transferred from the Linux Agent to the server.
#24768	Added the ability to kill Linux Agent process plug-in.
#24786	Automatically removed leading and trailing spaces in the data-server username in the local.conf file that was causing the web console not to start
#24816	Added a function to automatically move the cursor to the password input box when an ID is entered as long as the length set in the Windows Agent authentication window.
#24876	Streamlined user application menu by adding the MAC/device authentication restriction processing option instead of having to go to admin settings.
#24879	Added latest platform version information to Linux Agent.
#24894	Improved transmitting UDP event packets from NAC process when the size is larger than the MTU.
#24921	Enable connection to the LDAP server using a certificate when performing LDAP authentication interlocking and information synchronization.

Issues Fixed

Key	Description	Affects Version/s
#24625	Fixed an issue where an agent version upgrade was treated as a new addition rather than an update to the agent software list.	4.0
#24725	Fixed an issue where the Linux Agent was not displayed on Debian11 based platforms.	5.0.0
#24741	Fixed an issue where the detailed screen was not displayed when moving between information among node details.	5.0.38
#24784	Fixed an issue where the result of the IP application form was displayed in a language other than the one being used.	5.0.11
#24792	Fixed an issue where the Linux Agent Authentication Allow MAC policy function did not work.	5.0.41
#24798	Fixed an issue where the node's authenticated user was not found when syncing Google G Suite information and SAML authentication.	5.0.19
#24811	Fixed an issue where the old value is refilled when saving user ID/PW is canceled and saved again in Windows Agent Wireless Connection Manager.	5.0.0
#24835	Fixed an issue where the MAC information was stored in lowercase letters when the agent registered the node.	
#24845	Fixed an issue where an error appeared due to incorrect data format when calling the IP application system automatic rejection processing API.	5.0.14 4.0.149

continues on next page

Table 24 – continued from previous page

Key	Description	Affects Version/s
#24867	Fixed an issue where activating the Printer Shared Folder Control option did not result in control.	4.0.125 5.0.22 4.0.150
#24939	Fixed an issue where synchronization was not possible due to incorrect application of the paging parameter value when synchronizing information through REST API Server.	5.0.38
#24981	Fixed an issue where a virtual interface (Teredo Tunneling Pseudo-Interface) on the PC was falsely detected as a MAC/IP Clone.	5.0.0

23.2.9 Genian NAC v5.0.47 Release Notes (Jun 2022)

Release Date: 2022/6/15, Last Updated: 2022/6/29 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#24156	Added feature making it possible to set prohibit changes when registering csv nodes in bulk.
#24450	Added agent deletion function through Linux Agent authentication code.
#24451	Added macOS Network Shared Folders plugin.
#24464	Added installation time information to macOS Agent operating system information collection plug-in.
#24507	Added new platform information for Linux Agent.
#24545	Added a subnet parameter to the sensor which made it possible for the unused IPs to be assigned in a large subent.
#24616	Added integrity verification function for Linux Agent policy and management server information.
#24924	Added authentication user ID parameter to the Get node list (GET /nodes) API of REST API.
#25062	Added macOS Ventura support to MAC Agent.
#23947	Improved the Agent by addressing vulnerabilities identified with Secure coding check.
#24433	Improved Linux Agent so it checks for OS update using update item instead of version name.
#24463	Improved TLS communication in Linux agent by changing the cipher suite used.
#24548	Improvements have been made so that node information is displayed as a tooltip in the IP link of the audit log.
#24562	Improved the agent to use the default web browser.
#24633	Improvement made to allow units other than time units when setting the node group condition.
#24638	Improved log filter administrator activity and IP conflict alarm transmission check value to default off.
#24643	Improved to output the node list in terms of widget data criteria (node/equipment).
#24728	Improved to encrypt button link parameters in the IP use application form.
#24832	Improvements have been made so that unused IPs are also displayed when selecting all nodes in the tree on the screen.
#24918	Improved process for assigning an IP to a user so that the IP is limited to the management IP control range option.

Issues Fixed

Key	Description	Affects Version/s
#21894	Fixed an issue where a node with an unclassified node type would not be deleted when the IP/MAC usage timeout expires.	5.0.31
#24449	Fixed an issue that caused the button to become unresponsive in the Uninstall a Program plugin.	5.0.42(LTS)
#24502	Fixed the problem that the value of the option that has not been changed is corrected when the policy is modifieda.	5.0.44
#24523	Fixed an issue where certain columns were missing when exporting users.	4.0.7 5.0.42(LTS)
#24554	Fixed the problem that the paging output option was restored when the condition was deleted on the node group detail screen.	5.0.12
#24560	Fixed an issue where files in the C:program Files (x86) path could not be executed.	5.0.0
#24568	Fixed an issue where allowed APs were blocked by WLAN control.	
#24592	Fixed an issue where related data did not appear on the page moved to the button created when system log collection was completed.	5.0.40
#24608	Fixed an error in the web console smart help and linked DOCS documentation.	5.0.43
#24620	Fixed an issue where the node list was not displayed when viewing the filter and status menus.	5.0.42(LTS)
#24626	Fixed an error log output when clicking the close list button on the node detail screen.	5.0.38
#24628	Fixed an issue where the integrity check function did not work properly in macOS Agent.	5.0.27
#24630	Fixed the problem that the tooltip of the control policy column of the node registered in the center was displayed incorrectly.	5.0.27
#24645	Fixed an issue where editing of the management view was not reflected in the status & filter tag screen.	5.0.9
#24649	Fixed blocking malfunction by the Windows Firewall control plug-in when multiple rights objects were registered in the control policy.	5.0.28
#24663	Fixed the problem were the condition setting malfunctions when a comma is present in the condition setting of a node action.	5.0.0
#24665	Fixed the problem that free space on the local disk does not work when performing a backup through an external storage device.	4.0.19 4.0.149
#24685	Fixed an issue where blocked IPs set to be used were assigned when using the Allow Blocked IPs option.	4.0.12
#24701	Fixed problem were the external authentication linkage function does not work when the BASE64 encryption method is used.	5.0.0
#24707	Fixed an issue where the node list was not displayed when moving.	5.0.33
#24729	Fixed a problem where an error occurred when approval/rejection of one or more items were done individually.	4.0.113 5.0.10 4.0.149
#24733	Fixed the problem that the action policy was not executed when there are many script contents to be executed.	4.0.46 5.0.0 4.0.149
#24767	Fixed the problem that the domain information of the node was not updated by NETBIOS scan.	4.0
#24791	Fixed so that when the management IP control range is set only those IPs will be listed in the Matrix view.	
#24797	Fixed a collection error due to incorrect data format when registering a switch through SNMP information collection.	4.1.4
#24802	Fixed the problem that the real-time monitoring forced control option for V3 vaccine did not work.	5.0.0
#24808	Fixed an issue where the HTTPD daemon was duplicated when restarted and left an audit log.	4.0.149

continues on next page

Table 26 – continued from previous page

Key	Description	Affects Version/s
#24846	Fixed an issue where the IP list of the IP use application was not displayed as the IP allocation band set for the purpose.	5.0.13
#24897	Fixed a database error in macOS related settings where an audit log would occur.	5.0.45
#24905	Fixed the problem where the node is changed to the UP state when the agent is in the Down state.	5.0.47

23.2.10 Genian NAC v5.0.46 Release Notes (APR 2022)

Release Date: 2022/4/15, Last Updated: 2022/5/3 Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#17595	Added macOS Agent Device Control plugin.
#21279	Improved to be able to attach files when sending email through AWS SES.
#24178	Added Clam Antivirus information collection for Linux Agent.
#24319	Added function to handle re-registration event when Linux Agent node is deleted.
#24262	Improved the problem that mail is delivered to all users when using the Forward All option after not specifying an approver when filling out an IP application.
#24263	Improved to display the authentication user domain and authentication source in the audit log when linking SMTP authentication.
#24267	Improved to be able to set 3 or more authentication servers in Agentless AD SSO environment.
#24278	Improved to be able to change the plugin of node action even if node action is assigned as condition to node group.
#24281	The commands supported in the web console action selection menu have been improved so that they are also available as REST APIs.
#24294	Improved so when the RADIUS daemon is started, ADSDOMAINNAME not defined is not displayed when configuration is valid.
#24312	When using syslog TLS, it has been improved to use only 1.1 or later.
#24316	Added a method to delete setting values by matching IP address and HOST in Windows Agent DNS control plug-in.
#24330	Improvements have been made so that the PentaSSO extension plug-in can periodically update the authentication status.
#24458	Improved so that the wireless connection manager window is not displayed if there is no AP that can be connected.
#24469	It has been improved so that the DHCP node IP update function can be used even when registering a node through a switch.
#24493	Added ESET Endpoint Security Antivirus information collection for macOS Agent.
#24340	Improvements have been made to enable OTP and Webhook 2FA authentication in the macOS Agent agent authentication window.
#24301	Improved so that passwords are not stored in plain text when setting up SFTP for backup.
#24545	When requesting an IP within a large subnet, added the sensor's subnet parameter to the REST API so that an unused IP in the subnet can be assigned.

Issues Fixed

Key	Description	Affects Version/s
#22689	Fixed a problem where the web console device name was not changed when changing the hostname in CLI.	5.0.33
#23710	Fixed an issue where authentication could not be canceled when using the authentication restriction function in the macOS Agent authentication window.	5.0.17
#24181	Fixed an issue where the agent deletion method option did not apply in macOS Agent.	5.0.41
#24187	Fixed the problem that the hide option does not work when using wired in Windows Agent Wireless Connection Manager.	5.0.0
#24241	Fixed the problem of detecting/registering the network sensor as a normal node when there are multiple network sensors in the same band.	5.0.46
#24244	Fixed an issue where an error message was displayed during backup in the HA configuration policy server.	4.0.119 5.0.16
#24245	Fixed an issue where Windows Agent was displayed as an internal network in the tray icon tooltip when it was unable to communicate with the policy server.	5.0.43
#24266	Fixed the problem that the sensing subject of MAC/IP Clone information detected by the agent is displayed as the sensor.	5.0.46
#24290	Fixed an issue where a warning message was displayed in the sysinspect script used when checking NAC.	4.0.120 5.0.17
#24300	Fixed the problem that the Run after authentication option did not work when using the file path macro in the Windows Agent Authentication Window plug-in.	5.0.0
#24303	Fixed an issue with the IP/MAC node group CSV header if it is entered in uppercase.	5.0.43
#24314	Fixed an issue where with the display of IP information when inquiring the target node access authentication page (CWP) in the node details.	5.0.40
#24327	Fixed an issue where an error page was displayed when adding a dashboard widget audit log filter.	4.0.13 5.0.46
#24329	Fixed an issue where tags were displayed on the Windows Agent notification message and notice screen.	5.0.42(LTS) 5.0.46
#24338	Fixed the problem that the debug log was repeatedly generated when controlling the auto-run option in the Windows Agent Security Settings plug-in.	4.0.109 5.0.6
#24360	Fixed the problem that the location of the node is included in the policy server even after the agent sensor is installed on a node that does not have a management sensor.	5.0.40
#24406	Fixed an issue where automatic approval did not work when applying for a new IP through REST API.	5.0.8
#24407	Fixed an issue where the same IP was batch approved when there was not enough allocated IP when batch approval of new IP applications.	4.1.4 5.0.46
#24410	Fixed an issue where an error screen was displayed when using the user authentication component in the IP management message priority setting and the CWP design template.	4.0.143 5.0.40
#24418	Fixed the problem where the agent authentication window shutdown prohibition could be terminated by an external program.	4.1.0 5.0.0
#24424	Fixed an issue where the return button on the node detail screen would intermittently display a different screen.	5.0.31
#24430	Fixed an issue where the CWP Standard template was applied to IP Management Block nodes when using IP Management message preference.	5.0.14
#24496	Fixed an issue where the hostname of the node collected by the agent was changed by the sensor.	4.0.25 5.0.46
#24301	Fixed an issue where LOGs were not sent when backing up with SFTP.	5.0.45
#24563	Fixed an issue where some plugins with a cycle would work even if the action condition was unsatisfactory.	5.0.0

continues on next page

Table 28 – continued from previous page

Key	Description	Affects Version/s
#24577	Fixed an issue where some plug-ins with cycles worked even when macOS action conditions were unsatisfactory.	5.0.0
#24631	Fixed the problem that there is no assigned IP even though there is an unassigned IP when bulk approval of new IP applications.	5.0.46
#24660	Fixed an issue where a node's platform information was changed from Microsoft Windows to Unknown Platform.	5.0.42(LTS) 5.0.45

23.2.11 Genian NAC v5.0.45 Release Notes (FEB 2022)

Release Date: 2022/2/08, Last Updated: 2022/2/08

Description The last (R) mark is an additional release patch item.

New Features and Improvements

Key	Description
#23825	Added a function to operate an action with the last policy received when the Linux Agent center connection fails.
#23953	Added the ability to renew a self-sign certificate and register an externally generated SSL certificate in the web console.
#23221	Added Chrome and Edge control options to Windows Agent Control Web Browser Settings plugin
#23772	Added Linux Agent interface control plugin.
#22074	Improved to support more than one authentication information provider (IdP) when integrating SAML authentication.
#23468	Improvements have been made so that other webhook APIs can be called using the result of the webhook API call.
#23644	Improved filesystem checking on GenianOS system boot.
#23749	Added Linux Agent TmaxGooroomOS latest update check plugin.
#23752	Added new distribution and version information in Linux Agent.
#23865	Added Windows Agent hostname authentication custom plugin.
#23869	Added Windows Agent HTTP URL Authentication custom plugin.
#23880	Improved agent abnormal behavior when changing Linux Agent OS login user or logout/re-login.
#23943	Improved the part where Korean is displayed when creating an English audit log in the web console.
#23945	Added a plug-in to control the security options of the Edge browser in Windows Agent.
#23964	Improvements have been made to display the virtual type in the connection method in the Web console node information > interface information.
#24010	When changing the network sensor name in the web console, the changed sensor name in the list is applied immediately.
#22690	Improved the part where all audit logs are displayed even when the manager node management scope is restricted.
#23189	Added screensaver and desktop control options to the macOS Agent Appearance and Personalization plugin.
#23817	When using the IP application system email step-by-step approval, the step-by-step approver sends an email to other administrators when the application is approved.
#23918	Improvements have been made so that more than one node action of the same single plugin cannot be assigned to a node policy.
#23980	Improved the ability to send query reports to multiple emails in the audit report.

continues on next page

Table 29 – continued from previous page

Key	Description
#24082	The REST API /nodes/{nodeid}/tags API has been improved so that node/MAC/user tags can also be viewed.
#24165	Improvements have been made so that HTML tags are not displayed on the recipient screen when HTML tags are entered in the Web console instance message.
#24172	Improvements have been made so that Tomcat version information is not exposed when Bad Request (400) occurs when accessing the web console.
#23653	In case of RADIUS CoA interworking with Cisco Switch, it has been improved so that only minimal information is transmitted through CoA.
#23961	Improvements have been made so that virtual interfaces are not included in the wired/wireless interface conditions among the node group conditions.
#24302	A macro has been added so that encryption method MD5 (MD5B64) can be used when interworking with webhook authentication.
#23802	Improvements have been made to distinguish between patches and upgrades when software update guidance is provided.
#21279	Improved to be able to attach files when sending email through AWS SES.

Issues Fixed

Key	Description	Affects Version/s
#23819	Fixed an issue where the tomcat webapps folder did not exist, preventing setting up a custom web application.	5.0.40
#23835	Fixed an issue where the Add Equipment Lifecycle field could not be used as a condition in the node group condition item.	5.0.40 4.0.147
#23894	Fixed an error that occurred if the date limit of the end of use of additional fields was not set in the IP application form.	5.0.43
#23917	Fixed an issue where Virtual IP settings were not being applied in the Web Console Sensor IP Settings page.	5.0.41
#23923	Fixed an issue where the node information was deleted by collecting information without a value from the Windows Agent information collection plug-in.	5.0.0
#23925	Fixed an issue where packets forwarded from the Alias IP network sensor were forwarded to the Default Gateway.	5.0.42
#23949	Fixed an issue where an approval request email was sent even if visitor email approval was not used when registering a new user.	4.0.M8
#23950	Fixed the problem that synchronization fails in case of HTTPS URL when information synchronization DB type is set to CSV and the file location is used as URL.	4.0.5 4.0.147
#23952	Fixed a problem where automatic login to the IP application system was not possible with HTTP protocol.	5.0.27
#23962	Fixed an issue where control policy permissions were not assigned to control policy if the object name contained special characters.	4.0.M8
#23997	Fixed an error that occurred when creating a network object in the permission object setting screen and moving back to the network object editing screen.	5.0.25
#24002	Fixed an issue where the Linux Agent tray icon was not displayed.	5.0.42
#24005	Fixed an issue that prevented the file distribution plugin from downloading files when using HTTPS URLs.	5.0.0 4.0.147
#24011	Fixed an issue where RADIUS authentication would fail if the number of RADIUS Attributes is large.	5.0.24

continues on next page

Table 30 – continued from previous page

Key	Description	Affects Version/s
#24071	Fixed the problem that the CWP new user registration screen did not display even if the user authentication option was used.	5.0.42
#24110	Fixed an issue where incorrect authentication values were linked with the Smart NAC alternative authentication plugin.	5.0.41
#24136	Fixed the problem that incorrect information was displayed in the node group item setting value when there is in the node action name.	5.0.14
#24113	Fixed a problem where menu settings were not processed when modifying the web console default management role	5.0.0
#24120	Fixed an error that occurred when creating a service role for API integration.	5.0.42
#24139	Fixed an issue that incorrectly expressed the total amount of storage devices collected by Windows Agent.	5.0.0 4.0.147
#24147	Fixed an issue where is displayed in the tooltip of the audit log description column.	5.0.22
#24153	Fixed the problem that incorrect text is displayed in the background when is present in the IP management matrix view tooltip.	4.0.12
#24194	Fixed an issue where user groups were not renewed when user passwords were updated in plain text.	5.0.44
#23855	When registering a switch manually, the sensor tree switch information is updated if there is a switch IP of a different band in the same switch.	4.0.117 5.0.14
#24092	Fixed the problem that the input items did not change depending on the selection when setting the node group condition.	5.0.20
#24188	Fixed the problem that the screen does not move when processing the application for priority use approval in the mail approval waiting item in the IP application system.	5.0.13
#24254	Fixed an issue where the winbindd daemon would not shut down when the RADIUS daemon was shut down.	5.0.35 4.0.147
#24261	Policy Server HA Configuration Fixed an issue where the device type of the Virtual IP node was registered as a node other than the Policy Server.	5.0.40 4.0.148
#24268	Fixed an issue where automatic generation of audit log node snapshot reports failed.	
#24350	Fixed the problem that the setting UI was not displayed normally when the execution type of the node action being used was changed.	
#24364	Fixed a problem where multiple IP collision protection settings were not available in the web console.	5.0.42
#24434	Fixed the problem that the contents were not saved even if the node type was specified on the node detail screen.	5.0.44
#24467	Fixed a problem that the column was not displayed in the list when adding a rank column in the node management list.	5.0.33
#24479	Fixed an issue where the license exceeded text was displayed even if the license was not exceeded in certain environments.	4.1.M3 5.0.42
#24429	Fixed an issue that took a long time to complete information synchronization	5.0.23
#24415	Fixed an issue where a Lib error occurred when synchronizing information with Oracle 11g r2 or later.	

23.2.12 Genian NAC v5.0.44 Release Notes (DEC 2021)

Release Date: 2021/12/07, Last Updated: 2021/12/07

Description The last (R) mark is an additional release patch item.

Security Advisories

- *GN-SA-2021-003: Genian NAC - Multiple Log4j Vulnerabilities*

New Features and Improvements

Key	Description
#23391	For On-Prem Genian NAC, the Linux Kernel version has been upgraded to 5.10.60 to support the latest drivers.
#23658	Added MDNS real-time hostname detection to existing hostname detection capabilities.
#23771	Improved the sensor system restart option so that a sensor can be restarted even when the keepalive status is down.
#20083	Improved the node batch task menu option to include progress bar that displays status of task completion.
#22673	Added OS category to Add Agent Action window in Node Policy which allows Admins to filter Agent Actions by OS version.
#23366	Separated Agentless AD SSO settings from LDAP authentication integration. – sent recommended page improvements to Kyeyeon
#23516	Added an option to terminate applications on shutdown to the Windows Agent shutdown plug-in.
#23570	Improved to enable multiple selection / deselections via shift key in IP matrix view.
#23583	In the node management list, improved the department level displayed to include multiple levels of department membership.
#23602	Improved CLI DB Migration process to display detailed step-by-step status and progress.
#23618	Improved display of conditions when searching for hardware from the node list to include required conditions.
#23344	The Beta Features / Lab menu has been removed from the Preferences menu and features previously listed moved to permanent menu location.
#23367	Added 2-Step Authentication (2FA/MFA) options to RADIUS Policy.
#23895	Added Oracle Database version 19c option to Data Synchronization menu.
#23896	Improved performance of Management menu display for large enterprise environments.
#24020	Added a date range search option to the REST API for search parameters.

Issues Fixed

Key	Description	Affects Versions
#23217	Fixed a problem where all users could be deleted due to a file read error when synchronizing CSV user information.	4.0.1
#23440	Corrected the problem that the network drive is included in the entire scan through Antivirus integration	4.1.0 5.0.0
#23519	Fixed an issue where the number of nodes in the software collection status did not match the number of nodes in the node management.	5.0.38
#23534	Fixed an issue where GDPI links for nodes registered with agents were not displayed.	5.0.39

continues on next page

Table 32 – continued from previous page

Key	Description	Affects Version/s
#23553	Fixed the problem that the html tag is displayed when a file upload error is output on the CWP user registration page.	4.0.106
#23571	Fixed an erroneous error that was displayed during configuration of a custom button related to file uploads.	4.0.106
#23599	Fixed the problem that if tags are deleted without updating the node detail screen, the tag is not deleted.	5.0.22
#23609	Fixed the incorrect minimum value of the node health check minimum interval option of the network sensor.	5.0.38
#23625	Fixed the problem that an error occurred on the login page when the administrator account WEBUI access IP was set to any /0 value other than 0.0.0.0/0	5.0.41
#23657	Fixed an issue where the license file was not registered in Genian Syncer.	4.0.144 5.0.41
#23755	Fixed the problem that Syslog audit log filter addition/deletion did not work properly in the environment setting audit log.	4.0.145
#23773	Improved to the Log > Debug > system menu to display only the list of files and folders in the current path.	5.0.44
#23788	Fixed the problem that data could not be searched when sorting the use location on the IP use application result inquiry screen.	4.1.0 4.0.23
#23804	In the switch management menu, corrected an error that was displayed when the administrator checks admin down in the port setting.	4.0.106
#23845	Fixed an error that occurred when displaying the results of the audit log search filter in an analysis chart.	4.0.14
#23026	Fixed the problem that the file upload addition field for IP application did not work properly.	5.0.36
#23948	Fixed an issue where SNMPv3 switch information was abnormally collected during the SNMP information collection process.	5.0.41
#24025	Fixed the problem that the function of adding nodes to the node basket in the web console node list did not work.	5.0.44
#24066	Fixed an issue where synchronization failed due to file read failure when using information synchronization with CSV files.	4.0.146 5.0.44
#24072	Fixed the problem that Tomcat could not use the DB password registered in the Config file.	4.0.146 5.0.44
#24118	Fixed to collect some missing information from the macOS Agent software info-gathering plugin.	5.0.0
#24122	Fixed the problem that the contents of the set column were not displayed when multiple administrators added the custom management view in the Web console node management.	5.0.42

23.2.13 Genian NAC v5.0.43 Release Notes (SEP 2021)

Release Date: 2021/10/06, Last Updated: 2021/11/05

Important: There are incompatible API changes in this release. Network sensors and agents must be upgraded to the same version as the policy server.

Description The last (R) mark is an additional release patch item.

Security Advisories

- *GN-SA-2021-002: Genian NAC - Multiple Vulnerability*

New Features

Key	Description
#22536	Added Windows Agent extension plug-in to the image so that it installs along with the first installation of the product.
#22591	Added a function to collectively register wireless LANs in the web console wireless LAN management menu.
#22890	Added check action only for Linux Agent execution condition.
#22084	Added execution condition check function to Linux Agent action.
#23211	Added Linux Agent Tray Icon display function.
#23350	Added the ability to display the Linux Agent Tray Menu and program information screen.
#23260	Windows Agent supports Windows 11.

Improvements

Key	Description
#23075	Added case conversion macro to syslog audit log filter macro.
#22607	Added a function to load and add a CSV file when entering node group IP/MAC.
#23185	Improved so that an audit log is left when password change is forced in basic information when user information is modified.
#22847	Added SSO plug-in to Windows Agent for authentication linkage with Nets' ESSO system.
#22542	Export and search functions have been added to the Web Console Status & Filter > Risk Node Status screen.
#22966	Improvements have been made so that the expiration date is reflected when applying for a new application using an Excel file in the IP application system.
#23110	When the subnets of the network sensor and the agent are different, the broadcast method is selected by adjusting the options.
#23190	Improved to support macOS Monterey of macOS Agent.
#23323	Improved the output of the dangerous node status list in the web console node management status & filter.
#23348	Improvements have been made so that the port number is not entered in the ICMP protocol when creating a service object.
#23435	Added an option to filter by sensor status when checking the status of all network sensors in the Policy Server CLI.
#23175	When detecting the node connection method through SNMP information collection, the wireless connection has priority when detecting both wired and wireless.
#23723	When collecting SNMP switch information, it is improved to also collect MAC table information of a Juniper Switch.
#23627	Improved to perform version verification of licenses registered in the product.

Issues Fixed

Key	Description	Affects Version/s
#22821	Fixed an issue where some node types were not displayed in the dashboard node type widget.	5.0.40
#23119	Fixed an issue where the latest synchronization time information was not updated when an information synchronization error occurred.	5.0.17
#23127	Fixed an issue where unassigned nodes were found when searching for AgentActionName in the Web Console node condition search.	5.0.26
#23152	Fixed the problem with the daily report email.	5.0.26
#23187	Fixed an issue where information from SNMP Version 2 switches was not being collected.	5.0.17
#23220	Fixed an issue where synchronization would fail when using CSV User,Department,Title Synchronization as one setting.	4.0.0
#23292	Fixed the problem that the access AP information of the node remains even if the wireless LAN AP is deleted.	4.0.0
#23306	Fixed the problem that the domain information is updated with the information collected from the network sensor even though the agent exists in the node.	4.0.0
#23310	Fixed an issue where the total number of agents in the dashboard overview widget and the search results in node search did not match.	5.0.22
#23404	Fixed the problem that when deleting a node that does not belong to the network sensor management target IP, it is not excluded from the node group.	3.5.0
#23426	Fixed the problem that the number of devices in the web console license information and the number of nodes in the node list displayed when clicked do not match.	5.0.26
#23460	Fixed a problem that Internet connection sharing was not released through the Windows Agent interface control plug-in.	4.1.0, 5.0.0
#23489	Fixed the problem that the node platform widget link does not work when the node platform name contains an apostrophe.	5.0.20
#23761	Fixed an issue where file management/file distribution actions could not be assigned in the node policy creation wizard.	5.0.36
#23780	Fixed an issue where the values were not saved as values written in CSV when importing users to CSV in the User Management menu.	5.0.41

Cloud

Key	Type	Description	Affects Version/s	Fixed Version/s
#23639	Improvement	Improved the problem that OS-related images are not displayed on the policy menu node group list screen.		5.0.43

23.2.14 Genian NAC v5.0.41 Release Notes(JUN 2021)

New Features

Key	Description
#22438	Added a function to input the policy server IP during the Windows Agent installation process if there is no policy server IP information detected.

Improvements

Key	Description
#22210	The Windows Agent Manage Files plugin can now create folders if they do not exist when distributing files.
#22261	Improved User interface when using Google OTP for administrator login.
#22463	Improved column sorting function for Node Groups and node lists in the Web Console.
#22471	macOS Agents can be deleted by the end user without a verification code.
#22484	Added macro support for custom button links in the captive web portal.
#22501	Added logging support for device model name and serial number.
#22516	Improved macOS Agent CPU info collection error handling for M1 endpoints.
#22522	Added boot configuration collection to the Windows Agent OS information collection plugin.
#22613	VLAN interface DHCP client options added to the Policy Server and Network Sensor Installation Wizard.
#22619	Windows Agent authentication plugin failed attempt lockout function has been improved to persist even if the Agent is terminated.
#22621	Added department structure (Device info) verbosity options to logs.
#22635	Timezone settings have been removed from the Policy Server and Network Sensor Installation Wizard.
#22676	Policy change confirmation popups have been improved to use Agent Action plugin names rather than numbers.
#22707	Improved UI support for the main menu bar when displayed in narrow windows.
#22771	Improve performance when of the cache function when using the Policy Server as a Windows Update proxy.
#22942	Removed the ability to stop the Windows Agent via DOS command.

Issues Fixed

Key	Description
#22411	Fixed an error where Node Policy authentication options could not be changed.
#22433	Fixed an error where the file upload function in the user registration captive portal screen did not work.
#22778	Fixed an error where the node name could not be used in the node search bar.
#22514	Improved performance of the Windows Agent Uninstall Programs plugin.
#22517	Fixed an error where the Web Console Quick Search and detailed results did not match.
#22543	Fixed an error where logs were not generated after synchronizing device lifecycle info.
#22560	Improved the accuracy of Windows Agent Collect OS Information plugin when detecting Appearance and Personalization info.
#22568	Fixed an error where IPAM policy status as a search criteria did not provide accurate results.
#22584	Fixed an error where computer reboots interfered with Windows Agent reathentication function.
#22623	Fixed an error where CLI batch config did not support dhcp commands.

continues on next page

Table 39 – continued from previous page

Key	Description
#22649	Fixed an error where logging was not generated by changing MAC address compliance settings in specific bands.
#22674	Fixed an error where WLAN policies could be deleted while in use.
#22677	Fixed an error where the captive portal login lock did not work.
#22684	Fixed an error where Policy change confirmation popups listed inaccurate info.
#22708	Fixed an error where node tags could not be set from the node list in the node details view.
#22736	Improved the function of macOS Agent integrity check and repair function.
#22751	Fixed an error where the tag display widget did not redirect to a list of nodes with the selected tag.
#22763	Fixed an error where the node type of MAC/IP Clones were incorrectly identified.
#22788	Fixed an error where Windows Agent Collect OS Information plugin could not detect domain info in an Active Directory environment.
#22800	Fixed an error where temporary user account requests were not shown in the Genian NAC Monitor app.
#22801	Fixed an error where changes to the reconnection settings in the Windows Agent ontrol wireless connection manager plugin were not applied.
#22834	Fixed an error where Node Policies and Enforcement Policies could not be deleted and an incorrect error message was displayed.
#22884	Fixed an error that occured when Windows Agent plugins were updated before the base agent software.
#22938	Fixed an error where the Policy Server process crashed due to abnormal processing of keepalive events.

Cloud

Key	Type	Description
#22301	New Feature	Platform Detection upgraded to use the GDPI API.
#22724	Problem	Fixed an issue where the Policy Server was not displayed in the Sensor tree if there were no Network Sensors registered in the Policy Server.

23.2.15 Genian NAC v5.0.40 Release Notes (APR 2021)

New Features

Key	Description
#21832	Added TLS SNI filtering function for FQDN network group when performing access control.
#22176	Display authenticated users owned equipment in the Wake on LAN screen in the Captive portal
#22240	Added the ability to manually register a new node for a previously registered device.
#22351	Added the ability to set IP conflict and change prevention on a designated network segment/subnet.

Improvements

Key	Description
#21239	Added support for setting failsafe options independently on each sensor interface
#21598	Added an "additional" button to the node group config menu to easily add multiple conditions
#21620	Added the ability to display device life cycle information columns in the node management screen.
#21937	Added performance improvements to the windows agent sensor.
#21940	Improved Virtual IP accounting of High availanility interfaces.
#22015	System Debug logs have been moved to the main logs screen.
#22076	The user list CSV export format has been improved so that it matches with the supported user import CSV format.
#22168	Added an improvement so when a node is deleted the corresponding IP change/conflict prevention rules are also deleted.
#22202	Added a feature so that sensor alias interfaces will be displayed in the tree panel with an "SA" icon.
#22203	Added support for importing additional field data when manually registering a node.
#22212	Improved the captioning and instructions for 2 factor authentication for admin web console access.
#22238	The inactive node policy update option has been improved so that it can be applied for each node policy.
#22254	When using SSL connections to the captive web portal attempted insecure connections will automatically be redirected to use HTTPS.
#22219	Added an option to send using a new socket when sending Windows Agent Keepalive.
#21970	Improved to update AP information using agent interface information plugin.
#22184	Improved stability of the agent user interface.
#22186	Improved the user management function so that departments can be deleted without removing the department info from all users.
#22201	Added an option to perform two-step verification when exporting information to XLS files from the web console.
#22205	Added the ability to specify NMAP scan options under sensor settings.
#22296	Fixed a problem where Vlan interface and alias interfaces with the same number cause internal errors.
#22326	Improved authentication logging to include more node and device information.
#22341	Added an option to delete dormant users in the User Management menu.
#22355	Added the ability to enable or disable debug logs keepalive of policy server and sensor.
#22366	Improved the stability of Agentless Active Directory SSO to function when the authenticated node changes IP addresses.
#22380	Improved the ability to detect and display WPA3.
#22391	Added input validation for Node-Type when registering nodes using REST API.
#22407	Upgraded Tomcat version for improved security.
#22408	Added the ability to detect 802.11ax using the Windows Agent Control Wireless LAN plugin.
#22620	Improved performance when exporting web console info in Excel spreadsheet format.

Issues Fixed

Key	Description
#22056	Fixed a problem in which additional fields were not updated through the user selector in the web console new node detail screen.
#22093	Fixed an issue where the information of nodes not managed by the sensor were displayed when outputting Matrix View of the Web console.
#22153	Fixed an issue where the information update would intermittently fail when a secondary IP was present on the PC interface.
#22161	Fixed a problem where sorting by CVE-ID in the Web console CVE status list did not work.

continues on next page

Table 43 – continued from previous page

Key	Description
#22165	Fixed a problem where logs could not be displayed within a time range starting with 00:00.
#22171	Fixed an issue where the code authentication function did not work in the Windows Agent interface control plug-in .
#22206	Fixed a problem where the Windows Agent wireless LAN control plugin caused a database data duplication error.
#22231	Fixed a problem where the hint phrase was not displayed in the password change screen in the captive portal.
#22285	Fixed a problem where the Check Conditions agent plugin does not check all conditions.
#21500	Fixed a problem where the Captive Portal preview template is applied to the actual captive portal before admin confirmation.
#21860	Fixed a problem where nodes registered via switch SNMP query incorrectly formatted the MAC address and were registered as duplicate nodes.
#22042	fixed an issue where the macOS Agent Keepalive failed to transmit.
#22241	Fixed a problem where some update items could not be searched when performing Windows Agent Windows Update through a proxy.
#22258	Fixed an issue where the Windows Agent GnPMS process would intermittently crash.
#22303	Fixed an issue where the CWP page customization button was not centered when used in 2 lines.
#22315	Fixed an issue where nodes could not be grouped by motherboard type when the type value was "unknown."
#22317	Fixed an issue where additional fields (10-20) were not entered in the web console node property import.
#22327	Fixed an issue where the anomaly detection policies with special characters were not assigned to the node policy.
#22345	Fixed an issue where the captive portal user import page did not properly display error messages.
#22383	Fixed a problem where an error screen was displayed when clicking the mirror sensor IP (0.0.0.0) in the IP matrix view of the web console.
#22406	Fixed a problem where node groups containing terms like "UPDATE" and "BY" could not be searched for without causing an error.
#22424	Fixed an issue where values such as maintenance expiration date were not updated when uploading a license file.
#22441	fixed an issue where the macOS Agent tray could only be displayed in English.
#22464	Fixed a time check related error on the macOS Agent OS Update plugin.
#22469	Fixed an issue where the Windows Agent OS information collection plugin performed updates when no change had occurred.

Cloud

Key	Description
#22385	Fixed an issue where the syscollect feature did not work.
#22292	Added Amazon AWS public IP info in the web console system port menu.

23.2.16 Genian NAC v5.0.39 Release Notes (FEB 2021)

Click here to watch the highlights

New Features

Key	Description
#20093	Added a widget to compare the number of nodes in different groups using various chart formats.
#21827	Added a status/filter screen and multiple widgets for displaying CVE's that are recently associated with managed nodes.

Improvements

Key	Description
#15682	Added the option to enable or disable backup when performing a system update.
#21269	Improved the custom button feature so that deleting the button also deleted the associated image file.
#21529	[macOS Agent] Added Support for macOS Big Sur (Intel). New Hardware support is planned.
#21782	Improved to show "EarlyRole" policies in the Web Console (Policies that the mirror sensor can apply to unregistered nodes).
#21899	Improved display layout of the captive web portal.
#21985	Improved the Web Console to be more resistant to XSS attacks.
#22004	Improved Device Platform Intelligence and CVE display for nodes registered by Genians Agent.
#22018	Added optional debug logging for Webhook notifications.
#22081	Improved macOS node detection to avoid duplicate detection .
#22089	[Windows Agent] Added the option to launch pop-up forms using the default browser.
#22091	Improved kernel debugging for the sensor enforcer.
#22117	Improved the Web Console behavior when editing network objects.
#22133	[Windows Agent] Improved the image quality of the Agent UI when using display magnification.
#22134	Improved multi-language support. English text is substituted when the selected language is not available.
#22136	Added an option to define custom fields as required.

Issues Fixed

Key	Description
#22078	Fixed an issue where custom field content could not be set as a node group condition.
#22108	Fixed an issue where the Web Console did not correctly reflect failover in High Availability deployments.
#22163	Corrected the Link from the "Genian Data" section in the Web Console to the Platform Information update log.
#22182	Fixed a problem where log event for user deletion was duplicated.

23.2.17 Genian NAC v5.0.38 Release Notes (DEC 2020)

New Features

Key	Description
#21674	[Windows Agent] The Windows agent MSI file no longer needs to be manually configured before distributing to endpoints.
#21933	Added a function for Data Synchronization using REST API.
#21964	Added a function to activate/deactivate network sensors from the Policy Server CLI.
#21997	Added a function to check the status of network sensors from the Policy Server CLI.
#21270	Added the ability to download Node/Log/Wireless LAN reports.

Improvements

Key	Description
#19820	Improved responsiveness of the CWP when the "Require User Reauthentication" command is executed on a node.
#21254	Improved responsiveness when changing Agent action execution cycle times.
#21605	Improved logging of changes to monitored switches and ports.
#21896	Improved internal system logging for the Policy Server process.
#21935	Added the ability to manage Aruba virtual controllers using SNMP using the Switch Management feature set.
#21965	Removed unnecessary NTP related content from the Sensor installation process.
#22019	Updated Nmap version for node discovery.
#22034	Increased max character length for Agent pop-up notification titles.
#20973	Added the ability to register a public certificate (ssl.cer) in the web console.

Issues Fixed

Key	Description
#21947	Fixed a problem where previously configured input validation was not properly disabled.
#21982	Fixed a problem where Windows OS patch status was set as both compliant and non-compliant.
#22008	Fixed a problem where the CWP showed the wrong Time Zone.
#21882	Fixed a problem where the CWP did not accept correct responses to user security questions.
#21943	[Agent] Fixed a problem where user authentication via the agent did not trigger the program specified in the "Run After Authentication" option.
#22045	[Agent] Fixed a problem where agent log collection from the Web Console failed due to connection time out.
#21958	Fixed a problem where users could not access the CWP through a VPN interface.
#22006	Fixed a problem where the User Department tree list did not properly display in the Web Console.
#22010	[macOS Agent] Fixed a problem where information updates failed due to duplicate data.
#22037	Fixed a problem where a prohibited virtual interface on an endpoint was not blocked.
#22101	[macOS Agent] Fixed a problem where agent actions were not performed at their set interval.
#22177	Fixed a problem where tags applied via REST API did not trigger a policy update.
#22141	Fixed a problem where custom node fields could not be configured properly.

23.2.18 Genian NAC v5.0.37 Release Notes (NOV 2020)

Click here to watch the highlights

New Features

Key	Description
#20192	[Agent] Added the ability to collect Windows multi-boot (BCD) information using the "Collecting Computer OS Information" plugin
#21876	Added a function to import audit logs written in CSV format to the log server has been added.

Improvements

Key	Description
#21028	**AD/LDAP Group Membership** inclusion condition has been added as a detailed option in the **RADIUS policy** condition setting item **User-Name**.
#21379	Added a display icon to show if the Policy Server can support agents in an IPv6 environment.
#21778	Improved the loading speed of the Switch Management tree menu.
#21780	Added the ability to change the Permission etting of the Default Enforcement Policy.
#21784	Added support for grouping nodes by their installed software versions.
#21808	Added support for grouping nodes by the date of their consent to usage policies(captive portal) and support for multiple consent forms.
#21831	[Agent] Added the ability to download endpoint agent logs from the web console.
#21853	Added the ability to separately enable or disable ARP Enforcement for Local Network traffic or Remote Network traffic.
#21869	Added the ability to filter incoming syslogs using regular expressions.
#21870	[Agent] Added the ability to initiate endpoint agent log collection from the web console.
#21878	Added support for SHA-256 password encryption for the policy server database access account
#21879	A security vulnerability in the captive portal that allowed for stolen authentication authority has been fixed.
#21885	Changed the sensor registration method so that added sensors will be identifed by a static IP if one is configured

Issues Fixed

Key	Description
#21798	Improved error checking has been added when changing the data-server access-list in the Policy Server CLI
#21815	Fixed an issue where the Policy Server and Network Sensor did not consistently enforce policy.
#21819	An error requiring administrator information when using the captive portal password search function has been corrected.
#21830	Fixed a problem where the detection source of a nodes platform info was incorrectly listed as DHCP Server Scan

23.2.19 Genian NAC v5.0.36 Release Notes (OCT 2020)

New Features

Key	Description
#21743	Added support for gathering sensor settings via REST API.

Improvements

Key	Description
#21396	Improved SQL syntax checking in the Node Management search bar.
#21530	Improved Captive Portal password recovery to show both SMS and Email methods.
#21681	[macOS Agent] Network information collection plug-in has been improved to collect DHCP usage information.
#21692	Improved performance of Agentless AD SSO feature.
#21696	Improved performance of user info sync feature.
#21725	[Agent] Uninstall Programs plug-in setting has been improved so that multiple program names can be set.
#21761	Improved product SOAP to support Server Name Indication (SNI).
#21802	Improved NAC backup to be able to use SMB2 version in external storage device CIFS method.
#21823	Added a search function to the web console debug log tree.
#21828	Web console node group management list output performance has been improved.

Issues Fixed

Key	Description
#20914	Fixed an error impacting Windows products platform detection.
#21583	[Agent] Fixed instability of the Windows Agent in AD environments.
#21678	Fixed a problem where some column information was not properly registered when importing user information in bulk.
#21732	[Agent] Fixed instability when changing agent exectuion account on Windows endpoints.
#21746	Fixed a problem where files in the VC directory of the MASTER policy server could be deleted in the policy server HA environment.
#21754	Fixed an issue where the Captive Portal Password recovery menu behaved abnormally.
#21757	Fixed an issue where the node connection method detected by the switch SNMP was changed to outdated information after the node scan.
#21769	Fixed a problem where the system error page was displayed when the security question was not entered when using forgot administrator password.
#21787	Fixed a problem where the node information could be checked despite screen view restriction set for the admin account.

23.2.20 Genian NAC v5.0.35 Release Notes (SEP 2020)

Click here to watch the highlights

New Features

Key	Description
#21721	Added Policy Server AMI to the AWS Marketplace.
#20077	Added the ability to reassign a Switch Port VLAN through SNMP in an Enforcement Policy.
#21037	An operation status indicator has been added to the web console switch management list.

Improvements

Key	Description
#20144	[macOS Agent] Added improvements to the execution options of the file management plugin.
#20329	Added a link from the switch port view page to the SNMP Community Assignment page.
#21544	Improved Webhook Authentication integration content-type options.
#21546	[Windows Agent] Improved the Wireless Connection Manager Plugin to show when SSID signal is undetected.
#21549	Added Cisco-AVPair detailed attribute key to RADIUS policy.
#21550	Improved to leave an audit log when receiving a RADIUS account packet even if the RADIUS authentication based Single sign on is not used.
#21552	[macOS Agent] Added improvements to the execution options of the file deployment plugin.
#21579	Improved compatibility with Cisco AnyConnect VPN.
#21587	Web console connection port/switch/port term has been changed to connection device/connection port/connection device/connection port.
#21588	Web console 802.1x menu name has been changed to RADIUS policy .
#21590	Added Audit records for RADIUS policy and RADIUS ACCOUNT information.
#21592	When receiving a DHCP request the device has been improved to transmit NAK for a request that is not Offer.
#21601	The RADIUS policy column has been added to the RADIUS audit record.
#21621	Improved CWP user information page so that passwords are not displayed in plain text when using developer tools on the user terminal.
#21634	Added macro support for url-redirect RADIUS CoA values.
#21647	The database server in the product has been upgraded to 5.6.48.
#21650	[Agent] The ability to detect and recover when agent GnStart service properties are changed has been added.
#21660	Added support for spaces in custom node type names.
#21676	Improved the speed of results from the node search feature.

Issues Fixed

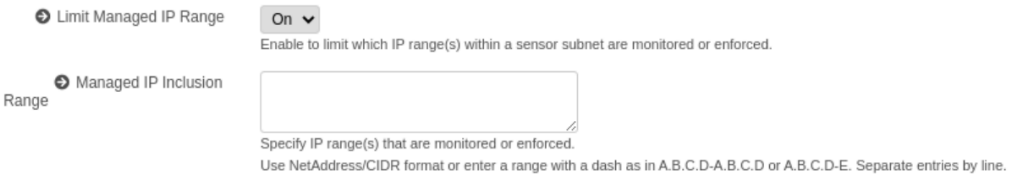
Key	Description
#20724	Fixed a problem where RADIUS server client authentication keys could not be modified.
#21556	Fixed a problem where multiple authentication guidance messages displayed following delayed loading of the Captive Portal authentication page.
#21592	Fixed an issue where the processing date was not displayed in the IP usage request result message.
#21595	Fixed a problem where debug logs older than 30 days were delted without warning after running log collection(syscollect).
#21612	Fixed a problem in which AD join fails when the AD server's Pre-Win2k domain and AD domain are different and authentication is linked with the RADIUS AD server.
#21622	Fixed a problem where the password of a general user account could be changed in the function of finding the administrator password on the web console login page.
#21632	[Agent] Fixed an issue that prevented the agent from collecting network information from certain PCs.
#21639	Fixed a problem where the tag assignment time was not set on the node detail screen while using Internet Explorer.
#21658	Fixed a problem in which only the currently running node information was updated when the node's hostname/domain information was updated.
#21707	Fixed a problem wherethe search filter did not work when the search range of the IP application system application processing result is within the applicant ID.

23.2.21 Genian NAC v5.0.34 Release Notes (AUG 2020)

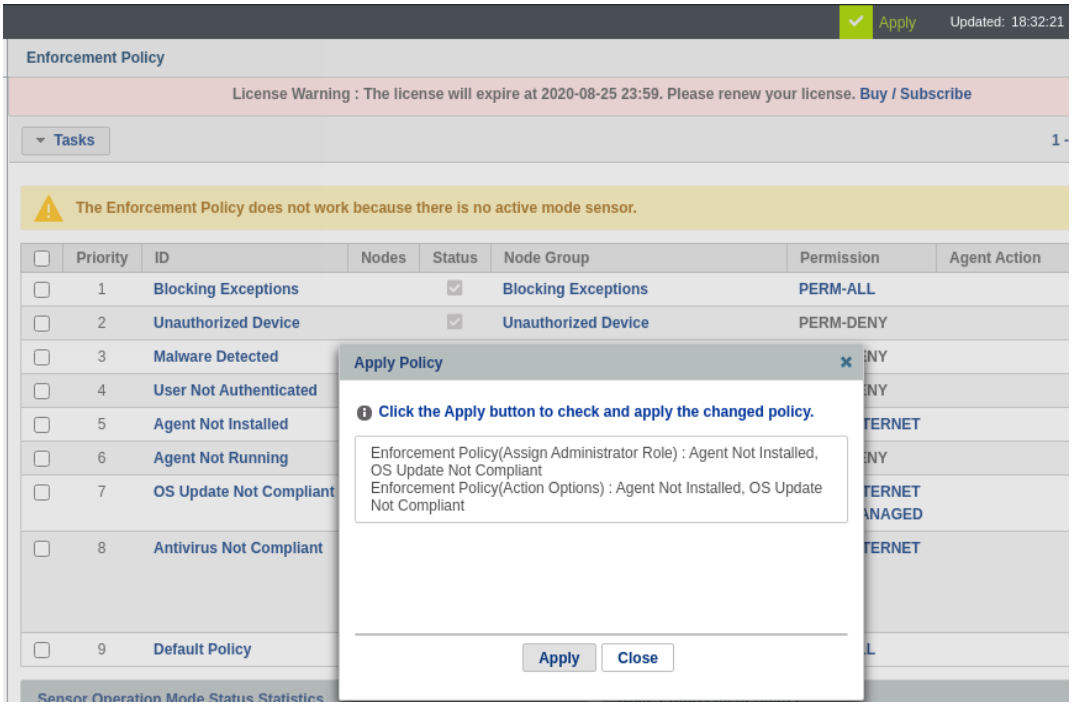
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

- Added Multi-domain support for RADIUS 802.1X Authentication(#21416)
- Added the ability to limit managed IP range of the Sensor(#21328)



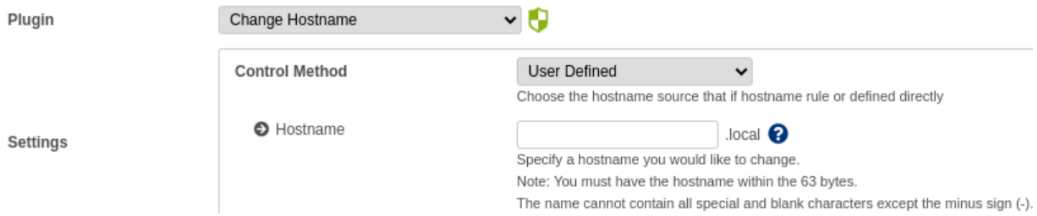
- Added Enforcement Policy change review before applying policy(#20476)



- Added option to pin agent launched web browser window above other windows(#21521)
- Added Self-signed certificate renewal via CLI command(#21547)

```
genian# do cert-reissuance
Are you sure to reissue certificate (y/N): y
Are you sure to backup existing certificate (Y/n): y
Do you want to start service after reissue certificate? (Y/n): y
Starting backup cert...done
Starting genssl key...done
Stopping Service...done
Starting Service...done
Backup certificate Path: /disk/data/CERTBACKUP/certs-20200804182350.tar.gz
genian#
```

- Allow for installation via bootable USB creating using Etcher(#21266)
- [macOS Agent] Added host name change plugin(#21427)



Issues Fixed

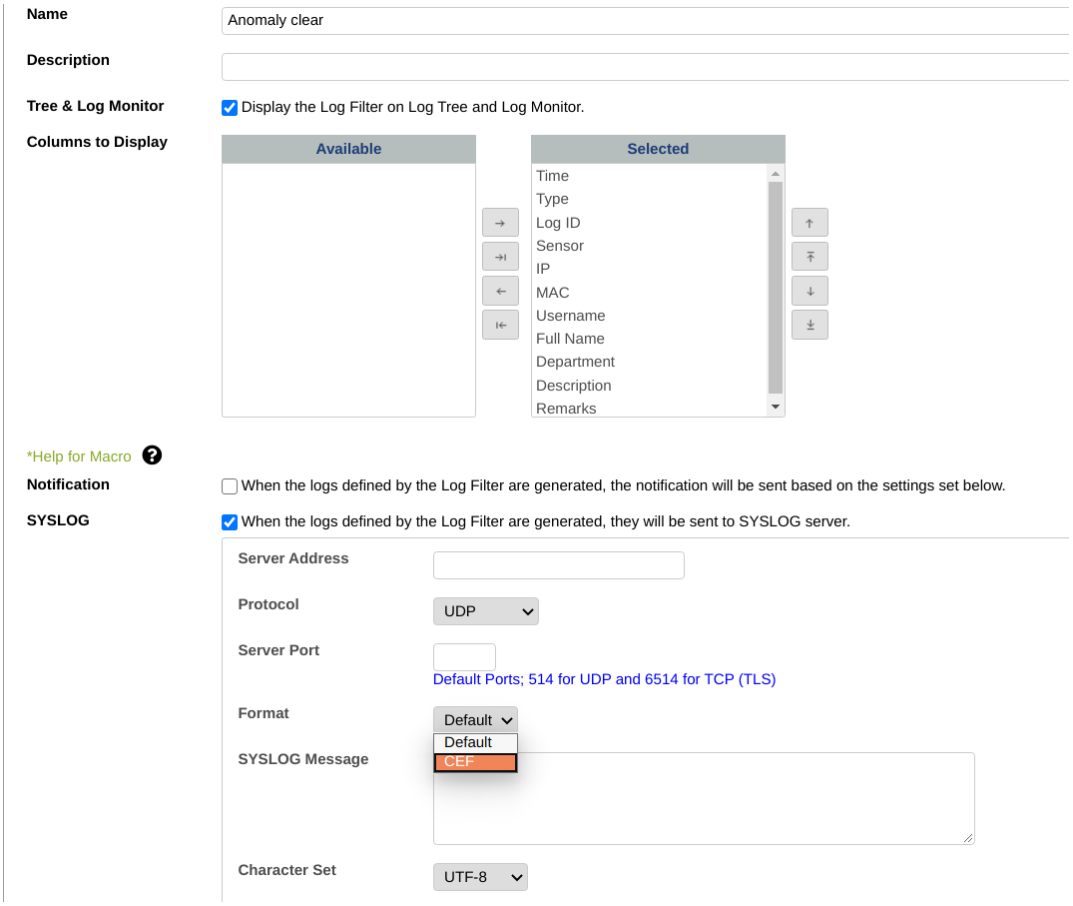
- Improved Internet Explorer browser support for Captive Portal preview(#21223)
- Fixed an issue where RADIUS log IDs were displayed in the wrong log section(#21501)
- Fixed an issue where user account history was not completely deleted(#21481)
- Fixed an issue where entered passwords were not shown in Internet Explorer(#21462)
- Fixed an issue where 802.1X policy could be created without a name(#21452)
- Fixed an issue where the Sensor was unable to send pings from the correct source IP in the CLI(#21412)
- Fixed an issue where using "-" in a cloud site name caused database errors(#21401)
- Fixed an incorrect error message shown when a login attempt used the wrong password(#21363)
- Fixed an incorrect error message for browser time zone/admin account time zone mismatch(#21273)
- Added a time range caption to the graph column of the report section(#21271)
- Fixed an issue where node groups cannot be created using conditions without user inputs(#21438)
- Improved the speed of RADIUS and Agentless WMI SSO(#21692)
- [macOS Agent] fixed an issue where logs were not generated(#21381)

23.2.22 Genian NAC v5.0.33 Release Notes (JUL 2020)

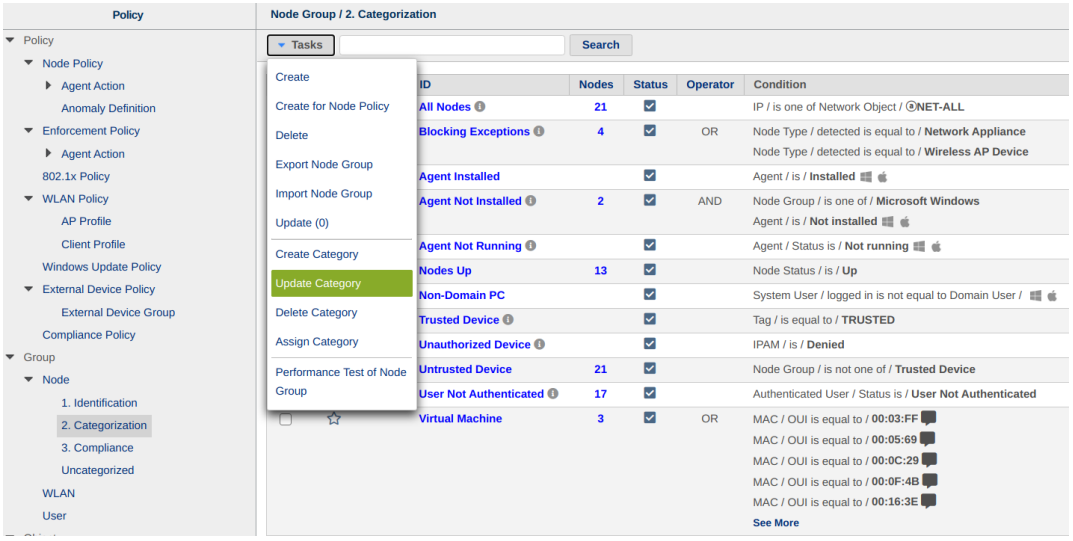
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

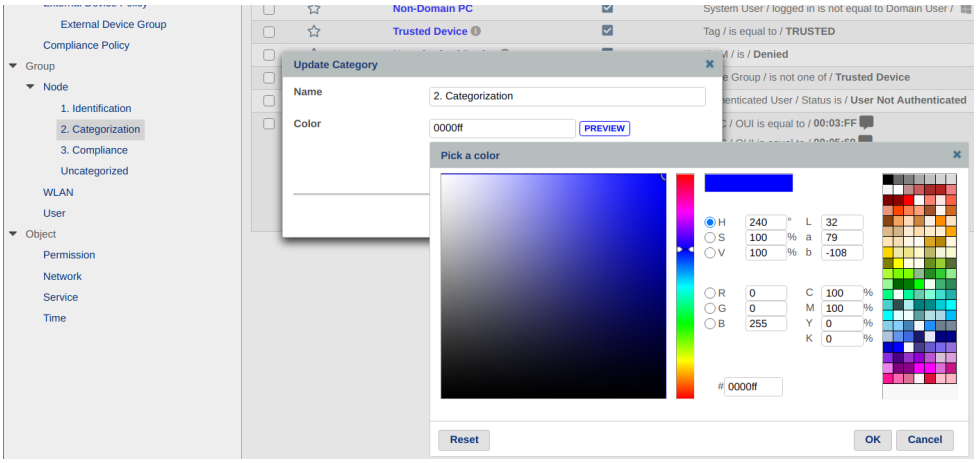
- Added function to send NAC audit records in CEF format when sending them to Syslog(#13772)



- Web console node group management UI has been improved to display important node groups and change the color of categories(#19701)



  - **Select Category color**



- The operating system and version information are added to the node information using the general-purpose OS(#19519)
- Added dashboard widget to check the version status of each node's operating system(19673
- Improved to set the timeout value of the web server running on the policy server(#21377)
- [macOS Agent]AP connection control function added to macOS WLAN control plug-in(#20695)

Issues Fixed

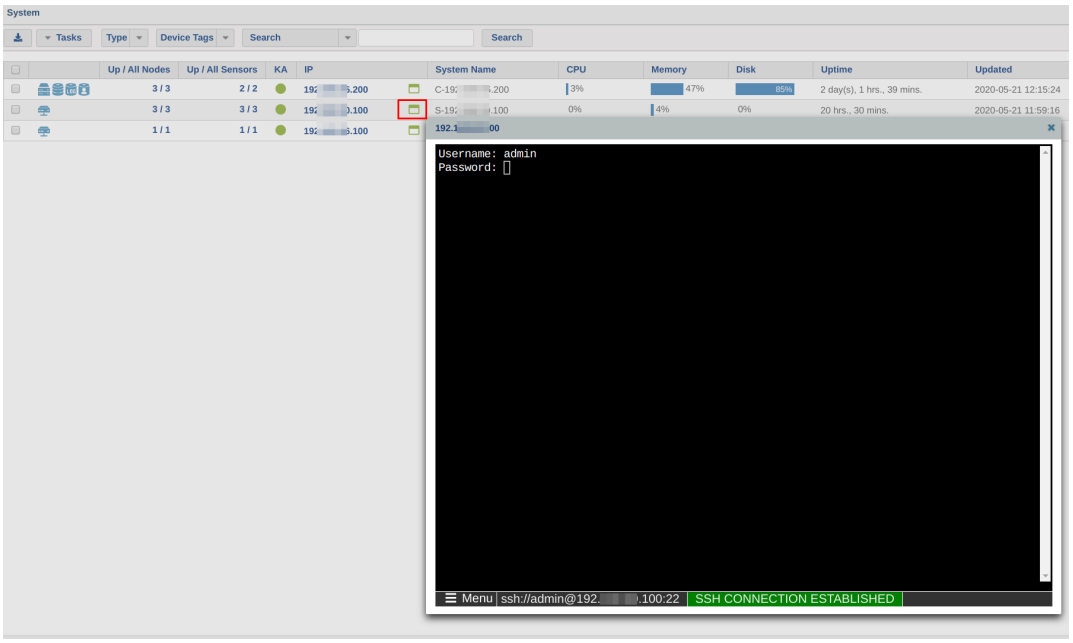
- Fixed CWP mobile version layout broken issue(#21293)
- Fixed an issue where Elasticsearch query report file was not created through CLI(#20566)
- Fixed a problem that syslog does not work right after Cloud NAC creation(#21285)
- [Windows Agent] Fixed an issue where the window disappeared when the policy was reapplied while the authentication window or authentication pop-up was displayed(#21604)
- [Windows Agent] Fixed an issue where the image of the dialog displayed through the system control plug-in was cut off when the magnification setting was changed to a value other than 100% in the display settings of the PC(#21332)
- [macOS Agent] Fixed an issue where the agent authentication window popped up intermittently in macOS authentication status (#21307)

23.2.23 Genian NAC v5.0.32 Release Notes (JUN 2020)

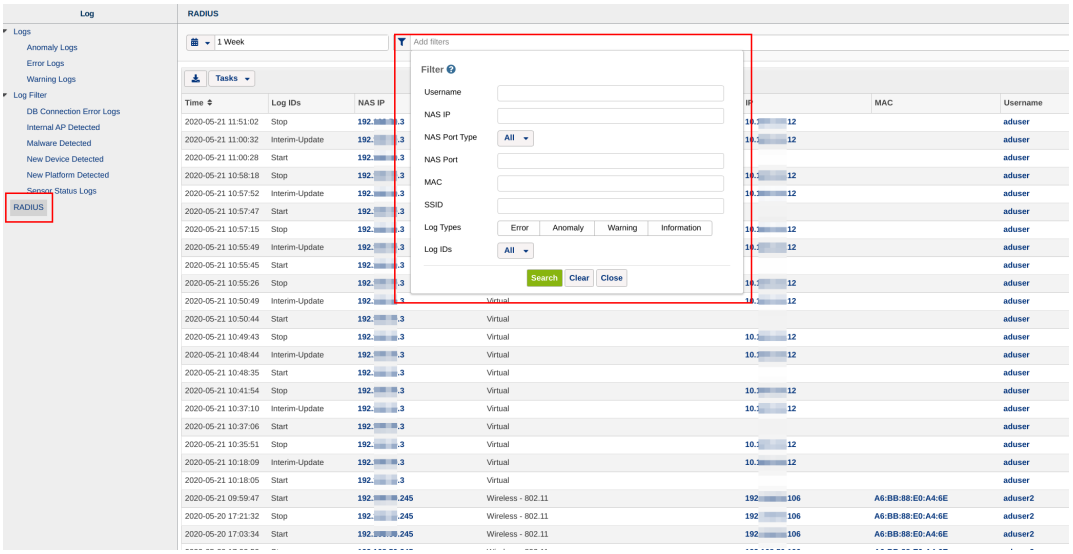
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

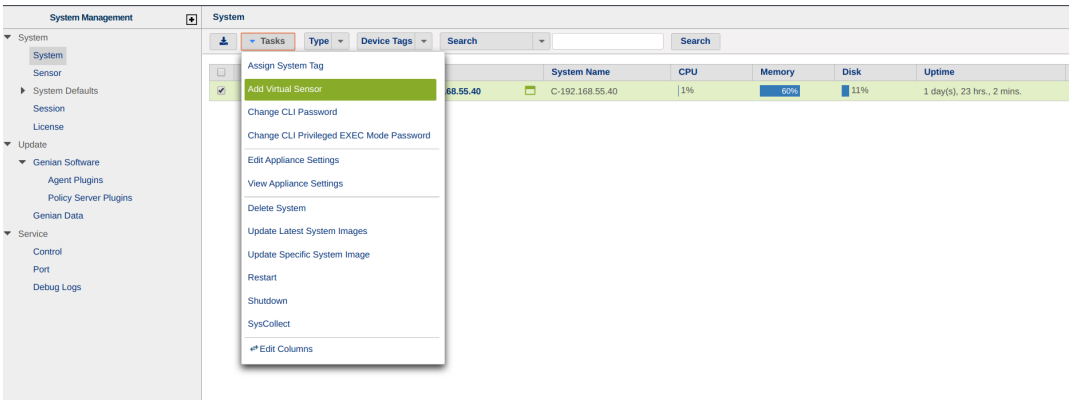
- Added function to allow SSH access of Genian devices from the management WebUI(On Premise version only)(#19822)



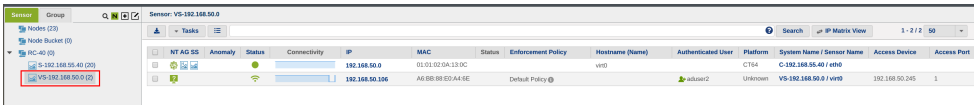
- Added the ability to save the RADIUS audit log as a log filter (#20845)



- Added a virtual sensor that performs node scan function for the remote network(Register a node without going through the sensor)(#21082)



– **Virtual Sensor Nodelist**



- Improved management WebUI switch management menu to support hierarchical structure as sensor tree of "Management> Node"(#20978)
- Improved to enable AD authentication integration through RADIUS PAP authentication method(#21079)
- Improved to use SMB2 when integrating with Windows domain(#21361)
- Removed the account field that is additionally entered when selecting "Local System Account" from the agent "Execution Account" in the node policy(#21065)
- [Windows Agent] The "Allow automatic administrative logon" control option has been added to the "Configure Windows security settings" agent(#20191)
- [Windows Agent] Changed the "Copy" option name of the agent file distribution plugin to "Download"(#21252)
- [macOS Agent] Improved to display the remaining waiting time when the macOS system shutdown plugin works(#20711)

Issues Fixed

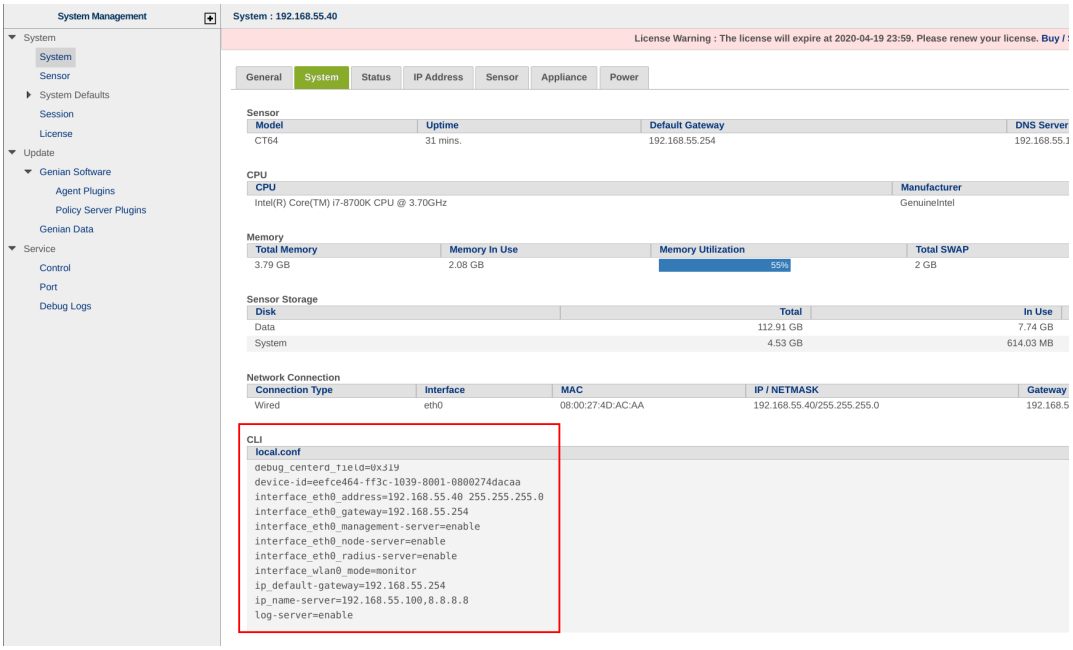
- Fixed an error page displayed when accessing an unauthorized page from an account with restricted access(#20899)
- Fixed an issue where the tooltip was displayed as blocked even if the device management policy was not specified in the "External Device Control Policy" column in "Management> Node> View Criteria - By Node-External Device View"(#21182)
- Fixed an error in which user information deleted from the AD server after being synchronized with the AD server is not deleted from the local DB(#21190)
- Fixed an issue where the AP status widget graph of the management WebUI wireless LAN access was not displayed normally.(#21202)
- Fixed an issue in which DeviceIDs were duplicated when different terminals physically used the same USB LAN card(#21261)
- [macOS Agent] Fixed an issue where the macOS "Update" plugin did not work in a VPN environment(#20975)

23.2.24 Genian NAC v5.0.31 Release Notes (MAY 2020)

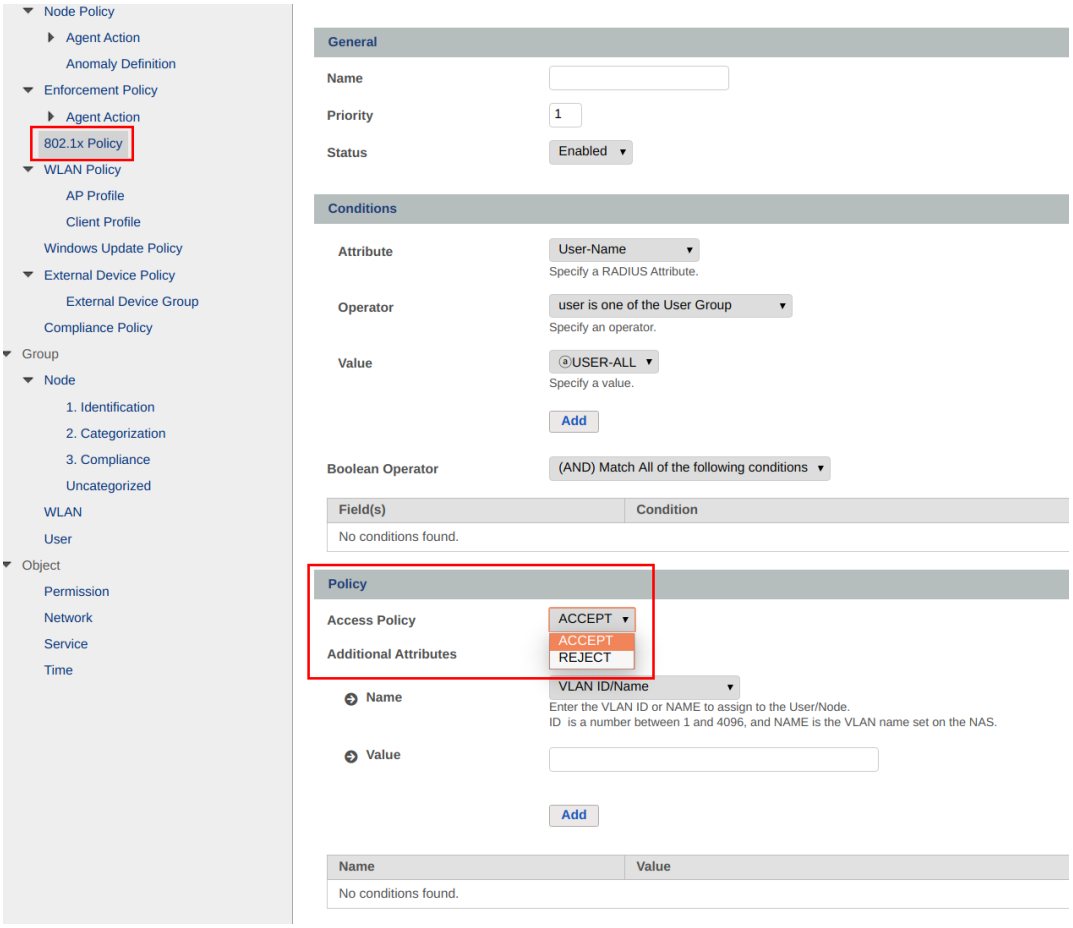
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

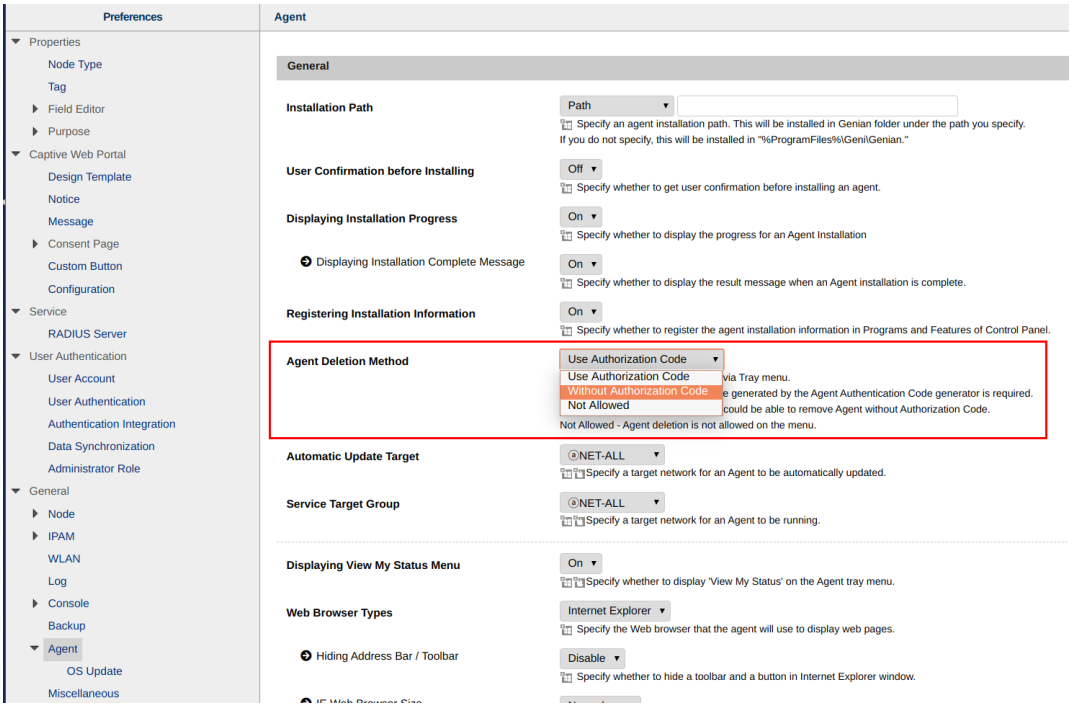
- Added the ability to check the Genians Policy Server or Network Sensor CLI configuration through the WebUI "System> system" system information (#20683)



- Improved to create an authentication access/reject policy according to the detailed authentication conditions in the "Policy> Enforcement Policy> 802.1x Policy" (#20966)



- [Windows Agent] The deletion method of the Windows agent has been changed to allow the end user to delete an agent with an authentication code, without authentication code , or to prohibit deletion(#20929)



- In case of RADIUS authentication, if the Auth MAC of user information is registered, the function has been improved so that the user is authenticated only with the device with the corresponding MAC(#20951)
- Improved to use both the locally stored user and AD authentication integration when setting RADIUS authentication. (Local> AD)(#20683)
- Enhanced platform detection using SSDP (Simple Service Discovery Protocol)(#16845)
- Added the function to automatically register the MAC of the first connected device a user authenticates from as the authorized MAC for authentication (#20945)
- AD server monitoring for AD SSO in an agentless environment has been changed to allow the Sensor or the Policy Server to query AD .(#20772)
- Agentless AD authentication In the alternative environment, the sensor is improved to use the NTLMv2 authentication method when connecting to the AD server(#21043)
- The learned MAC address is displayed on the switch trunk port, and the accuracy of the switch port connection information is improved(#20962)
- Added ability to share admin WebUI dashboard tabs(#20970)
- Audit log has been improved to check the contents of SNMP TRAP(#20972)
- Node group conditions have been added with node inclusion criteria for before agent action(#20900)
- Audit log search filter has been improved to use IP pattern matching when using IP filter(#20992)
- Add node group and agent action search function when creating node policy(#21036)
- [Windows Agent]A basic inspection product item has been added to the required software inspection plugin(#20896)
- [Windows Agent]The option to pin the verification popup window to the center of the screen has been added to the Windows agent password verification plug-in(#20916)
- [Windows Agent]Improved the user notification message so that the CWP page can be accessed even when the CWP URL is not entered(#20823)
- [Windows Agent]Windows Firewall Control Plug-in adds a notification message when setting custom rules(#20885)
- [macOS]The file distribution plugin has been added to the macOS agent(#20630)
- [macOS]ARP management plugin added to macOS agent(#20677)
- [macOS]Improved to prevent scraping (crawling) using CWP URL(#19934)
- [macOS]Improved to show update operation status in update action execution result(#20827)

Issues Fixed

- Fixed an issue where the UP / DOWN status of the sensor and the center did not match(#20796)
- Fixed an issue where the number of authentication nodes in user management was not displayed normally(#20846)
- Fixed an error that occurred when clicking the "User> Users> Department based User" menu(#20878)
- Fixed an issue where device information was not added when class name was directly entered when adding a device group(#20980)
- Fixed an issue where a node that is not joined to an AD domain becomes AD fallback authentication when logging in to AD when using AD fallback authentication in an agentless environment(#20987)
- Fixed an issue where the WNAC license and general license permission error messages were displayed on the action details screen(#20995)

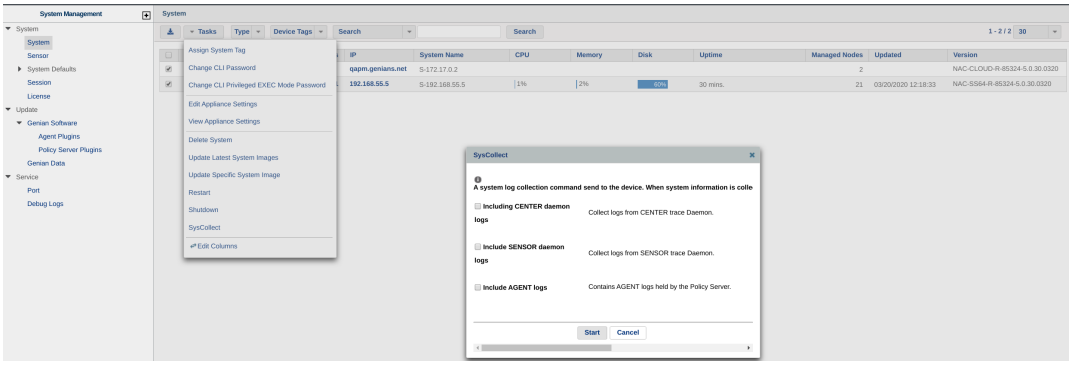
- [Windows Agent]Fixed an issue where an incorrect audit log was displayed due to the Windows security settings plugin(#20905)
- [Windows Agent]Fixed an issue that failed to install once for the first time when upgrading the plugin version(#18722)
- [Windows Agent]Fixed an issue where an interface cannot be set as an allowed gateway after the interface is blocked due to the use of an unauthorized gateway(#20390)
- [Windows Agent]Fixed an issue where the wireless LAN control plug-in's control hold time option operated for 1 minute even if it was set for more than 1 minute(#20955)
- [Windows Agent]Fixed an issue where the name was changed to a string of 15 bytes or more when the name was changed through the computer name change plug-in(#21039)
- [Windows Agent]Fixed an issue where the agent authentication window was not displayed in the center of the screen(#21041)
- [macOS]Fixed an issue where the authentication related tray menu was activated even if the macOS node was not in the service target group(#20425)
- [macOS]Fixed an issue where the font download popup window did not close when the macOS agent installation environment was closed(#20996)

23.2.25 Genian NAC v5.0.30 Release Notes (APR 2020)

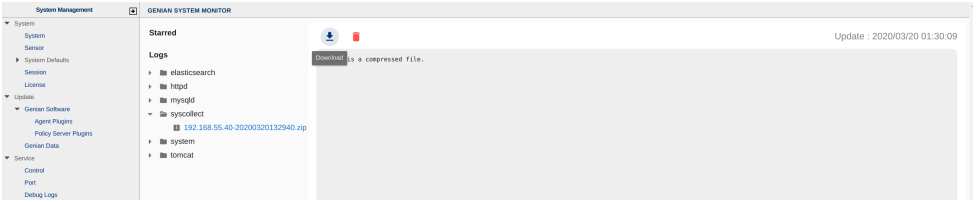
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

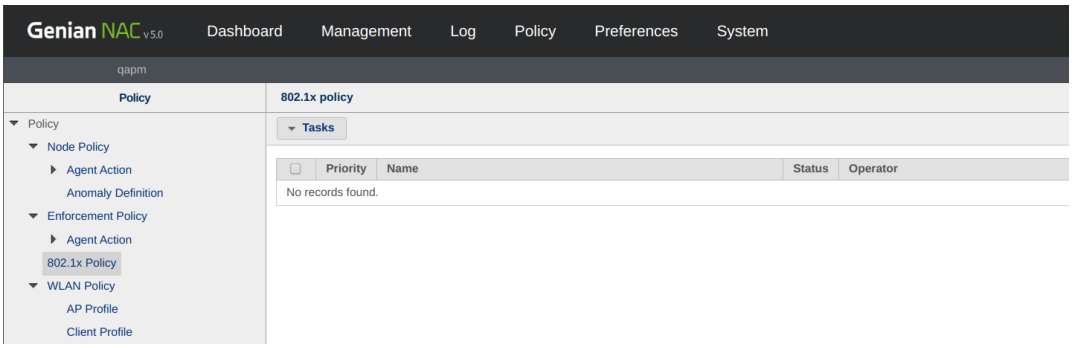
- Added system log (syscollect) collection function through management WebUI(#19997)



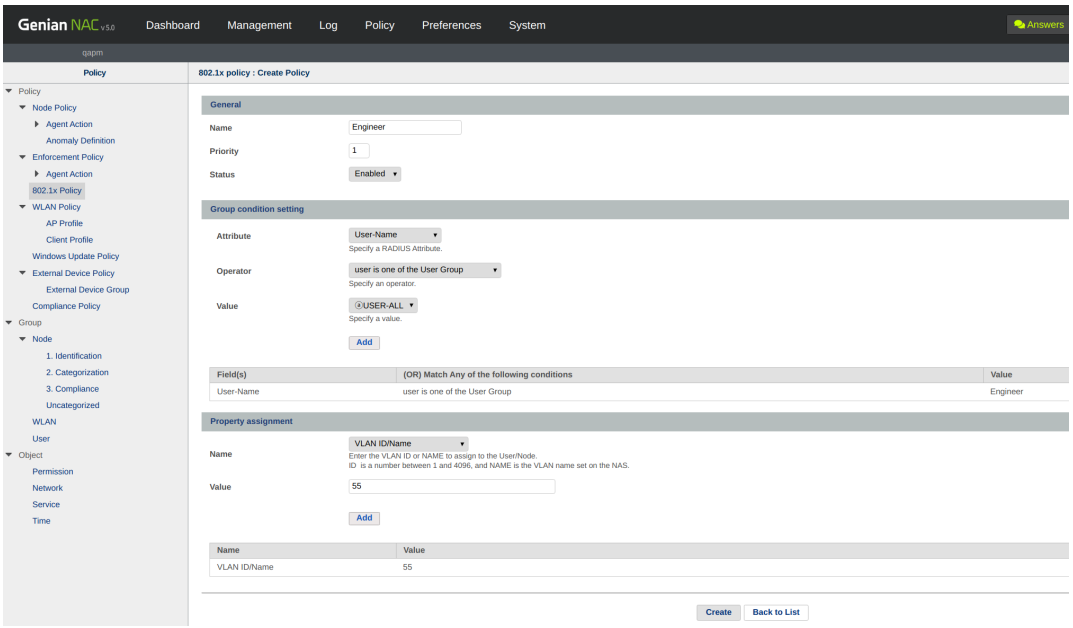
  - **Download syscollect**



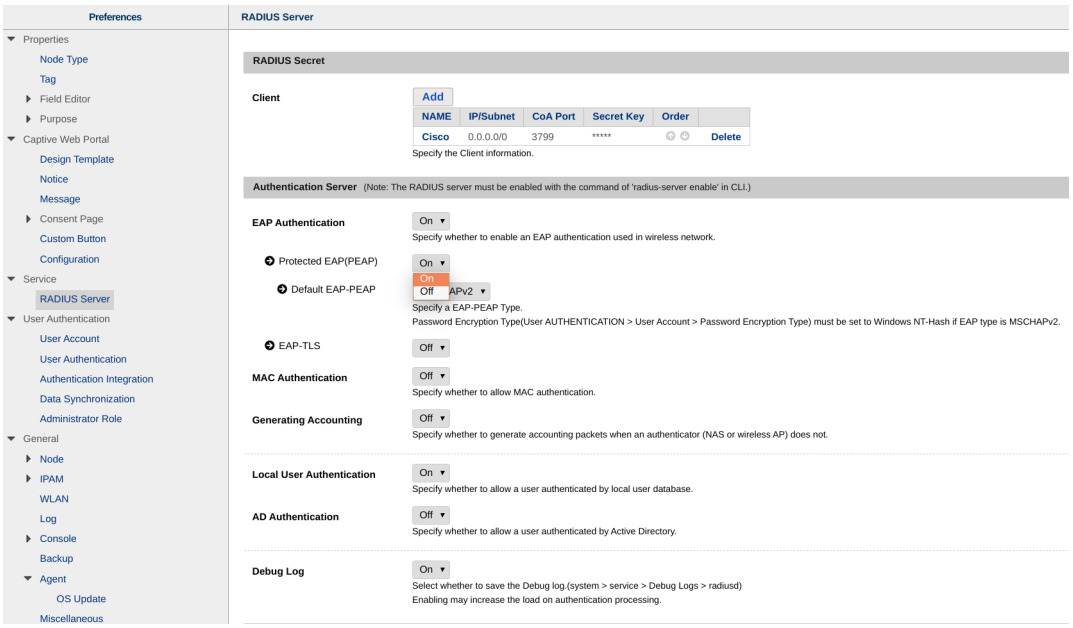
- RADIUS-based 802.1x policy setting menu has been added as a submenu of enforcement policy(#20450)



- Added function to use RADIUS attributes other than VLAN assignment using RADIUS-based authorization policy(#20089)



- Improved to provide ON / OFF option for PEAP in RADIUS setting (#20804)



- Added the ability to change the port VLAN of the switch through the switch port management function(#20448)
- Improved to check error for column name when uploading through CSV file in some menus of management WebUI(#20690)
- Improved to be able to set multiple server addresses when setting Oracle information synchronization (#20743)
- Improved to display a guide message when the file size is large when viewing the entire log file in the Admin WebUI debug log(#20847)
- Improved to keep NAS IP information in the log when accessing the wrong authentication key in the authentication alternative environment using RADIUS accounting packets(#20865)
- Bash vulnerability (shellshock) has been patched (#20874)
- Improved the GET method cross site scripting (XSS) vulnerability (#20875)
- Improved to limit the number of agent installation nodes according to the limit on the number of agents included in the IPAM license(#20775)
- Tomcat version has been upgraded to 7.0.99> 7.0.100(#20928)
- [macOS Agent]Added a wireless LAN control plug-in that can collect APs detected on macOS(#20631)

Issues Fixed

- Fixed an error in which external authentication linkage sent incorrect information from the agent when using Host authentication (#20688)
- Fixed the error that the equipment ownership department is output as the department code instead of the department name when outputting the node list Excel(#20713)
- Fixed an error where uploading of data from the Genian syncer to the policy server failed because of license check failure (#20769)
- Fixed an error where the start page remained set even if the start page setting option of the IE security option control plug-in was removed(#20789)
- [Windows Agent]Fixed an error that did not send interface information immediately even if the interface of the terminal communicating with the center was changed(#20820)

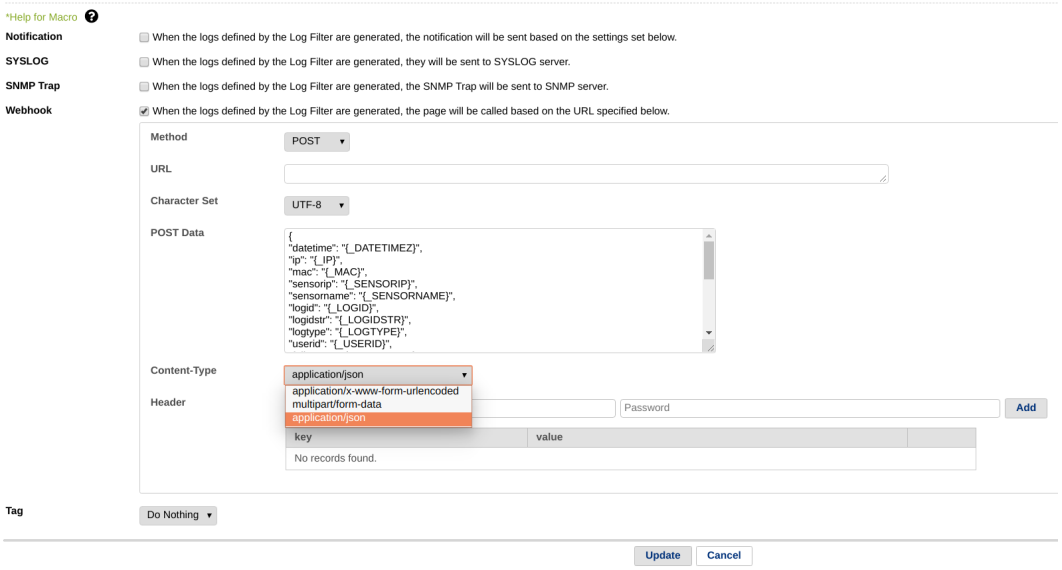
- [Windows Agent]Fixed an error that the agent could not collect some software list (# 20843)

23.2.26 Genian NAC v5.0.29 Release Notes (MAR 2020)

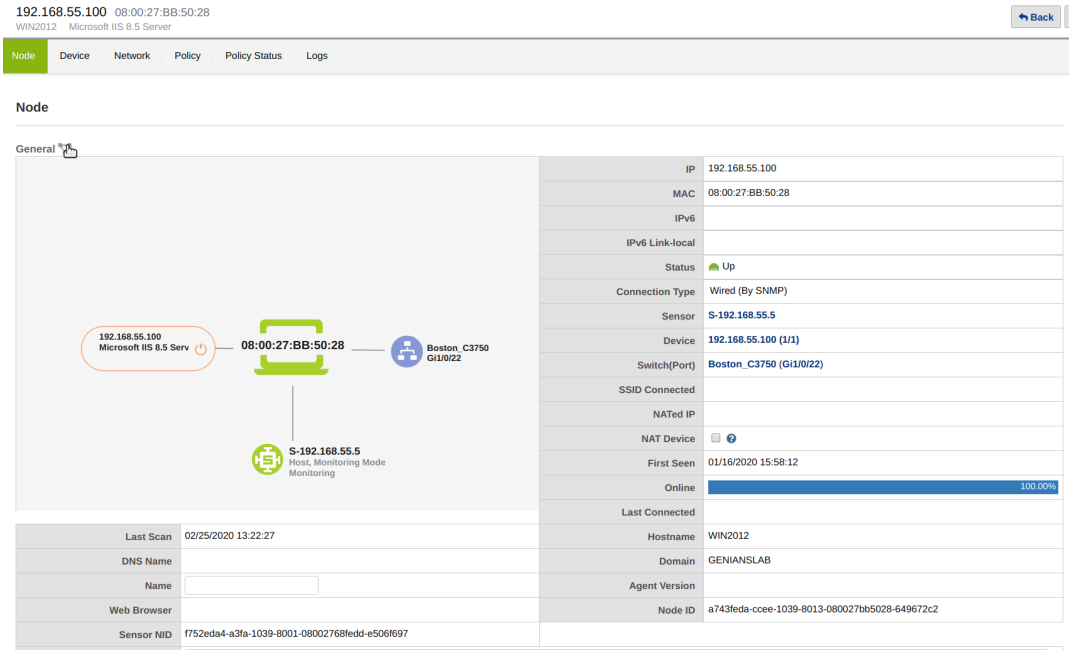
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

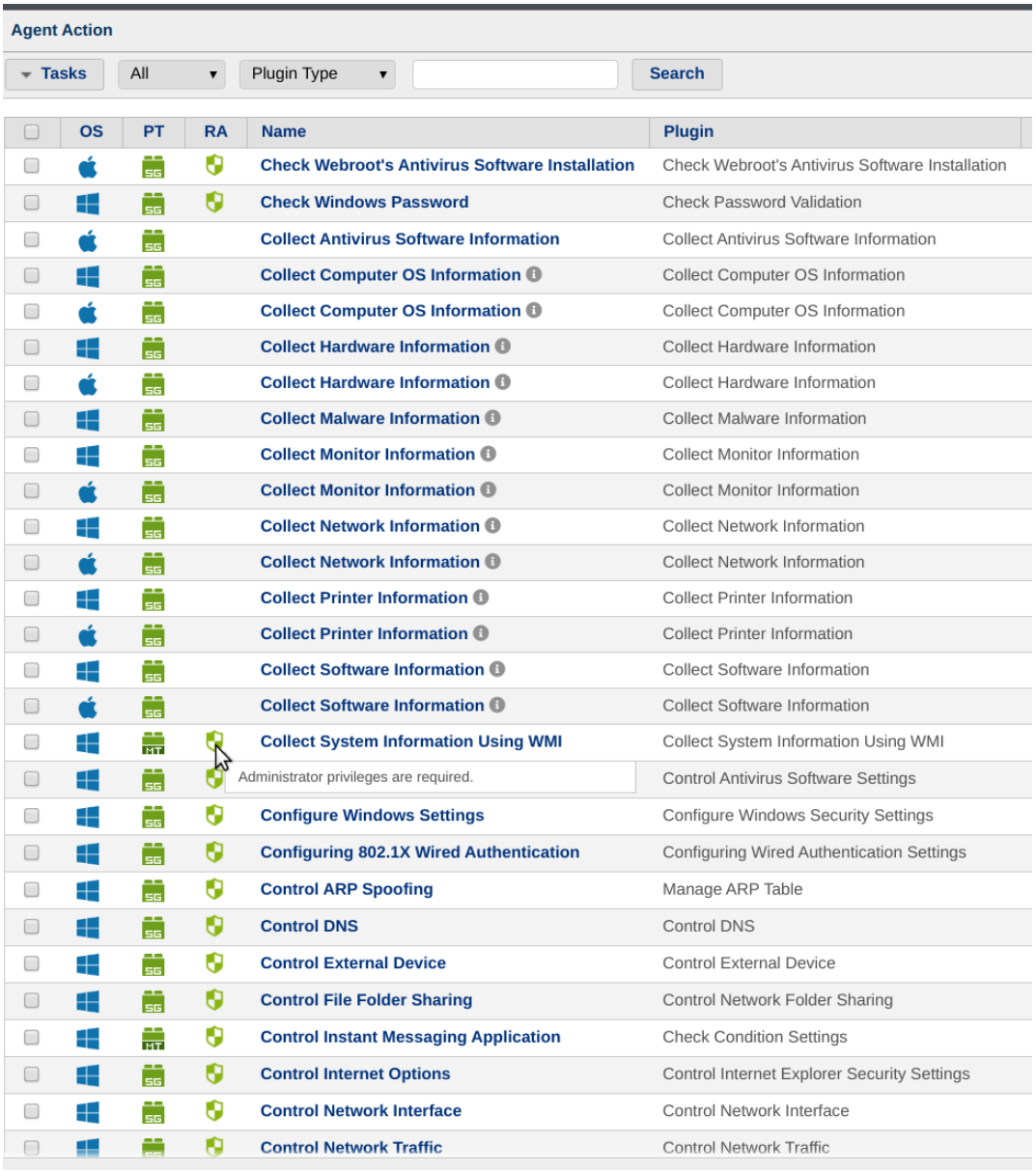
- Log filter Webhook call provides standard JSON data by default, and the current input method is improved to use a custom form. (#18604)



- "Management > Node - Click Node IP - Node General - Click diagram icon" Added diagram display function for the node. (#20094)



- [Windows Agent] Added the ability to show permissions for performing agent actions(#20483)



- Added the function to display the time of last modification of policy, group and object (#20031)
- [macOS Agent] Added custom button display to "Preferences> Captive Web Portal > Custom Button" tray menu(#19850)
- [Windows Agent] Added FALCON PREVENT antivirus information collection function to antivirus information plug-in(# 20656)

Issues Fixed

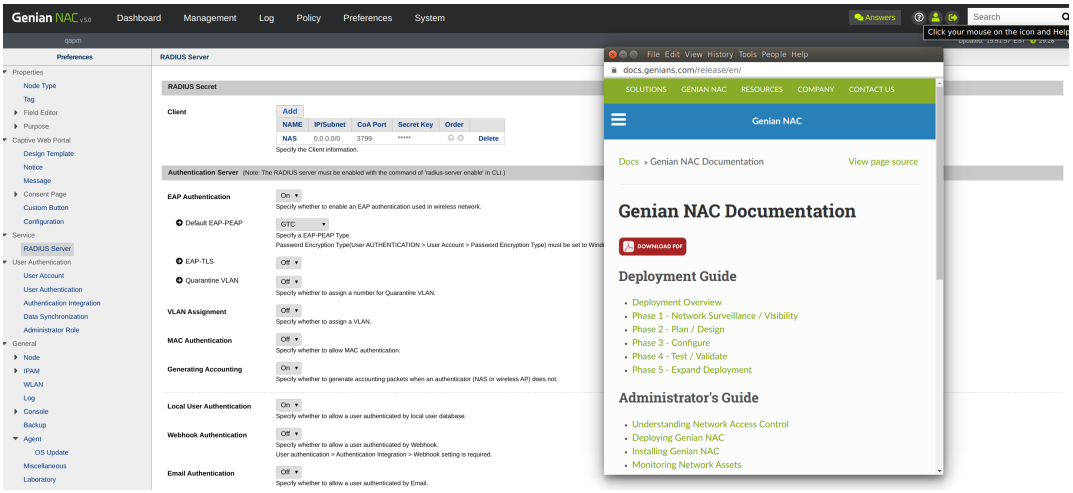
- Fixed an issue where license error intermittently when restarting equipment (#20559)
- Fixed an issue where sessions in the audit log live mode popup window are maintained after logout(#20066)
- Fixed an issue where some note type images did not display correctly in IE(#20685)
- Fixed the issue where the detail log display is displayed as a code when changing the widget setting(#14270)
- [Windows Agent] Fixed an issue where the IE Security Option Control plug-in Trusted Site Removal does not work with the last slash (/) character difference(#20719)
- [Windows Agent] Fixed an issue with reboot option after copying from file deployment plugin(#20580)
- [Windows Agent] Fixed an issue that all selected checkboxes of language and applied OS are unchecked when plug-in creation or modification fails(#20651)
- [macOS Agent] Fixed an issue that prevented the collection of real-time monitoring information from ESET vaccines.(#20625)
- [macOS Agent] Fixed an issue where the password does not exist in the account but it is marked as set(#18733)
- [macOS Agent] Fixed an issue where the agent authentication window did not pop up(#20634)

23.2.27 Genian NAC v5.0.28 Release Notes (FEB 2020)

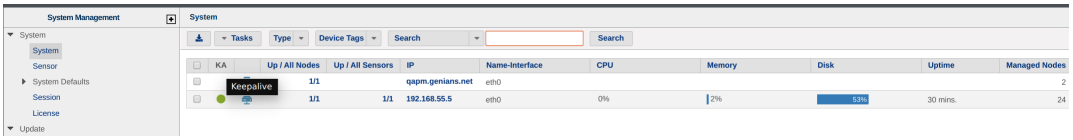
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

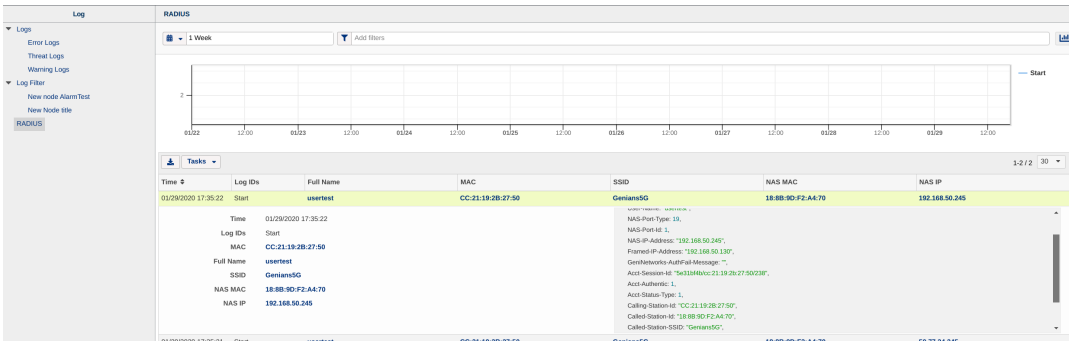
- Added online help function(#18859)



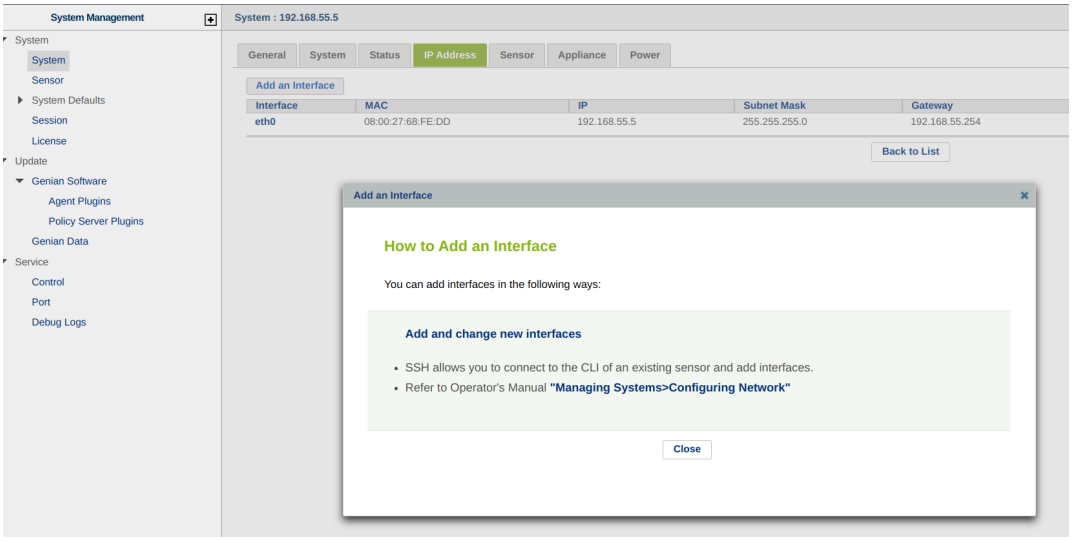
- Improved display of sensor operating status by "KA" as "keepalive"(#20404)



- Improved accounting log view from source in RADIUS log(#20058)



- Added additional IP setting guide page(#20535)



- The terminology of the sensor's operating mode has been changed from "Passive" to "Monitoring" and "Active" to "Enforcement". The sensor mode "None" is also changed to "Inactive"(#20484)
- Improved operation status icons to be displayed differently for each wired / wireless(#20090)
- Improved the function so that the switch port blocking function of the enforcement policy is performed on the corresponding switch management sensor(#16453)
- [Windows Agent] Added “Windows Security Settings” power management option(#20104)
- [Windows Agent] Add “Network Control” plugin (#18890)
- [macOS Agent] Add process termination function(#17682)
- [macOS Agent] Add file management plug-in(#17681)

Issues Fixed

- Fixed an issue where the page would hang due to certificate expiration when accessing the admin web console in the latest version of Chrome(#20807)
- Fixed an issue where VLANs were not assigned as Username criteria when logging in as an AD domain user using the "Automatically use Windows logon name and password" option(#20807)
- Fixed a problem where a Malware Icon was displayed in the node list when there was no Anomaly Definition setting (malware detection) in the policy(#20481)

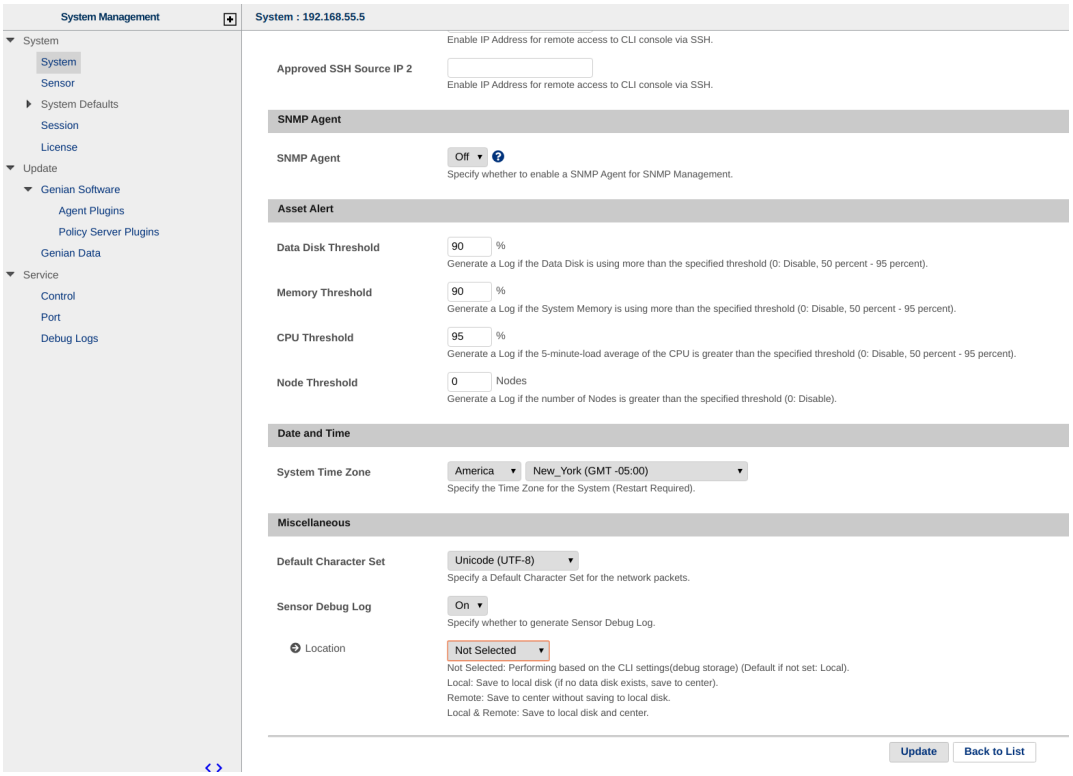
- Fixed the problem that screen size is not restored by using "esc" key after switching Dashboard Full Screen(#20568)
- Fixed a problem where the PC version screen was displayed when accessing CWP page on mobile(#20489)
- Fixed a problem where node policy was not updated when changing node information through Genian Data update(#20428)
- [Windows Agent] Fixed an issue where wireless authentication did not work under certain conditions in environments where Windows 10 devices use AD(#20301)
- [Windows Agent] Fixed an issue where the Exclude virtual printer collection option did not work in the printer information collection plug-in(#20180)
- [macOS agent] Fixed an issue where macOS was detected as 00:00:00:00:00:00 when macOS uses VPN(#20439)

23.2.28 Genian NAC v5.0.27 Release Notes (JAN 2020)

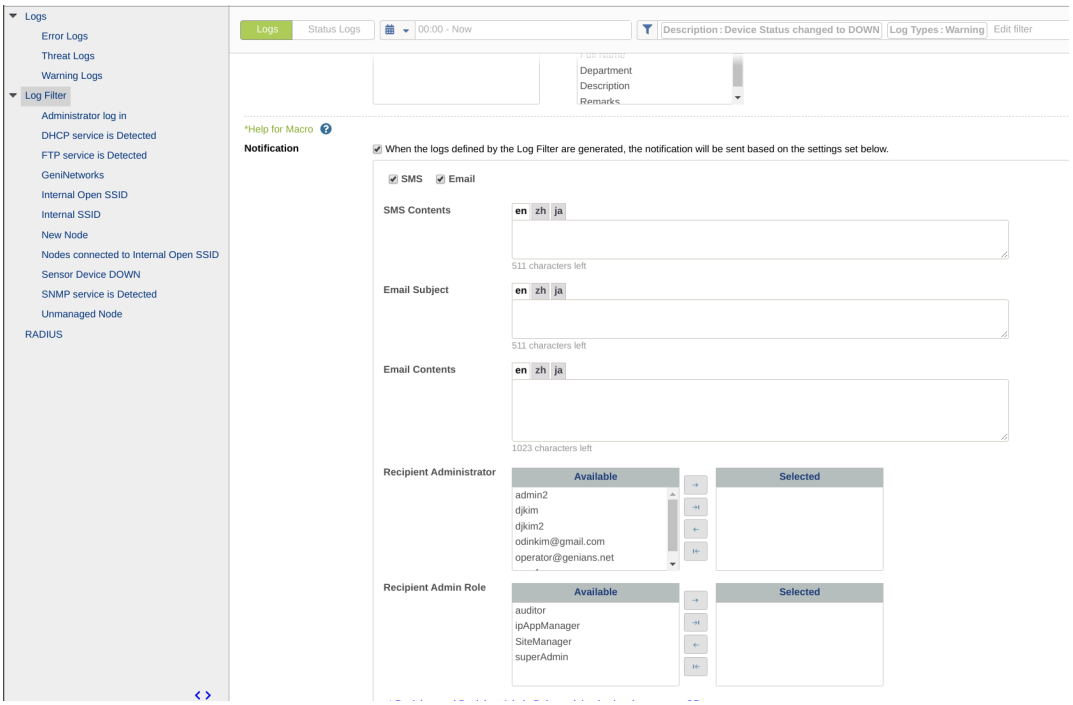
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

- Improved debugging by making remote sensor logs available in the admin console ("System > Appliance > Miscellaneous")(#12430)



- Improved log filter options by allowing separate sms or email notifications(#19739)



- Optional upgrade to new default node group configuration (#19794)
- Added the ability to collect IoT-related protocol information through the NSE(#20048)
- Added condition for Platform EOL / EOS status to nodegroup conditions(#20423)
- [macOS agent]Added macOS user notification plugin(#19737)
- Added Cloud provider information to Cloud Site License Places(#20364)

Issues Fixed

- Fixed an issue where the "Policy Server" is upgraded with a sensor image when upgrading an "Update Specific System Image"(#20265)
- Fixed an issue where IP assignment is not possible due to discovery packet relayed from sensor local dhcp server(#20276)
- Fixed a problem where added node type is not displayed in node detail screen(#20278)
- Fixed an issue where the previous condition was incorrectly displayed in the WLAN dashboard information query(#20326)
- Fixed a problem where the host authenticated node is classified as unauthenticated in the current "status & filter" (#20335)
- Fixes a problem where the wireless information is not updated after a certain time on the MiniPC device(#20361)

23.2.29 Genian NAC v5.0.26 Release Notes (DEC 2019)

For instructions on installing and updating Genian NAC, please see *Managing System Software*

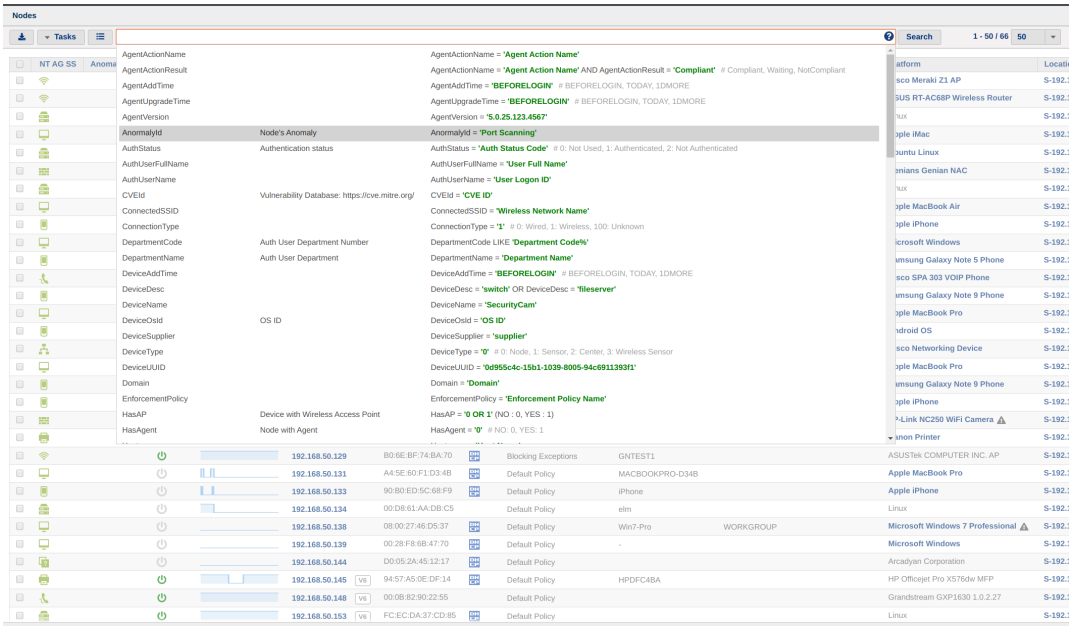
Genian NAC Version 5.0.26 is now available!

A major new feature in this release is enhanced node search capability. Now you can perform advanced searches by attributes like installed software, services, or associated CVE. Our second major feature addition is agentless Windows OS update via WMI integration. For enhanced network management, we have also added support for Custom DHCP option assignment. Now your sensors can be used to help configure IP phones, PXE and more! Additional improvements for WLAN Visibility, Node Grouping, and Agent function have also been added, including Agent based SSO support for Azure AD.

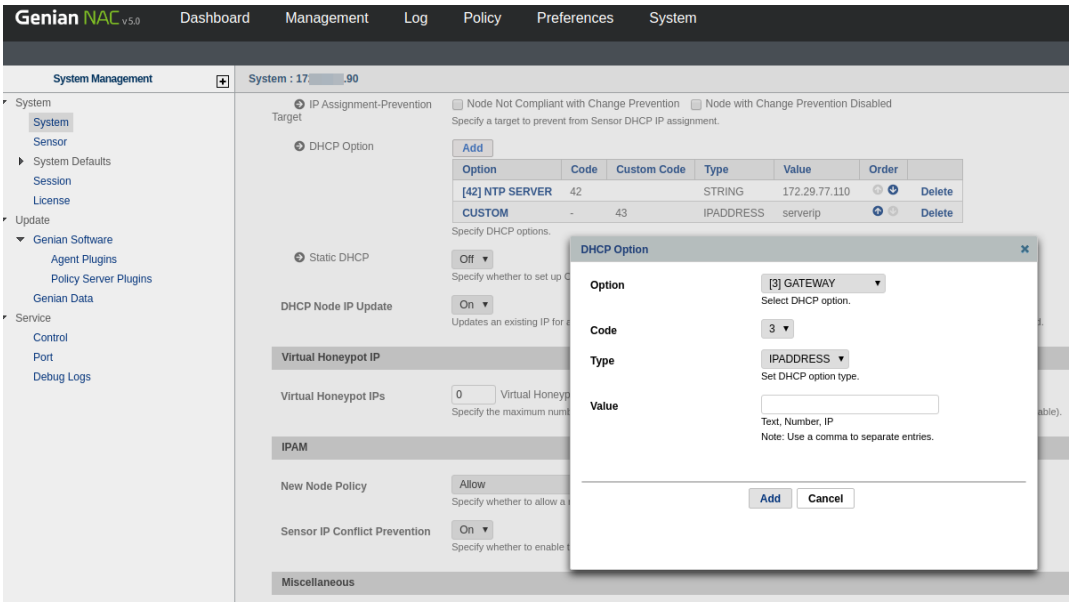
Please address any questions to your private Slack channel (clients and partners) or #qna channel. Thank you!

New Features and Improvements

- Improved search function to allow enhanced searching by node details(#20295)



- Added the ability to add DHCP custom option Fields to DHCP server functionality (#18558)



- Added Agentless collection function for update status of operating system and antivirus via WMI (#20099)
- Improved case sensitivity when retrieving the SSID of WLAN management(#19955)
- Improved to create categories in the node group creation and modification screen (#20079)
- [Windows Agent] Added SSO Support for endpoints logged into Azure AD(#20576)
- [Windows Agent] Improved function to set agent Failsafe function by agent action (#19928)
- [macOS Agent] Improved to reissue remote agent deletion code (#19860)

Issues Fixed

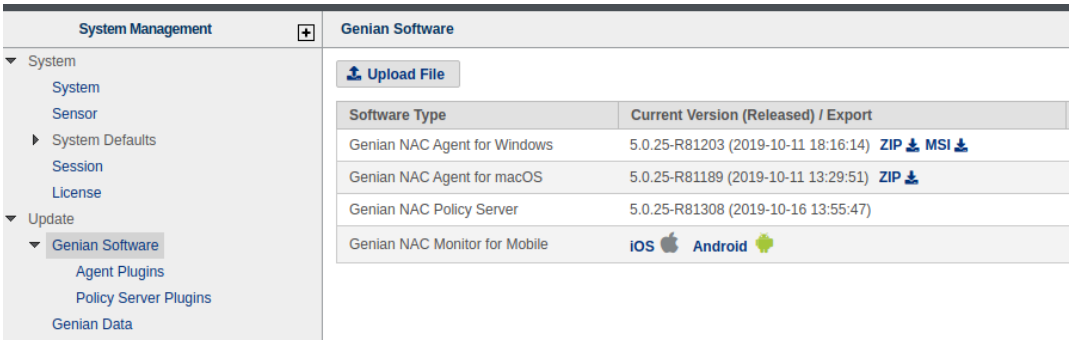
- Fixed an issue where the SNMP network information collection function did not work properly after changing the management sensor of the switch node in the management console [#16559]
- Fixed an issue where part of sensor alias was not applied to matrix view (#18864)
- Fixed an issue where the license warning pops up even though the license is normal (#19678)
- Fixed an issue where Switch Management supports SNMP Write community but the checkbox of Admin DOWN is not selected (#20255)
- [macOS Agnet] Fixed an issue where update checking and installation did not work when "Settings> Preferences> Agent> macOS Update> Connection Method" was connected via NAC.(#20235)

23.2.30 Genian NAC v5.0.25 Release Notes (NOV 2019)

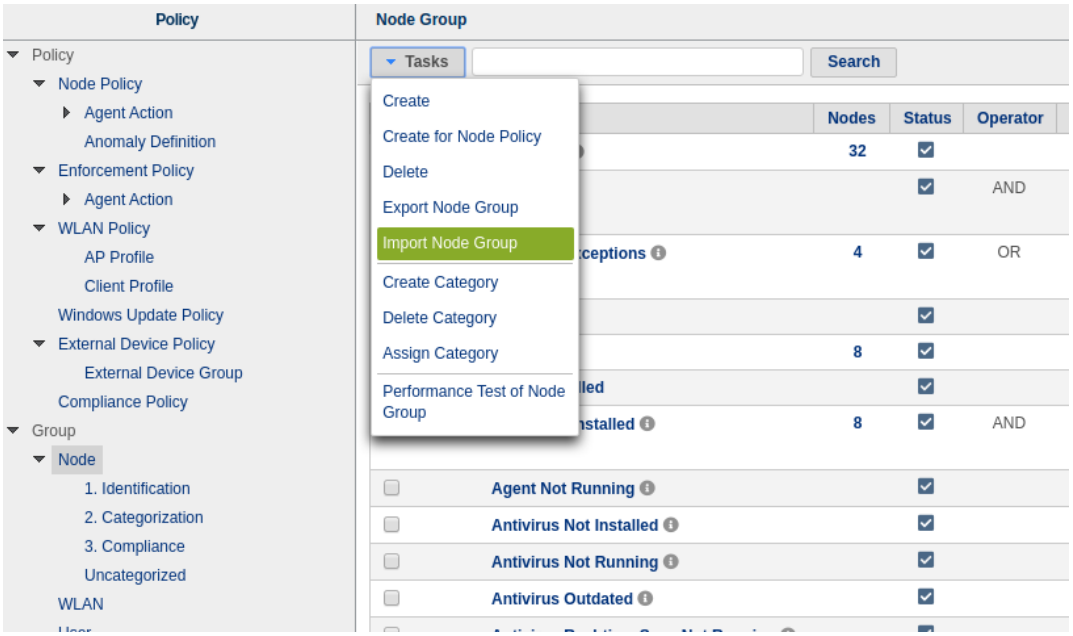
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

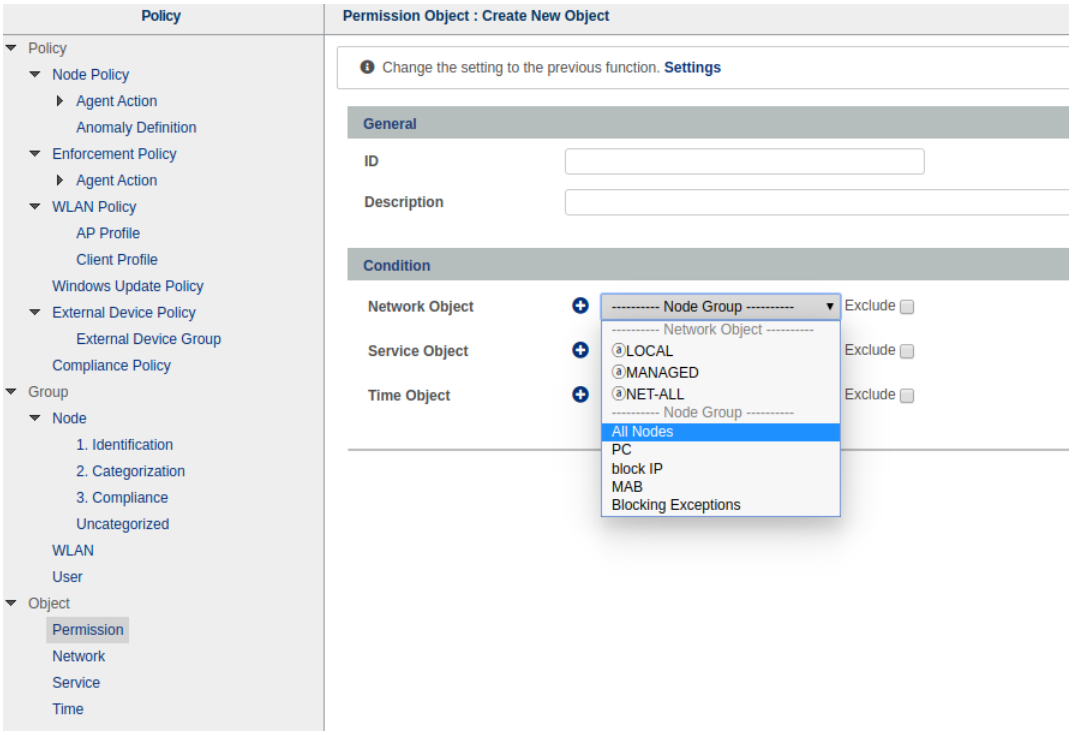
- Add MSI installation file to product package and add download function through management console (#18679)



- Added node group export and import node group saved as file (#19804)



- [Beta] Added a function to assign a node group to a network object during the condition setting of permission (#19917)



- PERM-DNS permission used for Captive Portal have been removed. If a CWP setting exists in the Enforcement policy, it is automatically processed. (#17137)
- Added agentless AD Single Sign-On and system information collection using WMI. (#19274)
- Added new node registration function through 802.1X RADIUS authentication processing (#19825)
- Added the function to set the validity time of the authentication code during SMS verification (#19542)
- Improved support for multiple shared secrets on RADIUS servers (#19744)
- Support UEFI installation (#20282)

Issues Fixed

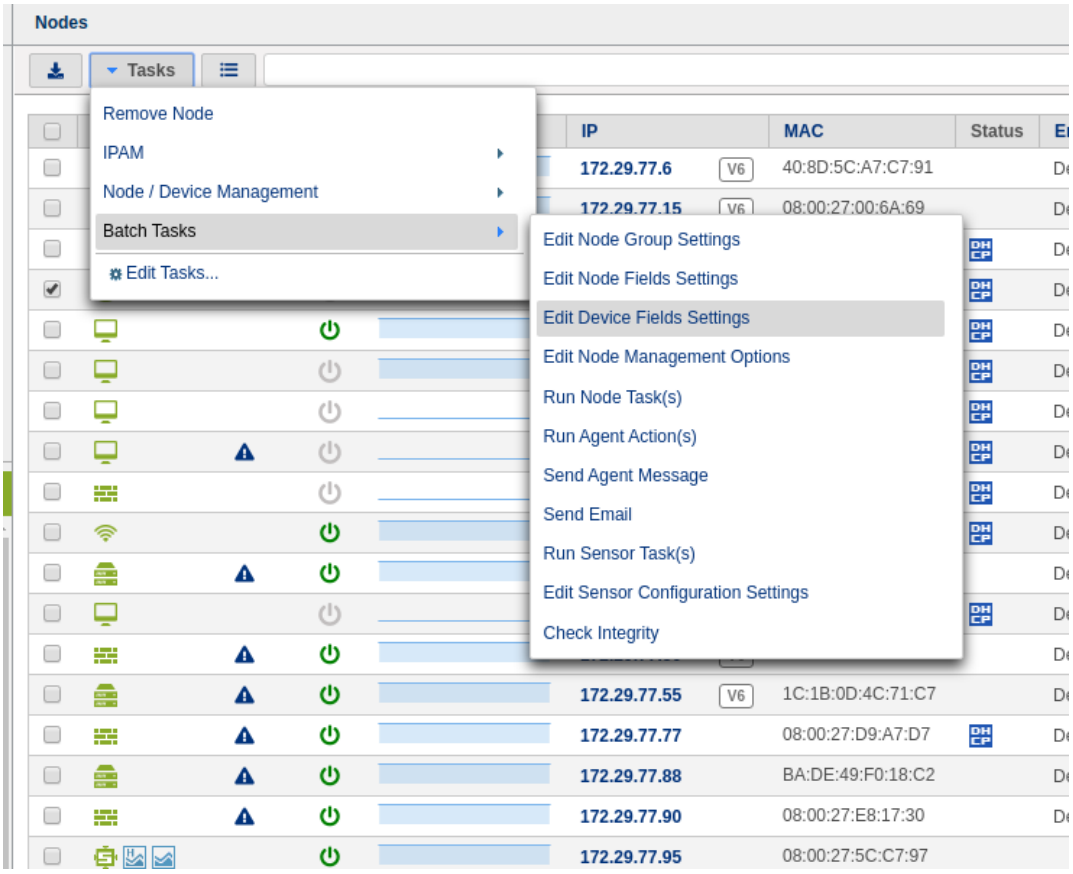
- Fixed an issue where the automatic creation of an email sending report was successful but a failed audit log was left (#19966)
- Fixed an issue where the percentage status was incorrect in the 802.1x status notation widget on the switch (#20024)
- Fixes a problem where duplicate error occurs during dbmigration of SAML related default DB value (#19971)
- [macOS] Fixed an issue where the agent behavior was shown as stopped when changing the interface (#19861)
- [macOS] Fixed the problem that the operation / deactivation is repeated when controlling the screen saver (#19868)

23.2.31 Genian NAC v5.0.24 Release Notes (OCT 2019)

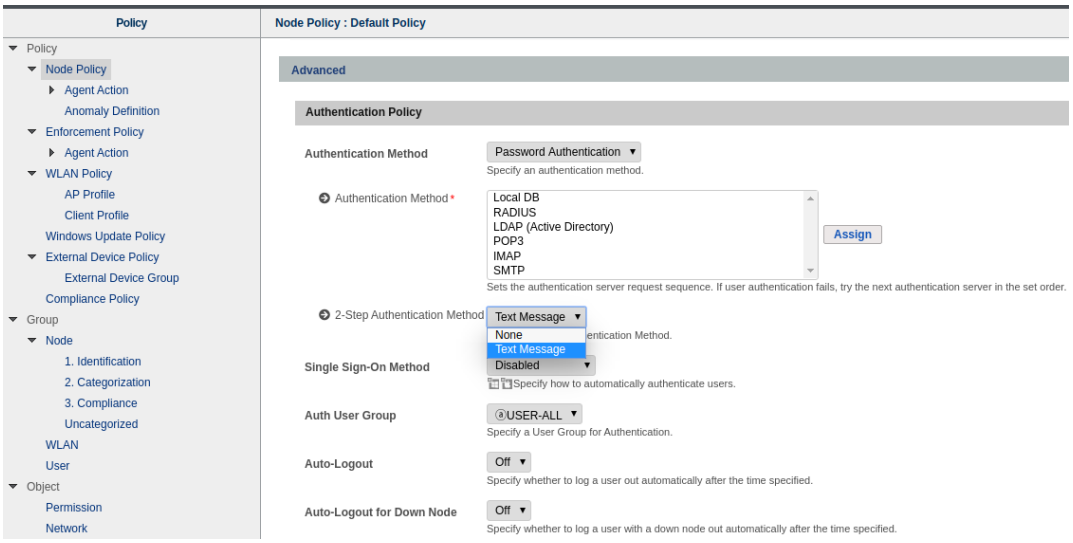
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

- Added "Edit Device field settings" to Batch Tasks #19747



- Added two-factor authentication using "Text Message" in global version #19727



- Improved to use NIC Vendor as platform information when platform is not classified #19671
- [Windows Agnet] Added McAfee Total Protection VirusScan and McAfee Endpoint Security antivirus information collection #17739
- [Windows Agent] Added Cylance PROTECT antivirus information collection #19668
- [Windows Agent] Added Symantec Endpoint Protection antivirus information collection.#19840

Issues Fixed

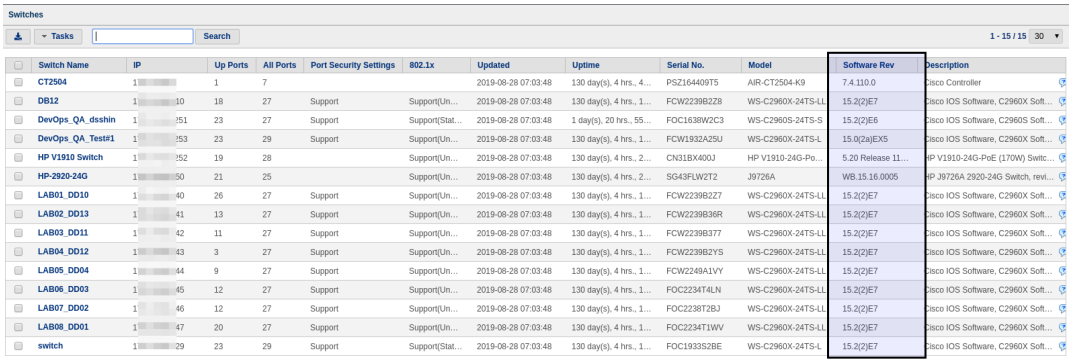
- Fixed an issue where agent information deletion time check did not work properly #19602
- Fixed the problem where audit record is incorrectly deleted due to long-term downtime when deleting by agent use of node policy #19799
- Fixed an issue where uploading a new CA certificate file from Radius server settings did not update with the uploaded CA certificate information #19921
- Fixed a problem where a "license warning" message is displayed when the administrator Web Console first login after a product upgrade #19883
- [macOS Agent] Fixed the problem where macOS agent stops working when changing event port #19725
- [macOS Agent] Fixed a problem where the agent log is displayed repeatedly when deleting network services on macOS #19755
- [macOS Agent] Fixed a problem in which the agent did not work after performing an agent update for macOS nodes #19773

23.2.32 Genian NAC v5.0.23 Release Notes (SEP 2019)

For instructions on installing and updating Genian NAC, please see *Managing System Software*

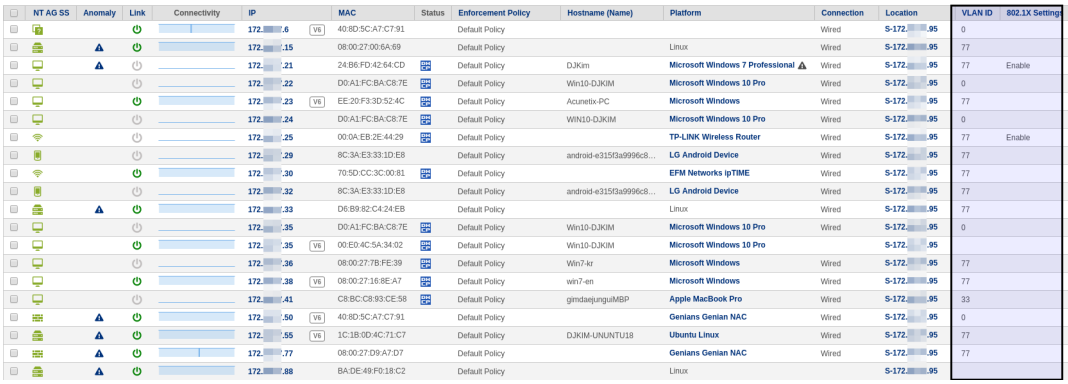
New Features and Improvements

- Added a column to display switch software version on the switch management (#19485)



Switch Name	IP	Up Ports	All Ports	Port Security Settings	802.1x	Updated	Uptime	Serial No.	Model	Software Rev	Description
CT2504	1	1	7			2019-08-28 07:03:48	130 day(s), 4 hrs., 4…	PSZ164409T5	AIR-CT2504-K9	7.4.110.0	Cisco Controller
DB12	1 :10	18	27	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FCW2239B2Z8	WS-C2960X-24TS-LL	15.2(2)E7	Cisco IOS Software, C2960X Soft…
DevOps_QA_dsshin	1 :51	23	27	Support	Support(Stat…	2019-08-28 07:03:48	1 day(s), 20 hrs., 55…	FOC1638W2C3	WS-C2960S-24TS-S	15.2(2)E6	Cisco IOS Software, C2960S Soft…
DevOps_QA_Test#1	1 :53	23	29	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FCW1932A25U	WS-C2960X-24TS-L	15.0(2a)EX5	Cisco IOS Software, C2960X Soft…
HP V1910 Switch	1 :52	19	28		Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 2…	CN31BX400J	HP V1910-24G-Po…	5.20 Release 11…	HP V1910-24G-PoE (170W) Switc…
HP-2920-24G	1 :50	21	25		Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 2…	SG43FLW2T2	J9726A	WB.15.16.0005	HP J9726A 2920-24G Switch, revi…
LAB01_DD10	1 :40	26	27	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FCW2239B2Z7	WS-C2960X-24TS-LL	15.2(2)E7	Cisco IOS Software, C2960X Soft…
LAB02_DD13	1 :41	13	27	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FCW2239B36R	WS-C2960X-24TS-LL	15.2(2)E7	Cisco IOS Software, C2960X Soft…
LAB03_DD11	1 :42	11	27	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FCW2239B377	WS-C2960X-24TS-LL	15.2(2)E7	Cisco IOS Software, C2960X Soft…
LAB04_DD12	1 :43	3	27	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FCW2239B2YS	WS-C2960X-24TS-LL	15.2(2)E7	Cisco IOS Software, C2960X Soft…
LAB05_DD04	1 :44	9	27	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FCW2249A1VY	WS-C2960X-24TS-LL	15.2(2)E7	Cisco IOS Software, C2960X Soft…
LAB06_DD03	1 :45	12	27	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FOC2234T4LN	WS-C2960X-24TS-LL	15.2(2)E7	Cisco IOS Software, C2960X Soft…
LAB07_DD02	1 :46	12	27	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FOC2238T2BJ	WS-C2960X-24TS-LL	15.2(2)E7	Cisco IOS Software, C2960X Soft…
LAB08_DD01	1 :47	20	27	Support	Support(Un…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FOC2234T1WV	WS-C2960X-24TS-LL	15.2(2)E7	Cisco IOS Software, C2960X Soft…
switch	1 :29	23	29	Support	Support(Stat…	2019-08-28 07:03:48	130 day(s), 4 hrs., 1…	FOC1933S2BE	WS-C2960X-24TS-L	15.2(2)E7	Cisco IOS Software, C2960X Soft…

- Added the switch interface information column "VLAN ID", "802.1X Settings" to the node management (#19731)



NT AG SS	Anomaly	Link	Connectivity	IP	MAC	Status	Enforcement Policy	Hostname (Name)	Platform	Connection	Location	VLAN ID	802.1X Settings
				172. .6 V6	40:8D:5C:A7:C7:91		Default Policy			Wired	S-172. .95	0	
				172. .15	08:00:27:00:6A:69		Default Policy		Linux	Wired	S-172. .95	77	
				172. .21	24:B6:FD:42:64:CD		Default Policy	DJKim	Microsoft Windows 7 Professional	Wired	S-172. .95	77	Enable
				172. .22	D0:A1:FC:BA:C8:7E		Default Policy	Win10-DJKIM	Microsoft Windows 10 Pro	Wired	S-172. .95	0	
				172. .23 V6	EE:20:F3:3D:52:4C		Default Policy	Acunetix-PC	Microsoft Windows	Wired	S-172. .95	77	
				172. .24	D0:A1:FC:BA:C8:7E		Default Policy	WIN10-DJKIM	Microsoft Windows 10 Pro	Wired	S-172. .95	0	
				172. .25	00:0A:EB:2E:44:29		Default Policy		TP-LINK Wireless Router	Wired	S-172. .95	77	Enable
				172. .29	8C:3A:E3:33:1D:E8		Default Policy	android-e315f3a9996c8…	LG Android Device	Wired	S-172. .95	77	
				172. .30	70:5D:CC:3C:00:81		Default Policy		EFM Networks ipTIME	Wired	S-172. .95	77	
				172. .32	8C:3A:E3:33:1D:E8		Default Policy	android-e315f3a9996c8…	LG Android Device	Wired	S-172. .95	77	
				172. .33	D6:B9:82:C4:24:EB		Default Policy		Linux	Wired	S-172. .95	77	
				172. .35	D0:A1:FC:BA:C8:7E		Default Policy	Win10-DJKIM	Microsoft Windows 10 Pro	Wired	S-172. .95	0	
				172. .35 V6	00:E0:4C:5A:34:02		Default Policy	Win10-DJKIM	Microsoft Windows 10 Pro		S-172. .95		
				172. .36	08:00:27:7B:FE:39		Default Policy	Win7-kr	Microsoft Windows	Wired	S-172. .95	77	
				172. .38 V6	08:00:27:16:8E:A7		Default Policy	win7-en	Microsoft Windows	Wired	S-172. .95	77	
				172. .41	C8:BC:C8:93:CE:58		Default Policy	gimdaejunguiMBP	Apple MacBook Pro	Wired	S-172. .95	33	
				172. .50 V6	40:8D:5C:A7:C7:91		Default Policy		Genians Genian NAC	Wired	S-172. .95	0	
				172. .55 V6	1C:1B:0D:4C:71:C7		Default Policy	DJKIM-UNUNTU18	Ubuntu Linux	Wired	S-172. .95	77	
				172. .77	08:00:27:D9:A7:D7		Default Policy		Genians Genian NAC	Wired	S-172. .95	77	
				172. .88	BA:DE:49:F0:18:C2		Default Policy		Linux		S-172. .95		

- Added a column to disaply last login IP on the user management (#19506)
- Added a audit log when RADIUS MAC authentication (MAB) fail (#19515)
- Added a function to automatically limit the number of available IPs when approving a new user application through CWP (#19162)
- Improved to show why failure occurs during agent upload via Web UI (#15960)

Issues Fixed

- Fixed a problem where a node belongs to an unauthenticated node group even when actual authentication information remains on the node when setting user re-authentication on an authenticated node (#16751)
- Fixed a problem in which Global DHCP mode did not work unless a local sensor was added to the Policy Server (#19652)
- [Windows Agent] Fixed a problem where disk serial information of certain PCs was displayed as garbled characters (#19560)
- [Windows Agent] Fixed issue where Windows Product Key was not collected properly (#19661)

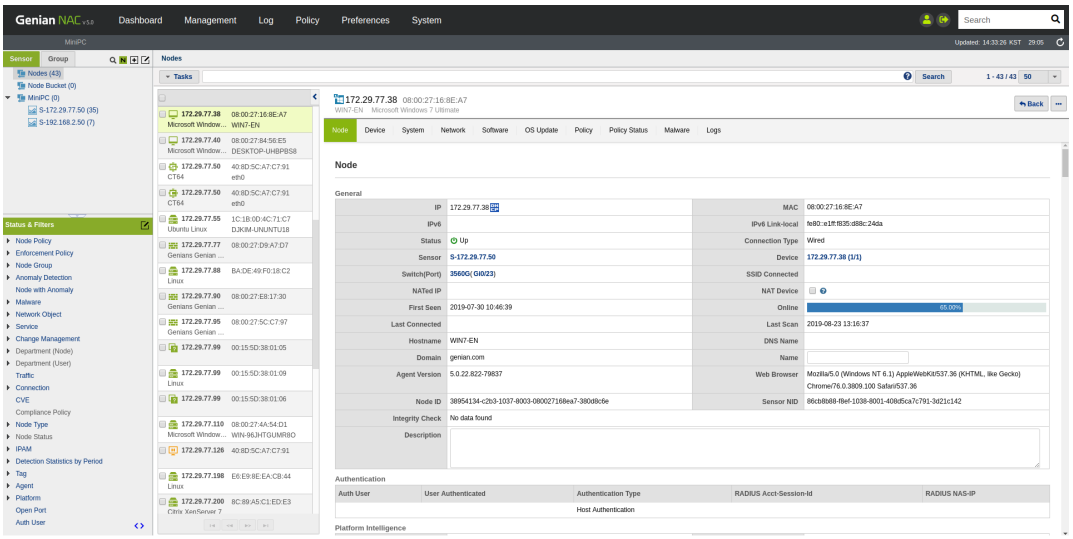
- [macOS Agent] Fixed an issue where the agent not work properly in OS X Mavericks (#19528)
- [macOS Agent] Fixed an issue where the agent tray icon was displayed as unauthenticated when the macOS device was subject to host authentication policy (#19546)
- [Windows Agent] Fix problems that the agent cannot view user information when using SSO (#19431)

23.2.33 Genian NAC v5.0.22 Release Notes (AUG 2019)

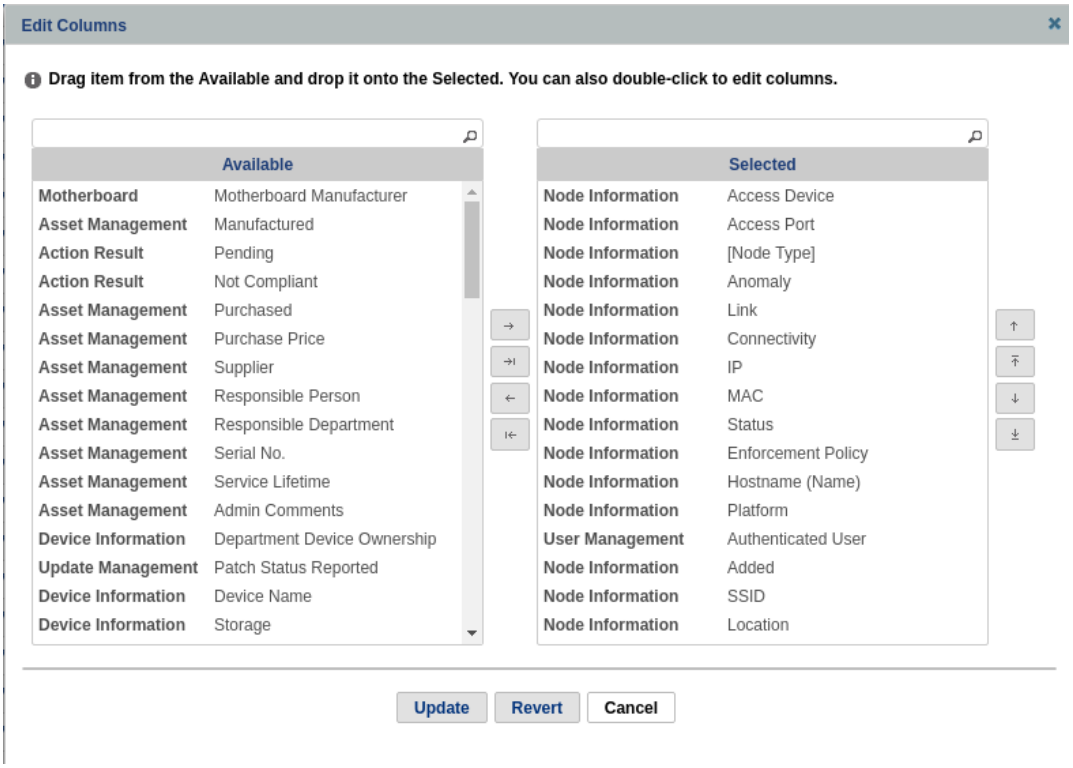
For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

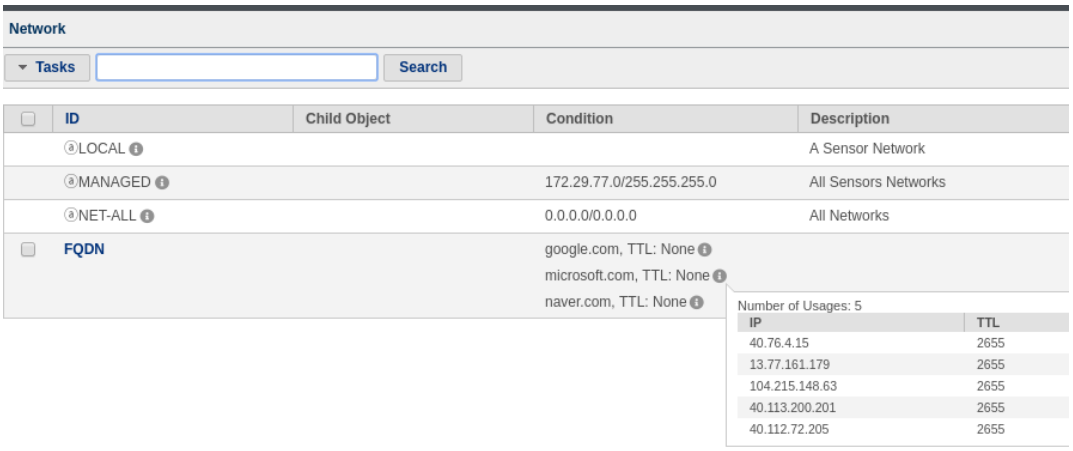
- Improved node management detail screen (#18852)



- Improved the ability to manage the columns in the node management list without restriction by view and to categorize them. (#19294)



- Added a function to preview the query result of "network object" entered as FQDN in the tooltip. (#19182)



- Added new feature to upload device lifecycle management information as batch input as CSV file (#19152)
- Added condition "Calling (Called) -Station-Id (MAC) to Node Group" in RADIUS VLAN assignment (#19335)
- Added FTP / SFTP port setting function for remote backup (#19465)
- Improved to be displayed login window when user clicks on the pre-expiration notification popup (#19420)
- [Win Agent]Added exception option for printer management share in "Control Network Folder sharing" plug-in. (#19443)

Issues Fixed

- Fixed an issue where the center daemon was abnormally terminated intermittent ly when DB connection failed. (#19442)
- [Win Agent]Fixes the problem where GnPlugin terminates abnormally when using antivirus information collection plug-in (#19869)
- [Mac Agent]Fixed an issue where overwriting an archive file fails when inter- process communication failures or duplicate clicks occur when clicking the Error Reporting button. (#19372)

23.2.34 Genian NAC v5.0.21 Release Notes (JUL 2019)

For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

- Added the ability to set the start time of the tag. (#18804)
- If the license is exceeded, a warning message will be displayed for the first 90 days, and then the specific information will be changed to hide. (#18834)
- Cloud NAC Information Synchronization Enhanced to Work. (#18449)
- [Agent] Add required software check action plug-in. (#18018)

Issues Fixed

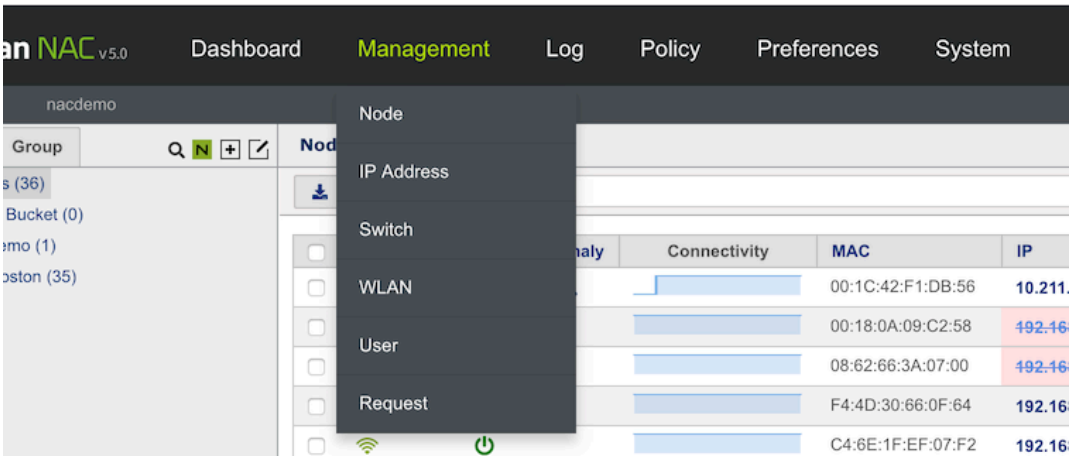
- Apply Opensshd CVE-related patches (#19317)
- Fixed a problem where the risk detection default setting does not apply (#19625)
- [Agent] Fixed an issue where the computer name change plugin was not renamed to a separate Execution Account (#19603)
- [Agent] Fixes a problem where desktop wallpaper location is enforced differently than policy in Windows 7 and earlier.(#19595)
- [Agent] Fixed an issue where the agent tray icon does not appear on the screen when the policy is not received. (#19536)
- [macOS] Fixed issue where macOS AD alternative authentication function does not work (#19421)

23.2.35 Genian NAC v5.0.20 Release Notes (JUN 2019)

For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

- Top menu navigation has been changed to top-down. (#18853)



- A "memberOf" entry has been added to synchronize the user's group information (memberOf) during Active Directory user information synchronization. (#18752)
- Added the ability to query the past node list and node group members by storing a daily list of the status of nodes belonging to the node group. (#17994)
- The "CWP accessible group" option has been added to allow access to CWP pages only on allowed networks. (#18657)
- RADIUS Server improved to display certificate information and restart internal RADIUS server after registering EAP-TLS certificate. (#19202)
- Regularly updated NAC operational data has been remove from backup to reduce backup size. (#19379)
- It is improved to be able to set the execution cycle in the "Control External Device" plug-in. (#19171)
- [Mobile APP] The mobile management app has been modified to receive an notification when an (IP/Device)Request or node change occurs. (#18840)

Issues Fixed

- Fixed a problem where "Retry Interval" and "Retry Attempts" options of the macOS agent plug-in action policy did not work. (#18887)
- Fixed a problem that when using "Genian Agent User Authentication" window, authentication fails when entering a password longer than a certain length. (#18987)
- Fixed an issue where "Enforcement Policy> RADIUS CoA" control option only works when the RADIUS isolation VLAN setting is ON. (#19335)
- Fixed an issue where only some tasks run when running multiple "Run Script" plugin tasks in the node policy. (#19352)
- Fixed a problem where the sensor map does not appear in the Admin console dashboard. (#19410)

23.2.36 Genian NAC v5.0.19 Release Notes (May 2019)

For instructions on installing and updating Genian NAC, please see *Managing System Software*

Warning:

Starting with this version, the way to connect to the management
console has been changed. You must connect to port 8443 as follows (On-Premises Only):

https://x.x.x.x:8443/

New Features and Improvements

- Support for user authentication via SAML, for use with services such as Google G Suite, OKTA, OneLogin. See *Integrating User Directories* (#18446)
- EAP-TLS support on the RADIUS server. See *Configuring 802.1x* (#18614)
- Network group (Permission) support for FQDN. See *Creating Permissions* (#18675)
- Added CVE (Common Vulnerabilities and Exposures) information about the platform of the node (#18870)
- Support for SMTP mail server MSA/STARTTLS (tcp/587) method for user authentication, as used by Office 365. See *Setting up Outbound Mail Server (SMTP)* (#18893)
- Web management console changed to connect to a separate port 8443. (#18753)
- When authenticating against an external server using GTC, the RADIUS server now supports settings configured under the authentication integration menu. (#18952)
- Error notifications since last login display in the management console menu bar (#18943)

Issues Fixed

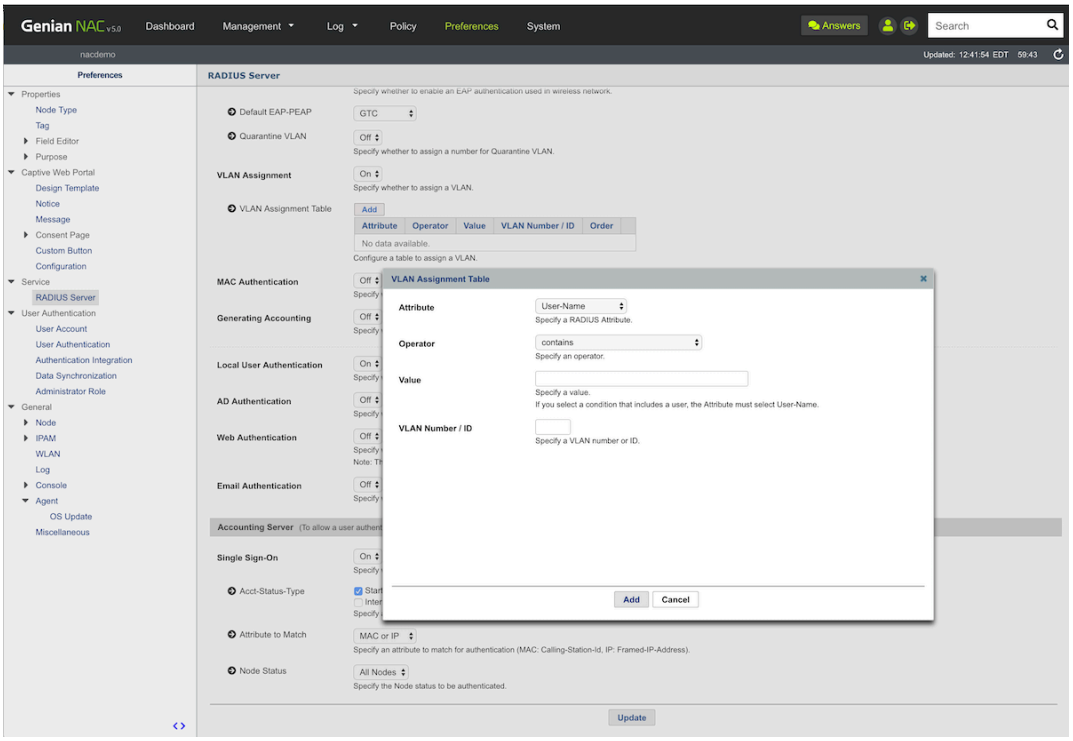
- Fixed an issue where Windows Update can not be installed on Windows 10 in Offline environment (#18928)

23.2.37 Genian NAC v5.0.18 Release Notes (April 2019)

For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

- #18027 Added dynamic VLAN assignment based on RADIUS (802.1x) Attributes



- #18043 Added **inline** sensor operation mode.

  An operation mode is added in which a network sensor is located between an internal network and an external network, such as a firewall, to perform access control on a forwarding packet.

- #18696 Added Rogue DHCP server detection to abnormal detection

Issues Fixed

- #18830 Fixed a problem where URL setting of CWP Ok button does not apply
- #18725 Fixed a problem where {_SENSORIP} macros did not work when sending messages through audit log search filter
- #18715 Fixed a problem where some messages displayed "% s" when the agent working in Japanese Windows

23.2.38 Genian NAC v5.0.17 Release Notes (March 2019)

Release Date: 3/25/2019

For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

- #17136 Dissolvable Agent Option

  The existing agent was a way to immediately report the change of information while continuously running in the end user's system. However, if you want the agent to collect system information and exit immediately depending on your environment, you can now select it as an option. See, *Configuring Agent Settings by Node Policy*

- #17354 Google G Suite support for syncing user information
- #11614 Added 802.1x connection manager plugin for wired LAN
- #18145 Added network access control using RADIUS Change of Authorization (CoA) messages in the enforcement policy
- #18459 Show information about recent synchronization status on information synchronization list screen
- #18474 Added Sophos antivirus information collection to Windows anti-virus information collection plug-in
- #18430 Added macOS monitor collection plugin
- #18496 Added macOS power control plugin
- #16514 Management > Node > Sensor / Group tree search function added
- #17756 Added switch port shutdown prevention string setting function
- #17833 SNMP Version 3 support for SNMP information collection and switch port blocking

Issues Fixed

- #18488 Fixed a problem where the quantity of system list managed nodes was calculated incorrectly
- #18608 Fixed a problem that network interface device names were collected incorrectly
- #18653 Fixed a problem where missing columns were generated on the screen when exporting node list.

23.2.39 Genian NAC v5.0.16 Release Notes (January 2019)

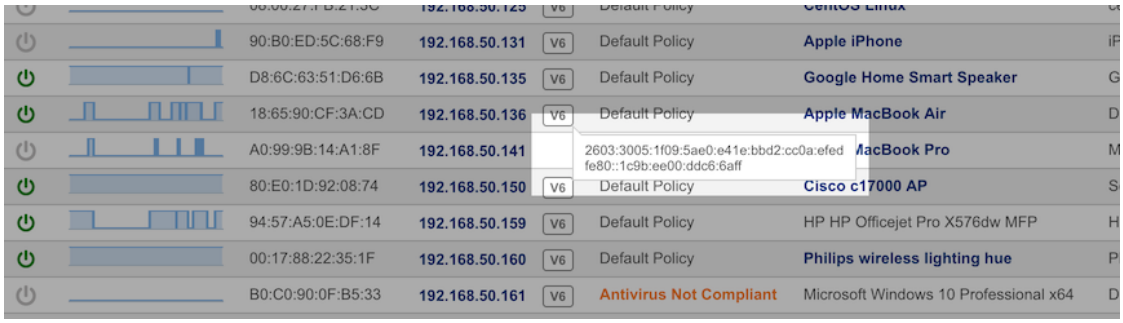
Release Date: 1/7/2019

For instructions on installing and updating Genian NAC, please see *Managing System Software*

New Features and Improvements

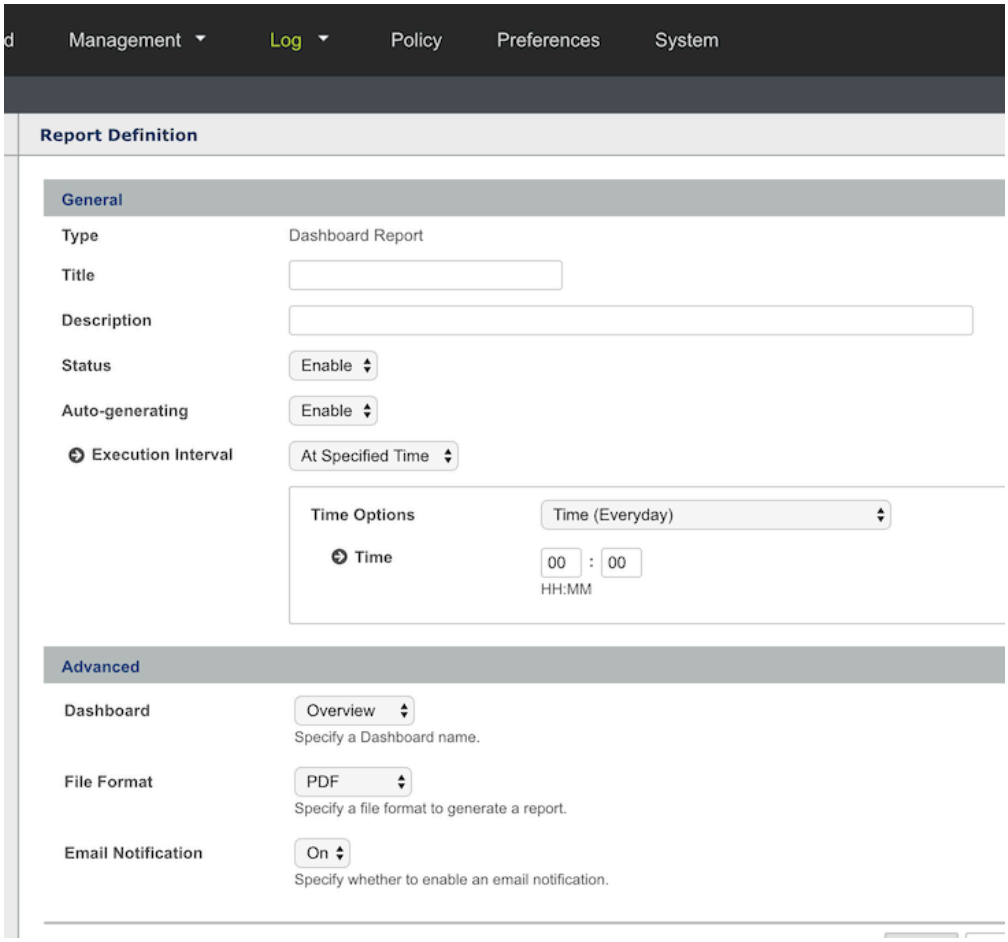
- #12840 Added Sensor-based IPv6 support

  You may now find IPv6 enabled Nodes detected via Network Sensor and configure Node Group Condition settings accordingly to block IPv6 Nodes as needed.



- #18273 Scheduled export of Dashboard Report to PDF and email delivery

  You may now export a Dashboard using PDF format and configure the Dashboard Report settings to be scheduled and emailed.



- #18234 User authentication execution time monitoring and processing delay warning function added
- #18182 Display SSID information of Node when RADIUS Accounting SSO is enabled
- #12441 Improved problem that does not display version information by Agent platform in Widgets and Status
- #17638 Added Google mail server (Google OAuth2 authentication) when setting outgoing mail server for mail notifications
- #17855 Improved to select Antivirus name when creating Node Group conditions for Antivirus information
- #18034 Term changed, Threat -> Anomaly

- #18201 Added Authorization header Settings to Log Filter Webhook settings

Issues Fixed in 5.0.16

- #18418 OS update via NAC Proxy does not work on Windows 10
- #18164 CLI vlan setting does not work if input is long
- #18260 Some programs are not removed by the Uninstall Program
- #18312 Wireless Connection Manager can not connect to 802.1x (GTC) when deleting GnEapGTC.dll from system folder
- #18334 Fixed an issue where Node information would not remain in the Log when the tag was automatically removed due to expiration
- #18368 Fixed an error of duplicate click events for Submit button when submitting for IP Request
- #18370 Agent did not work properly after installing IPv6 feature in Windows XP Fixed
- #18411 Device Name / Device Description of Node Group Condition settings do not work properly and the duplicate Condition Criteria have been fixed
- #18597 Critical interface blocking for virtual interfaces not working
- #18473 Improved to remove if the Node information detected by the network scan is no longer valid

23.2.40 Genian NAC v5.0.15 Release Notes (October 2018)

Release Date: 10/25/2018

For upgrading system software, please see *Managing System Software*

New Features

- #18009 Add HTTP header setting function to log filter web-hook settings. You can set Authorization, Content-type and more headers
- #17944 Add multi-domain setting function with LDAP authentication integration
- #17081 Add ability to collect open port information in macOS network information collection plug-in
- #17680 Add macOS agent appearance and personalization plugin
- #17949 Add Windows device chassis type information (laptop, desktop, etc.)

Enhancements

- #18357 RADIUS server now provided in professional edition.
- #18171 RADIUS authentication and accounting secrets and client IP settings are combined into single setting.
- #18102 Policy menu structure change. Moves the Windows Update and External Device menus that were under Node Policy to the top and move device under a group to external device policy.
- #18154 Add a virtual machine default node group using most popular hypervisor vendor's MAC OUI.
- #17969 Add node group condition's agent needs indication icon for easy to determine agent is required.
- #17081 Add ability to collect open port information in macOS network information collection plug-in.

- #17927 Add a hyperlink to switch and port information in node details.
- #18011 Add audit record if log filter's web-hook return error code.
- #18088 Add to switch management screen so that MAC can be output as tooltip in IP column.
- #18161 User Information Synchronization Error Audit Record Improved to stay in detail.

Bug Fixes

- #17924 Fixed an issue where wireless LAN information collection did not work through agent action in Windows 10 with virtual wireless LAN interface.
- #17967 Fixed an issue where SSID is displayed as MAC in log when using HP Aruba Access Point.
- #18012 Fixed an issue where the "Promiscuous enabled interface does not exist" node group condition was abnormal.
- #18114 Fixed an issue where after inputting value in search condition of audit log, search is not performed when hit the enter key.
- #17997 Fixed a problem where the menu bar was hidden in the matrix when scrolling occurred when enlarging the matrix view.

23.2.41 Genian NAC v5.0.14 Release Notes (August 2018)

Release Date: 8/13/2018

For upgrading system software, please see *Managing System Software*

New Features

- #17919 Enabled Port Mirroring enforcement mode, see *Policy Enforcement Methods*
- #16373 Quarantine VLAN ID assignment via RADIUS, see *Authentication using RADIUS (802.1x)*
- #17599 Export Dashboard to PDF format, see *Managing Dashboards*
- #17125 Mobile App. for Administrator, see *Download Mobile App*
- #17880 Ability to disable IPv6 configuration of Network Interface added to Agent Action, see *Controlling Network Interface*
- #17891 Added a Node Group Condition for the IPv6 Activation Status of an Interface
- #17635 Added ARP Enforcement Strict Mode option
- #17663 Added function to unlock by Authentication Code when Screen Lock is applied, see *Controlling Screen Lock*
- #17436 Added macOS agent Scan Condition Settings, see *Scan Condition Settings*

Enhancements

- #15257 Improved Captive Web Portal. (Separate CWP can be applied to each node policy, Improved customization, Ability to modify CSS and Layout)
- #17379 Improved the ability to Enable/Disable ports in the Port Scan list
- #12581 Improved RADIUS Authentication success log to display actual Username instead of anonymous ID
- #17588 Improved Agent Action Execution Condition to change according to OS Type
- #17669 Removed Hyphenation Validation when entering Cell Phone Numbers
- #17676 Added Bitdefender Anitvirus information collection function to Collect Antivirus Information action
- #17821 Added Kaspersky Antivirus information collection function to Collect Antivirus Information action (Kaspersky Endpoint Security 11 for Windows)
- #17731 RADIUS Configuration options consolidated into the "RADIUS Server" menu
- #17812 Improved to be listed in the selected subnet when returning from node management screen in Matrix view
- #17862 Improved processing performance when deleting multiple sensors
- #17876 Improved problem that difficult to distinguish OS of agent action when node group condition is added

Bug Fixes

- #17719 Agent down after trying macOS Agent Update
- #17911 Plugin does not work if period is specified for periodic execution of agent action
- #18003 api-ms-win-crt-runtime-l1-1-0.dll error when installing agent on a specific PC
- #18153 macOS agent and CWP display authentication status differently
- #17514 Fixed an issue where the alarm on the audit record filter for the new MAC detected does not work
- #17526 Fixed MatrixView tooltips that do not work properly
- #17558 Fixed the problem that the tooltip of macOS agent menu bar icon is broken
- #17640 Some monitor information may only be displayed when using multiple monitors
- #17650 When OTP code is generated in QR code for cloud, image is broken and security key reset button is not visible
- #17696 Fixed problem with 802.1x authentication due to EAP-GTC plugin unregistered on Windows
- #17776 Fixed the SNMP Write community string showing as always invalid
- #17818 Duplicate contents are sent to the same recipient when sending alarm by audit log filter
- #17868 There is a possibility that both devices can be maintained as Master when the policy server redundancy is configured
- #17926 Corrected time value incorrectly displayed among the collected antivirus information
- #18055 Invalid Agent Action permissions in Basic Edition fixed
- #18117 Fixed a problem where patch download fails if there are multiple interfaces of Policy Server or Distribution Server

23.2.42 Genian NAC v5.0.13 Release Notes (April 2018)

Release Date: 4/18/2018

New Feature & Improvement

- #17206 Improved policy server to enable external connections through Proxy server setting.
- #17088 Improved to leave audit records before certificate expiration.
- #17127 Add CUBRUD DB to DB list that can synchronize information.
- #17253 Add the ability to check the allowed IP when the administrator logs in for the first time.

Bug Fix

- #17394 Fixed a problem where html tag is output when password input error of computer name change (agent action).
- #17425 Fixed a problem where the CWP URL could not be set if the CWP domain configuration contained a detailed address after '/'.
- #17393 Fixed problem where search condition is initialized when audit log filter is modified.
- #17407 Fixed a problem that the host name of the node is continuously changed by the MDNS packet.
- #17230 Fixed a problem where the platform information of the node where the agent is installed is displayed as "Unknown" on the terminal with the latest operating system installed.
- #17424 Fixed a problem that when the version information is compared with the execution condition of the action, the version does not work if the version is only a number without the delimiter.
- #17452 [Agent] Corrected the display error status of IPv4 and IPv6 in Windows node interface information.
- #17362 [Agent] Fixed a problem where macOS agent remote agent deletion hidden function does not work.
- #17378 [Agent] Fixed a problem where NAT was detected when changing the IP of a PC with macOS agent installed.

23.2.43 Genian NAC v5.0.12 Release Notes (February 2018)

Release Date: 2/8/2018

New Feature & Improvement

- #17214 Support LSI Logic SAS adapter
- #17156 Improved to send user secondary verification SMS authentication code to 6 digits
- #17095 Support MacOS agent for High Sierra
- #17112 Add account expiration time setting function from user management screen
- #16232 Add ability to gather locally configured IPv6 information with agent installedBug Fix

Bug Fix

- #17316 Fixed the problem of not operating the wireless LAN card on Intel NUC NUC6CAY
- #17071 Fixed a problem where the user tries to delete the backup file if free space can not be secured
- #17104 Fixed the problem that mssql.log file is not generated when synchronizing information with MSSQL server
- #17145 Fixed an error that could not be applied to a policy even after entering a value that is out of acceptable range for the node action

- #17128 Fixed a problem where the same device information appears duplicated in USB device information
- #17161 Fixed an issue where agent unassembly nodes were included in the agent information related node group
- #17107 Fixed the problem that the center IP is designated as virtual IP when the virtual IP is automatically set in the center band sensor
- #17128 [Agent]Fixed a problem where tray icon is not displayed when macOS agent is installed
- #17131 [Agent] Fixed an issue where agent authentication window does not exit when Agent Failsafe operation

23.2.44 Genian NAC v5.0.11 Release Notes (December 2017)

Release Date: 12/5/2017

New Feature & Improvement

- #16828 Added the ability to check the port information used by the product
- #16807 Improve node group matching speed with large number of conditions
- #16564 Added verified node type and platform name functionality
- #17076 The improved to leave the superuser ID and IP as audit records when manually remove the risk
- #16907 Improved validation check order when registering with user's existing user ID
- #16536 Added Device Lifecycle Management function
- #16575 [Agent] Added ability to monitor system resources (CPU, Memory, Network, Disk) usage

Bug Fix

- #17179 Fixed an issue that caused errors in user 2-step authentication in CWP
- #17064 Fixed the problem that automatic reauthentication does not work when authentication is expired while using AD alternate authentication
- #16896 Fixed a problem where the start date end date is initialized when the user input date pattern is not yyyy-MM-dd when searching the audit log
- #16954 Fixed the problem that user list screen of user group is displayed incorrectly
- #16960 Fixed the problem that initial MAC grant does not work when platform is detected when registering new node
- #17033 If node group condition operation is AND, fix problem that satisfies matching condition but does not match actual node
- #17131 [Agent] Fixed the problem that macOS agent plug-in execution is infinitely repeated

23.2.45 Genian NAC v5.0.10 Release Notes (October 2017)

Release Date: 10/19/2017

New Feature & Improvement

- #16579 HTTPS CWP Redirect Support
- #16312 Improved to select whether to register node when receiving GARP packet
- #14300 Added "Select language" option to admin login page
- #16666 Add trend graph to node / wireless LAN group big number widget

- #16747 Charset option Change from global option to per-sensor option
- #16447 Improved to count output for items in the tree of the switch management screen
- #16685 [Agent] Improved macOS agent program information window design

Bug Fix

- #16810 Pop-up window does not close after changing password in secret change dialogue after enforcing administrator password
- #16626 Status chart error on reregistration after node deletion
- #16725 Problems with blank selection when setting sensor-based management limits
- #16604 Error when setting netmask value to 0.0.0.0 when creating network object
- #16800 [CLI]IP pattern check error when setting ip name-server
- #16722 [Agent] Fixed a problem that sends Keep Alive transmission to wrong center when using multicenter list
- #16297 [Agent] Fixed the problem that Windows automatic update can not be turned off in Windows 10

23.2.46 Genian NAC v5.0.9 Release Notes (August 2017)

Release Date: 8/16/2017

New Feature & Improvement

- #16457 Add multi-node registration function to IP MatrixView
- #16400 Added VIRTIO driver for Xen based virtualization system
- #16537 Add new node / AP / audit log inquiry widget registered since last login
- #16535 Upgrading the latest version of Kernel
- #16406 Improved agent download screen
- #16440 [Agent]Added USB device information collection function to Collect Hardware Information plug-in
- #16053 [Agent]Improve System32 folder check method for 64-bit Windows
- #16469 [Agent]Added auto update function for macOS's Agent

Bug Fix

- #16348 Node type management does not register normally when registering icons.
- #16424 The network usage chart only shows up or down
- #16230 The conditions are not immediately reflected when uploading a CSV file from a network object
- #16462 Problem that caused SQL error when registering Agent Plugin
- #16651 Fixed problem where node group regular expression matching condition does not work
- #16670 Fixed the problem of HTTP connection when CWP redirection

23.2.47 Genian NAC v5.0.8 Release Notes (May 2017)

Release Date: 5/22/2017

New Feature & Improvement

- #15992 – Add user count and link to user group list
- #16015 – Support for MySQL DB connection via SSL when synchronizing user information
- #16134 – Improved to leave audit log when untagged
- #16199 – Improved to separate general and administrative privileges from the CLI
- #16231 – Added "security question" method to lost password recovery method
- #16366 – Added ability to sort node group nodes count
- #16432 – Opensshd Vulnerability Patch (CVE-2016-6210, CVE-2016-6516)
- #16133 – Change the origin of macOS agent from Unknown to identified developer
- #15883 – Notify when the set time zone and browser time zone are different after administrator login
- #15853 – Agent support High GDPI on Windows

Bug Fix

- #16236 – Layout corruption when modifying dashboard tabs
- #16247 – NTP server settings among DHCP options are sent to DNS entries
- #16280 – Agent custom icons do not work
- #16306 – DB backup file download list incorrectly displays backup file size
- #16310 – Problems that do not show QR code image on OTP authentication screen
- #16335 – Abnormal termination of program when Internet Connection Sharing is controlled by the interface control plug-in
- #16379 – Node Management> Status chart is displayed incorrectly

23.2.48 Genian NAC v5.0.7 Release Notes (March 2017)

Release Date: 3/27/2017

New Feature & Improvement

- #15779 – Improved the license registration method (copy & paste)
- #15912 – Added options for node registration, manual node scan by command line.
- #15913 – Added Excel Export function for job position / department list
- #15935 – Added a System Default Log Filter (New device detected, New platform detected, New internal SSID detected)
- #15947 – Enhanced Email notification (Change email title, Show Timezone, Same type message combine, Administrator Console Link..)
- #15977 – Added Uncategorized Node Group list under node group tree
- #16031 – Added Node registration in IP Matrix view
- #16036 – Improved to create with the Center / Sensor Integrated CD when creating the 5.0 installation CD

- #16108 – Support Microsoft Hyper-V Hypervisor
- #16190 – Support UEFI installation
- #15977 – [AGENT] Improved WMI plugins to allow direct input of Namespaces

Bug Fix

- #16057 – List not updated immediately after software manual upload
- #16088 – Some plugins do not delete when deleting remote agent
- #16111 – Dashboard does not display patch information for nodes
- #16138 – User Authentication is not allowed due to case sensitivity of MAC
- #16144 – Fixed icon size and patch icon on location information tab of WLAN details
- #16146 – [AGENT] Problems with shutting down process when changing macOS agent AD authentication status
- #16147 – [AGENT] Unable to control online account with password verification plugin

23.2.49 Genian NAC v5.0.6 Release Notes (February 2017)

Release Date: 2/24/2017

New Feature & Improvement

- #15863 – Improve product management console screen output with iPad Pro
- #15899 – LDAP over SSL support for user information synchronization
- #15907 – Switch – Improved to display corresponding switch port information when clicking on the traffic top 10 widget link
- #15945 – Switch List Improved to Display as Port Number if Switch Port Name is Missing
- #15952 – Add WLAN count and link to WLAN group list
- #15957 – Add link to sensor / IP / MAC in audit log screen
- #14538 – Add Dashboard Widget for Software, Open Port
- #15870 – [AGENT] Added agent notification function before expiration by password change cycle
- #15877 – [AGENT] Added agent notification function before user account expiration
- #15985 – [AGENT] Add information about Windows Server 2016

Bug Fix

- #15849 – SoftwareUpgrade screen does not output upgrade information.
- #15881 – TOP menu update time does not change according to time zone setting.
- #15882 – Problems with node policy output with nonexistent risk definitions.
- #15946 – WLAN Group Include Group Name in Numbered Log in Problem
- #15976 – RADIUS Accounting Could Cause Center to Shut Down When Receiving Packet
- #15818 – [AGENT] Administrator-approved patches are not installed on Japanese Windows.

CHAPTER

TWENTYFOUR

SECURITY ADVISORIES

24.1 GN-SA-2023-001: Genian NAC - Multiple Vulnerabilities

24.1.1 Date

- Aug 15, 2023

24.1.2 Serverity

- High

24.1.3 Summary

The following vulnerabilities were identified related to the Genian Update server(s):

- Missing Encryption of Sensitive Data vulnerability(CVE-2023-40251)
- Improper Control of Generation of Code (Code Injection) vulnerability(CVE-2023-40252)
- Improper Authentication vulnerability(CVE-2023-40253)
- Download of Code Without Integrity Check vulnerability(CVE-2023-40254)

Note: Server side actions were taken to mitigate threats, however, customers running the version(s) mentioned below are advised to update to the fixed version(s) as soon as possible. Not updating may leave customers vulnerable as well as prevent customer policy servers from obtaining the latest updates from the Genian Update server infrastructure.

24.1.4 Affected Products

- Genian NAC 5.0.42 LTS (Revision 117460 or lower)
- Genian NAC 5.0.54 or lower
- Genian ZTNA 6.0.15 or lower

24.1.5 Affected Components

- Policy Server
- Network Sensor
- Agent

24.1.6 Resolution

The vulnerabilities contained in this advisory can be addressed by upgrading to version listed below:

- Genian NAC 5.0.42 LTS (Revision 117461 or higher)
- Genian NAC 5.0.55 or higher
- Genian ZTNA 6.0.16 or higher

24.1.7 Workaround

- None

24.2 GN-SA-2021-003: Genian NAC - Multiple Log4j Vulnerabilities

24.2.1 Date

- Dec 20, 2021

24.2.2 Serverity

- High

24.2.3 Summary

Geinans has released updates that address multiple log4j vulnerabilities as detailed below.

Vulnerability Details (1)

CVE-2021-44228 - Log4j Remote Code Execution

Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed.

Vulnerability Details (2)

CVE-2021-44228 - Log4j Malicious Data Input

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack. Log4j 2.15.0 makes a best-effort attempt to restrict JNDI LDAP lookups to localhost by default. Log4j 2.16.0 fixes this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

Vulnerability Details (3)

CVE-2019-17571 - Log4j Deserialization of Untrusted Data

Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.

24.2.4 Affected Products

- Genian NAC v5.0.43 or less
- For LTS, Genian NAC v5.0.42 revision 101421 or less

24.2.5 Affected Components

- Policy Server

24.2.6 Resolution

The vulnerabilities contained in this advisory can be addressed by upgrading to version listed below:

- Genian NAC v5.0.44 or higher
- Genian NAC v5.0.42 (LTS) revision 101422 or higher

24.2.7 Workaround

- None

24.3 GN-SA-2021-002: Genian NAC - Multiple Vulnerability

24.3.1 Date

- Nov 5, 2021

24.3.2 Serverity

- High

24.3.3 Summary

Geinans has released updates that address multiple security vulnerabilities including the two critical vulnerabilities listed below as well as several other vulnerabilities.

- A problem in which a command injection vulnerability exists in a specific API called by a network sensor to obtain a shell of the system.
- When changing the password for a user authenticated to the node in the agent, there is a vulnerability that can change the password for a user other than the authenticated user.
- And few minor vulnerabilities.

24.3.4 Affected Products

- Genian NAC v5.0.41 or less
- Genian NAC v5.0.42 (LTS) revision 100181 or less
- Genian NAC v4.0.145 or less

24.3.5 Affected Components

- Policy Server
- Network Sensor
- Agent (Windows / macOS)

24.3.6 Resolution

The vulnerabilities contained in this advisory can be addressed by upgrading to version listed below:

- Genian NAC v5.0.42 (LTS) revision 100182 or higher
- Genian NAC v5.0.43 or higher
- Genian NAC v4.0.146

24.3.7 Workaround

- None

24.4 GN-SA-2021-001: Genian NAC - SQL Injection Vulnerability

24.4.1 Date

- Aug 9, 2021

24.4.2 Serverity

- High

24.4.3 Summary

Geinans has released updates to the Policy Server that address a security vulnerability in SQL query escape processing.

A vulnerability exists whereby an attacker may utilize a SQL Injection attack on system databases. This leaves the database vulnerable to the attacker who may then view, modify, add or delete data within a database. Retrieving data for malicious use or creating admin accounts are two examples of many scenarios that could occur if the vulnerability is left unpatched.

24.4.4 Affected Products

- Genian NAC v5.0.41 or less
- Genian NAC v4.0.144 or less

24.4.5 Affected Components

- Policy Server

24.4.6 Resolution

The vulnerabilities contained in this advisory can be addressed by upgrading to Policy Server version listed below:

- Genian NAC v5.0.42 (LTS)
- Genian NAC v4.0.145

24.4.7 Workaround

- None

CHAPTER

TWENTYFIVE

SERVICE LEVEL AGREEMENT

This document outlines the service levels for Genians Next-Gen NAC solution, which includes the Genian NAC Software with the valid maintenance, Cloud-managed NAC Subscription and Genian NAC 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 NAC Appliances. The following services are provided only to the customer who purchases Genian NAC 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.