Genian ZTNA

Release 6.0.25

GENIANS, INC.

Jul 02, 2024

관리자 가이드


DOWNLOAD PDF

CHAPTER

ONE

ZTNA(ZERO TRUST NETWORK ACCESS)의 이해

1.1 ZTNA란 무엇인가?

ZTNA(Zero Trust Network Access)는 네트워크가 아닌 애플리케이션에 대한 액세스를 기반으로 보안을 제공하는 네트워크 보안 접근 방법입니다.

ZTNA를 사용하면 네트워크 내부에 있는지 여부에 관계없이 사용자, 장치 및 애플리케이션에 대한 액세스를 검증하고 제어할 수 있습니다. 이를 통해 네트워크가 침해되었더라도 악성 사용자가 민감한 데이터에 액세스하지 못하도록 보호할 수 있습니다.

Genian ZTNA는 ZTNA 솔루션으로서 네트워크가 아닌 애플리케이션에 대한 엑세스를 기반으로 보안을 제공하는 클라우드 및 Onpremiss 솔루션입니다.

Genian ZTNA는 다음과 같은 다양한 기능을 제공합니다.

사용자 및 장치 인증

Genian ZTNA는 사용자 이름, 암호, 생체 인식 또는 SSO와 같은 다양한 방법을 사용하여 사용자 및 장치를 인증할 수 있습니다.

애플리케이션 제어

Genian ZTNA는 사용자, 장치 및 애플리케이션에 대한 액세스를 검증하고 제어할 수 있습니다.

위협 탐지 및 대응

Genian ZTNA는 데이터 암호화, 사용자 인증 및 위협 탐지와 같은 다양한 보안 기능을 제공합니다.

정책 기반 액세스 제어

Genian ZTNA는 역할 기반 액세스 제어(RBAC), 사용자 지정 정책 및 감사 추적과 같은 다양한 방법을 사용하여 액세스를 제어할 수 있습니다.

1.2 Genian ZTNA의 다양한 이점

보안 강화 : 네트워크가 침해되었더라도 악성 사용자가 민감한 데이터에 액세스하지 못하도록 보호합니다.

비용 절감 : 기존 네트워크 보안 아키텍처의 복잡성과 비용을 줄일 수 있습니다.

유연성 향상 : 사용자와 애플리케이션이 어디에 있든 액세스할 수 있도록 하여 유연성을 향상시킬 수 있습니다.

규정 준수 향상 : HIPAA, PCI DSS 및 GDPR을 포함한 다양한 규정을 준수하는 데 도움이 될 수 있습니다.

1.3 ZTNA가 해결해주는 문제점들

데이터 유출

Genian ZTNA는 사용자, 장치 및 애플리케이션에 대한 액세스를 검증하고 제어함으로써 데이터 유출을 방지할 수 있습니다.

악의적인 사용자의 공격

Genian ZTNA는 사용자와 애플리케이션 간에 보안 터널을 설정함으로써 공격으로부터 애플리케이션을 보호할 수 있습니다.

보안 아키텍처의 복잡성과 비용

Genian ZTNA를 사용하여 많은 보안 솔루션들로 이루어진 보안 아키텍처들을 단순하게 하고 그로인해 비용을 줄일 수 있습니다.

허가되지 않은 기기의 무단 반입

ZTNA가 구현되지 않은 네트워크는 사내에 존재하는 이더넷 포트에 어떠한 기기를 연결하더라도 즉시 네트워크를 사용할 수 있게 된다. 이는 사무실이 물리적으로 매우 안전하게 보호되고 있다 하더라도 직원들이 회사의 자산이 아니거나 허용되지 않은 기기를 네트워크에 연결하여 Worm이나 Ransomware 등으로 인해 사내 IT 시스템에 심각한 손상을 초래할 수 있게 된다. ZTNA는 이 문제를 해결하기 위해 모든 연결되는 기기에 대해 인증하고 일정 수준 이상의 보안 요구사항을 충족하는 경우에만 네트워크를 사용할 수 있게 해 준다.

보안사고 발생 시 IP 추적 불가

대부분의 보안시스템은 감사기록을 통해 IP주소를 남긴다. 보안사고 발생 시 감사기록 확인을 통해 문제가 되는 IP를 확인하더라도 현재 그 IP가 과거에 사용되었던 시스템과 같은 시스템인지 사용자는 누구인지, 어떤 시스템인지에 대한 정보를 얻는 것은 굉장히 어렵고 복잡한 일이다. ZTNA는 지속적인 네트워크 감시를 통해 연결 되는 모든 단말에 대한 기록을 남겨두어 수개월 전 특정 시점에 해당 IP를 사용했던 단말에 대한 다양한 정보를 제공해줄 수 있다.

보안 규제에서 요구되는 IT 자산관리

오늘날의 IT 환경은 BYOD, IoT 등으로 인해 과거에 비해 훨씬 복잡 다양해졌다. 이로인해 기업에 요구되는 많은 보안 규제에서 IT 자산에 대한 관리가 철저히 이루어질 것을 요구하고 있다. 하지만 IT 자산을 정확하게 파악하고 그 상태를 항상 확인하는 것은 관리자에게 어려운 문제이다. IT 자산을 관리하기 위해서는 MAC 주소와 같은 식별 값부터 단말의 제조사, 제품명, 이름, 위치 (스위치 포트 또는 물리적 위치), 사용자명, 네트워크 연결/단절 시각등의 정보가 정확히 수집되어야 한다. ZTNA는 네트워크에 연결되는 IT 자산에 대해 실시간으로 감시하여 항상 원하는 데이터를 출력할 수 있도록 해서 관리자의 부담을 크게 줄여준다.

무선랜 접속장치의 공유 비밀번호

스마트폰과 같은 모바일 기기들이 확산되고 그것들이 업무에 활용되면서 무선랜 사용이 점차 증가되고 있다. 고가의 관리형 무선 접속장치를 사용하는 경우 향상된 보안시스템이 적용되어 무선랜 접속 시 각 개인의 비밀번호를 이용한 사용자 인증이 이루어질 수 있다. 하지만 많은 네트워크에서 공유 비밀번호를 통해 무선랜에 접속하는 것이 현실이다. 공유비밀번호는 손쉽게 노출될 수 있고 접속자에 대한 식별이 불가능하여 추적이 어렵다. 회사의 공유 비밀번호는 원칙적으로 그 비밀번호를 아는 직원이 회사를 떠나게 될 경우 변경해야 한다. 하지만 전 직원이 쓰는 비밀번호를 매번 변경하는 것은 쉬운일이 아니다. 이를 위해 무선랜 접속시 개인의 비밀번호를 이용하여 인증할 수 있도록 해주는 802.1X 시스템이 필요하다. ZTNA는 기본적으로 802.1X를 지원하여 보다 향상된 무선랜 보안을 구축할 수 있게 해 준다.

허가되지 않은 외부 네트워크 접속

네트워크 기술이 발전함에 따라 사용자의 단말은 자신이 속한 기업에서 제공하는 네트워크 이외에도 다양한 형태의 외부 네트워크 접속이 가능해졌다. 스마트폰을 이용한 Hotspot이나 Public WiFi와 같이 손쉽게 이용 가능한 접속을 통해 기업의 보안시스템을 우회하는 인터넷 연결을 만들어 내부자료 유출과 같은 문제점이 발생될 수 있다. ZTNA는 기업 내부에서 접속 가능한 WiFi를 모니터링하고 어떤 사용자가 접속하는지를 관리, 통제할 수 있으며 또한 사용자 단말에서 IT 관리자가 설정하지 않는 네트워크 대역에 접속하는 이벤트 등을 모니터링해서 내부 보안시스템을 우회하려는 시도를 차단해준다.

필수 소프트웨어 미설치 및 구동

관리자는 다양한 보안 문제를 해결하기 위해 사용자의 시스템에 설치해야 할 필수적인 소프트웨어나 운영체제 설정을 직원들에게 요구하게 된다. 하지만 모든 사용자의 단말이 그 요구사항을 항상 준수하는 것은 아니기 때문에 보안사고는 끊임없이 발생되고 있다. ZTNA는 Antivirus와 같이 단말에 필수적으로 필요한 소프트웨어나 화면보호기와 같은 필수적인 설정이 규정에 맞게 올바르게 되어있는지 지속적으로 모니터링하여 규정을 위반한 경우 차단, 치유, 격리할 수 있게 해 준다.

운영체제 최신 보안패치 미적용

단말의 보안을 위해 무엇보다 가장 중요한 것은 최신 보안패치의 적용이다. ZTNA는 단말의 보안패치 적용 상태를 지속적으로 모니터링하여 패치가 적용되지 않은 단말을 네트워크에서 격리한다. 이는 제어가 단말이 아닌 네트워크 수준에서 동작한다는 점이 기존의 단말을 관리하는 소프트웨어가 제공하는 것과 크게 다르다. 관리자는 네트워크 제어를 통해서 사용자가 우회할 수 없는 강력한 정책을 수행할 수 있게 된다.

1.4 ZTNA와 Firewall의 차이점

ZTNA(Zero Trust Network Access)와 방화벽은 모두 네트워크를 보안하는 데 사용되지만 작동 방식과 제공하는 보안 수준이 다릅니다.

방화벽은 네트워크의 출입구를 보호하는 데 사용되는 네트워크 보안 장치입니다. 방화벽은 IP 주소, 포트 및 프로토콜과 같은 다양한 기준에 따라 패킷을 필터링하여 네트워크에 들어오거나 나가는 것을 차단할 수 있습니다.

ZTNA는 네트워크가 아닌 애플리케이션에 대한 액세스를 기반으로 보안을 제공하는 보안 접근 방법입니다. ZTNA는 네트워크 내부에 있는지 여부에 관계없이 사용자, 장치 및 애플리케이션에 대한 액세스를 검증하고 제어할 수 있습니다. 이를 통해 네트워크가 침해되었더라도 악성 사용자가 민감한 데이터에 액세스하지 못하도록 보호할 수 있습니다.

ZTNA와 방화벽의 주요 차이점은 ZTNA는 네트워크가 아닌 애플리케이션에 대한 액세스를 기반으로 보안을 제공한다는 것입니다. 즉, ZTNA는 네트워크 내부에 있는지 여부에 관계없이 사용자, 장치 및 애플리케이션에 대한 액세스를 검증하고 제어할 수 있습니다. 반면 방화벽은 네트워크의 출입구를 보호하는 데만 사용됩니다.

Genian ZTNA는 기존 NAC의 기능을 통하여 기존까지 제공하던 단말 중심, 동적인 정책, 내/외부망에 대한 장점을 그대로 활용 할 수 있습니다.

네트워크 중심 vs 단말 중심

Firewall은 그 구성 위치상 일반적으로 두개 이상의 네트워크 중간에 위치하여 양 네트워크를 오가는 통신에 대한 접근제어를 제공하는데 반해 ZTNA는 각 단말 간의 통신에 대한 접근제어를 제공한다. 예를 들어 동일한 서브넷에 존재하는 두 PC간에 이루어지는 파일공유에 대해서 일반적으로 Firewall은 제어하지 못하는 반면 ZTNA는 제어를 할 수 있다.

정적인 정책 vs 동적인 정책

Firewall의 정책은 일반적으로 5 Tuples라 불리는 출발지/목적지의 주소, 포트와 같은 객체를 통해서 이루어진다. 최근 차세대 방화벽에서 사용자와 같은 추가적인 객체를 통한 제어를 제공하기 시작했으나 그 수가 많지 않다. 반면 ZTNA의 경우는 통상 수 백개 이상의 조건을 통해 단말들의 그룹을 구성하면 각 단말의 상태 변경에 따라 구성된 그룹에 자동으로 포함/해제가 되고 그에 따라 정책이 적용되는 구조를 제공한다. 예를 들어 Antivirus를 구동 중이지 않은 단말이라는 그룹이 있다고 가정하면 이 그룹에 속한 단말은 상태에 따라 실시간으로 변화하게 된다.

외부망 vs 내부망

이 같은 이유로 인해 Firewall은 단말의 사용자를 특정할 수 없고 상세한 정보를 수집할 수 없는 외부 사용자와 내부 시스템간의 접근제어의 목적에 보다 적합하고 ZTNA는 다양한 상태 정보를 얻을 수 있는 내부 사용자에 대한 접근제어 시스템으로 적합하다.

두 개의 제품은 각각의 역할에 맞는 위치 및 구성으로 네트워크 보안을 보다 효과적으로 구축할 수 있는 상호 보완적인 역할을 수행한다.

1.5 ZTNA 구축단계

가시성 확보

ZTNA를 구축하는 궁극적인 목적은 관리자가 정한 보안규정을 준수하지 않는 단말이 네트워크에 접속해서 사용하는 것을 통제하고 관리하는 것이다. 하지만 이 목적을 위해 단말에 대한 통제기능을 네트워크 및 단말에 즉시 적용하기는 매우 어렵습니다. 예를 들어 802.1X를 각 스위치 별로 설정하기에 앞서 네트워크에 있는 스위치들이 모두 802.1X를 지원하는지 그리고 현재 각 스위치에 연결된 단말이 802.1X 인증을 지원하는지, 지원하지 않는다면 MAC 주소 기반 인증을위해 필요한 각 단말의 MAC 주소는 어떻게 수집할 것인지 등의 많은 사전 고려사항이 필요하다. 때문에 네트워크에 대한 가시성을 확보하는 것이 가장 처음으로 해야 할 작업이다. 이때 통제 없이 가시성이 확보가 가능해야 하는데 802.1X는 제어가 이루어져야만 가시성을 얻을 수 있는 구조이기 때문에 가시성 확보만을 위한 목적으로 적합하지 않다.

가시성은 단말이 가진 IP/MAC 주소와 같은 기본 정보를 시작으로 어플리케이션, 사용자를 식별하고 플랫폼 종류/이름/제조사, 호스트명, 연결 스위치/포트, 연결 SSID, 서비스포트, 동작상태와 같은 정보들이 제공되어야 한다. 추가적으로 단말에 대한 보다 상세한 가시성을 위해 ZTNA Client를 제공하고 있습니다.

단말의 분류

가시성이 확보되면 그 데이터를 기반으로 보안정책을 수립해야 한다. 보안정책 수립의 첫 단계는 수집된 데이터를 바탕으로 단말을 분류하는 것이다. ZTNA에서 제공되는 다양한 조건을 이용하여 단말을 분류하고 제어가 필요한 그룹이 어떤 그룹인지에 대해서 결정해야 한다. 단말을 분류하는 기준은 관리자의 일상적인 관리업무에 필요한 그룹이나 기업이 따라야할 규제에서 요구되는 보안규정 미준수 단말을 식별하는것이 우선적으로 고려될 수 있다.

네트워크 접근제어

제어의 방법은 한 가지가 아니라 네트워크 환경이나 단말의 상태에 따라 다양한 방식으로 적용할 수 있어야 한다. 802.1X는 물론 ARP통제, 스위치 제어, SPAN방식, 에이전트 기반, 타 보안시스템 연동까지 여러 가지 옵션을 놓고 선택적으로 사용할 수 있어야 한다. 접근제어 단계에서 가장 먼저 고려되는 것이 단말에 대한 사용자의 인증이다. 단말을 어떤 사용자가 사용하는 것인지 식별하는 작업은 매우 중요한 작업인데 이때 사용되는 사용자 데이터베이스는 일반적으로 기업이 이미 보유한 인증시스템과 연동하는 것이 권장된다. Microsoft Active Directory와 같은 LDAP 연동이나, Google G-Suite, Office 365와 같은 기업용 서비스, 이메일, 심지어는 RDBMS까지 다양한 외부 시스템과의 연동이 고려된다. 그다음 단계로 사용자가 단말의 속성에 따라 역할 기반 접근제어가 제공되어야 한다. 영업 조직과 기술 조직이 각기 다른 접속 권한을 가질 수 있도록 VLAN을 할당하거나 연결을 차단하는 제어를 수행한다.

접근제어를 통해 연결이 차단된 사용자에게는 웹 브라우저 사용 시 관리자가 지정한 페이지로 사용자의 접속을 우회시켜 사용자가 스스로 필요한 조치를 취할 수 있도록 하는 Captive Web Portal 페이지를 구성할 수 있다. 이 페이지를 통해 사용자는 자신에게 요구되는 보안정책을 확인하고 조치를 취해서 네트워크에 접속 가능한 상태로 스스로 조치할 수 있도록 도와준다.

IT보안 자동화

자동화는 사용자들이 따라야 할 보안규정 (운영체제 업데이트 및 설정, 필수 소프트웨어 설치 및 동작등)을 관리자가 정한 정책에 따라 자동으로 적용되도록 해주는 것이다. 제어가 필요한 단말에 대해서 인증과 같이 제어 자체가 목적을 달성하는 수단이 되기도 하지만 또 다른 경우에는 제어에 앞서 자동화를 통해 사용자의 단말이 치유되는 것이 더 필요할 수 있다. 예를 들어 전체 사용자의 90%가 준수하지 않는 보안정책이 있다고 했을 때 90%의 사용자에 대해 네트워크 접근제어 정책을 수행하는 것보다는 에이전트를 통하여 자동으로 정책을 따르도록 처리된다면 보다 손쉽게 ZTNA를 도입할 수 있을 것이다. 또한 자동화는 기존에 사내에 보유한 다양한 시스템들과의 연동을 통해 상호 정보나 이벤트를 주고받아 관리자의 개입 없이 업무가 자동적으로 처리될 수 있도록 해준다.

보다 자세한 구축방법 및 고려사항에 대해서는 구축 고려 사항 을 참고하기 바란다.

1.6 Genian ZTNA의 특징

1세대 ZTNA

1세대 ZTNA는 사용자와 장치를 인증하고 애플리케이션에 대한 액세스를 허용하거나 거부하는 데 중점을 둡니다.

2세대 ZTNA는 1세대 ZTNA의 기능을 확장하여 사용자 및 장치의 행동을 모니터링하고 이상 징후를 식별합니다. 또한 애플리케이션과 데이터를 보호하기 위한 추가 보안 기능을 제공합니다.

클라우드 기반 보안서비스

Genian ZTNA는 클라우드 기반 솔루션이므로 관리 및 유지 관리가 간편하며 클라우드 기반 보안 서비스는 위협 탐지, 데이터 암호화 및 사용자 인증과 같은 다양한 보안 기능을 제공합니다.

ZTNA 게이트웨이

ZTNA 게이트웨이는 사용자와 애플리케이션 간의 보안터널을 생성하여 통신하는 데이터를 보호하고 이상 징후를 식별하는데 사용합니다.

사용자 및 장치 인증

Genian ZTNA는 사용자 이름, 암호, 생체 인식 또는 SSO와 같은 다양한 방법을 사용하여 사용자 및 장치를 인증할 수 있습니다.

애플리케이션 제어

Genian ZTNA는 사용자, 장치 및 애플리케이션에 대한 액세스를 검증하고 제어할 수 있습니다.

네트워크센서 기반의 진보된 가시성

Genian ZTNA는 각 네트워크의 브로드캐스트 도메인에 직접 연결되는 네트워크센서를 사용해 기존 IT 인프라와의 연동을 최소화하여 도입이 간편하고 허브와 같은 레거시 네트워크 환경에서도 문제없이 동작한다. 더불어 네트워크 가시성 확보에 필요한 각 서브넷의 중요 트래픽 - Broadcast(ARP, DHCP, uPNP, mDNS), Multicast - 을 모니터링할 수 있기 때문에 네트워크 장치와 연동을 통한 ZTNA 제품군에 비해 진보된 가시성을 제공한다.

진보된 단말 플랫폼 정보

Device Platform Intelligence 로 불리는 차별화된 단말 식별 및 정보제공 시스템을 통해 가장 정확하고 단말에 대한 다양한 정보를 통해 IT 관리자의 일상적인 관리업무을 손쉽게 만들어준다. 제공정보의 종류: 판매 종료, 지원 종료, 네트워크 연결방식, 제조사 도산, 제조사 합병, 제조국가, 발표된 취약점 목록 등

다양한 접근제어 방식

접근제어는 802.1X부터 ARP통제, DHCP 서버, 스위치 제어, SPAN 기반 제어, 에이전트 기반 제어, 타 솔루션과의 연동을 통한 제어 등 기존 ZTNA 제품 대비 가장 폭넓은 제어 방식을 지원하여 관리자의 요구사항에 맞게 단계적인 보안정책을 수립하기 쉽게 해 준다. (참고 제어 방법)

다양한 IT보안 자동화

Genian ZTNA에서 제공되는 에이전트는 단말의 정보수집을 넘어서 운영체제 설정 관리, 애플리케이션 관리, 장치 제어, 업데이트 관리 등 관리자가 원하는 다양한 IT보안 자동화를 손쉽게 구축할 수 있게 해 준다. 또한 다양한 신청/승인 시스템을 제공하여 IT 관리자의 일상 업무를 단순화시켜주고 사용자에게는 편리성을 제공한다.

향상된 무선랜 보안

네트워크센서 및 에이전트를 통해 무선 정보를 수집하여 Rogue AP 탐지, 비인가 무선랜 접속 모니터링 및 제어, Soft AP차단 등의 무선랜 보안 기능을 제공한다.

뛰어난 연동성

REST API, Webhook, Syslog와 같이 표준적인 연동 기술을 제공하여 기존 IT시스템과의 다양한 연동을 통해 시큐리티 오케스트레이션 도구로서 활용할 수 있다.

다양한 구성 방식

On-Premises 또는 Cloud-managed의 운영방식을 지원하여 자체적인 운영조직이 있거나 없는 경우 모두에 적합한 솔루션을 제공한다. 아울러 지정된 하드웨어를 통해서만 구동이 가능한 Appliance 방식이 아닌 소프트웨어형 제품으로 사용자가 하드웨어를 선택할 수 있어 가상 머신이나 사내 유휴장비를 이용한 구축이 가능하다.

용도에 맞는 Edition

Genian ZTNA은 위에서 설명한 구축 단계에 맞게 3가지의 *Edition* 으로 구분되어 있다. Basic Edition은 ZTNA구축 초기단계에 필요한 가시성 제공을 주목적으로 한다. Basic Edition을 통해 기존 네트워크 구성의 변경 없이 빠르게 가시성을 확보할 수 있다. Professional Edition은 그 위에 802.1X, ARP 통제, SPAN제어와 같은 방식의 네트워크 접근제어 기능을 제공한다. Basic Edition을 통해 통제가 필요한 네트워크나 단말이 확인되면 Professional Edition으로 업그레이드하여 단말들을 제어할 수 있다. 마지막으로 Enterprise Edition은 대규모 기업에서 즉시적인 접근제어를 적용하기 어렵거나 다양한 기존 시스템과의 연동이 필요한 경우 고려될 수 있다.

CHAPTER

TWO

GENIAN ZTNA 구축

이 장에서는 Genian ZTNA를 설치하기 전에 알아야 할 기본 정보를 소개합니다.

2.1 구성 요소 이해

Genian ZTNA를 구축하려면 다양한 구성 요소가 필요합니다. 이 장에서는 각 구성 요소의 역할 및 설치에 대해 설명합니다.

2.1.1 정책 서버

정책서버는 ZTNA의 모든 데이터 및 설정을 저장하는 중앙 관리 시스템입니다. 다른 구성 요소들은 정책서버로부터 정책을 수신한 다음 수집된 정보를 정책서버로 전송합니다. 일반적으로 정책 서버는 조직의 데이터 센터에 상주하며 실제 서버 또는 가상 시스템에 설치 됩니다. 정책서버는 또한 클라우드 환경에 설치할 수 있습니다.

정책서버의 또 다른 역할은 관리자의 관리 웹 UI 콘솔을 제공하는 것입니다. 다른 구성 요소를 구성 및 관리 할 수 있습니다. 웹 기반 관리 콘솔을 통해 수집 된 정보를 보고 조직의 보안 정책을 수립 할 수 있습니다.

Note: 정책서버는 On-premise 또는 Cloud managed 두 가지 운영방식을 지원합니다.

2.1.2 네트워크센서

네트워크센서는 각 네트워크 세그먼트에 위치하며 네트워크를 모니터링하고 정보를 수집하여 정책 서버로 전송합니다.

네트워크센서는 일반 네트워크 액세스 포트에 연결되며 포트 미러링과 같은 특수 설정이 필요하지 않습니다. 그러나 하나의 물리적 센서로 여러 VLAN 정보를 수집 할 때는 802.1Q를 통해 트렁크 포트로 구성해야합니다.

네트워크센서는 ARP 또는 DHCP와 같은 브로드 캐스트 패킷을 모니터링하여 새로운 장치를 감지합니다. 또한 UPNP, NetBIOS 등 다양한 브로드 캐스트 패킷을 통해 플랫폼을 탐지하거나 장치 정보를 수집할 수 있습니다.

따라서 **네트워크센서는 모든 브로드 캐스트 도메인** 에 연결 되어야합니다. WAN에 연결된 원격 사이트가 있는 경우, 각 네트워크 마다 별도의 네트워크센서가 필요합니다.

무선 센서

무선 센서는 무선 LAN 네트워크 인터페이스를 통해 무선 신호를 모니터링하여 센서 주변의 SSID 및 무선 장치를 감지합니다. 이를 통해 WLAN과 관련 된 보안을 모니터링 할 수 있습니다. 무선 센서는 네트워크센서 시스템에 무선 LAN 인터페이스를 추가하여 작동시킬 수 있습니다. 그러나, 센서의 위치는 무선 네트워크의 특성으로 인해 검출 될 수 있는 영역에 크게 영향을 미치기 때문에, 네트워크센서와 별도의 하드웨어로 구성 될 수 있습니다.

무선 관련 기능을 사용하는지 여부에 따라 무선 센서를 사용할 수 있습니다.

네트워크 제어

네트워크 제어는 조직의 정책을 위반하는 장치에 대해 독립적인 네트워크 접근 제어 기능을 제공하는 구성 요소입니다. 이를 통해 기존 네트워크 인프라의 도움없이 장치 자체를 격리 할 수 있습니다.

각 네트워크 세그먼트에 설치된 네트워크센서에서 제어기능을 활성화 하면 ARP Layer 2 기반 제어가 제공됩니다. 추가 하드웨어 없이 네트워크센서로 네트워크 액세스 제어를 제공하는 가장 쉬운 방법입니다.

다른 제어 방법은 SPAN 포트 (미러링)를 사용하여 코어 스위치에 연결하여 권한이 없는 네트워크 액세스가 감지되면 세션을 종료 할 수 있습니다. 이를 위해서는 네트워크 트래픽의 양에 따라 처리 할 수있는 별도의 독립 하드웨어가 필요합니다.

2.1.3 에이전트

에이전트는 사용자의 데스크톱 시스템에 설치된 소프트웨어입니다. 주기적으로 운영체제, 하드웨어 및 소프트웨어 관련 정보를 수집하고 변경이 감지되면 이를 정책 서버로 전송합니다. 또한 데스크톱 구성 관리 기능을 제공하므로 조직의 보안 정책 설정에 따라 필요한 항목을 쉽게 관리 할 수 있습니다.

에이전트 설치는 선택적 요소이므로 에이전트 없이 ZTNA 시스템을 구성할 수 있습니다.

에이전트는 관리자의 설정에 따라 종료 방지 및 삭제 방지 와 같은 자체 보안 기능을 제공합니다.

2.1.4 Geni Update Server

Genian Data

Geni Update Server에서 CVE 정보, NODE 정보, OS 업데이트 정보, 플랫폼 정보 등의 업데이트가 가능합니다.

Genian Software

정책서버, 네트워크센서, 및 에이전트의 소프트웨어 업데이트는 관리 Web UI > 시스템 > 소프트웨어 메뉴에서 가능합니다.

Genians Cloud 구독 가입자의 경우 정책서버 소프트웨어는 자동으로 업데이트됩니다.

2.2 구축 고려 사항

2.2.1 Genian ZTNA를 통한 성공적인 ZeroTrustNetwork 구축

ZeroTrustNetwork를 구축하는 것은 네트워크 환경의 다양한 변화로 이어질 수 있습니다. 사용자의 가용성을 확보하기 위해 단계별 구축과정이 중요합니다. Genian ZTNA는 수많은 프로젝트 경험을 토대로 아래와 같은 구축 단계를 권장합니다.

1 단계 : 네트워크 자산에 대한 가시성 확보

네트워크 및 사용자 환경을 이해하는 것은 보안 정책을 설정하고 네트워크 접근 제어를 성공적으로 구축하는데 가장 중요한 요소입니다.

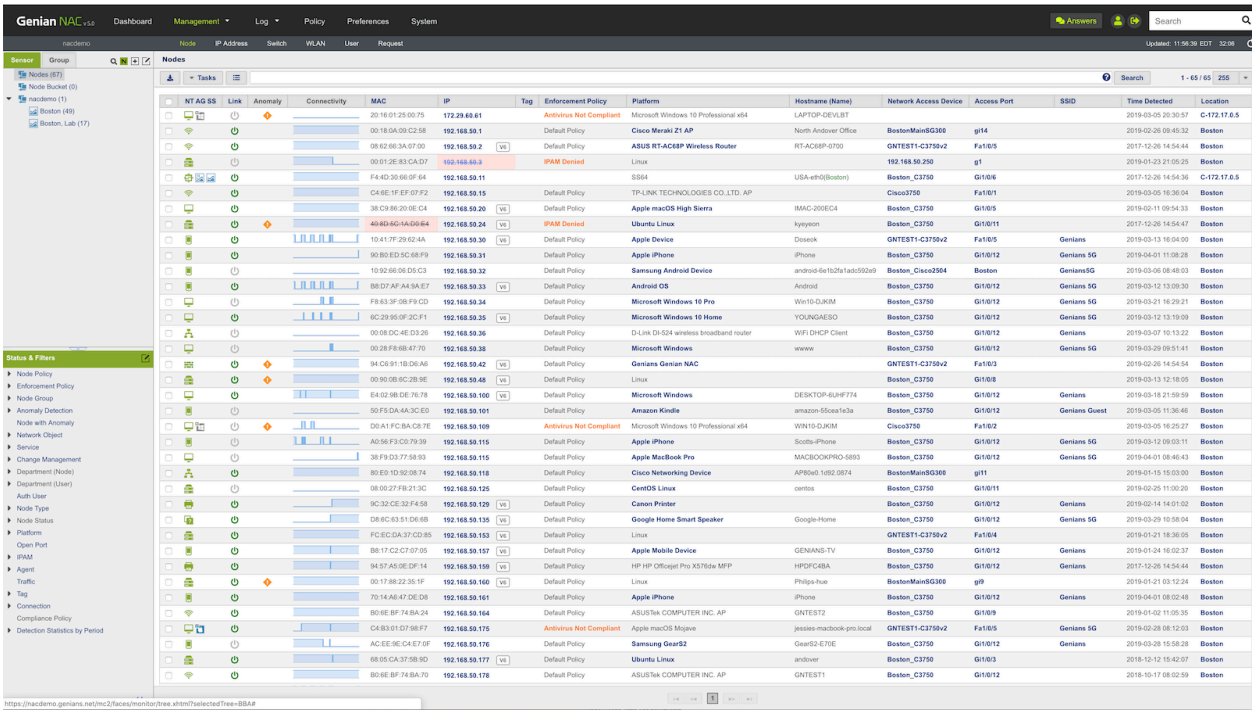
네트워크 및 사용자 단말에 대한 가시성을 가짐으로써 실시간으로 다음 정보를 모니터링 할 수 있습니다.

- 네트워크에 있는 단말의 유형과 수량을 정확하게 파악
- 네트워크를 구성하는 스위치 / 라우터와 같은 단말의 유형 / 수량 / 구성을 식별
- 사용자 단말의 운영 체제 / 하드웨어 / 소프트웨어 정보 확인
- 사무실의 무선 LAN 환경 이해

이러한 가시성을 확보하는 데는 여러 가지 방법이 있습니다. 많은 고객사로 부터 구현 복잡도가 높은 802.1x 액세스 제어 방법을 통해 가시성을 달성하지 못하였다고 전해 들었습니다. 802.1x는 가시성이 아닌 제어를 위해 설계된 기술이므로 제어를 하기 전 먼저 가시성을 확보해야합니다. 따라서 802.1x기술 만을 통해 점진적인 네트워크 액세스 제어환경을 구축하는 것은 매우 어렵습니다.

802.1x보다 가시성을 확보하는 방법으로 SNMP / CLI를 통한 스위치 단말 통합을 통한 정보수집이 있습니다. 이를 통하면 단말들을 제어하지 않고 가시성을 확보 할 수 있으므로 가시성을 쉽게 얻을 수 있습니다. 그러나 관리중인 스위치 제조업체, 모델, 관리되지 않는 스위치 장비들과의 호환성을 고려하여야합니다.

이러한 복잡성과 호환성 문제를 해결하기 위해 Genian은 별도의 독립적 **네트워크센서** 를 통해 가시성을 확보하는 방법을 제공합니다. 네트워크센서는 각 서브넷 (브로드 캐스트 도메인)에 연결되어 구성 될 수 있습니다. 기존 네트워크 환경이나 설정을 변경하지 않고 일반적으로 네트워크센서를 설치하여 전체 네트워크 가시성 확보 기간은 약 2 ~ 3 일 이내에 완료 됩니다.

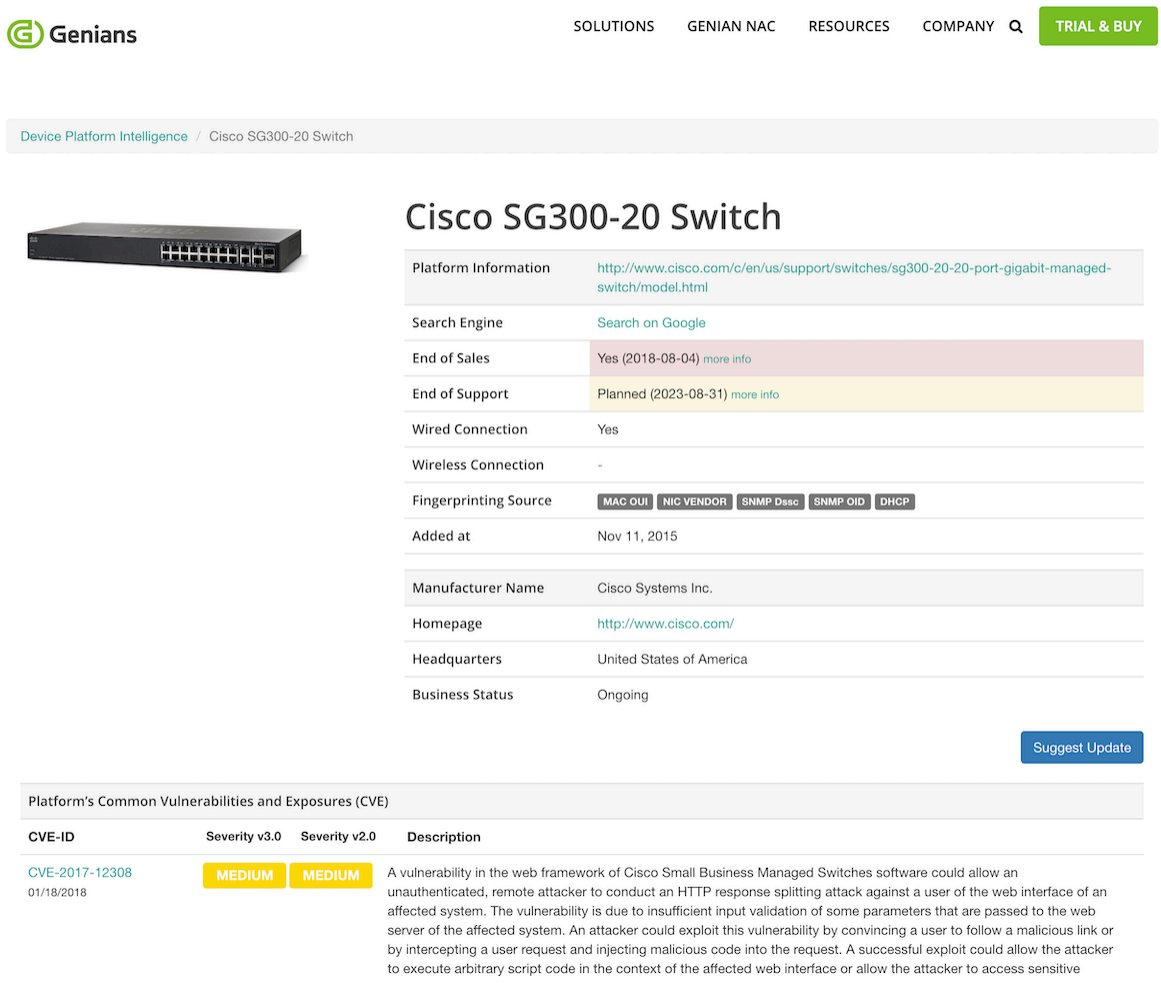


Genian ZTNA는 또한 Windows 및 MacOS 운영 체제에 대한 가시성을 높이기 위해 **Agent** 소프트웨어를 제공합니다. 사용자의 시스템에 설치되어 관리자가 원하는 정보 (운영 체제 / 하드웨어 / 소프트웨어 / 업데이트 등)를 수집하고 조회 할 수 있습니다.

2 단계 : 자산 분류 및 준수 확인

IT 자산의 가시성이 확립되면 다음 단계는 알려진 자산을 분류하는 것입니다. 자산을 IT 관리자 또는 사용자가 개인적으로 또는 공개적으로 사용되는지 여부와 같은 여러 가지 관점으로 분류하고 정렬해야합니다.

이를 위해 Genian ZTNA의 Device Platform Intelligence에서 제조 업체/제품 이름/모델 정보, 연결 방법 등 다양한 추가 정보를 제공합니다.



관리 분류 이외에도 보안 규정을 위반하는 단말를 분류하는 것은 매우 중요합니다. 일반적으로 다음 보안 조항을 고려 할 수 있습니다.

- 네트워크에 연결된 BYOD 단말 (개인 디바이스)
- 바이러스 백신 소프트웨어를 설치하지 않고 PC 사용
- Wi-Fi를 허용하지 않는 네트워크에서 iPad와 같은 무선 연결만 제공하는 단말 감지

Genian ZTNA는 단말과 조건이 일치하는지 여부를 실시간으로 확인하기 위해 500 가지 이상의 다양한 조건을 제공합니다.

3 단계 : IT 보안 정책 및 수정 수립

IT 보안 정책이 수립되면 이를 위반하는 단말를 제어해야합니다. 그러나 식별된 모든 위반 단말를 한 번에 제어하는 것은 쉽지 않습니다. 이를 위해서는 단계별 자동 접근이 필요합니다.

IT 보안 정책이 수립되면 이를 위반하는 단말을 제어해야합니다. 그러나 식별된 모든 위반 단말을 한 번에 제어하는 것은 생각보다 어려운 일이며 단계별 대응이 필요합니다. 이를 위해 Genian ZTNA는 사용자 개입 없이 다양한 보안 설정 및 구성을 자동으로 처리할 수 있도록 액션 플러그인을 제공합니다. 더불어 CWP(Captive Web Portal)을 통해 사용자가 수행해야 할 작업을 안내합니다.

제어 작업에 대한 자세한 내용은 다음을 참조하십시오. 엔드포인트 제어

4 단계 : 네트워크 액세스 제어 적용 및 비준수 장비 차단

위 단계를 통해 인증되지 않은 단말들을 제거하고 사용자 단말에 필요한 보안 조치를 완료한 후, 나머지는 보안 규정 준수 여부를 지속적으로 모니터링하고, 규정을 위반하는 단말을 더 이상 네트워크를 사용하지 않도록 제어할 수 있습니다. 이 단계에서 네트워크 환경 및 필요한 보안 수준에 따라 다양한 제어 방법을 선택할 수 있습니다. Genian ZTNA는 이를 위해 다양한 제어 기능을 제공합니다.

- 802.1x
- 레이어 2 (ARP, DHCP)
- SNMP / CLI (포트 종료)
- 포트 미러 (SPAN)
- 타 솔루션과의 연동 (방화벽, VPN 등)
- 에이전트

각 제어 방법에 대한 자세한 내용은 다음을 참조합니다. 제어 방법

2.2.2 기술적 고려 사항

Topic	Layer 2 Sensor/Enforcer	SNMP/CLI	Port Mirror (SPAN)	802.1x	Agent
Access Control at Layer 2	Yes	Yes	No	Yes	No
Access Control at Layer 3	RBAC	Switch Port ACL	RBAC	Switch Port ACL	OS Firewall
Post-admission Control	ARP, DHCP	VLAN/ACL/Shutdown	TCP RST, ICMP unreach.	CoA*	OS Firewall
Additional Hardware	Network Sensor	Managed Switches	Full traffic capable Device, Tap Device, SSL Decryption Device	802.1x Switch/AP	No
Endpoint Dependency	No	No	No	802.1x Supplicant	Agent required
WLAN Security	Monitoring (WNIC on Sensor)	Monitoring (SNMP with Controller)	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

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

2.2.3 관리 고려 사항

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

2.2.4 정책서버 모델

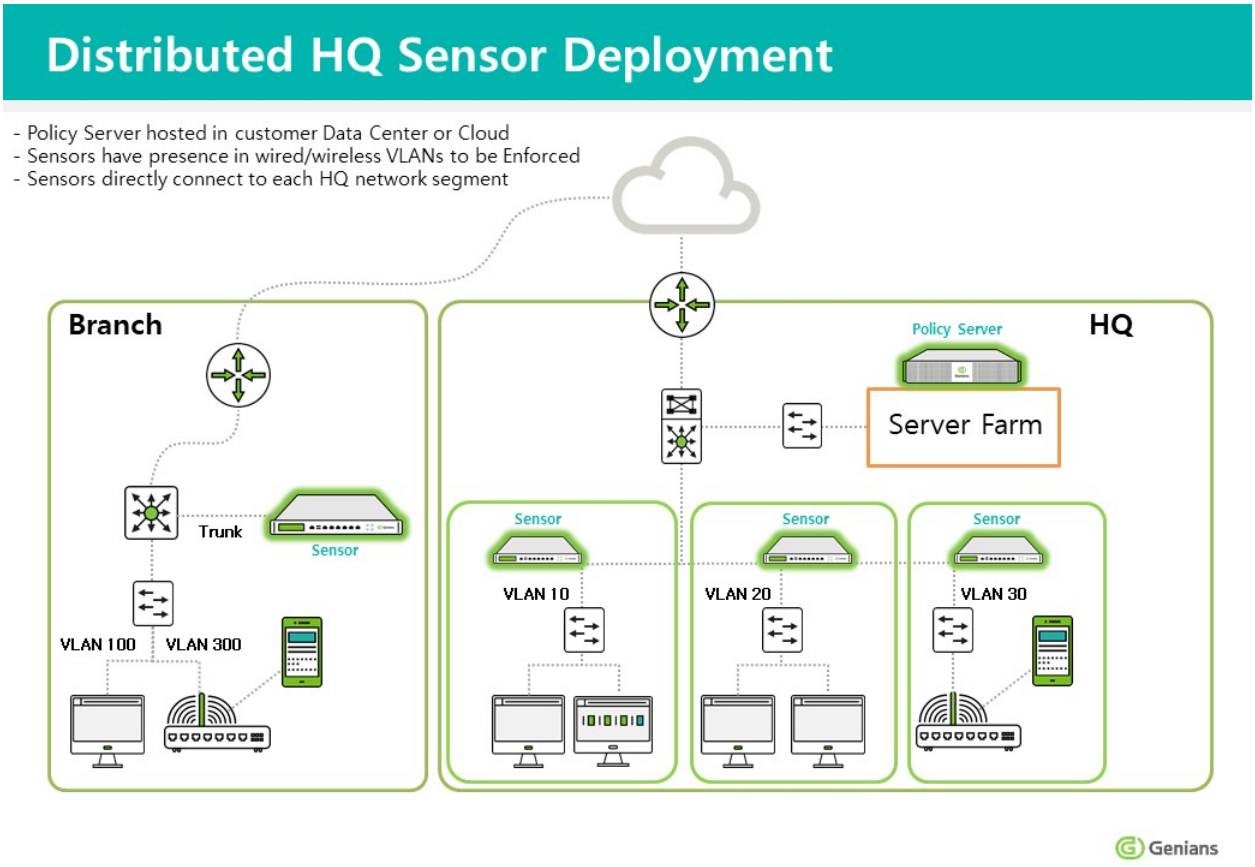
On-Premises

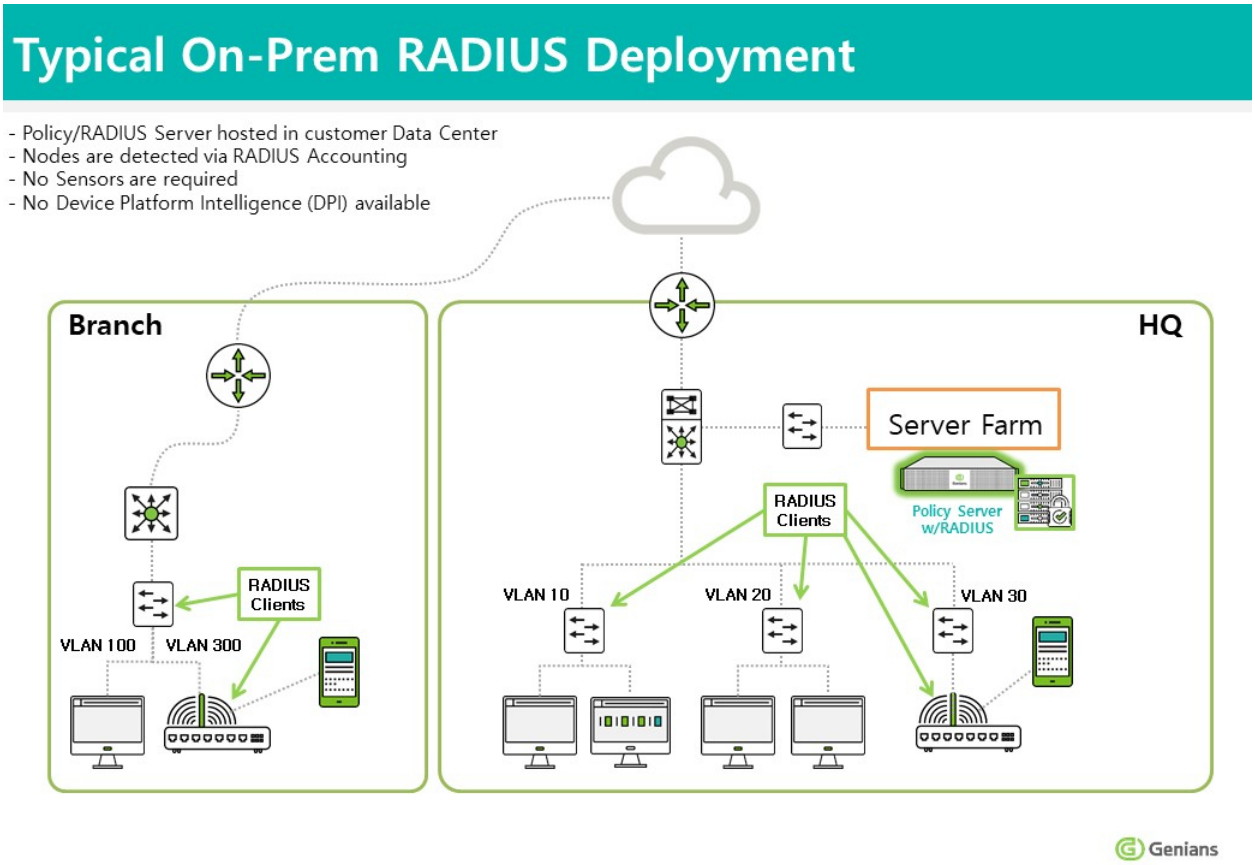
정책서버 및 **네트워크센서** 는 아래와 같이 구성하여 구축 할 수 있습니다.

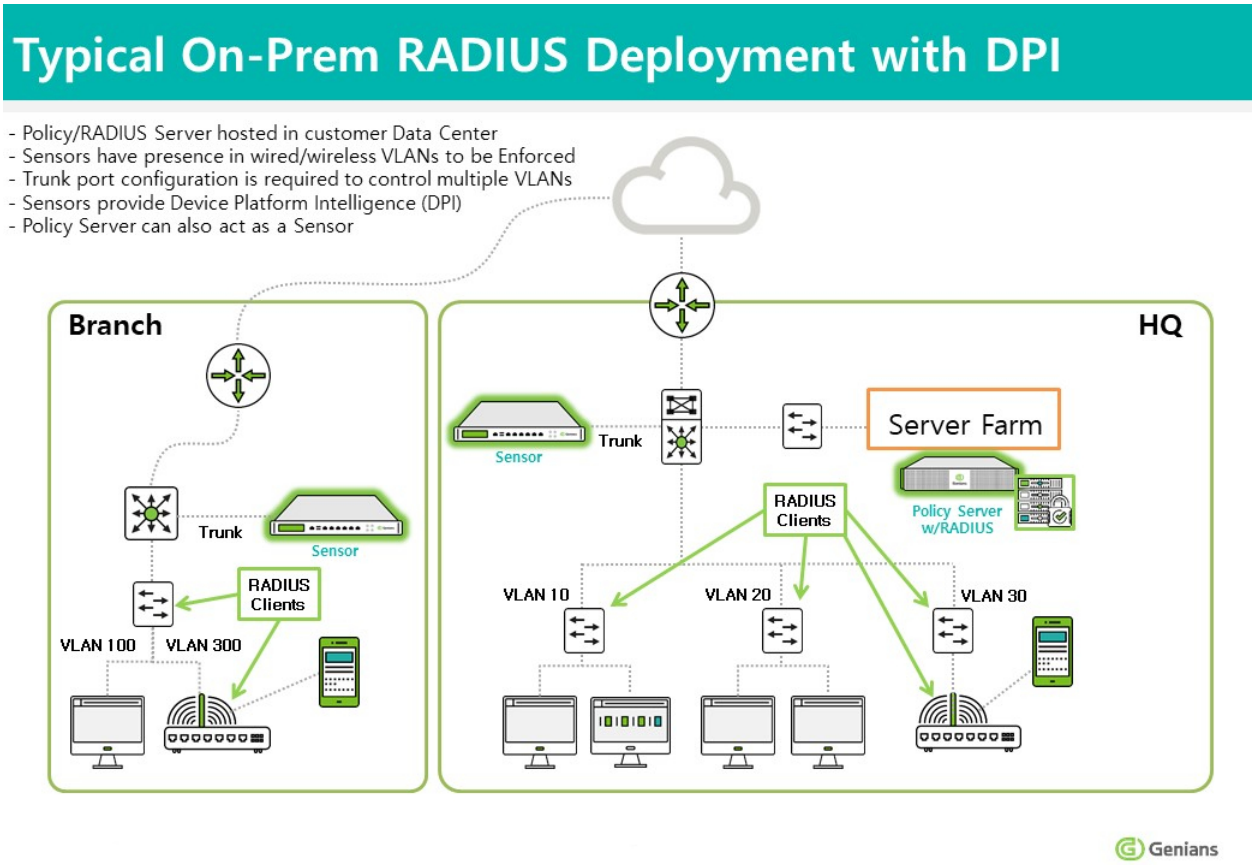
스위치 포트는 표준 엑세스 포트이거나 최대 128(권장 64개) 개의 VLAN에 대한 트렁킹 포트가 될 수 있습니다. 하나의 네트워크센서에 128 개 이상의 VLAN이있는 경우 두 번째 네트워크센서가 필요합니다. (동일한 네트워크에 두 개의 네트워크센서가 있거나 *802.1q* 환경에서 중복되는 네트워크가있는 경우에 중복된 노드를 갖는 것은 문제가 되지 않으며, 단지 주의해야 할 사항일 뿐입니다.)

다른 구축 유형

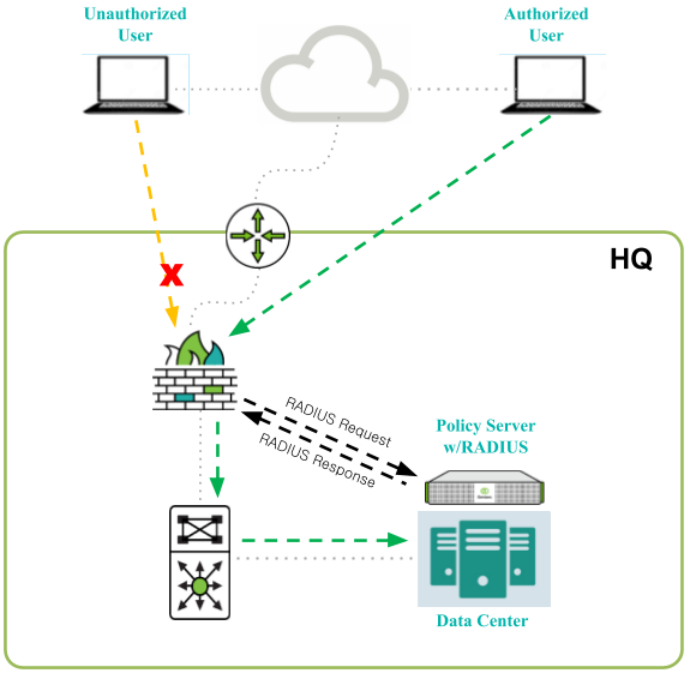
On-Premise




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
Policy Server w/RADIUS
RADIUS Clients
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



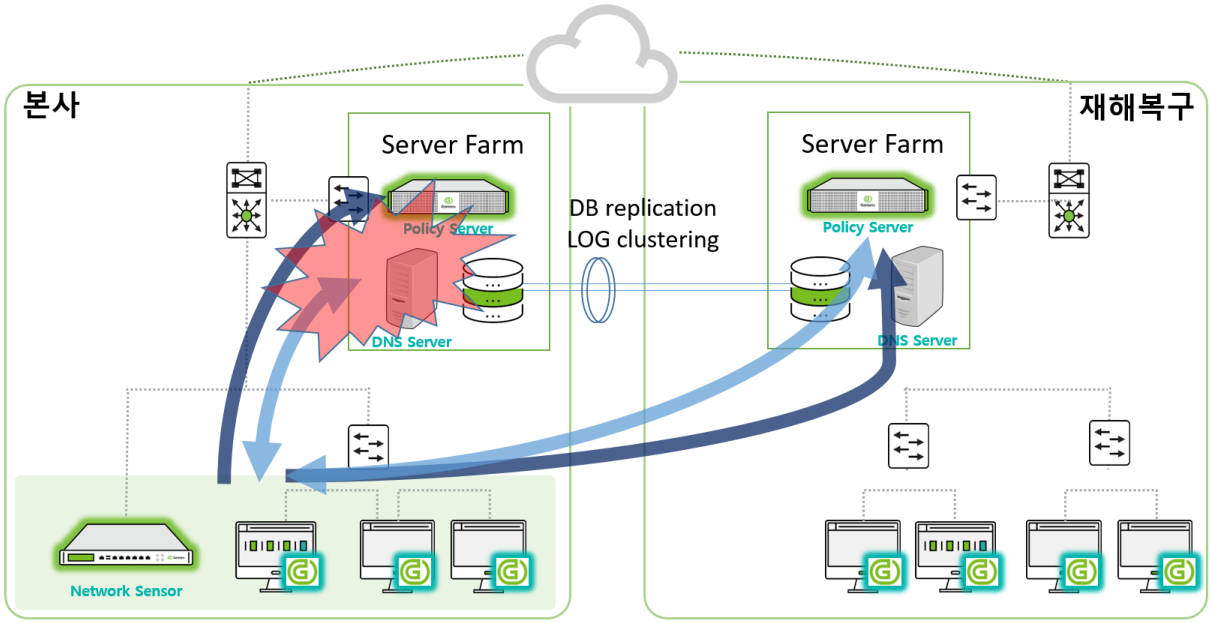
Highlights:
No Agent Required
AD/Local User Accounts
No RADIUS CoA Required

RADIUS Enforcement

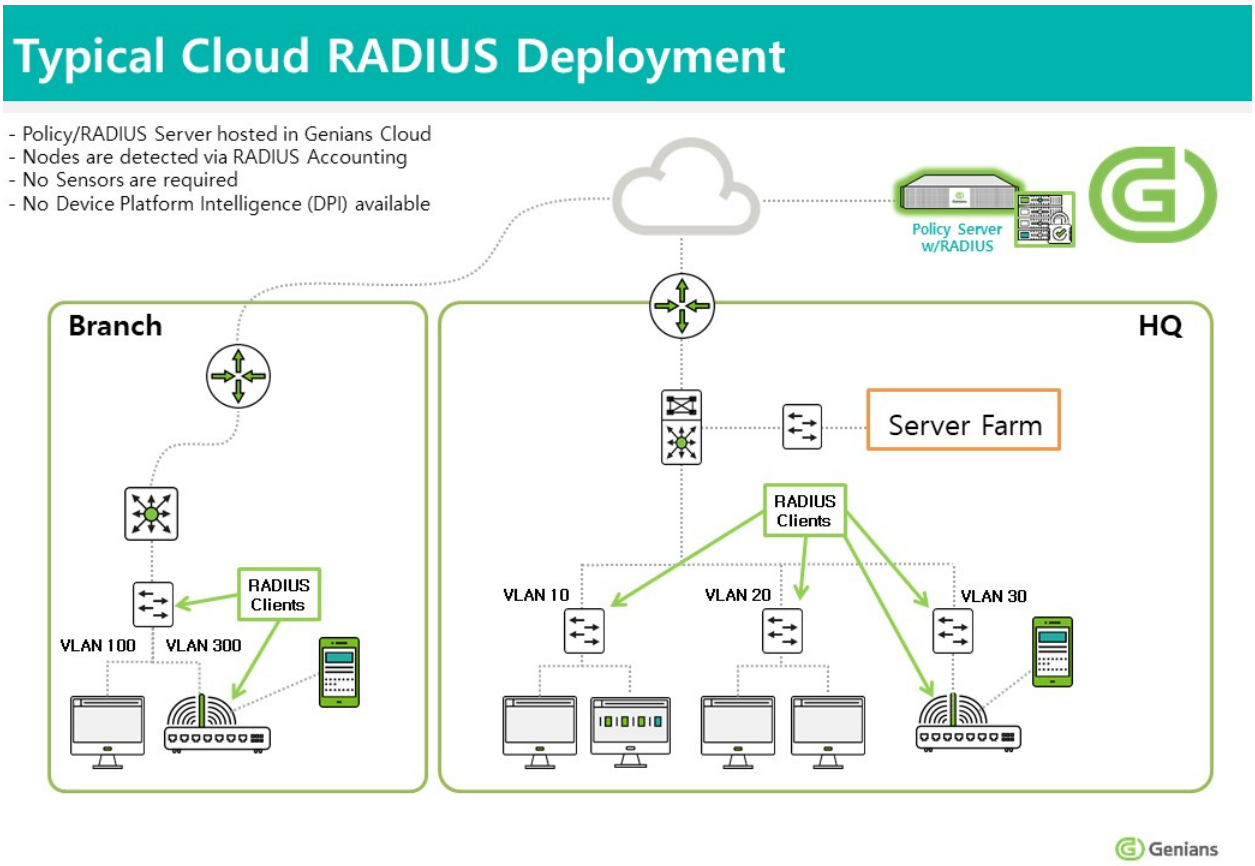
- VPN Firewall/Server Sends Request to Genians
- Genians Responds with Access-Reject Message
- User Unable to Establish VPN Connection

Genians

일반적인 NAC 재해복구 구축

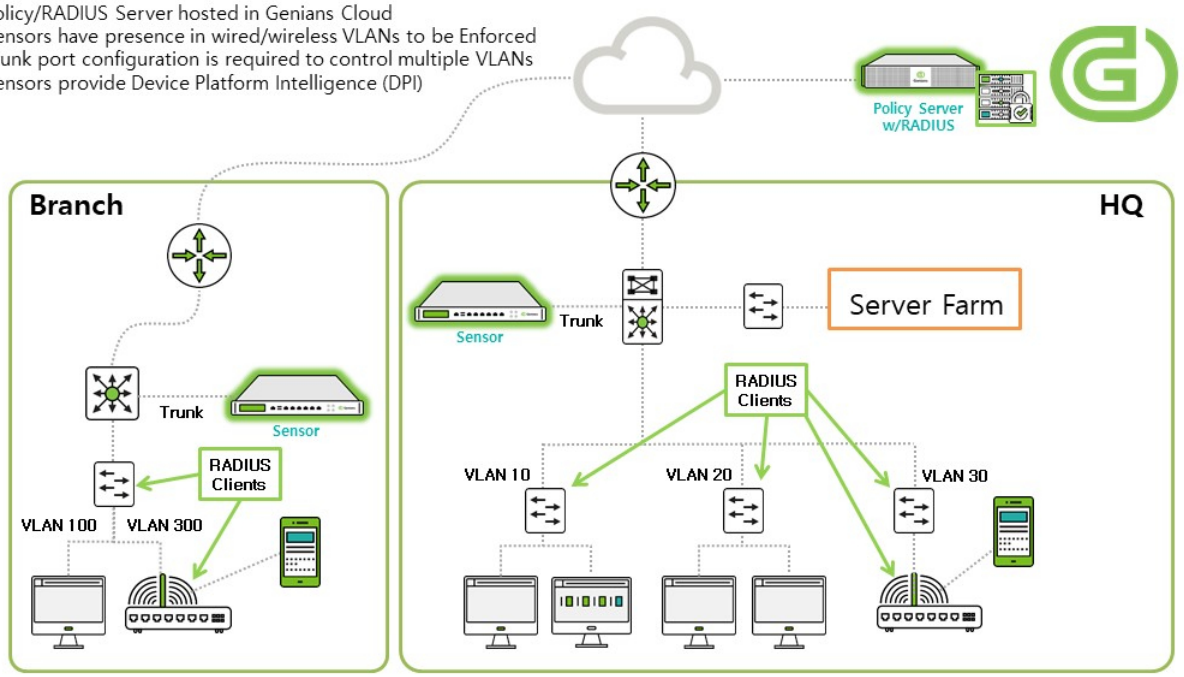


Cloud


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

Typical Cloud RADIUS Deployment with DPI

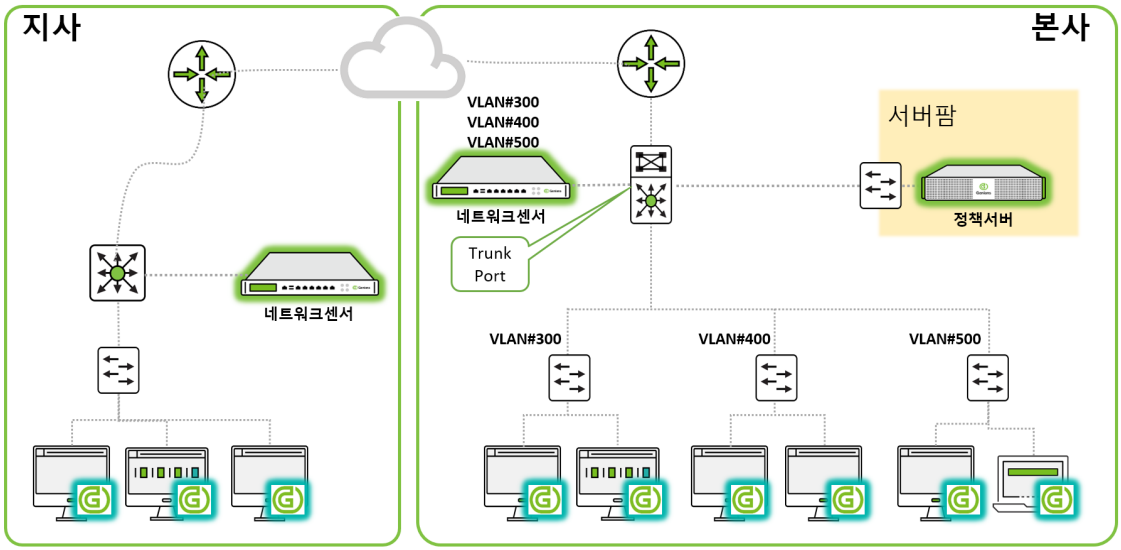
- Policy/RADIUS Server hosted in Genians Cloud
- Sensors have presence in wired/wireless VLANs to be Enforced
- Trunk port configuration is required to control multiple VLANs
- Sensors provide Device Platform Intelligence (DPI)



Genians

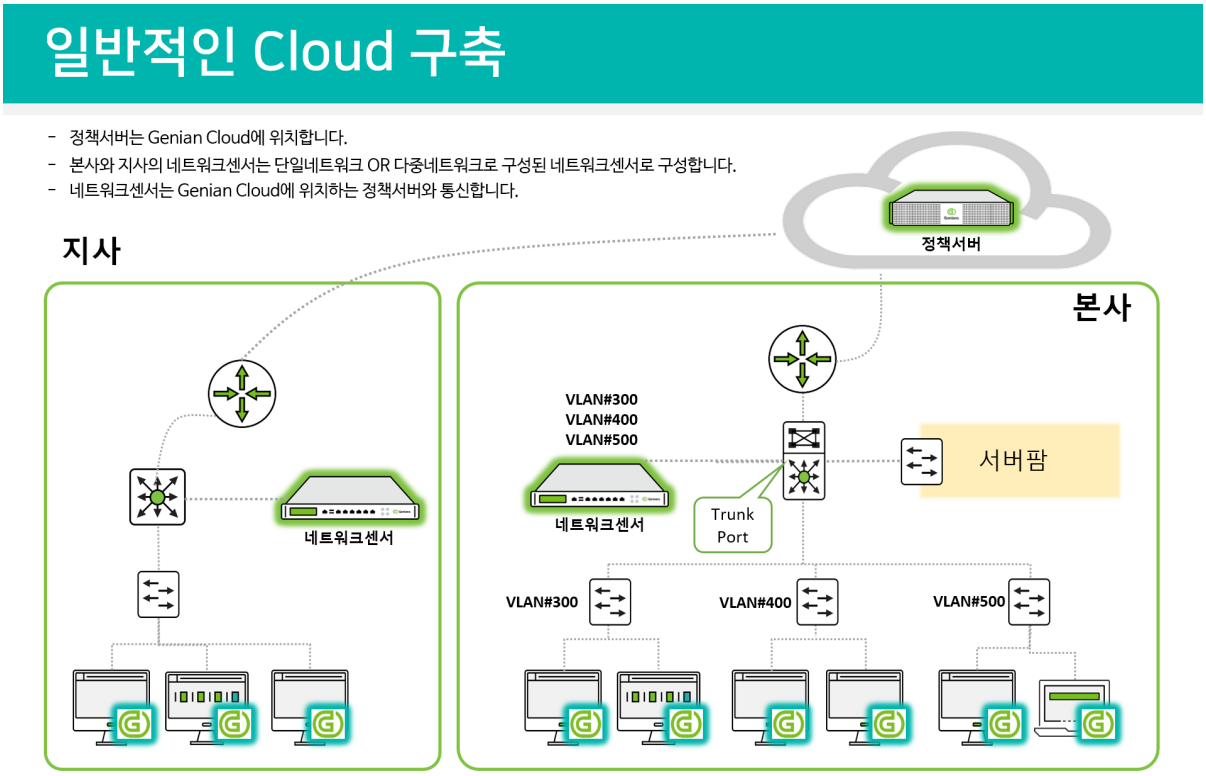
일반적인 On-Premise 구축

- 정책서버는 고객사 내부에 위치합니다.
- 본사센서는 여러 개의 VLAN을 사용하는 네트워크 센서로 설치됩니다.



CLOUD

정책서버 는 클라우드에 설치가 되며 **네트워크센서** 는 원격 사이트 위치의 Edge Switch에 연결하여 설치 할 수 있습니다. Edge Switch 포트는 엑세스 포트이거나 최대 128 개의 VLAN을위한 트렁킹 포트 일 수 있습니다. 네트워크센서에 128 개 이상의 VLAN이있는 경우 두 번째 **네트워크센서** 가 필요합니다.



2.3 에디션 비교

Genian ZTNA는 Basic, Professional 및 Enterprise 등 세 가지 에디션으로 제공됩니다.

각 에디션의 기능 범위는 다음과 같습니다.

Basic

네트워크 및 IT 자산에 대한 **모니터링** 을 제공합니다.

Professional

IT 보안 정책에 따라 네트워크 **접근 제어** 를 제공합니다.

Enterprise

Active Directory 연동, Desktop management, API 연동 등 다양한 **IT 자동화 플랫폼** 을 제공합니다.

제품을 에디션별로 구축할 수 있으므로 비용이 절약되고 기능에 따라 제품을 선택하기가 더 쉽습니다. 아래의 각 에디션에 대한 기능 비교표를 참고하여 적절한 에디션을 선택하십시오.

카테고리	특징	Basic	Profes-sional	Enter-prise
가시성	IP 활성화 단말 감지 / 모니터링	Yes	Yes	Yes
	단말 플랫폼 인텔리전스 (이름, 유형, 사진, End Of Life, 연결, CVE)	Yes	Yes	Yes
	스위치 포트 정보	Yes	Yes	Yes
	무선랜 모니터링 / 보안 (악성 / 잘못된 AP)	Yes	Yes	Yes
	Windows / macOS Agent에 의한 기본 엔드 포인트 정보 (OS, HW, 소프트웨어)	Yes	Yes	Yes
	조건 기반 동적 노드 그룹	Yes	Yes	Yes
	구성 가능한 대시 보드	Yes	Yes	Yes
	변경 사항 추적 / 감사 기록 추적	Yes	Yes	Yes
	네트워크 이상 탐지 (MAC Spoofing, Rogue Gateway, Ad-hoc)	Yes	Yes	Yes
	기본 보고서 (노드, 무선랜, 로그)	Yes	Yes	Yes
	맞춤 보고서		Yes	Yes
사용자 인증	Captive Portal 로그인		Yes	Yes
	Active Directory SSO		Agent Based	Agent-less
	외부 사용자 디렉토리 통합 (LDAP / RADIUS / SMTP / POP3 / IMAP)			Yes
	다중 인증		Admin Only	Yes
네트워크 액세스 제어	역할 기반 액세스 제어		Yes	Yes
	ARP 기반 Layer 2 Control		Yes	Yes
	802.1x 기반 제어 (RADIUS 서버, VLAN 할당, CoA)		Yes	Yes
	포트 미러링 (SPAN) 기반 제어		Yes	Yes
	스위치 통합 (SNMP) 기반 제어		Yes	Yes
	DHCP 서버		Yes	Yes
클라우드 보안*	클라우드 워크로드 가시성			Yes
	CLI 인터페이스를 통한 클라우드 제어 자동화			Yes
	클라우드 보안그룹 (Security Group) 관리			Yes
재택 근무*	ZTNA Client (SSL-VPN)			Yes
	FIDO (생체) 인증 for MFA			Yes
	Always on ZTNA			Yes
제로 트러스트 네트워크 접근 (ZTNA)*	역할기반 권한정책			Yes
	권한 객체에서 동적 목적지그룹 (노드그룹) 지원			Yes
	Security Service Edge (SSE) 를 제공하는 클라우드 ZTNA 게이트웨이 - AWS, Azure, GCP			Yes
	안전한 지점 접속을 위한 터널링 (IPSec/GRE)			Yes
	트래픽 가시성 (netflow)			Yes
	URL 및 어플리케이션 필터링			Yes
	IP Mobility (VxLAN, Always on ZTNA)			Yes
데스크탑 관리	보안규제준수 검사 (안티 바이러스, OS 업데이트, 필수 SW, OS 설정)		Yes	Yes
	OS 구성 관리 (화면 잠금, 인터넷 옵션, DNS)			Yes
	Windows Update 관리 (오프라인 업데이트, 캐시 업데이트, 승인)			Yes
	외부 장치 제어 (USB 등)			Yes

continues on next page

Table 1 – continued from previous page

카테고리	특징	Basic	Profes-sional	Enter-prise
	802.1x 연결 관리자			Yes
	무선랜 제어 (SSID 화이트리스트, SoftAP 블록)			Yes
통합	사용자 디렉토리 동기화 (RDBMS, LDAP)			Yes
	Webhook / Syslog / SNMP 트랩 (아웃 바운드)			Yes
	REST API (인바운드)			Yes
	Syslog Listener (인바운드)			Yes
비즈니스 프로세스	요청 / 승인 (IP, 장치, 사용자, 외부 장치)			Yes
	역할 기반 관리자			Yes
	사용자 정의 필드 (노드, 장치, 사용자)			Yes
	목적을위한 포털 포털 페이지			Yes
	다국어 지원			Yes
확장성 및 가용성	고 가용성 (정책 서버 / 네트워크센서)			Yes
	인터페이스 채널 본딩			Yes
	장애 복구 (DB 동기화, 정책 서버 이중화)			Yes

- Genian ZTNA 6.0 추가기능

2.4 네트워크 준비

네트워크에 ZTNA 구축을 계획할 때 몇 가지 고려 사항이 있습니다.

- 장비를 어디에 두어야 하나요?
- 스위치에 어떻게 연결 하나요?
- 몇 개의 장비가 필요한가요?
- Genian ZTNA가 통신하려면 어떤 포트를 열어야 하나요?

2.4.1 유선 연결

정책서버는 Core Switch 포트에 액세스 포트로 직접 연결 되어야합니다. 네트워크센서는 액세스 포트 또는 트렁크 포트가 될 수 있는 Edge 스위치 포트에 연결 되어야합니다.

Switches

네트워크센서는 브로드 캐스트 패킷을 볼 수 있어야하므로 관리되는 모든 서브넷에 연결해야합니다.

VLANs

단일 포트를 통해 여러 VLAN (최대 128 개, 권장 64개)을 모니터링 하려면 스위치 포트가 802.1Q 트렁크로 구성되어 있고 모니터링하려는 모든 VLAN이 해당 포트에서 허용되는지 확인합니다.

스위치 제조사 마다 Trunk 설정을 구성하는 방법이 다릅니다.

다음은 Cisco 스위치의 VLAN 10,20,30 및 40에 대한 802.1Q 트렁크 포트를 구성하는 예입니다.

```
Switch> enable
Switch# configure terminal
Switch(config)# interface fa0/1
Switch(config-if)# switchport trunk encapsulation dot1q
```

(continues on next page)

(continued from previous page)

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30,40
```

SNMP

- Genian은 SNMP 버전 1, 2c 및 3를 지원합니다.
- 읽기 전용 커뮤니티 문자열은 노드가 SNMP를 지원하는지 확인하는데 사용됩니다.
- 네트워크센서가 노드정보를 수집하는 과정 중 노드가 SNMP 요청에 응답하면 센서는 SNMP 쿼리를 통해 BRIDGE-MIB를 지원하는지 확인함으로써 노드가 스위치인지 확인합니다.
- 읽기, 쓰기 커뮤니티 문자열은 스위치 포트 설명 및 셧다운 등 스위치를 변경하는데 사용됩니다.
- SNMP를 이용하여 무선 컨트롤러의 정보를 수집하는 등 다양한 부가 기능에 사용할 수 있으며, 장치의 플랫폼 정보를 탐지합니다.

Note: 동일한 네트워크 세그먼트에 있는 모든 스위치의 액세스 목록에 네트워크센서를 추가하고 모든 OID를 보기 위해 사용자 / 그룹에 필요한 권한을 할당합니다. 자세한 정보는 다음을 참고 스위치 찾아보기

원격지

원격지에 관리해야할 또 다른 네트워크가 있는경우 해당 위치에 별도의 네트워크센서가 필요합니다.

2.4.2 무선 연결

무선 NIC를 포함한 네트워크센서는 주변의 모든 무선 패킷을 감지하고 SSID를 식별합니다. 센서는 대상의 무선 신호를 탐지할 수 있는 물리적으로 인접한 위치에 설치해야 하며, 무선 NIC의 신호가 닿는 중심에 배치하면 대부분의 SSID를 탐지 할 수 있습니다.

2.4.3 방화벽 요구 사항

Genian ZTNA가 제대로 동작하려면 아래의 포트들이 방화벽으로부터 개방되어야합니다.

[On-Premises]

SRC IP	DST IP	Service	Note
정책서버 IP	52.78.17.154 (geniup-date.geninetworks.com)	TCP/80, TCP/443	**GENIAN Data** Update
네트워크센서 IP	정책서버 IP/FQDN	UDP/3870, UDP/3871 TCP/80, TCP/443 UDP/514, TCP/6514	Keep Alive Update Information/Policy Syslog
PC IP (에이전트)	정책서버 IP/FQDN	UDP/3870, UDP/3871 TCP/80, TCP/443, TCP/8000	Keep Alive Update Information/Policy Windows Update
Management PC	정책서버 IP, 네트워크센서 IP	TCP/3910 TCP/8443	SSH Web Console

[Cloud managed]

SRC IP	DST IP	Service	Note
정책서버 IP	52.78.17.154 (geniup-date.geninetworks.com)	TCP/80, TCP/443	**GENIAN Data** Update
네트워크센서 IP	정책서버 IP/FQDN	UDP/Random TCP/80, TCP/443 UDP/Random, TCP/Random	Keep Alive Update Information/Policy Syslog
PC IP (에이전트)	정책서버 IP/FQDN	UDP/Random TCP/80, TCP/443, TCP/Random, TCP/Random	Keep Alive Update Information/Policy Windows Update

Note: 운영정보 데이터를 다운로드 하기 위해서는 정책서버가 외부 통신이 가능해야 합니다.

Note: Cloud managed의 경우 정책서버가 Cloud 환경에 존재하므로 목적지 port가 랜덤으로 설정됩니다.

CHAPTER

THREE

GENIAN ZTNA 설치

이 장에서는 Genian ZTNA를 시스템에 설치하고 관리자 웹 및 CLI 콘솔에 액세스하는 과정을 안내합니다.

3.1 Ubuntu OS 설치

ZTNA를 설치하기 위해서는 사전에 **Ubuntu OS (20.04.4 LTS)** 설치가 필요합니다.

3.1.1 하드웨어 준비

물리적 시스템 또는 가상 시스템에 정책서버를 설치할 수 있습니다.

시스템 할당 자원(최소 요구사항)

ZTNA Policy Server

- CPU : Intel(R) Celeron(R) CPU G3900 @ 2.80 GHz 이상
- 메모리 : 8GB 이상
- 디스크 : 120GB 이상 권장

ZTNA Network Sensor

- CPU : Intel(R) Celeron(R) CPU J1800 @ 2.41 GHz 이상
- 메모리 : 8GB 이상
- 디스크 : 64GB 이상 권장

가상머신

가상 시스템에 정책서버를 설치할 수 있습니다. Genian ZTNA는 VMWare, VirtualBox, XenServer와 같은 다양한 하이퍼 바이저를 지원합니다.

3.1.2 사전준비

1. 이미지 파일 준비

- **Ubuntu 20.04.4 LTS 이미지 파일은** 우분투 공식 홈페이지 **에서 다운로드 할 수 있습니다.**
  - Ubuntu Desktop과 Ubuntu Server 모두 사용 가능 합니다.

2. H/W에 설치하는 경우, 부팅USB를 제작해주시기 바랍니다.

부팅 가능한 USB 드라이브 만들기

Genian ZTNA 정책 서버를 실제 장비에 설치하려면 먼저 UNETbootin 을 사용하여 USB 드라이브를 만듭니다.

UNETbootin 얻기

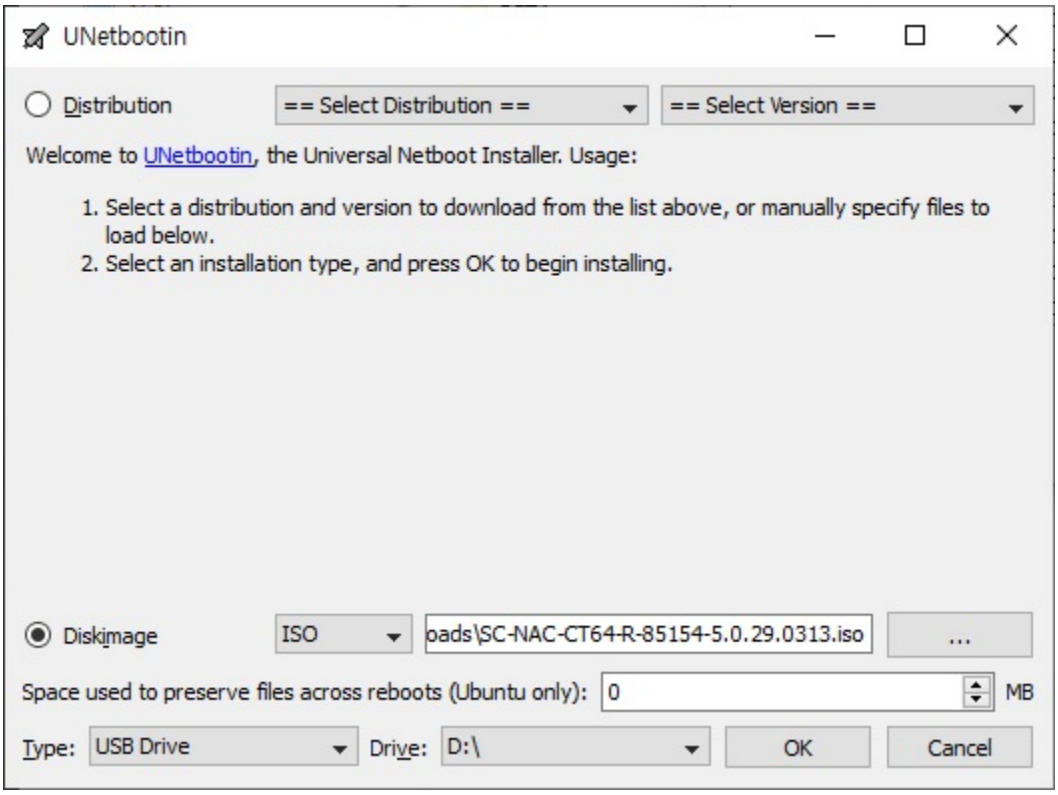
Genians 는 CD를 굽지 않고 Genian ZTNA 설치용 USB 플래시 드라이브를 만들 수있는 UNETbootin 을 권장합니다. UNETbootin을 다운로드하려면 운영 체제를 선택하십시오.

USB 드라이브 만들기

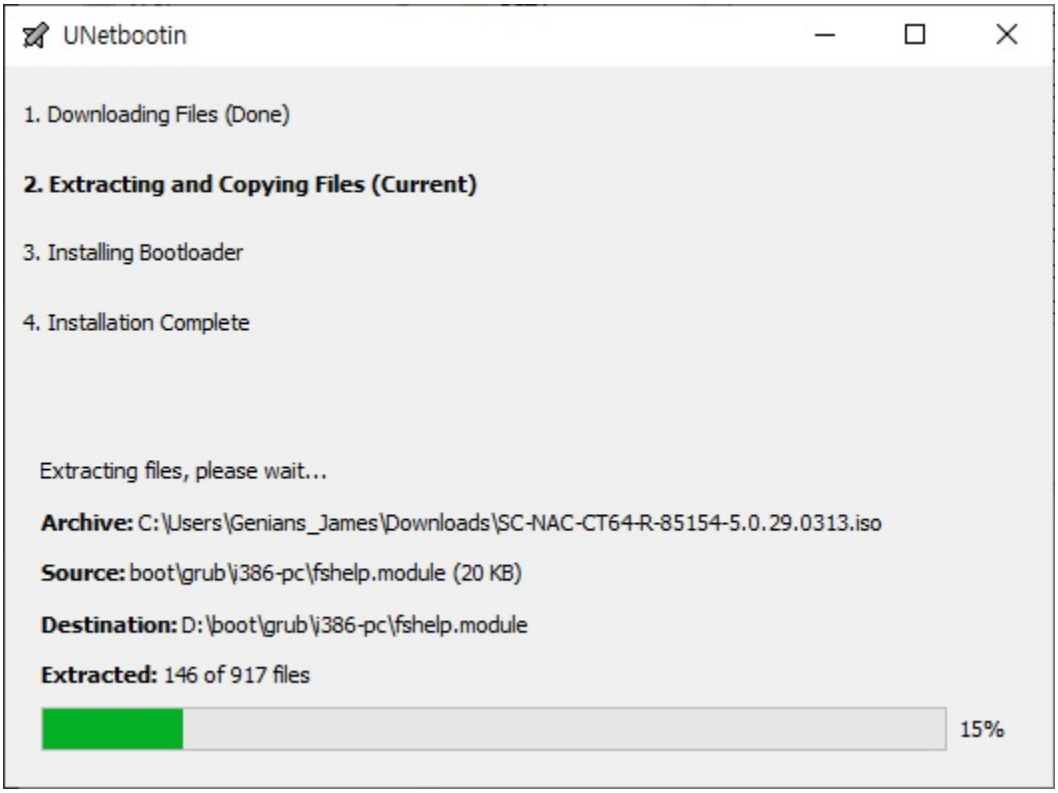
USB 드라이브가 포맷 된 FAT32인지 확인하십시오. 다른 파일 시스템은 지원되지 않을 수 있습니다.

UNETbootin 이 설치되면 다음 단계를 수행 하십시오.

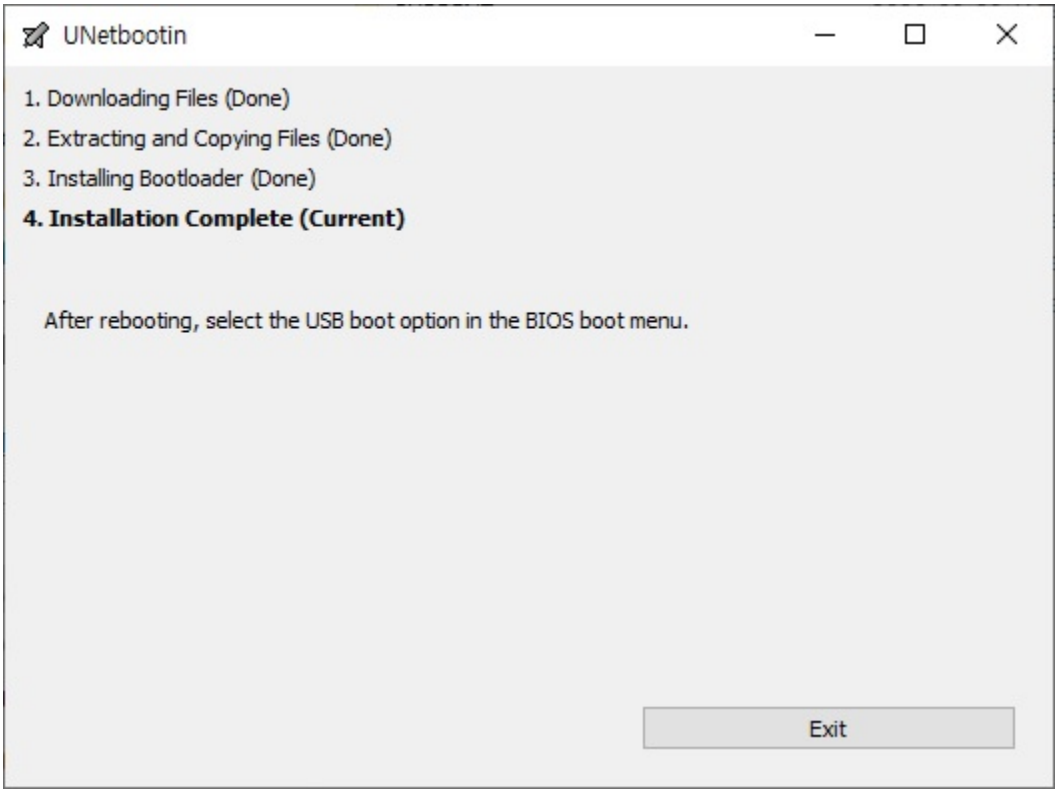
1. Diskimage 불러오기



2. 확인을 클릭하고 계속합니다.



3. 나가기를 클릭하십시오.



이제 Genian ZTNA 를 원하는 장비에 설치하기위한 USB 드라이브가 생성 되었습니다.

문제 해결 하기

- 오류 메시지: "BOOTMGR is missing" indicative of improperly formatted USB drive.(잘못 포맷 된 USB 드라이브를 나타내는 "BOOTMGR 이 없습니다".)

3. AWS 인스턴스에 설치하는 경우 , 인스턴스 생성 방법 을 참고하여 설치해 주시기 바랍니다.

3.1.3 Ubuntu OS 설치 - Ubuntu Desktop

Ubuntu 공식 홈페이지 이미지 파일을 이용하여 Ubuntu Desktop 설치를 진행할 수 있습니다.

Step 1: 장비 부팅

- **H/W 혹은 가상머신에 설치하기**
  - 부팅 USB를 통해 H/W 장비를 부팅 합니다.
  - 다운로드한 ISO파일을 가상머신에 업로드합니다.

Step 2: 최초 Ubuntu 설치

1. Ubuntu Desktop 설치 이미지가 있는 부팅 가능한 USB 드라이브로 부팅 합니다. 가상 머신일 경우 다운로드한 ISO 파일을 가상 머신에 업로드 한 후 가상머신을 실행 시킵니다.

2. 사용자 환경에 맞는 Ubuntu Desktop 언어 설정을 하고 **Install Ubuntu** 를 클릭합니다.

3. 키보드 레이아웃을 선택하고 **Continue** 버튼을 클릭합니다.

4. ZTNA 구축에 불필요한 프로그램 설치를 하지 않기 위하여 설치 옵션을 **Minimal Installation** 선택하고 **Continue** 버튼을 클릭합니다.

5. 설치 타입을 **Erase disk and install Ubuntu** 를 선택하고 **Install Now** 를 클릭합니다.
   - 설치 타입 **Something else** 를 선택시 운영체제의 파티션 · 파일 시스템을 직접 구성 할 수 있습니다.

6. 파티션 변경 사항을 확인하고 **Continue** 를 클릭합니다.

7. 타임존을 설정하고 **Continue** 를 클릭합니다.

8. Ubuntu OS 사용자 정보를 입력하고 **Continue** 를 클릭합니다. **Continue** 클릭 시 설치가 진행됩니다.

Note:

필드 명	설명
Your name	사용자 이름 입력
Your computer's name	장비 이름 입력
Pick a username	사용자가 Ubuntu에 로그인 시 사용할 계정(ID) 입력
Choose a password	사용자가 Ubuntu에 로그인 시 사용할 계정 비밀번호 입력
Confirm your password	사용자가 Ubuntu에 로그인 시 사용할 계정 비밀번호 재입력

---

9. 설치가 완료 되면 **Restart Now** 버튼을 클릭해 재부팅 합니다.

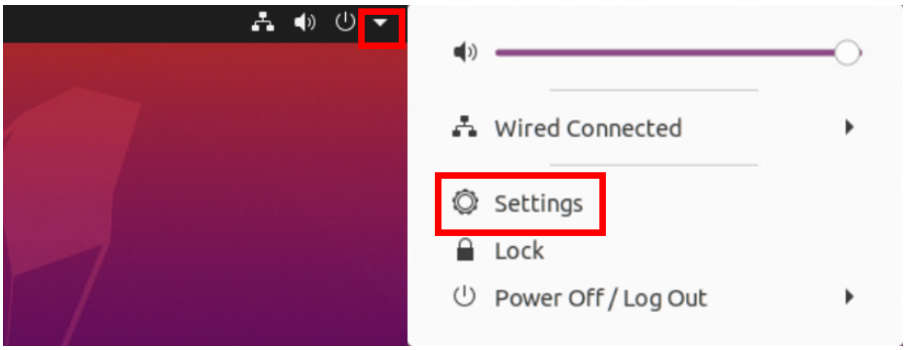
10. 부팅 가능한 USB를 제거하고 **Enter** 키를 입력합니다. 가상화 장비일 경우 바로 **Enter** 키를 입력하여 다음 과정으로 넘어 갑니다.

11. 사용자 계정을 클릭하고 8번 과정에서 입력 했던 사용자 정보로 로그인 합니다.

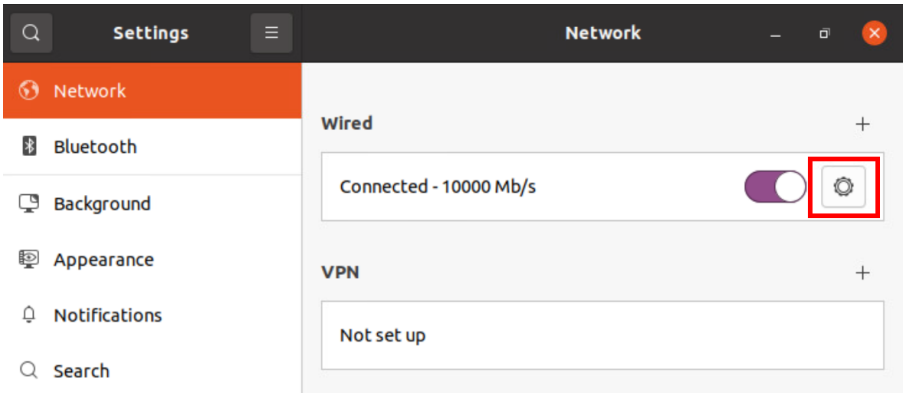
Ubuntu Desktop 네트워크 설정

- 고정 IP를 할당하여 장비를 운용하는 것을 권장 합니다. 동적 IP 사용시, 장비의 IP가 변경될때 마다 장비 configuration을 수정해야 합니다.
- On-premise 환경에서 Ubuntu Desktop의 고정 IP 설정 방법이 작성된 문서입니다.

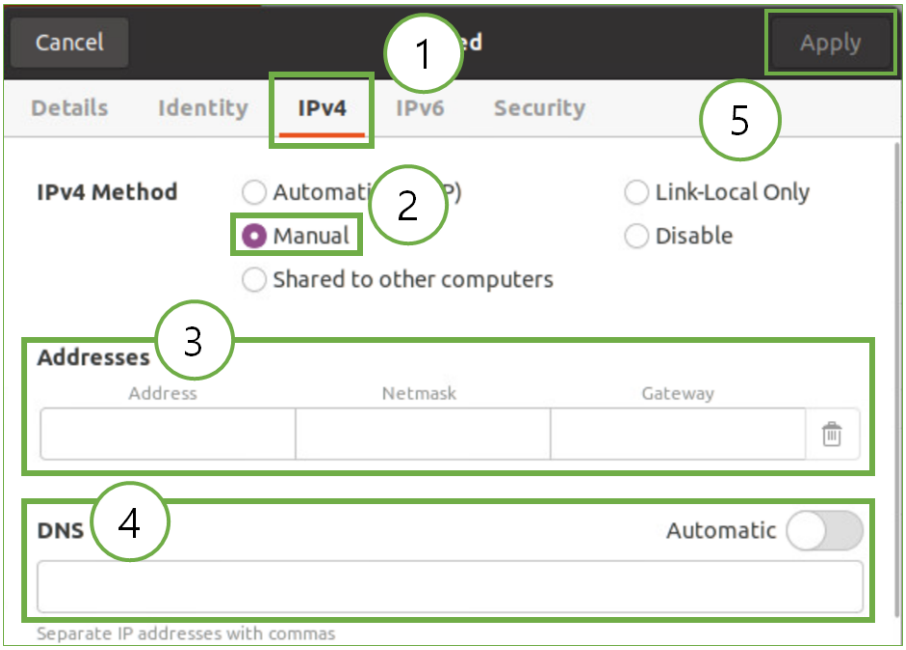
1. 바탕화면 우측 상단 ▼ => **Settings** 를 클릭합니다.



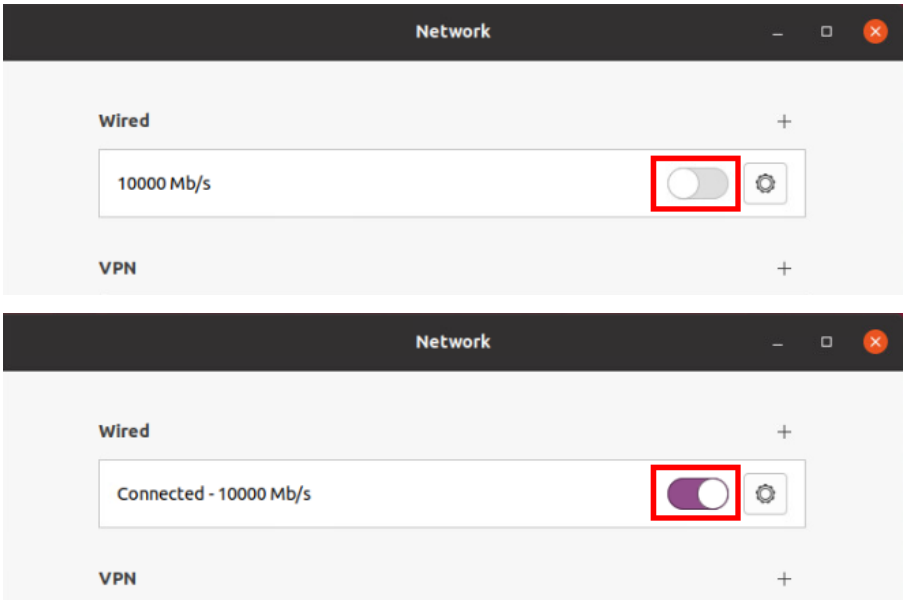
2. **Network => Wired** 안에 있는 톱니바퀴 아이콘을 클릭합니다.



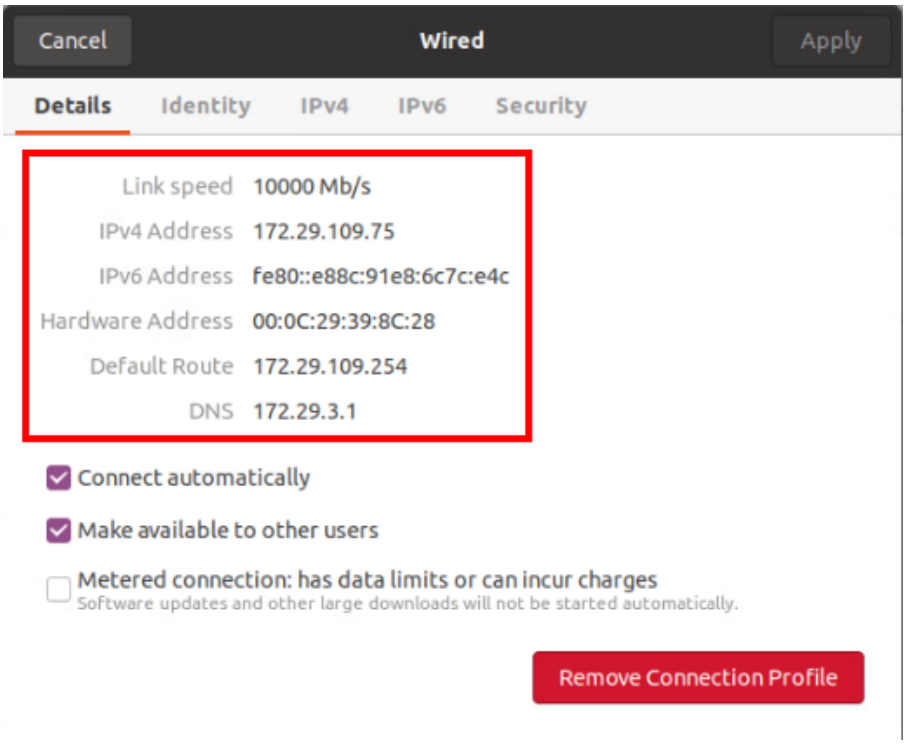
3. **IP Method => Manual** 선택 후 IP 설정을 진행 합니다.



4. 설정 완료 후 Wired 옵션을 비 활성화 한 다음, 다시 활성화 시킵니다.



5. Wired의 톱니바퀴 아이콘을 클릭해 IP 주소 입력이 제대로 적용 되었는지 확인합니다.



3.1.4 Ubuntu OS 설치 - Ubuntu Server

Ubuntu 공식 홈페이지 이미지 파일을 이용하여 Ubuntu Server 설치를 진행할 수 있습니다.

Step 1: 장비 부팅

- **H/W 혹은 가상머신에 설치하기**
  - 부팅 USB를 통해 H/W 장비를 부팅 합니다.
  - 다운로드한 ISO파일을 가상머신에 업로드합니다.

Step 2: 최초 Ubuntu 설치

1. Ubuntu Server 설치 이미지가 있는 부팅가능한 USB 드라이브로 부팅합니다. 가상 머신일 경우 다운로드한 ISO 파일을 가상 머신에 업로드 한 후 가상머신을 실행 시킵니다.

2. 사용자 환경에 맞는 언어를 선택합니다.

3. 키보드 레이아웃을 설정 합니다.

4. 네트워크 연결 설정을 위해 사용중인 네트워크 인터페이스를 선택합니다.

5. **Edit IPv4** 를 선택합니다.

6. **Automatic (DHCP)** 옵션을 **Manual** 로 바꾸어 선택합니다.

7. 하단의 표를 참고 하여 각 항목에 알맞은 값을 입력하고 **Save** 를 선택합니다.

Note:

항목(필수 입력)	내용
subent(필수 입력)	서브넷 마스크 입력
Adress(필수 입력)	해당 장비에서 사용할 IP 주소
Gateway(필수 입력)	게이트 웨이 주소
Name Server(필수 입력)	DNS 서버 주소
Search domains	공란

8. 네트워크 인터페이스 하단에 설정한 IP가 있는지 확인합니다.

9. Proxy Address를 입력하지 않고 **Done** 을 선택합니다.

10. 리눅스 업데이트 서버 설정 과정은 수정하지 않고 **Done** 을 선택합니다.

11. 리눅스 업데이트 진행 여부를 묻는 과정 입니다. **Continue without updating** 을 선택해 업데이트를 실시하지 않고 설치를 진행합니다.

- 리눅스 업데이트 진행 시, ZTNA 설치가 정상적으로 안 될 수 있습니다.

12. **Use an entire disk** 와 **Set up this disk as an LVM group** 를 체크하고 **Done** 을 선택합니다.

- 12번 과정 진행 중 **Custom storage layout** 을 선택하면 운영체제의 파티션 · 파일 시스템을 직접 구성할 수 있습니다.

13. 변경되는 파티션과 파일 시스템을 확인 하고 **Done** 을 선택합니다.

14. 파티션 변경 사항이 이상이 없을 경우 **Continue** 를 선택합니다.

15. Ubuntu OS 사용자 정보를 입력하고 **Done** 을 선택합니다.

Note:

필드 명	설명
Your name	사용자 이름 입력
Your computer's name	장비 이름 입력
Pick a username	사용자가 Ubuntu에 로그인 시 사용할 계정(ID) 입력
Choose a password	사용자가 Ubuntu에 로그인 시 사용할 계정 비밀번호 입력
Confirm your password	사용자가 Ubuntu에 로그인 시 사용할 계정 비밀번호 재입력

16. Ubuntu 개발 회사인 Canonical의 유료 기술 지원을 받기 위한 Token을 설정하는 과정은 값을 입력하지 않고 **Done** 을 선택합니다.

17. 운영을 위해 외부 Terminal 접속이 필요한 환경일 경우 **Install OpenSSH server** 를 체크 합니다. 필요하지 않은 경우 체크 하지 않고 **Done** 을 선택 합니다.

18. Ubuntu Server에서 추가 기능 설치 부분은 추가 하지 않고 **Done** 을 클릭합니다.

19. 좌측 상단에 **Install complete** 가 출력되면 **Reboot Now** 를 선택합니다.

20. 부팅 USB가 연결되어 있을 경우 제거하고 **Enter** 를 입력합니다.

21. 15번 과정에서 입력한 사용자 정보로 로그인을 진행합니다.

Ubuntu Server 네트워크 설정

- 고정 IP를 할당하여 장비를 운용하는 것을 권장 합니다. 동적 IP 사용시, 장비의 IP가 변경될때 마다 장비 설정을 수정해야 합니다.
- On-promise 환경에서 Ubuntu Server 고정IP 설정 방법이 작성된 문서입니다.

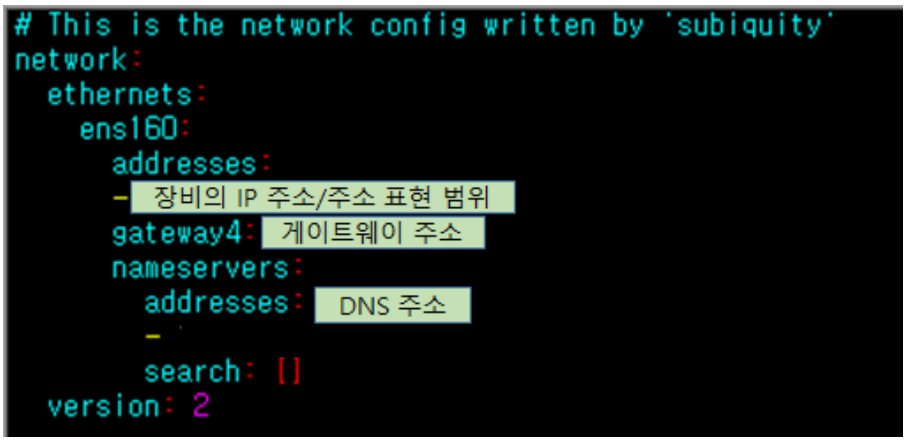
Note: Ubuntu Server 설치 과정에서 네트워크 설정을 하지 못했을 경우 해당 문서를 참조 하십시오.

---

1. root 계정으로 전환합니다.
2. 장비의 네트워크 인터 페이스를 확인합니다.
3. **/etc/netplan** 경로로 이동합니다.
4. 해당 경로에 존재하는 .yaml 파일을 편집기로 수정합니다.

```
$ sudo su # root 계정으로 전환
$ ifconfig # 장비의 네트워크 인터페이스 확인
$ cd /etc/netplan # yaml파일 설정을 위해 디렉토리 이동
$ vim 파일명.yaml # 파일 편집기를 통해 yaml파일 수정
```

5. 2번 과정에서 확인한 인터페이스가 .yaml파일에 있는지 확인합니다.
6. 고정 IP 설정을 진행합니다.




```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens160:
      addresses:
      - 장비의 IP 주소/주소 표현 범위
      gateway4: 게이트웨이 주소
      nameservers:
        addresses: DNS 주소
        -
        search: []
  version: 2
```

7. 장비를 재부팅 하고 해당 문서의 2번 과정을 통해 IP가 정상적으로 변경 되었는지 확인합니다.

3.1.5 외부 접속을 위한 OpenSSH-Server 설치 방법

SSH 접근을 위해 Ubuntu OS 장비에 OpenSSH-Server 설치가 필요 합니다.

```
$ sudo su # root 권한 획득
$ apt install openssh-server # openssh-server 설치
$ systemctl status ssh # openssh-server 동작 상태 확인
```

- OpenSSH-Server 설치 후 , SSH Client를 통해 장비에 접속 합니다.

3.2 정책서버 설치

3.2.1 구축 형태

정책서버는 규모 또는 관리 방식에 따라 두 가지 방법으로 설치할 수 있습니다.

On-premises

내부 네트워크에 정책서버를 설치하여 고객의 정책 및 네트워크를 관리하는 시스템입니다.

Cloud managed

클라우드 환경에 가상의 정책서버를 설치하는 시스템입니다. 관리자는 클라우드 시스템에 접근하여 정책 및 네트워크를 관리합니다.

3.2.2 구성 방식

Genian ZTNA는 통합 구성, 단독 구성으로 구축이 가능 합니다.

- 통합 구성 : ZTNA Policy Center와 ZTNA Netwrok Sensor를 한 Ubuntu OS 장비에 설치 하는 구성 입니다.
- 단독 구성 : ZTNA Policy Center와 ZTNA Netwrok Sensor를 서로 다른 Ubuntu OS 장비에 설치 하는 구성 입니다.

3.2.3 하드웨어 준비

물리적 시스템 또는 가상 시스템에 정책서버를 설치할 수 있습니다.

물리적 장비

구축 시 최소 요구 사양 (ZTNA Policy Center)

- CPU : CPU Intel(R) Celeron(R) CPU G3900 @ 2.80 GHz 이상
- 메모리 : 8GB
- 디스크 : 120GB
- 운영체제 : Ubuntu 20.04 (Kernel Linux 5.4.0) 64bit

Note: 관리 노드수에 따라 하드웨어 요구 사양이 달라질 수 있습니다.

가상 머신

가상 시스템에 정책서버를 설치할 수 있습니다. ZTNA는 VMWare, VirtualBox, XenServer와 같은 다양한 하이퍼 바이저를 지원합니다.

3.2.4 네트워크 연결 준비

Genian ZTNA는 적어도 하나의 고정 IP 주소로 네트워크 연결을 요구합니다. On-premise 구성으로 설치하는 경우 해당 인터페이스를 관리 인터페이스로 사용할 수 있습니다.

Genian ZTNA는 네트워크의 브로드캐스트 도메인에 연결되어 모든 브로드캐스트 패킷을 모니터링합니다.

관리하려는 네트워크가 WAN을 통해 연결되어 있다면 물리적으로 분리된 네트워크센서가 별도로 필요합니다.

Note:

가상 머신을 사용하는 경우 **Bridge** 모드에서 네트워크 인터페이스 유형을 선택해야합니다.
VMWare ESXi 를 802.1Q trunk 포트와 함께 사용하려고하면 VGT 모드를 활성화해야합니다.
https://kb.vmware.com/s/article/1004252 를 참조 하십시오.

3.2.5 소프트웨어 다운로드

물리적 장비 설치용 부팅 USB를 생성합니다.

3.2.6 정책서버 설치 (On-premises)

1. 장비 부팅
   - 부팅 USB를 컴퓨터에 연결하십시오.
   - BIOS 설정에서 USB가 먼저 부팅되도록 부팅 순서를 변경합니다.
   - 가상 컴퓨터에서 설치를 진행 할 ISO 파일을 선택합니다. (가상 머신인 경우)

초기 구성 (On-premises)

1. Ubuntu 계정을 root 계정으로 전환 합니다.
2. 패키지 업데이트 및 업그레이드를 진행 합니다.
3. ZTNA 설치에 필요한 Curl을 설치 합니다.
4. 하단의 명령어를 통해 ZTNA Policy Center를 설치 합니다.

```
$ sudo su # root 계정으로 전환
$ apt-get upgrade # 패키지 업그레이드
$ apt install curl # Curl 설치
$ curl -s https://docs.genians.com/install/ztna-server.sh | sudo SITELOCALE=ko␣
↪BRANCH= bash
```

   - ZTNA-server.sh 는 ZTNA Policy Server 설치에 필요한 파일을 다운로드 하고 설치 하는 과정을 자동화 해주는 쉘 스크립트 파일 입니다.

5. 설치가 완료되면 화면에 출력된 Public URL 주소에 접속하여 , 정상적으로 설치가 되었는지 확인 합니다.

> **Warning:** 설치가 완료 되면 WebUI 주소와 관리자 ID · PW 가 화면에 출력 됩니다. admin 계정의 비밀번호는 임의로 변경이 불가능 합니다. 분실하지 않도록 주의가 필요합니다.

3.2.7 정책 서버 설치(Cloud Managed)

클라우드 환경에 ZTNA Policyt Center를 구축할 경우 먼저 AWS 클라우드 환경 구성을 진행해 주시기 바랍니다.

AWS 클라우드 환경 설정 방법

AWS 인스턴스에 **ZTNA Policy Server** 또는 **ZTNA Network Sensor** 를 구축 하기 위해서는, 사전에 AWS 클라우드 환경 설정이 필요합니다.

이 장에서는 AWS 환경 설정이 진행되는 개별 콘솔의 역할과 설정 방법을 설명 합니다.

AWS VPC 설정 방법

AWS VPC

AWS VPC(Virtual Private Cloud)란 AWS 클라우드 내 논리적으로 격리된 가상 네트워크 입니다. 선택한 범위에서 VPC의 IP 주소 공간을 정의합니다.

AWS VPC 설정 방법

Note: VPC 설정은 구축 환경에 맞추어 커스텀하게 설정합니다.

---

1. AWS 웹 콘솔 접속 후, 검색 창에 VPC를 입력하여 VPC 웹 콘솔로 이동합니다.
2. VPC 웹 콘솔에서 좌측 상단에 있는 **VPC 생성** 을 클릭합니다.
3. VPC 설정에서 VPC의 세부 설정을 하기 위해 **VPC등** 을 선택합니다.
4. VPC의 이름 태그를 설정하고, CIDR 표기법을 이용해 VPC의 시작 IP와 크기를 지정합니다.
5. VPC의 가용 영역 수(AZ)를 설정합니다.
6. 퍼블릭 서브넷 수와 프라이빗 서브넷 수를 설정합니다.
7. NAT 게이트웨이와 VPC 엔드포인트를 설정합니다.
8. DNS 옵션을 설정 합니다. 설정이 완료되면 하단의 **VPC 생성** 을 클릭합니다.
9. 생성이 완료 되면 **View VPC** 를 클릭합니다.

AWS 보안 그룹 설정 방법

보안 그룹은 인스턴스에 도달하는 리소스의 인바운드 · 아웃 바운드 트래픽을 제어 할 수 있습니다.

Note: ZTNA에서 사용 하는 서비스 포트 입니다. 보안그룹 생성 시 참고하여 생성해 주시기 바랍니다.

포트	설명
TCP/80	HTTP
TCP/8443,TCP/443	HTTPS
UDP/3871,UDP/3870	KeepAlive, Event
TCP/22	SSH
UDP/1194 (OpenVPN)	OpenVPN
TCP/5555 (IPsec)	for Remote VPN Session info
UDP/500 (IPsec)	ISAKMP
UDP/4500 (IPsec)	NAT Traversal
UDP/3799 (IPsec)	CoA
Random	Syslog
Random	Radius Authentication
Random	Radius Accounting
Random	Data Server
Random	Log Server

1. EC2 대시보드 **좌측 메뉴바 -> 네트워크 및 보안 -> 보안 그룹** 을 클릭합니다.
2. 우측 상단 **보안 그룹 생성** 을 클릭합니다.
3. 보안 그룹의 이름과 설명을 설정합니다. VPC 항목은 VPC 생성 문서에서 생성한 VPC로 지정합니다.
4. 인바운드 규칙을 설정합니다.
5. 아웃 바운드 규칙을 설정합니다.
6. 설정이 완료 되었으면 우측 하단의 **보안 그룹 생성** 을 클릭합니다.
7. 정상적으로 생성되 었는지 확인 하기 위해 아래와 같은 알림이 웹 콘솔에 출력 되는지 확인합니다.

AWS Access key 발급 방법

AWS Access key는 IAM 사용자, 루트 사용자의 장기 자격 증명을 말합니다.
해당 Access Key를 사용하여 AWS의 인스턴스 생성 · 삭제 · 자원 할당을 할 수 있습니다.

---

1. AWS 웹 콘솔 좌측 상단에 있는 검색창에 **IAM** 을 검색해 **IAM 웹 콘솔** 로 이동 합니다.
2. IAM 웹 콘솔에서 좌측에 있는 **사용자** 를 클릭 합니다.
3. 사용자 이름을 클릭 합니다.(사용자가 없을 경우 루트 계정을 통해 IAM 사용자를 생성 합니다.)
4. **보안 자격 증명 탭** 을 클릭 합니다.
5. **액세스 키 만들기** 를 클릭 합니다.
6. **.csv 파일 다운로드** 를 클릭해 액세스키 ID와 비밀 액세스 키가 저장된 csv 파일을 다운로드 받습니다.

> **Warning:** 액세스 키가 저장된 CSV 파일은 한번 만 다운로드 할 수 있습니다. 또한 엑세스 키가 외부에 유출 되지 않도록 주의 해주시기 바랍니다.

7. 다운로드 받은 CSV 파일을 열어 엑세스 키 ID와 비밀 엑세스 키를 확인 합니다.

AWS EC2 인스턴스 생성 방법

1. AWS EC2 대시보드에 접속한 뒤 우측 상단의 **인스턴스 시작** 을 클릭 합니다.
2. 인스턴스의 이름을 설정 합니다.
3. 인스턴스의 이미지를 선택 합니다.
   - **Ubuntu Server 20.04 LTS** 를 선택합니다.
4. **인스턴스의 유형** (하드웨어 리소스)을 선택 합니다.
   - **t2.large** 이상의 인스턴스 유형을 선택합니다.
5. 새 **키 페어** 생성을 클릭해 새로운 **키 페어** 를 생성 합니다.
6. 키 페어 이름을 지정 하고 키 페어 유형과 프라이빗 키 파일 형식을 (RSA , .pem) 설정 한 후 키 페어 생성을 클릭해 키 페어 파일을 다운 로드 합니다.

> **Warning:** 키 페어 파일은 1회만 다운로드 할 수 있습니다. 다운로드 받은 키 페어 파일은 재발급이 되지 않습니다.

7. 네트워크 설정에서 우측 상단 **편집** 을 클릭 합니다.
8. VPC를 클릭하여 생성한 VPC로 설정한 후 , **퍼블릭 IP 자동 할당을 활성화** 합니다.
9. 방화벽(보안 그룹)에서 **기존 보안 그룹 선택** 을 클릭 합니다.
10. **일반 보안 그룹** 을 클릭하여 이전에 생성한 보안 그룹을 선택 합니다.
11. 스토리지 구성에서 인스턴스에 할당 할 볼륨의 크기를 입력 합니다.
    - 40GB 이상의 볼륨크기를 입력합니다.
12. 하단 부에 있는 **인스턴스 시작** 을 클릭 합니다.
13. 인스턴스 시작(생성)이 완료되면 모든 인스턴스 보기를 클릭 한 후 , 인스턴스가 생성 된 것을 확인 합니다.

AWS 인스턴스 SSH 접근 방법

Note: 본 문서는 Secure CRT를 사용하여 인스턴스와 SSH 연결하는 방법이 작성된 문서 입니다.

1. AWS EC2 대시보드에서 생성한 **인스턴스의 인스턴스 ID** 를 클릭합니다.
2. 출력 되는 인스턴스 요약 팝업 창에서 확인 되는 **퍼블릭 DNS , 퍼블릭 IP** 를 확인합니다.
3. SecureCRT를 실행합니다.
4. 좌측 상단의 **File -> Quick Connect** 를 클릭합니다.
5. 하단의 표처럼 설정합니다.

Protocol	SSH2
Hostname	퍼블릭 DNS 또는 퍼블릭 IP 입력
Port	22
Firewall	None
Username	Ubuntu

6. **Public Key** 를 클릭하고 **Properties** 를 클릭합니다.

7. **Use Session Public Key Setting** 을 클릭한 다음 **Use identity or certification file** 에 다운로드 받은 Pem 키를 등록하고 Ok를 클릭합니다.

8. 입력이 완료되었으면 **Connect** 버튼을 클릭합니다.

9. New Host key 팝업창이 출력되면 **Accept&Save** 를 클릭합니다.

10. 정상적으로 연결이 되는지 확인합니다.

AWS 탄력적 IP 설정 방법

인스턴스의 고정 IP 설정을 위해 탄력적 IP 설정이 필요 합니다. 탄력적 IP 미 설정시 인스턴스 중지 후 재구동 시 퍼블릭 IP가 변동 됩니다.

Note: 클라우드 환경에서 ZTNA Center · Sensor 구축 시 2개의 탄력적 IP가 필요합니다.

---

1. AWS 웹 콘솔 좌측 상단에 있는 검색창에 EC2를 검색해 해당 콘솔로 이동 합니다.

2. EC2 웹콘솔 좌측에 있는 **탄력적 IP** 를 클릭 합니다.

3. 웹 콘솔 우측 상단에 위치한 **탄력적 IP 주소 할당** 을 클릭 합니다.

4. 네트워크 경계 그룹을 설정 하고 하단의 할당 버튼을 클릭 합니다. (서울 리전 : ap-northeast-2)

5. 생성된 탄력적 IP 주소를 선택 하고 우측 상단에 위치한 **작업** 을 클릭 후 , **탄력적 IP 주소 연결** 을 클릭합니다.

6. 리소스 유형과 인스턴스, 프라이빗 IP 주소를 선택하고 **연결** 을 클릭 합니다.
   - 인스턴스는 ZTNA Policy Center · Sensor 를 설치하기 위해 생성한 인스턴스를 선택하여 주시기 바랍니다.

7. 설정이 완료되면 해당 인스턴스 정보를 확인해 탄력적 IP 주소가 할당 되었는지 확인 합니다.
   - 인스턴스 ID를 클릭하여 인스턴스 요약을 확인해 주시기 바랍니다.

초기 구성(Cloud Managed)

1. 우분투 계정을 root 계정으로 전환 합니다.

2. 아래의 명령어를 입력하여 ZTNA Policy Center를 설치 합니다.

```
$ sudo su # root 계정으로 전환
$ curl -s https://docs.genians.com/install/ztna-server.sh | sudo SITELOCALE=ko␣
↪BRANCH= bash
```

3. 설치가 완료되면 화면에 출력된 Public URL 주소에 접속하여 , 정상적으로 설치가 되었는지 확인 합니다.

- ZTNA-server.sh 는 ZTNA Policy Server 설치에 필요한 파일을 다운로드 하고 설치 하는 과정을 자동화 해주는 쉘 스크립트 파일 입니다.

Warning: 설치가 완료 되면 WebUI 주소와 관리자 ID · PW 가 화면에 출력 됩니다. admin 계정의 비밀번호는 임의로 변경이 불가능 합니다. 분실하지 않도록 주의가 필요합니다.

3.2.8 지원되지 않는 하드웨어

설치가 정상적으로 진행이 되지 않는 경우 담당 파트너 엔지니어 또는 기술지원센터 에 문의해주세요.

Note: 가상 환경에 설치할 때 저장 장치 또는 네트워크 인터페이스가 인식되지 않으면 저장소 유형을 SATA로 변경하거나 네트워크 인터페이스 드라이버를 E1000과 같은 Intel 계열로 변경하십시오.

지원되지 않는 하드웨어보고

Genian ZTNA 설치 중에 저장 장치, 이더넷 어댑터 또는 무선 LAN 어댑터와 같이 지원되지 않는 하드웨어가있는 경우 절차를 통해 정보를 수집하고 help@genians.com으로 보내주십시오.

1. Ubuntu 와 같은 일반 리눅스 배포판 설치
2. 터미널 열기
3. 다음 명령을 입력하여 report.txt를 만듭니다.

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

4. report.txt 파일을 보내주세요.

3.3 네트워크센서 설치

네트워크센서는 사용자의 내부 네트워크 또는 AWS(인스턴스)에 설치되고 정보를 수집하여 정책 서버로 전송합니다. 네트워크 구성에 따라 하나 이상의 논리적 / 물리적 네트워크센서를 설치해야 할 수 있습니다.

3.3.1 하드웨어 준비

물리 시스템이나 가상 시스템에 네트워크센서를 설치할 수 있습니다.

물리적 장비

테스트 및 소규모 배포를 위해 HP, Dell 또는 Mini PC와 같은 일반 인텔 서버를 사용할 수 있습니다.

가상 머신

가상 머신에 네트워크센서를 설치할 수 있습니다. 다양한 하이퍼 바이저를 지원합니다.

3.3.2 네트워크 연결 준비

Genian ZTNA는 하나 이상의 고정IP 주소로 네트워크 연결이 필요합니다.

네트워크센서는 네트워크상에 뿌려지는 브로드 캐스트 패킷(ARP, DHCP, uPNP 등)을 모니터링 해야하며 관리하려는 모든 세그먼트(브로드 캐스트 도메인)에 연결되어 있어야합니다.

VLAN으로 구성된 스위치가 있는 경우 하나의 물리적 인터페이스로 여러 네트워크를 모니터링하도록 802.1Q trunk port를 설정할 수 있습니다.

가상 환경에 네트워크센서를 설치하는 경우 VM(센서)은 모니터링 및 제어하려는 모든 세그먼트와 직접 통신이 가능해야합니다.

Note: 가상 머신을 사용하는 경우 **Bridge** 모드에서 네트워크 인터페이스 유형을 선택해야합니다.

네트워크센서가 무선LAN 정보를 수집하려면 호환되는 무선 네트워크 어댑터를 설치해야합니다. 하단 문서 참고

무선 어댑터 호환성

Genian ZTNA와 호환되는 무선 어댑터 리스트입니다.

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

continues on next page

Table 1 – continued from previous page

Vendor	Model Name	Chipset	Band	Type
Lenovo	03T8726	RT5572	2.4G/5G	USB
Linksys	AE1000	RT3572	2.4G/5G	USB
Linksys	AE3000	RT3593	2.4G/5G	USB
Linksys	DMC350 Wireless Module	RT2870	2.4G	USB
Linksys	WUSB600N v1	RT2870	2.4G	USB
Linksys	WUSB600N v2	RT3572	2.4G/5G	USB
Loopcomm	LP-7767	RT3572	2.4G/5G	USB
Motorola	TER/NUSB1-N1	RT2770	2.4G	USB
Netis	WF2150	RT5572	2.4G/5G	USB
Netis	WF2151	RT5572	2.4G/5G	USB
Realtek	RTL8821AE		2.4G/5G	HMC
Rosewill	RNX-N600UB	RT5572	2.4G/5G	USB
Rosewill	RNX-N600UBE v1	RT3572	2.4G/5G	USB

Note: 위 목록에 없는 어댑터에 대해서는 Slack에 문의 부탁드립니다. (https://www.genians.com/slack)

Access port

스위치 Access Port를 통해 단일 네트워크를 모니터링하는 경우에는 스위치의 추가 설정이 필요하지 않습니다. 두개 이상의 NIC가 있는 시스템에 네트워크센서를 설치하는 경우 엑세스 포트를 통해 여러 세그먼트를 모니터링 할 수 있습니다.

Trunk Port

단일 인터페이스에서 여러개의 VLAN을 모니터링하려면 802.1Q 프로토콜을 사용하여 스위치 포트를 Trunk Port로 설정해야합니다. 아래는 Cisco와 HP 스위치에서 트렁크포트 802.1Q를 설정하는 예시입니다.

Cisco switch 설정 예제

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

HP switch 설정 예제 (태깅된 인터페이스로 port 48 생성)

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

Note: 트렁크 인터페이스에 VLAN 인터페이스를 설정하는 방법은 해당 문서를 참조해 주시기 바랍니다. 다중 *VLAN* 설정

3.3.3 ZTNA Nerwork Sensor 설치

ZTNA Network Sensor는 단독 구성 또는 통합 구성으로 설치가 가능합니다.

- 통합 구성 : ZTNA Policy Center와 ZTNA Netwrok Sensor를 한 Ubuntu OS 장비에 설치 하는 구성 입니다.
- 단독 구성 : ZTNA Policy Center와 ZTNA Netwrok Sensor를 서로 다른 Ubuntu OS 장비에 설치 하는 구성 입니다.

통합 구성

ZTNA Policy Center가 설치된 우분투 장비에 접속합니다.

```
$ sudo su # Ubuntu 계정을 root 계정으로 전환합니다.
$ cd /usr/geni/conf # genian.conf 파일 수정을 위해 conf 디렉토리로 이동합니다.
$ vim genian.conf # 수정을 위해 텍스트 편집기로 genian.conf 파일을 실행합니다.
5번 라인에 위치한 DKNS_ENABLED 값을 no -> yes로 수정합니다.
$ cd /usr/geni
$ ./compoese.sh start # compose 명령어를 통해 Network Sensor를 설치합니다.
$ ./compose.sh start dkns # compose 명령어를 통해 Network Sensor를 구동시킵니다.
$ ./compose.sh ps # compose 명령어를 통해 Docker Container가 정상적으로 구동되는지 확인합니다.
Web UI 접속 후 [시스템] -> [시스템 관리] 클릭, 추가된 미승인 센서를 체크 후 [작업 선택] -> [미승인 센서 승인]
클릭하여 승인합니다.
```

- **If you are sure to continue, Enter 'kernel update'** 라는 키워드가 나올 경우 **kernel update** 를 입력 해주시기 바랍니다.

단독 구성 (On-premise 환경에 Sensor 설치)

- 범용 *OS* 설치 를 참고 하여 먼저 Ubuntu OS 설치를 진행하여 주시기 바랍니다.

```
$ sudo su # Ubuntu 계정을 root 계정으로 전환 합니다.
$ apt-get update # 패키지 업데이트를 진행 합니다.
$ apt install curl # curl를 설치합니다.
$ curl -s https://docs.genians.com/install/ztna-sensor.sh | sudo BRANCH= bash -s -␣
↪[POLICY SERVER IP] # 명령어를 통해 ZTNA Network Sensor를 설치 합니다.
$ cd /usr/geni # /usr/geni 로 이동 합니다.
$ ./compose.sh ps # compose 명령어를 통해 Docker Container가 정상적으로 구동되고 있는지 확인
합니다.(State 값이 up인지 확인)
Web UI 접속 후 [시스템] -> [시스템 관리] 클릭, 추가된 미승인 센서를 체크 후 [작업 선택] -> [미승인 센서 승인]
클릭하여 승인 합니다.
```

단독 구성(Cloud-Managed(AWS) 환경에 Sensor 설치) - CLI를 통한 수동 설치

- 인스턴스 생성 방법 을 참고하여 ZTNA Network Sensor를 설치 할 인스턴스를 먼저 생성합니다.
- 인스턴스 설치 후 SSH 클라이언트를 사용하여 인스턴스에 연결 합니다.

```
$ sudo su # root 계정으로 전환합니다.
$ curl -s https://docs.genians.com/install/ztna-sensor.sh | sudo BRANCH= bash -s -␣
↪[POLICY SERVER IP] # 명령어를 통해 ZTNA Nerwork Sensor 를 설치합니다.
커널 다운그레이드 진행 시,다운그레이드 후 설치가 진행 됩니다. 다운그레이드가 완료 되면 재부팅이 수행됩니다.
$ sudo su # root 계정으로 전환합니다.
$ cd /usr/geni # compose 스크립트 사용을 위해 디렉토리를 이동합니다.
$ ./compose.sh restart dkns # 센서 재시작 명령어를 입력합니다.
```

(continues on next page)

(continued from previous page)

```
$ ./compose.sh ps # compose 명령어를 통해 Docker Container가 정상적으로 구동 되고 있는지 확인
합니다.(State 값이 up인지 확인)
Web UI 접속 후 [시스템] -> [시스템 관리] 클릭, 추가된 미승인 센서를 체크 후 [작업 선택] -> [미승인 센서 승인]
클릭하여 승인합니다.
```

단독 구성(Cloud-Managed(AWS) 환경에 Sensor 설치) - Web UI를 통한 자동 설치

1. Web UI 콘솔에 접속 합니다. [https:// (ZTNA Policy Server IP):8443/]
2. 상단 메뉴에서 **시스템 -> Cloud Provider 관리** 를 클릭합니다.
3. **작업선택 -> 생성** 을 클릭 합니다. 하단 표를 참고 하여 설정합니다.

설정 명	Cloud provider의 이름
Cloud	AWS
Access Key	발급 받은 Access key ID
Secret Key	발급 받은 Secret Access key

Note: Access Key 발급은 *AWS Access key 발급 방법* 을 참고하여 생성합니다.

4. 좌측 메뉴에 **시스템 -> 사이트** 를 클릭합니다.
5. **작업 선택 -> 생성** 을 클릭합니다. 하단 표를 참고 하여 설정합니다.

사이트 명	설정할 사이트의 이름 부여
타입	Hub/Branch
인프라	Cloud
Cloud Provider	3번 과정에서 생성한 Cloud Provider
Region	Policy Center가 생성된 인스턴스의 Region
VPC ID	Policy Center 구축 시 사용된 VPC

- 사이트 설정은 생성 후 수정이 불가합니다.

6. **시스템 -> 시스템 관리** 를 클릭합니다.
7. **작업 선택 -> Cloud 센서 추가** 를 클릭합니다. 하단 표를 참고 하여 설정합니다.

사이트 명	5번 과정에서 생성한 사이트명을 지정합니다.
AMI	사이트명 설정 시 자동 설정
Instance Type	인스턴스 유형 선택(t2.large 이상 선택 권장)
Size	인스턴스의 디스크 크기 지정(64GB 이상 권장)
Subnet ID	사이트명 설정 시 자동 설정
Key pair	센서 인스턴스 SSH 연결 시 사용할 Key pair 설정

8. **Check init** 을 클릭 합니다. **Check init** 이 완료 되면 **생성** 을 클릭합니다.
9. EC2 대시보드에 접속해서 센서 인스턴스가 생성된 것을 확인합니다.
10. Web UI 접속 후 **[시스템] -> [시스템 관리]** 클릭, 추가된 미승인 센서를 체크 후 **[작업 선택] -> [미승인 센서 승인]** 클릭하여 승인합니다.

Docker Container 확인 방법

ZTNA Nerwork Sensor 설치 후, 정상적으로 컨테이너가 동작하는지 확인이 필요합니다. 확인을 위해 **compose.sh** 스크립트를 사용하여 확인합니다.

```
$ cd /usr/geni  # compose.sh 스크립트 사용을 위해 디렉토리를 이동합니다.
$ ./compose.sh ps  # 해당 명령어를 통해 컨테이너의 동작 상태를 확인 할 수 있습니다.
State 항목이 Up 상태인지 확인합니다.
```

하단의 표를 참고하여, 각 컨테이너가 정상 동작 하는지 확인합니다.

종류	Container Name
ZTNA Network Sensor	geni_dkns_1
ZTNA Policy Center	geni_nac_1
DB Server	geni_dbserver_1
Log Server	geni_logserver_1
Log 수집기	geni_filebeat_1
업데이트 에이전트	geni_gnupdateinfo_1

3.4 관리자 콘솔

Genian ZTNA는 두 가지 유형의 관리 인터페이스를 제공합니다.

- **WEB 콘솔 (Web Console, Web interface, 웹 인터페이스)** : 웹 브라우저에서 액세스할 수 있는 사용자 인터페이스이며, 모든 관리 및 정책 설정을 제공합니다.
- **명령 줄 인터페이스 (Command-line interface, CLI, 커맨드 라인 인터페이스)** : 기본 서비스 구성 및 네트워크 구성과 같은 시스템 설정을 제공합니다.

3.4.1 WEB 콘솔

WEB 콘솔의 접속 방식은 정책서버의 설치 방식에 따라 다릅니다.

On-Premises / 소프트웨어 ZTNA

1. **웹 브라우저** 를 열고 다음 링크로 이동합니다.
2. 아래 링크를 복사하여 브라우저에 붙여 넣습니다.
3. **정책 서버 관리 IP 주소:8443** 를 실제 IP 주소로 변경합니다.

```
https://"정책 서버 관리 IP 주소:8443"/mc2/ (e.g. https://192.168.50.10:8443/mc2/)
```

Cloud managed

1. **웹 브라우저** 를 열고 다음 링크로 이동합니다.
2. 아래 링크를 복사하여 브라우저에 붙여 넣습니다.
3. **클라우드 정책 서버 도메인** 을 실제 등록된 이름으로 변경합니다.

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

3.4.2 CLI 콘솔

CLI(Command Line Interface) 콘솔은 SSH를 통해 접속할 수 있습니다.

1. SSH 접속 프로그램을 통한 CLI 콘솔 접속

Step1: 정책서버 SSH 접속을 위한 원격 액세스 설정하기

정책서버로 SSH 접속을 하기 위해서는 허용하는 IP주소 또는 네트워크 주소/CIDR 패턴을 추가해야합니다.

1. 상단 패널에 **시스템** 으로 이동합니다.
2. 왼쪽 **시스템** 항목에서 **시스템관리** 를 선택합니다.
3. **정책서버 IP** 를 클릭합니다.
4. **환경설정 탭** 을 선택합니다.
5. **보안설정** 항목에서 **CLI 콘솔 접속 IP** 를 입력합니다.(SSH 접속을 수행하는 단말 IP)
6. **수정** 버튼을 클릭합니다.

Step2: SSH 접속 프로그램을 통한 CLI 콘솔 접속하기

CLI 콘솔 접속 방식은 **On-premises** 와 **Cloud-Managed** 둘 다 동일 합니다.

- **Cloud managed** : 22
- **On-Premises** : 22

```
#ZTNA CLI 콘솔 접속
ssh "정책 서버 관리 IP" -p 22  (e.g. : ssh 192.168.50.10 -p 22)
```

Note:

소프트웨어 ZTNA의 CLI콘솔 접속이 되지 않는 경우에는 `systemctl restart sshd` 명령어를 통해 SSH 데몬을 재시작해주시기 바랍니다.

3.5 라이선스 설치

Genian ZTNA가 설치되면 기본적으로 무료 버전으로 작동합니다. 무료 버전에는 다음과 같은 제한 사항이 있습니다.

- Basic Edition 기능만 제공됩니다.
- 최대 300 개의 노드만 관리 할 수 있습니다.
- 지점의 센서를 추가 연결할 수 없습니다.

제어 및 연동이 필요한 경우 Professional 또는 Enterprise Edition에 대한 라이선스를 설치해야합니다. 평가판 라이선스 페이지 로 이동하여 30 일 동안 Professional / Enterprise Edition을 체험 할 수있는 평가판 라이선스를 얻을 수 있습니다.

Note: On-Premises 정책 서버만 라이선스가 필요합니다. 클라우드 관리 서비스는 라이선스가 필요하지 않습니다.

3.5.1 서버 ID 확인

1. 상단 패널의 **시스템** 을 클릭하십시오.
2. 왼쪽 **시스템** 패널에서 **시스템 > 라이선스** 로 이동하십시오.
3. **서버 ID 확인**

3.5.2 평가판 라이선스 받기

1. 평가판 라이선스 페이지
2. **서버 ID** 섹션을 찾아 정책 서버에있는 서버 ID를 추가하십시오.
3. **전체 이름, 회사 이름, 이메일** 을 입력하십시오.
4. **시범 사용권 얻기** 를 클릭하십시오.
5. —–BEGIN CERTIFICATE—– 부터 —–END CERTIFICATE—– 까지 **라이선스** 를 복사하십시오.

3.5.3 라이선스 설치

1. 상단 패널의 **시스템** 을 클릭하십시오.
2. 왼쪽 **시스템** 패널에서 **라이선스** 로 이동하십시오.
3. **라이선스 등록** 클릭하여 라이선스 파일을 업로드 하거나 복사 & 붙여넣기합니다.
4. **적용** 을 클릭 하십시오.

3.6 에이전트 설치

Genian ZTNA는 엔드포인트의 시스템 정보수집, 엑세스 제어, 사용자 인증 뿐만 아니라 엔드포인트의 보안 상태를 점검하는 역할을 수행합니다. 이를 위해 Windows 및 macOS에 에이전트를 수동 설치하거나 에이전트 미설치 차단정책을 통해 에이전트를 자동 설치하기도합니다. 설치 이후 엔드포인트의 보안정책 점검, 준수를 위해 정책서버와 통신합니다.

3.6.1 Windows Agent 설치

GPO, CWP (Captive Web Portal)를 통해 Windows 단말에 **에이전트** 를 설치 하거나 메일, USB 등을 이용하여 수동으로 **에이전트** 를 설치할 수 있습니다.

Windows 에이전트 설치

- 에이전트 다운로드 페이지를 통해 다운로드 및 설치
- *CWP*를 통한 에이전트 설치
- *Active Directory GPO*를 통한 에이전트 *MSI* 패키지 설치
- *Windows Agent* 설치 확인
- *Windows* 단말 에이전트 로그 위치

에이전트 다운로드 페이지를 통해 다운로드 및 설치

1. 에이전트 다운로드
   - https://(*IP* 또는 도메인)/agent
2. 에이전트 선택 : 파일명 충돌을 피하기 위해 파일 이름을 변경하지 마십시오.
   - Windows 설치 관리자 버전 : GnUpdate_(*IP* 또는 *FQDN*) .exe

Note: 사용자에게 파일 설치 권한이 없는 경우 설치 프로그램을 실행할 수 없으므로 파일 설치 권한으로 관리자 권한으로 실행해야합니다.

CWP를 통한 에이전트 설치

에이전트를 설치하지 않으면 제어정책에 의해 네트워크가 차단되고 에이전트 설치를 위한 CWP(Captive Web Portal)로 리다이렉션 될 수 있습니다. CWP 화면에서 에이전트 설치 버튼을 클릭하여 에이전트를 다운로드하고 설치합니다.

"에이전트 설치" 정책 옵션을 적용하려면

1. 상단 패널의 **정책** 으로 이동합니다.
2. **노드 정책** 으로 이동 하십시오.
3. "노드 정책 ID"를 클릭하여 정책을 적용 할 위치를 지정합니다.
4. **에이전트 정책** 항목을 찾습니다.
5. **에이전트** 체크박스에서 **on** 을 선택합니다.

6. 좌측메뉴의 **제어정책** 을 선택하여 **에이전트 미설치 차단** 정책을 활성화합니다.

Note: 노드 정책을 할당 받은 노드는 에이전트가 설치되지 않은 경우 제어정책(에이전트 미설치 차단 정책)에 의해 CWP 페이지로 리다이렉션 되고 CWP 페이지에 "에이전트 설치 버튼"을 표시합니다.

Active Directory GPO를 통한 에이전트 MSI 패키지 설치

MSI 설치패키지 다운로드

1. 관리 WebUI에 접속하여 상단 **시스템** 메뉴로 이동합니다. 좌측 **업데이트 관리 > 소프트웨어** 메뉴로 이동합니다.
2. 현재 정책서버에 에이전트가 업로드가 되어있다면 **Genian ZTNA Agent for Windows** 항목 우측의 `MSI` 버튼을 클릭하면 MSI 설치패키지가 다운로드 됩니다.

Note: Genian ZTNA 버전은 *Active Directory GPO정책을 이용한 에이전트 배포* 과정을 바로 진행합니다

MSI 파일 설정

설치패키지에 포함된 정책서버 IP는 단말에 에이전트가 설치가 된 이후에 에이전트가 등록될 정책서버의 IP입니다.

MSI 설치패키지에 정책서버IP를 설정하기 위해서는 Microsoft Orca 가 필요합니다.

Orca 다운로드 방법

Microsoft Orca는 윈도우즈 독립 실행형 SDK를 다운받아 그 안에 있는 Orca파일만 추출하여 사용합니다.

아래 단계를 따라 Orca를 설치합니다. :

1. 다운로드 링크 로 이동하여 하단 **Windows 10 SDK 다운로드** 클릭
2. 시작섹션의 .ISO 다운로드 클릭 (약 800MB)
3. 압축 해제 프로그램을 이용하여 ISO 파일을 압축 해제합니다.
4. 압축 해제한 폴더 안의 Istallers 폴더로 이동하여 **orca** 가 들어간 파일을 찾습니다. (eg. Orca-x86_en-us.msi)
5. orca msi 파일만 다른 폴더로 이동하여 실행합니다.
6. 설치에 필요한 **.cab** 파일이 없다고 에러가 발생할 것이며 이때 표시된 모든 파일을 찾아서 orca msi가 있는 폴더로 복사합니다.
7. 모든 파일이 복사가 되었다면 msi 파일을 실행하여 orca를 설치합니다.

MSI파일에 정책서버 IP 설정

아래 순서대로 MSI 파일 설정 변경을 수행합니다.

1. Orca 실행
2. **File > Open > 에이전트 MSI파일 선택**
3. 좌측 테이블에서 **CustomAction** 선택
4. **custom** 필드를 찾아 우측내용 작성 "-n:정책서버 `IP` 나 `Domain Name` 입력"
5. 저장 & 종료

Active Directory GPO정책을 이용한 에이전트 배포

Note: 로그인한 계정의 권한이 사용자권한일 경우 에이전트가 제대로 작동하지 않을 수 있으며 **로컬 시스템 계정** 으로 에이전트 수행 계정을 변경해야합니다.

아래 순서에 따라 노드정책 에이전트의 수행계정을 수정합니다.:

1. 상단 패널의 정책 으로 이동합니다.
2. 노드 정책 으로 이동 하십시오.
3. "노드 정책 ID"를 클릭하여 정책을 적용 할 위치를 지정합니다.
4. 에이전트 정책 항목을 찾습니다.
5. 수행 계정에 로컬 시스템 계정 선택
6. 수정 및 변경정책적용 클릭
7. Active Directory GPO를 통하여 MSI 패키지 배포

Active Directory GPO(Goup Policy Object) 설정

Genian Agent MSI 파일을 AD를 통해 배포할 수 있는 Active Directory GPO에 대해 설정하는 방법을 설명합니다.

1단계. 배포하는 MSI 파일에 대한 공유 폴더를 생성

- 에이전트 MSI 파일을 Genian에서 공유 폴더로 복사하거나 파일이 들어 있는 폴더를 공유 폴더로 설정합니다.

2단계. Group Policy Management(그룹 정책 관리) 를 열고 GPO 생성

- 윈도우 서버에서 **실행(Run) > gpmc.msc** 또는 **시작 > 관리 도구 > 그룹 정책 관리** 입니다.
- 왼쪽 항목에서 **[도메인 이름]** 을 선택 > 마우스 오른쪽 버튼에서 **이 도메인에서 GPO를 만들어 여기에 연결** 을 **클릭 > 새 GPO 이름(N): 입력창** 에 **이름(예: genian)** 을 입력 > **확인** 버튼을 클릭합니다.
- 생성 된 **genian** GPO 에 오른쪽 마우스 버튼을 클릭하면 **그룹 정책 관리 편집기** 가 표시 됩니다.

3단계. 그룹 정책 관리 편집기 를 구성

- 왼쪽 항목에서 **정책** 및 **소프트웨어 설정** 폴더 하위 트리를 확장 > **소프트웨어 설치** 항목에서 마우스 오른쪽 버튼을 클릭하고 **새로 만들기(N)** 및 **패키지** 를 클릭합니다
- (예: \[도메인]공유폴더)와 같은 공유 폴더 경로로 이동합니다. 선택한 다음 Agent MSI 파일 > **고급** 을 선택합니다.
- **고급 > 패키지 배포 시 언어 무시** 체크 > **확인** 을 클릭합니다.

4단계. 그룹 정책 관리 의 GPO 정책 적용

Note: GPO에는 **컴퓨터** 및 **사용자** 구성 모두 포함 될 수 있습니다.

```
GPO의 "컴퓨터 구성" 은 부팅 중에 적용 됩니다.
GPO의 "사용자 구성" 은 사용자 로그인 시 적용 됩니다.
```

- 왼쪽 항목의 마우스 오른쪽 버튼에서 **컴퓨터** 또는 **사용자** 폴더를 클릭합니다. > **기존 GPO 링크 > genian GPO** 선택

5단계. 검증

- **실행 > cmd >** gpupdate /force 명령을 수행합니다.

```
C:\Users\Administrator.GENIAN-ADSERVER>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
The following warnings were encountered during computer policy processing:

The Group Policy Client Side Extension Software Installation was unable to apply␣
↪one or more settings because the changes must be processed before system␣
↪startup or user logon.
The system will wait for Group Policy processing to finish completely before the␣
↪next startup or logon for this user, and this may result in slow startup and␣
↪boot performance.
User Policy update has completed successfully.

For more detailed information, review the event log or run GPRESULT /H GPReport.
html from the command line to access information about Group Policy results.
↪Certain Computer policies are enabled that can only run during startup.

OK to restart? (Y/N)
```

- **작업관리자** 내에서 **GnAgent.exe, GnPlugin.exe, GnStart.exe** 프로세스를 체크합니다.

- C:₩Program Files₩Geni₩Genian 에서 **GnAgent.exe, GnPlugin.exe, GnStart.exe** 와 같은 에이전트 파일들을 체크합니다.

Windows Agent 설치 확인

1. **관리 > 노드** 를 선택합니다.
2. 노드 리스트 창에서 **NT AG SS** 열을 클릭하십시오. (노드에 설치된 에이전트가있는 경우 에이전트 아이콘 이 표시 됩니다.)

Windows 단말의 Genian 에이전트 옵션

1. Windows 단말의 화면 우측하단 **TrayIcon** 위치로 이동합니다.
2. **Genians 에이전트 아이콘** 을 찾아 마우스 오른쪽 버튼으로 클릭합니다.
3. 나열된 옵션을 사용하여 다음을 수행 할 수 있습니다.
   - **공지사항 보기:** 관리자로부터 현재 공지 사항을 보여 줍니다.
   - **알림 메세지 보기:** 관리자의 현재 메시지를 표시합니다.
   - **내상태 확인:** 현재 단말의 보안정책 만족상태를 웹페이지를 통해 보여줍니다.
   - **사용자 인증 (L):** 사용자가 로그인 할 수 있으며 로그인 성공시 CWP 페이지가 표시 됩니다.
   - **사용자 인증 해제 (O):** 사용자가 로그 아웃 할 수 있습니다.
   - **사용자 인증 정보:** 사용자가 로그인 성공 시 계정 정보를 볼 수 있습니다.
   - **네트워크 연결 정보:** 사용자가 활성화 된 네트워크 연결 단말를 볼 수 있습니다.
   - **USB장치 정보:** 사용자가 USB 단말의 정보를 볼 수 있게합니다.
   - **원격 에이전트 삭제:** (사용자는 설치 된 에이전트를 삭제할 수 없습니다. 이 작업은 관리자가 수행해야합니다)
   - **프로그램 정보:** 설치 된 Agent에 대한 버전 정보를 볼 수 있습니다.

Windows 단말 에이전트 로그 위치

1. Windows 단말에서 **파일 탐색기** 열기
2. **C: / Program Files / Geni / Genian / Logs** 로 이동합니다.
3. **수정 된 날짜** 로 정렬

Note: 에이전트 설치와 관련된 인스톨로그는 Windows 디렉토리에 `Installer"년월일".log` 로 존재합니다.

Windows 지원 목록

Microsoft Windows OS (32bit/64bit)	v6.0.x
Microsoft Windows 8	6.0.0~
Microsoft Windows 8.1	6.0.0~
Microsoft Windows 10	6.0.0
Microsoft Windows 11	6.0.0~
Microsoft Windows Server 2012	6.0.0~
Microsoft Windows Server 2016	6.0.0~
Microsoft Windows Server 2019	6.0.0~

3.6.2 macOS 에이전트 설치

GPO(Group Policy Object), CWP(Captive Web Portal)를 통해 macOS 장치에 **에이전트**를 설치 하거나 이동식 저장 미디어를 사용하여 수동으로 에이전트 를 설치할 수 있습니다

macOS 에이전트 설치

1. 에이전트 다운로드
   - https://(*IP* 또는 도메인)/agent
2. 에이전트 선택 : 이름 충돌을 피하기 위해 파일 이름을 변경하지 마십시오.
   - macOS 버전 : GnAgent_(*IP* 또는 도메인).pkg

macOS 에이전트 설치 확인

1. **관리 > 노드**를 선택하십시오.
2. 노드 리스트 창에서 **NT AG SS** 컬럼을 클릭 하십시오.(노드에 설치된 에이전트가있는 경우 에이전트 아이콘이 표시됩니다)

macOS 지원 목록

OS X/macOS	버전	v6.0.x
macOS Big Sur	11.0(M1 포함)	6.0.0~
macOS Monterey	11.0(M1 포함)	6.0.0~
macOS Ventura	13.0	6.0.4~
macOS Sonoma	14.0(M1 포함)	6.0.16~
macOS Sequoia	14.0(M1 포함)	6.0.23~

3.6.3 Linux 에이전트 설치

CWP 페이지를 통하여 설치스크립트를 다운로드하고 스크립트 수행하여 에이전트를 설치 할 수 있습니다.

- Linux OS를 사용하는 단말은 플랫폼 분류를 통하여 **서버** 노드타입으로 등록됩니다.

CWP를 통한 Linux 에이전트 설치

Genian ZTNA에서 에이전트 설치방법은 여러가지가 존재합니다. 아래 다양한 방법중 가장 일반적인 CWP 페이지 접속하여 에이전트 설치방법 안내입니다.

- CWP 페이지 직접 접속하여 에이전트 설치파일 다운로드
- 에이전트 미설치단말을 차단하여 CWP로 유도하여 설치

1. CWP 페이지에 접속합니다. https://정책서버*IP*/agent
2. OS별 에이전트 아이콘에서 리눅스 아이콘을 선택하고 파일을 다운로드합니다.
3. Linux 배포판에서 **터미널** 열어서 **Download** 폴더로 이동합니다. (우분투 기준)

> **Note:** 리눅스 배포판에 따라서 리눅스 에이전트 설치 스크립트의 다운로드 경로가 다를 수 있습니다.

4. 다운로드디렉토리에 설치 스크립트를 아래와 같이 실행합니다.
   - cd ~/Download
   - chmod 755 ./lnxagent_*서버주소*.sh
   - sudo ./lnxagent_*서버주소*.sh

> **Note:** 사용자에게 파일 설치 권한이 없는 경우 설치 프로그램을 실행할 수 없으므로, 관리자 권한으로 실행해야합니다. 스크립트가 종료되면 자동으로 프로세스가 구동됩니다.

Linux 에이전트 설치 확인

1. WEB콘솔 접속을 합니다.
2. **관리 > 노드** 메뉴로 이동합니다.
3. 설치한 노드의 IP를 검색합니다.
4. 노드 리스트화면에서 에이전트 아이콘이 표시되면 정상적으로 설치 및 정보등록이 완료된 상태입니다.

Linux 배포판에서 에이전트 로그를 찾는 위치

- Linux 배포판에서 **터미널** 열어서 아래의 위치의 로그파일을 확인합니다.
  - 설치경로: /usr/share/genians
  - 로그경로: /var/log/genians
  - 설정 파일 경로: /usr/share/genias/GenianDB
  - PID 파일 경로: /var/run/genians

Linux 에이전트 지원 OS 목록

Linux OS	버전	v6.0.x 이상
Ubuntu	18 ~ 24	6.0.5 ~
Gooroom	2 ~ 4	6.0.5 ~
HamoniKR	3.0 ~ 4.0	6.0.0 ~
Hancom Gooroom	2 ~ 3	6.0.5 ~
Tmax Gooroom	2, 21	6.0.5 ~

3.6.4 에이전트 삭제

사용자 단말에서 에이전트를 제거하는 방법은 아래와 같습니다.

- 노드 정책의 **에이전트정책**
- 에이전트 설정의 **인증코드 사용**
- 에이전트 설정의 **인증코드 미사용**

노드정책의 에이전트정책을 사용하여 에이전트 삭제

다음은 관리자가 다수의 장치에서 에이전트를 일괄삭제하는 방법입니다.

1. **노드 그룹** 을 생성하여 에이전트를 삭제할 노드를 추가 하십시오.
2. **노드 정책** 을 생성하여 선택한 노드에서 에이전트를 삭제 하십시오.
   - 아래 : **노드정책** 에서 에이전트 정책 항목 메뉴의 Delete 옵션을 설정합니다.
3. 노드 정책을 작성한 후 오른쪽 상단 의 **적용** 옵션을 클릭하십시오.

그러면 노드 정책이 에이전트에서 업데이트 될 때 지정된 장치에서 에이전트가 자동으로 삭제 됩니다.

Note: Active Directory의 GPO정책으로 설치한 단말의 에이전트는 반드시 단말의 GPO정책을 제거해야합니다.

관리자 인증코드를 사용하여 에이전트 삭제

이 방법은 **인증코드 사용** 설정일때 사용합니다. 사용자가 삭제 요청 > 관리자 코드 발급 방식으로 진행됩니다.

엔드포인트 사용자 삭제 요청 :

1. Windows 또는 macOS 시스템의 작업 표시줄로 이동하여 Genians 아이콘을 찾습니다.
2. 로고를 마우스 오른쪽 단추로 클릭하고 **원격 에이전트 삭제 (D)** 옵션을 선택하십시오.
3. 팝업 창에서 **에이전트 코드** 를 찾아 Genian ZTNA 관리자에게 제공하여 **인증 코드** 를 요청하십시오.
4. 제공받은 **인증 코드** 를 입력하고 **삭제** 버튼을 클릭하십시오.

관리자 인증코드 발급 :

1. 정책서버 관리WebUI에 로그인하십시오.
2. 상단 **관리 > 신청** 메뉴를 선택하십시오.
3. 좌측 하단 **에이전트 인증코드 발급** 을 선택하여 **에이전트 인증코드 발급** 메뉴로 이동 하십시오.
4. 엔드 포인트 사용자가 제공 한 **에이전트 코드** 를 입력하고 **인증코드 발급** 버튼을 클릭하십시오.

5. **인증 코드** 가 표시 됩니다. 최종 사용자에게 이 코드를 제공하십시오.

Note:

1. 에이전트가 오프라인 상태여도 정책서버에서 발급한 인증코드를 사용하여 에이전트 삭제가 가능합니다.
2. 에이전트 인증코드 발급 결과 부분은 다음에 agent-authentication-code-result 참고하시기 바랍니다.

정책서버를 이용하여 삭제코드를 발급 할수 없는 경우

에이전트를 삭제하기 위해서는 에이전트 설치에 사용 된 정책 서버가 필요합니다. 이 정책 서버를 더 이상 사용할 수 없으면 새로운 정책 서버가 필요합니다.

1. 새로운 정책 서버를 설치하십시오.
2. 새 정책 서버의 에이전트를 설치하십시오. 기존 에이전트를 삭제하고 새 에이전트로 덮어쓰기 됩니다.
3. 노드 정책 또는 삭제 코드를 사용하여 에이전트를 삭제하십시오.

사용자 직접 삭제 방법

이 방법은 **인증코드 미사용** 설정일때 사용합니다. 사용자가 에이전트를 직접 삭제하는 방법입니다.

사용자 직접삭제 방법 :

1. Windows 또는 macOS의 트레이 바에서 ZTNA 아이콘을 찾습니다.
2. 아이콘을 마우스 우측 버튼으로 클릭하여 **원격 에이전트 삭제 (D)** 를 선택합니다.

Note: 에이전트 삭제방식이 **지원 안함** 인 경우에는 트레이 메뉴에서 에이전트를 삭제 할 수 없습니다.

CHAPTER

FOUR

네트워크 자산 모니터링

노드 자체 또는 IP 주소, 스위치 및 무선 LAN을 모니터링하여 네트워크 자산을 모니터링 할 수 있습니다.

4.1 네트워크 모니터링 이해하기

4.1.1 네트워크 및 엔드 포인트의 가시성 확보

네트워크 액세스 제어는 일반적으로 다음 단계를 통해 설정 됩니다.

- 네트워크 검색 및 정보 수집을 통해 자산의 가시성 확보
- 보안 정책 및 상태에 따라 수집된 자산 분류
- 분류 된 객체에 대한 네트워크 액세스 제어 정책 수립

Genian ZTNA는 네트워크센서 및 에이전트를 통해 다양한 네트워크 자산의 정보를 수집하고 네트워크 및 엔드 포인트에 대한 실시간 가시성을 제공합니다.

- 네트워크 노드
- 엔드 포인트
- IP 주소
- 스위치 / 포트
- 무선 랜

네트워크센서 및 에이전트는 관리 대상 네트워크 또는 엔드 포인트를 실시간으로 모니터링하고 새로운 정보 또는 변경된 정보를 정책 서버로 전송합니다. 관리자는 정책 서버가 제공하는 관리 콘솔을 통해 전체 관리 대상 네트워크 및 엔드 포인트 정보를 조회할 수 있습니다.

4.1.2 관리 메뉴

관리자 웹 콘솔의 관리 메뉴는 네트워크센서 및 에이전트를 통해 수집된 다양한 정보를 검색하고 정보를 검색 및 설정하기위한 메뉴입니다. 각 관리 화면은 세 영역으로 구분됩니다. 왼쪽의 트리 항목과 상태 및 필터 항목은 오른쪽 보기 창에 표시 할 대상 개체를 선택하는 데 사용됩니다.

트리 항목

트리 항목을 사용하면 보기 창에 센서 또는 관리자가 지정한 조건을 충족하는 그룹으로 표시 할 대상 개체를 선택할 수 있습니다.

상태 및 필터 항목

상태 및 필터 항목은 트리 항목에서 선택한 객체의 보다 상세한 필터링을 제공합니다. Genian ZTNA에서 수집한 다양한 정보를 기반으로 올바른보기 창에서 정보와 일치하는 개체를 쉽게 선택하고 표시할 수 있습니다. 또한 통계 정보는 제공되는 다양한 범주의 최상위가 선택 될 때 그래프 또는 표를 통해 제공 됩니다.

보기 창

상단에있는 검색 기능을 통해 출력된 개체를 검색하거나 각 항목을 선택 하여 **작업** 메뉴 에서 다양한 작업을 수행할 수 있습니다. 각 관리 메뉴에 대한 키 열의 링크를 클릭하면 개체에 대한 자세한 정보를 볼 수 있습니다. 각 관리 메뉴의 키 열은 다음과 같습니다.

- 노드: **IP**
- IP 주소: **Sensor**
- 스위치: 스위치, **포트**
- 무선랜: **MAC**

4.2 네트워크 노드 모니터링

다양한 관점에서 그룹화, 필터링 등 리스트화 하여 **노드** 를 모니터링 할 수 있습니다.

4.2.1 네트워크 노드 이해하기

네트워크 노드 및 장비

노드는 IP주소와 MAC주소의 조합으로 구성된 ZTNA의 논리적인 연결 단위입니다. 노드는 물리적 디바이스와 다른 논리적 개념입니다. 예를 들어 하나의 장비에 여러 개의 IP 또는 MAC이 있을 경우, 여러 개의 노드로 인식됩니다.

예)

- 하나의 장비가 여러 개의 NIC 카드 (유선 LAN, 무선 LAN)를 통해 네트워크에 연결 될 때
- 여러 운영 체제가 하나의 장비에서 다중 부팅을 통해 서로 다른 IP 주소를 사용 할 때
- 하나의 장비에서 가상 컴퓨터를 통해 여러개의 IP / MAC 조합으로 사용 될 때

Genian ZTNA는 다음과 같은 경우 하나의 장비에 연결된 다른 노드를 자동으로 인식합니다.

- 여러 노드가 동일한 MAC 주소를 사용할 때
- 에이전트를 통해 하나의 장비에 설치된 여러 개의 네트워크 어댑터를 확인했을 때

관리자는 화면에 노드를 표시할때 노드관점 또는 장비관점을 선택적으로 사용할 수 있습니다.

네트워크 노드 감지

Genian ZTNA는 네트워크센서 또는 에이전트를 통해 네트워크의 노드를 감지합니다. 네트워크센서는 네트워크 상에 발생되는 ARP broadcast 패킷을 통해 새로운 네트워크 노드가 연결되었음을 감지할 수 있습니다. 만약 네트워크에 새로운 노드가 연결되었을 경우 DHCP와 같은 broadcast 패킷을 통해 수신된 이더넷 프레임을 분석하여 새 노드가 연결 되었는지 확인합니다.

노드를 인식하는 또 다른 방법은 엔드 포인트 시스템에 에이전트를 설치하는 것입니다. 에이전트는 시스템의 IP / MAC 을 포함하여 다양한 정보를 수집하여 정책서버로 전송하고 노드로 등록합니다.

노드 정보 수집

네트워크센서는 노드로부터 수동적&능동적 방법 모두를 사용하여 정보를 수집합니다.

수동적 방법으로는 노드에서 주기적으로 발생되는 DHCP, NetBIOS, UPNP 및 mDNS와 같은 패킷에 포함된 정보를 수신하여 노드에 영향을주지 않고 정보를 수집할 수 있습니다.

능동적 방법으로는 포트 스캔을 통해 노드에 의해 제공된 서비스를 체크하고, 각 서비스에 따라 요청을 통해 정보를 수집합니다. 예를 들어, 노드가 HTTP 서비스를 제공하는 경우 TCP 80 포트를 통해 네트워크센서는 정보를 얻기 위해 최상위 페이지를 요청합니다.

능동적으로 수집된 정보는 대상 항목과 수집 기간을 설정할 수 있습니다. 자세한 내용은 다음을 참조하십시오. gathering-options

4.2.2 Genian Device Platform Intelligence (GDPI)

GDPI란 무엇인가?

오늘날 업무 환경에서 개인용 장비를 사용하는 BYOD 또는 모든 IT 장비가 네트워크에 연결되는 IoT는 네트워크를 이전보다 복잡하고 다양한 위협에 노출되게 합니다.

IT 관리자는 인증된 장비만 네트워크에 연결할 수 있도록 함으로써 여러 위협으로부터 네트워크를 보호해야 합니다. 그러나 조직의 여러 액세스 포인트에 연결된 다양한 장비를 식별하고 관리하는 것은 쉽지 않습니다.

Genian ZTNA는 Device Platform Intelligence를 제공하여 관리자가 장비들을 더욱 쉽게 관리할 수 있도록 합니다.

첫째, Device Platform Intelligence는 다양한 지능형 방법을 통해 네트워크에 연결된 장비의 제조업체, 제품 이름 및 모델명을 식별합니다. 식별된 장비 플랫폼을 통해 관리자는 장비가 보유한 다양한 정보를 조회할 수 있습니다.

- 장비 사진
- 장비 연결 유형 (유선, 무선)
- 장비의 EoL(End of Life) 상태
- 장비의 EoS(End of Sale) 상태
- 제조사
- 제조 국가
- 제조업체 비지니스 연속성 상태
- 제조업 자격취득

이러한 추가 정보를 통해 관리자는 네트워크상의 기기에 대한 가시성을 높여 IT를 보다 쉽게 관리할 수 있습니다.

장비 플랫폼 및 CVE

Common Vulnerabilities and Exposures (CVE)는 MITRE 에서 제공하는 IT 장비 및 소프트웨어의 취약점에 대한 데이터베이스입니다. 매월 1,000 건이 넘는 새로운 취약점이 발표되고 IT 관리자는 자신이 관리하는 IT 장비와 관련된 취약점을 식별해야합니다. Genian ZTNA는 네트워크에서 IT 장치를 식별하고 CVE를 표시하여 네트워크 관리를 보다 쉽게 할 수 있습니다.

장비 플랫폼을 찾는 방법

Genian ZTNA는 **네트워크센서** 가 수집한 다양한 정보를 활용하여 연결된 장비 플랫폼을 **감지** 합니다. 디바이스가 네트워크에 연결되면 센서와 패킷을 송수신하고, 센서는 디바이스가 서비스하고 있는 프로토콜의 정보를 얻을 수 있습니다. Genian ZTNA는 다음 프로토콜을 이용하여 장비 플랫폼 정보를 감지합니다.

능동적 방법

- HTTP / HTTPS 헤더 및 본문
- 웹 브라우저 사용자 에이전트
- TELNET / SSH / SMTP 배너
- 오픈 포트 (node-portscan)
- SNMP OID / Description
- SIP
- and more

수동적 방법

- 웹 브라우저 사용자 에이전트 (SPAN 포트 사용)
- MAC 주소
- 호스트 이름
- DHCP Request
- UPNP
- HPSLP
- and more

Genian ZTNA는 장비 플랫폼을 탐지하기 위해 자체 플랫폼 데이터베이스(GPDB)를 사용하고 있습니다. GPDB는 장비 정보와 일치하는 다양한 패턴을 통해 플랫폼이 정확하게 감지 되도록합니다. 최고의 정확도를 제공하기 위해 GPDB는 매주 업데이트 되어 시장에 출시된 최신 장비를 네트워크 내에서 신속하게 식별할 수 있습니다. (*Professional / Enterprise* 에디션의 *GPDB*는 매주 업데이트 되며, *Basic* 에디션의 *GPDB*는 매월 업데이트 됩니다.) 에디션 비교

노드 타입

각 장비 플랫폼에는 다음과 같은 노드 타입이 있습니다.

- 정책 서버
- 네트워크센서
- 가상 센서
- 스위치 포트
- 세컨더리 네트워크센서
- 가상 IP
- 무선 센서
- 정의되지 않음
- PC
- 모바일 단말
- 서버
- 네트워크 장비
- 무선 장비
- 라우터
- 스위치
- 보안 장비
- 프린터
- IP 전화
- 기타

이 노드 타입 정보를 기반으로 정책을 찾아 보거나 만들 수 있습니다.

Genian 플랫폼 데이터베이스 (GPDB)

GPDB는 GDPI와 관련된 장비 플랫폼 탐지 패턴 및 장비 플랫폼 정보를 저장하는 데이터베이스입니다. GPDB는 Genians의 장비 플랫폼 엔지니어를 통해 지속적으로 업데이트 됩니다. 따라서 추가 작업 없이 새로운 장비를 신속하게 감지할 수 있습니다.

마지막으로 업데이트 된 GPDB의 시간을 확인하려면

1. **시스템 > 업데이트 관리 > 운영정보 데이터** 로 이동합니다.

Device Platform Intelligence

Device Platform Intelligence 페이지를 통해 추가 장비 플랫폼 정보를 볼 수 있습니다.

개별 노드 정보를 보려면,

1. 상단 패널에서 **관리 > 노드** 로 이동합니다.
2. 원하는 **노드** 의 **플랫폼** 을 찾아서 클릭합니다.

노드 플랫폼을 수동으로 정의하기

1. 상단 패널에서 **관리 > 노드** 로 이동합니다.
2. 원하는 노드의 **IP 주소 선택**
3. **플랫폼상태** 탭에서 **플랫폼** 입력 **지정** 체크박스를 클릭하여 수동으로 입력
4. **수정** 버튼을 클릭합니다.

Note: 노드보기에서 플랫폼 이름 옆에 아이콘이 표시됩니다. 이 아이콘은 이것이 수동으로 정의되었음을 나타냅니다.

사용자 정의 노드 타입 작성

1. 상단 패널에서 **설정** 으로 이동합니다.
2. 왼쪽 설정 패널에서 **속성관리 > 노드타입 관리** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 노드타입명을 입력하고 아이콘 선택(커스텀 아이콘이 있는 경우 **추가** 버튼을 클릭하여 아이콘 이미지 파일을 업로드)
5. **생성** 클릭

Note: 사용자 정의 노드 타입을 수동으로 정의하고 노드에 추가해야합니다.

---

1. 상단 패널에서 **관리 > 노드** 로 이동합니다.
2. 원하는 노드의 **IP 주소** 를 클릭합니다.

아래에서 기본정보 탭

1. **노드타입** 의 **지정** 을 클릭하여 노드타입을 **수동으로 정의** .
2. **노드타입** 을 선택합니다.
3. **수정** 을 클릭합니다.

알 수 없는 / 잘못된 플랫폼 감지 보고

어떤 이유로 Genian ZTNA가 장비의 플랫폼을 감지 할 수없는 경우 다음 중 하나가 원인 일 수 있습니다.

- **정보 부족** : 장비가 패킷을 보내지 않거나 요청에 응답하지 않습니다. OS의 방화벽이 활성화 되어 있을 가능성이 있습니다.
- **GPDB에서 일치하는 패턴 없음** : 노드 정보에는 특정 플랫폼의 증거가 있지만 GPDB에는 아직 일치하는 패턴이 없습니다.

GPDB에 일치하는 패턴이 없는 경우 잘못된 플랫폼보고 대화 상자를 사용하여 해당 노드 정보를 Genian 클라우드로 보낼 수 있습니다. Genians가 보고서를 받으면 플랫폼 엔지니어가 패턴을 조사하여 GPDB로 업데이트 합니다.

알 수 없는 플랫폼 보고 기능 해제

기본적으로 Genian ZTNA는 알 수 없는 플랫폼 노드에 대해 잘못된 플랫폼 보고를 매일 전송합니다. 전송된 모든 정보는 장비 외부에서 읽을 수 있습니다. Genian Cloud에 잘못된 플랫폼 보고 전송을 비활성화하려면 다음 단계를 따릅니다.

1. 상단 패널의 **설정** 으로 이동합니다.
2. **환경설정 > 노드관리** 로 이동합니다.
3. **노드정보 검색 > 플랫폼미탐지보고** 옵션을 **OFF** 로 설정합니다.
4. 수정 버튼을 클릭합니다.

4.2.3 노드 관리 및 필터

센서 및 그룹 항목

센서 및 그룹 항목을 사용하면 노드를 빠르고 체계적으로 볼 수 있습니다. 상단 항목에서 **관리 > 노드** 를 클릭합니다.

- **센서 탭** : 모든 네트워크에 속한 모든 노드, 감지 된 네트워크 및 센서가 표시 됩니다.

*(*센서를 클릭하면 해당 센서와 관련된 모든 노드가 표시 됩니다.*)*

- **그룹 탭** : 현황 그룹 또는 정책 그룹별로 분류 된 모든 노드 및 노드가 표시 됩니다.

현황 & 필터 항목

현황 & 필터 항목에서 사전 정의된 필터를 사용하여 노드를 필터링 할 수 있습니다.

1. 상단 항목에서 **관리 > 노드** 를 클릭 하세요.
2. 왼쪽 항목의 **현황 & 필터** 에서 **항목** 을 클릭 한 다음 **하위 항목** 을 클릭합니다.

*(*항목을 클릭하면 항목 내의 노드에 대한 요약보기가 표시 됩니다.*)*

특정 Sensor가 관리하는 노드에서 "Microsoft Windows"로 사전 정의 된 필터를 보려면 :

1. 상단 항목에서 **관리 > 노드** 를 클릭합니다.
2. 왼쪽 항목의 **센서** 탭으로 이동합니다. 특정 센서를 클릭합니다.
3. 왼쪽 아래 항목에서 **현황 및 필터** 로 이동합니다. **노드 그룹 > 확인 > Microsoft Windows** 를 클릭합니다.

주 노드보기 화면에서 특정 센서가 관리하는 "Microsoft Windows" 노드 만 표시 됩니다.

현황 및 필터 사용자 정의

사용하지 않는 불필요한 카테고리는 숨길 수 있습니다.

1. 상단 항목에서 **관리 > 노드** 를 클릭합니다.
2. 왼쪽 항목에서 **현황 및 필터** 를 찾으십시오. **현황 및 필터** 왼쪽 항목의 오른쪽 상단에있는 **수정** 아이콘을 클릭합니다.
3. **드래그 앤 드롭** 원하지 않는 카테고리를 **선택** 에서 **사용 가능**
4. **수정** 을 클릭합니다.

Note: 사용자 정의 현황 및 필터는 현재 관리자의 보기에만 영향을 미칩니다.

네트워크센서로 노드 찾기

1. 상단 항목에서 **관리 > 노드** 로 이동합니다.
2. 왼쪽 항목의 **센서** 탭으로 이동합니다.
3. 검색을 사용하려면 검색 아이콘을 클릭합니다.
4. 네트워크센서의 이름 또는 `IP` 입력
5. 특정 센서 선택
    - 결과를 사용할 수없는 경우 공백을 입력하고 Enter 키를 눌러 전체 센서를 확인합니다.

Note: 네트워크센서 위치를 기반으로하는 기본 노드보기의 노드가 표시됩니다.

여러 센서에 대한 하위 폴더 편집 및 만들기

1. 상단 항목에서 **관리 > 노드** 로 이동합니다.
2. 왼쪽 항목의 **센서** 탭으로 이동합니다.
3. 오른쪽 상단의 **트리 편집** 아이콘을 클릭합니다.
4. 센서 선택 및 드래그 앤 드롭으로 네트워크센서 재배치
    - 네트워크센서가 많은 경우 만들기 옵션을 선택하여 하위 폴더를 만들 수 있습니다

노드 그룹 별 노드 찾기

1. 상단 항목에서 **관리 > 노드** 로 이동합니다.
2. 왼쪽 항목의 **그룹** 탭으로 이동합니다.
3. 사이트 이름 아래에는 **노드 그룹** 이 포함되어있는 네 개의 **노드 카테고리** 가 있습니다.
    - **Identification**
    - **Categorization**
    - **Compliance**
    - **카테고리 미지정**

Note: 이것들은 기본적으로 제공되지만, 노드 그룹 관리 로 가서 다른 것을 만들 수 있습니다.

센서 및 노드 그룹에 대한 노드 카테고리 편집 및 만들기

1. 상단 항목에서 **관리 > 노드** 로 이동합니다.
2. 왼쪽 항목의 **그룹** 탭으로 이동합니다.
3. 오른쪽 상단의 **트리 편집** 아이콘을 클릭합니다.
4. **센서** 또는 **노드 그룹** 을 할당하려면 사이트 이름을 마우스 오른쪽 버튼으로 클릭합니다.
   - **네트워크센서** 가 많은 경우에는 **생성** 옵션을 선택하여 하위 폴더를 생성 할 수 있습니다.
   - 할당을 선택하고 전환하여 **센서** 또는 **노드 그룹** 에 대한 옵션을 확인합니다.
5. 검색을 클릭하고 **체크 박스** 를 클릭합니다.
6. **확인** 을 클릭합니다.

다양한 보기로 노드 목록 표시

다양한 관점을 통해 **노드** 를 탐색 할 수 있습니다.

1. 상단 항목에서 **관리 > 노드** 로 이동합니다.
2. **작업** 버튼 오른쪽의 **메뉴** 아이콘을 클릭합니다.
3. **보기 기준 > 노드 별** 또는 **장비 별** 를 선택합니다.
4. 다음 관점에서 봅니다.
   - **요약뷰**
   - **노드뷰**
   - **IP관리뷰**
   - **위험뷰**
   - **운영체제 업데이트뷰**
   - **자산관리뷰**
   - **에이전트액션뷰**
   - **인증사용자뷰**
   - **장치사용 관리뷰**
   - **장비수명주기 관리뷰**

세부 정보 찾기

1. 상단 항목에서 **관리 > 노드** 로 이동합니다.
2. **노드** 의 원하는 **IP 주소** 를 찾아서 클릭합니다.
3. 포함 할 일반 정보 및 기타 정보 찾기 :
    - 에이전트가 설치되지 않은 경우
    - **기본 정보** - *IP, MAC, IPv6, IPv6* 링크 로컬, 호스트 이름, 플랫폼, 플랫폼 인텔리전스, 연결 유형, 사용자 인증, *RADIUS* 계정 세션 등
    - **장비 정보** - 이름, 장치 *ID,* 장치 수명주기, 장치의 노드
    - **네트워크 정보** - 트래픽, *WLAN, TCP* 연결, 서비스, 포트 열기
    - **이력 관리** - 로그, 현황 로그
    - **IP 관리** - *IP* 및 *MAC* 정책
    - **정책** - 인증 정책, 호스트 이름 정책, 노드 관리 옵션
    - **정책 현황** - 노드 정책, 적용 정책, 노드 그룹, 위험감지, 에이전트 액션 수행 결과
    - 에이전트가 설치된 경우 추가 탭이 있습니다. (표시된 정보는 할당 된 플러그인에 따라 다를 수 있습니다)
    - **기본 정보**
    - **장비 정보**
    - **시스템 정보** - 마더 보드, 메모리, 디스크, *OS,* 네트워크 연결, 인터페이스, 공유, 사용자 계정, *USB* 장치, 모니터, 프린터
    - **네트워크 정보**
    - **소프트웨어 정보** - 안티 바이러스 소프트웨어, 설치된 프로그램
    - **운영체제 업데이트 정보** - *Windows OS* 업데이트
    - **이력관리**
    - **IP관리**
    - **정책**
    - **정책 현황**

노드 세부정보 검색

모든노드 또는 선택한 센서/그룹에서 원하는 조건의 노드를 검색하는 방법:

1. 관리WebUI > 노드 메뉴 진입
2. 좌측 트리화면에서 전체노드 또는 센서/그룹 선택
3. 우측 리스트창 상단 검색란 클릭
4. 드롭다운 메뉴에서 검색할 속성 선택 및 MYSQL 연산자 선택
5. 찾고자하는 검색어 입력 후 검색버튼 클릭

- **지원하는 노드속성 :**
    - **IP**
    - **MAC**

- **현황**
- **노드 타입**
- **노드 정책**
- **제어 정책**
- **도메인**
- **인증 사용자명**
- **인증 사용자 아이디**
- **부서**
- **호스트명**
- **노드이름**
- **노드 설명**
- **플랫폼**
- **장비 이름**
- **장비 설명**
- **스위치**
- **스위치 포트**

기타 다수 지원

4.2.4 노드 태그 할당

태그 노드(MAC+IP) 또는 장비(MAC)에 적용되는 관리자 지정 꼬리표로 이런 꼬리표들을 직접 관리할 수 있습니다.

하나 이상의 태그를 노드 또는 장비에 적용할 수 있습니다. 태그는 로그 검색필터 기능을 통해 자동으로 적용되거나 노드그룹 조건으로 사용될 수도 있습니다.

노드태그는 MAC+IP주소 쌍에 적용됩니다. 정책을 추적하거나 정책을 특정 MAC주소에서 사용하는 단일 IP주소에 적용하는데 적합합니다. 노드태그는 MAC+IP에 적용되므로 고정IP, DHCP로 인한 IP변경, 단말의 네트워크 변경으로 인해 IP가 변경될때 태그가 장비를 따라가지 않습니다. 변경된 IP주소+MAC주소는 새로운 노드로 간주됩니다.

반대로 MAC 태그는 특정 MAC주소를 가진 모든 노드에 적용됩니다. 따라서 MAC태그는 DHCP를 사용하는 단말 또는 정기적으로 IP가 변경되는 장비 및 모바일 장비에 사용하는데 적절합니다.

- 노드, 장비, 사용자에 특정 감사로그가 발생하는 경우 검색필터를 이용하여 노드에 태그 자동설정 및 태그를 이용한 정책적용 연계에 활용
- 태그를 활용할 수 있는 정책: 노드정책, 제어정책, 장치제어, IP관리

기간설정	설명	자동해제 유무
무제한	태그가 설정된 이후 해제가 자동으로 수행되지 않습니다.	X
기간	태그가 설정된 이후 정해진 일자를 기준으로 해제가 수행됩니다.	O
기간+해제시각	태그가 설정된 이후 정해진 일자와 시간을 기준으로 해제가 수행됩니다.	O

Note: 태그를 할당할 수 있는 관리자 계정에 제한 설정은 다음 관리자 계정 참고하시기 바랍니다.

태그 생성

1. 상단 패널의 **설정** 으로 이동
2. **속성관리 > 태그 관리** 로 이동
3. **작업선택 > 생성**
4. **태그이름** 의 경우 고유 이름을 입력합니다.
5. **설명** 의 경우 이 태그의 용도에 대해 설명합니다.
6. **색상** 의 경우 원하는 색 선택을 클릭하고 **확인** 를 클릭합니다.
7. **기간설정** 의 경우, 이 옵션은 할당 및 만료에 대한 선택 사항입니다.
8. 관리자별로 사용가능한 태그를 할당하고 싶은 경우 **관리역할 제한** 에 체크를 하고 관리자를 선택합니다.
9. **저장** 을 클릭합니다.

개별 노드에 대한 태그

1. 상단 패널의 **관리 > 노드** 로 이동합니다.
2. **노드** 의 원하는 **IP 주소** 를 찾아 클릭합니다.
3. 노드상세정보 하단 **태그** 항목으로 이동
4. 태그주체(노드,MAC), 태그명, 태그할당시각을 선택하거나 입력
5. **추가** 버튼을 클릭합니다.
6. 화면 상단 **수정** 버튼을 클릭합니다.

여러 노드에 대한 일괄 태그

1. 상단 패널의 **관리 > 노드** 로 이동합니다.
2. 원하는 노드의 **체크박스** 를 찾아 클릭합니다.
3. **작업선택 > 노드 및 장비 > 노드 태그 설정** 선택합니다.
4. 노드 태그 설정 팝업창에서 태그설정 조건을 먼저 선택합니다.(선택한 태그 추가, 교체, 삭제, 설정된 태그 모두 삭제 중 택일)
5. 원하는 **태그** 를 목록에 **체크박스** 를 선택합니다.(하나 이상의 옵션을 선택할 수 있음)
6. **설정** 을 클릭합니다.
7. 선택 한 노드에 **태그** 설정이 일괄 적용 되었는지 노드리스트에서 확인합니다.

MAC 태그

1. 상단 패널의 **관리 > 노드** 로 이동합니다.
2. MAC태그를 설정할 노드의 **IP 주소** 클릭합니다.
3. 노드상세정보 하단 **태그** 항목으로 이동
4. 태그주체(노드,MAC), 태그명, 태그할당시각을 선택하거나 입력
5. **추가** 버튼을 클릭합니다.
6. 화면 상단 **수정** 버튼을 클릭합니다.

Note: 특정 MAC 주소에 태그를 할당 할 때, 해당 MAC 주소의 모든 노드에도 태그가 자동으로 할당 됩니다.(장비 기준의 태그 설정)

개별 노드에 대한 태그 해제

1. 상단 패널의 **관리 > 노드** 로 이동합니다.
2. **노드** 의 원하는 **IP 주소** 를 찾아 클릭합니다.
3. 노드상세정보 하단 **태그** 항목에 추가된 태그 우측 **삭제** 를 클릭합니다.
4. 상단 **수정** 버튼을 클릭합니다.

여러 노드에 대한 태그 해제

1. 상단 패널의 **관리 > 노드** 로 이동합니다.
2. 원하는 노드의 **체크박스** 를 찾아 클릭합니다.
3. **작업선택 > 노드 및 장비 > 노드 태그 설정** 선택합니다.
4. 노드 태그 설정 팝업화면에서 패널의 왼쪽 상단 모서리에 있는 드롭다운항목의 **선택한 태그 삭제** 를 선택합니다.
5. 원하는 **태그명** 에 **체크박스** (하나 이상의 옵션을 선택할 수 있음)
6. **설정** 을 클릭합니다.
7. 선택 한 노드에 **태그** 삭제가 일괄 적용 되었는지 노드리스트에서 확인합니다.

Note: **설정된 태그 모두 삭제** 를 선택하여 노드에서 모든 태그를 제거합니다.

MAC에 대한 태그 해제

1. 상단 패널의 **관리 > 노드** 로 이동합니다.
2. **노드** 의 원하는 **IP 주소** 를 찾아 클릭합니다.
3. 노드상세정보 하단 **태그** 항목에 추가된 태그 우측 **삭제** 를 클릭합니다.
4. 상단 **수정** 버튼을 클릭합니다.

로그 필터로 태그 지정

특정 로그가 발생할 때 자동으로 노드에 태그를 지정하거나 태그를 해제 할 수 있습니다.

- 로그 검색필터 생성에 대한 자세한 내용을 보려면 다음을 참고합니다. 검색필터 생성
- 로그 검색필터를 사용한 태그 지정에 대한 자세한 정보 참고: 로그 발생 시 태그 할당

4.2.5 노드 관리

Note: 등록된 노드의 상태 확인 부분은 node-updown-status 문서를 참고하시기 바랍니다.

노드 추가

Genian ZTNA는 자동으로 활성 노드를 감지하여 노드 목록에 등록합니다. 또한 노드가 네트워크에 액세스하기 전에 노드를 허용하거나 거부할 때 노드를 사전 등록하고 사용 할 수 있습니다.

1. 상단 항목의 **관리 > 노드** 로 이동합니다.
2. **작업선택 > 노드장비관리 > 노드등록** 를 클릭합니다.
3. **노드등록** 팝업창에 내용을 입력합니다.

IP만 입력하거나 MAC만 입력하거나 둘 다 입력하여 노드를 등록 할 수 있습니다.(기타 값은 선택 사항)

1. **IP** 는 `IP` 주소 를 입력합니다.
2. 연속으로 노드의 IP를 여러개 등록하려면 **미사용 IP 다중등록** 항목을 선택합니다.
3. **특정 IP 정책을 설정하기 원한다면 IP 정책설정 항목을 선택합니다.**
    - **IP 허용 - 충돌보호 해제**
    - **IP 허용 - 충돌보호 설정**
4. 노드의 사용 시작 기간을 설정합니다. **IP 사용 시작** 체크 후 달력에서 시작 날짜 및 시간을 선택합니다.
5. 노드의 사용 종료 기간을 설정합니다. **IP 사용 종료** 체크 후 달력에서 시작 날짜 및 시간을 선택합니다.
6. **IP 사용 신규노드정책**
    - **MAC 허용**
    - **충돌보호 설정**
    - **변경금지 설정**
    - **충돌보호 설정 / 변경금지 설정**
7. **MAC** 은 `MAC` 주소 를 입력합니다.
8. 특정 MAC 정책을 설정하기 원한다면 **MAC정책설정** 항목을 선택합니다.
9. 노드의 사용 시작 기간을 설정합니다. **IP 사용 시작** 체크 후 달력에서 시작 날짜 및 시간을 선택합니다.
10. 노드의 사용 종료 기간을 설정합니다. **IP 사용 종료** 체크 후 달력에서 시작 날짜 및 시간을 선택합니다.
11. **관리센서** 노드는 등록 할 센서의 위치를 선택합니다.
12. **노드타입** 등록 할 노트 타입을 선택합니다.
13. **노드삭제 금지** 노드를 삭제 할 수 있는지에 대한 `on` 또는 `off` 여부를 선택합니다.
14. **등록** 버튼을 클릭합니다.

노드 일괄등록

CSV 파일을 사용하여 한 번에 여러 노드를 등록 할 수 있습니다.

1. 상단 항목의 **관리 > 노드** 로 이동.
2. **작업선택 > 노드장비관리 > 노드일괄등록**
3. 노드일괄등록 선택 후 **CSV** 의 **파일선택** 메뉴를 클릭합니다.
4. 파일 탐색기에서 등록포맷에 대한 생성 된 CSV 파일 을 선택합니다.
5. 노드를 등록할 드롭다운 메뉴에서 적절한 **센서** 를 선택합니다.
6. **가져오기** 버튼을 클릭합니다.

Note: CSV 파일의 형식이 올바르지 않으면 노드가 등록되지 않습니다.

노드삭제

비활성 노드 데이터를 삭제하여 네트워크 노드 보기를 더 잘 구성 할 수 있습니다. 정책을 통해 비활성 노드를 삭제할 수 있으며, 또는 노드를 네트워크에서 더 이상 찾을 수 없으므로 수동으로 삭제합니다.

비활성 노드 수동으로 삭제

1. 상단 항목의 **관리 > 노드** 로 이동
2. 원하는 비활성 노드를 찾아 **체크박스** 을 클릭합니다.
3. **작업선택 > 노드장비관리 > 노드삭제** 를 클릭합니다.

Warning: 네트워크에 연결되고 동작 중인 노드를 실수로 삭제하면 해당 노드가 즉시 새롭게 등록 됩니다.

정책을 통해 비활성 노드 제거

1. 상단 항목의 **정책** 으로 이동
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책 항목에서 **정책이름** 을 찾아서 선택합니다.
4. 노드정책 항목에서 **관리정책 > 비활성노드삭제**
5. 일정 기간 비활동 후 노드 삭제 시간을 설정: `30` (일정 기간 노드가 오프라인 일 경우 자동으로 삭제 됩니다. 기본값은 *30*일)
6. **수정** 을 클릭합니다.
7. 오른쪽 상단 모서리에서 **변경정책적용** 을 클릭합니다.

오래 된 노드 삭제

정책 서버는 IP가 변경된 후 다운상태의 노드 정보를 기본적으로 최대 3 일 동안 유지합니다.

1. **설정 > 환경설정 > 노드관리 > 노드정리**
2. **IP변경노드삭제** 메뉴 찾기
3. 노드 IP변경 시 설정된 날짜 이상 다운상태를 유지하는 오래 된 노드를 삭제 할 시간을 설정합니다. : 3 (기본값은 *3*일입니다.)
4. **수정** 을 클릭합니다.
5. 오른쪽 상단 모서리에서 **변경정책적용** 을 클릭합니다.

노드 호스트명 모니터링

호스트명 정책을 준수하기 위해 신규노드를 선별할 수 있습니다.

노드 정책에 따라 노드에 허용되는 호스트명을 지정 할 수 있습니다. 허용 된 노드 호스트명에 대한 기준은 인증 된 사용자 속성, IP주소 또는 템플릿을 기반으로 구성 할 수 있습니다.

1. 관리 WebUI 접속
2. 상단 **정책** , 좌측 패널의 **정책 > 노드정책**
3. 변경할 노드정책명을 클릭
4. **관리 정책** 의 **신규노드 호스트명제한** 항목 **On**
5. 표준 호스트명을 입력하거나 **설정** 을 클릭하여 템플릿을 설정할 수 있습니다.

윈도우 호스트 이름은 **호스트명 변경** 플러그인을 사용하여 변경할 수 있습니다.

참고: 호스트명 변경

노드바구니 사용법

노드바구니는 테스트나 모니터링 지정 노드 작업 등 다양한 관리 목적으로 사용할 수 있는 그룹화 툴입니다. 정책에는 사용할 수 없습니다.

노드바구니에 추가

1. 상단 **관리 > 노드** 이동
2. 원하는 노드를 찾아 좌측 **체크박스** 에 체크
3. **작업선택 > 노드 및 장비 > 노드바구니에 담기** 클릭
4. 팝업창에서 **확인** 클릭(추가된 노드는 좌측 **센서트리의 노드바구니** 항목에서 확인 가능)

노드바구니에서 제거

1. 상단 **관리 > 노드** 이동
2. 좌측 센서트리에서 노드바구니 항목을 선택
3. 우측 노드리스트에서 제거할 노드의 체크박스 선택
4. 상단 **선택 노드바구니 비우기 OR 전체 노드바구니 비우기** 클릭
5. 팝업창에서 **확인** 클릭

노드 타입 확인하기

노드타입은 네트워크 센서와 에이전트에서 수집되는 정보를 기반으로 시스템에서 정의된 항목으로 분류하는 추가적인 정보입니다.

Note:

1. 노드타입에 대한 분류에 대한 부분은 다음에 *Genian Device Platform Intelligence (GDPI)* 부분을 참고하시기 바랍니다.
2. 노드타입을 사용하여 노드그룹을 생성하는 부분은 다음에 노드그룹 상세정보 부분을 참고하시기 바랍니다.

노드 타입 신규로 생성하기

GDPI를 통해 식별된 장비 플랫폼을 시스템에서 관리하기 위해 노드타입을 지정하게 됩니다. 이때 시스템에서 정의된 노드타입이 아닌 사용자가 정의한 노드타입을 사용하기 위해서는 별도의 노드타입을 생성해야 합니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **노드타입 관리** 를 선택합니다.
3. **작업선택** 에서 **생성** 을 클릭합니다.
4. 이름과 아이콘을 설정한 후 **생성** 을 클릭합니다.

노드 타입 지정하기

시스템에서 정의된 노드타입은 시스템에서 자동으로 지정되나 사용자가 정의한 노드타입은 수동으로 지정해야 합니다.

Note: 확인된 노드타입으로 지정할 경우 수집되는 정보에 의한 노드타입 정보와 비교할 수 있습니다.

---

1. 노드타입을 지정할 **노드** 를 검색합니다.
2. 노드 IP를 선택하여 **노드정보 탭** 을 확인합니다.
3. **플랫폼상태** 항목에서 **노드타입, 지정, 확인된 노드타입** 부분을 설정합니다.
4. **수정** 버튼을 클릭합니다.

항목	설명
노드타입	시스템에서 자동으로 지정되는 타입으로 수집된 정보를 기반으로 지정됩니다. 수집되는 정보가 변경되면 노드타입은 변경됩니다.
노드타입(지정)	시스템에서 자동으로 지정되는 타입이 아닌 관리자가 수동으로 지정합니다. 수집되는 정보가 변경되더라도 타입은 지정된 형태로 유지됩니다.
노드타입(확인된)	시스템에서 자동으로 지정되는 타입과 별개로 관리자가 수동으로 지정합니다. 수집되는 정보가 변경되면 노드타입은 변경되나 확인된 노드타입은 지정된 형태로 유지됩니다.

4.2.6 노드 그룹 관리

노드 그룹 만들기

노드 그룹 은 **노드** 들의 그룹으로 특정 조건 기반의 유사함이 있습니다. **노드 그룹** 을 사용하면 여러 노드에 대해 동일한 작업을 동시에 수행할 수 있습니다. Genian ZTNA는 **노드정책** 및 **제어정책** 에 적용할 수 있는 두 가지 유형의 노드 그룹을 제공합니다.

- **정책 그룹**: 노드 타입, IP / MAC 정보, 사용자 정보, 인증 등과 같은 노드 관련 정보를 기반으로 하는 그룹입니다.
- **상태 그룹**: 노드 상태 및 관련 조건 결과에 의해 측정된 노드 상태를 기반으로 하는 그룹입니다.

1. 상단 항목에서 **정책** 을 클릭 하십시오.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 정책그룹 생성** 또는 **작업선택 > 상태그룹 생성** 을 클릭합니다.

아래 **기본정보** 를 설정합니다.

1. **Category** 의 경우 기본값 또는 새로 만들어 사용합니다.(*Node Groups*를 분류 할 수 있습니다)
2. **ID** 의 경우 고유 이름을 입력합니다.
3. **설명** 이 노드그룹에 대한 내용을 작성합니다.
4. **적용모드** : **사용함** 설정
5. 그룹 조건 설정:
   - 조건연산: “**AND**” or “**OR**” (”*AND*” 는 모든 조건이 만족되어야합니다. “*OR*” 는 조건 중 하나만 만족해도 됩니다)
   - 조건설정: **추가** 를 클릭합니다. (이 조건은 적절한 그룹화에 적용할 다양한 조건입니다.)
6. **추가** 버튼을 클릭합니다.
7. **생성** 버튼을 클릭합니다.
8. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

노드그룹 가져오기 / 내보내기

Genian ZTNA는 관리 WebUI에서 만들어져있는 노드그룹들을 내보내거나 가져오는 기능을 JSON형태 파일로 제공합니다.

다음 단계를 따르십시오:

1. 상단 **정책** 메뉴 클릭
2. 좌측 **그룹 > 노드** 클릭
3. 내보낼 노드그룹 좌측 체크박스를 선택
4. 상단 **작업선택** 버튼 클릭
5. **노드그룹 내보내기** 선택시 확장자 JSON형태의 파일이 PC에 다운로드
6. 가져오기는 상단 **작업선택 > 노드그룹 가져오기** 선택하여 JSON형태의 파일을 선택합니다.

4.2.7 노드 상세정보

Genian ZTNA에서 수집하는 정보 중 노드와 관련된 세부정보와 정책현황을 표시할 수 있습니다. 노드 상세정보는 네트워크 센서에 의해 수집되는 정보와 에이전트에 의해 수집되는 정보, 노드가 적용받는 정책으로 나눠지며 해당 정보를 통해 단말에 현황을 확인할 수 있습니다.

노드 상세정보에서는 대상노드작업 명령을 통해 노드에 적용되어 있는 정책을 확인하거나 정책을 재적용 할 수 있으며, 에이전트 관련 실시간 적용기능을 적용할 수 있습니다.

노드 상세정보 확인하기

1. 상단 패널에 **관리 > 노드** 로 이동합니다.
2. 상세정보를 확인할 노드의 **IP** 를 클릭합니다.
3. 우측에 표시되는 **노드 상세정보** 를 확인합니다.

항목(탭 이름)	수집주체	수집내용
노드정보	네트워크 센서	IP, MAC, 동작상태, 플랫폼 상태값등을 확인
장비정보	네트워크 센서	장비기반에 노드 리스트를 확인할 수 있으며, 장비 수명주기 관련 항목을 입력할 수 있습니다.
네트워크 정보	네트워크 센서	열린포트 및 탐지된 서비스 항목을 확인
	에이전트 플러그인(네트워크 정보수집, TCP 세션검사, 무선랜제어)	트래픽, AP(접속한 Access Point 정보), TCP세션(세션 상태) 정보를 확인
시스템 정보	에이전트 플러그인(하드웨어 정보수집, 모니터 정보수집, 네트워크 공유폴더, WMI 정보수집, 모양 및 개인설정)	시스템의 하드웨어 및 운영체제 정보를 확인
소프트웨어 정보	에이전트 플러그인(소프트웨어 정보수집)	시스템에 설치된 소프트웨어 정보를 확인
운영체제 업데이트 정보	에이전트 플러그인 (Windows 업데이트)	Windows OS 업데이트 정보를 확인
정책	정책서버	노드에 적용된 IP관리 정책과 사용자 인증정책을 확인
정책현황	정책서버	노드에 적용된 노드정책, 제어정책, 장치제어정책등을 확인
Malware	에이전트 플러그인 (Malware Detector)	단말에서 발생한 악성코드 정보를 확인
이력관리	정책서버(로그서버)	노드의 IP와 MAC을 기반으로 발생한 감사로그를 확인

4.2.8 노드그룹 상세정보

Genian ZTNA에서 생성할 수 있는 노드그룹은 타입은 노드정책 전용 노드그룹(정책그룹)과 일반 노드그룹(상태그룹)으로 나눠집니다.

일반적으로 노드그룹은 정책을 수립할 경우 사용되며, 노드정책과 제어정책에서 사용될 수 있습니다.

노드정책 전용 노드그룹 생성 조건 확인하기

노드정책 전용 노드그룹은 노드 타입, IP / MAC 정보, 사용자 정보, 인증 등과 같은 노드 관련 정보를 기반으로 하는 그룹입니다.

노드정책 전용 노드그룹은 노드정책에서 사용할 수 있습니다.

항목	설명
IPv6 주소	노드의 IPv6 주소를 기반으로 그룹을 생성합니다.
IP관리	ZTNA에서 사용하는 IP관리정책을 기반으로 그룹을 생성합니다.
IP주소	노드의 IPv4 주소를 기반으로 그룹을 생성합니다.
MAC+IP주소	노드의 IPv4 주소와 MAC 값을 기반으로 그룹을 생성합니다.
MAC주소	노드의 MAC 값을 기반으로 그룹을 생성합니다.
노드타입	ZTNA에서 분류한 노드타입을 기반으로 그룹을 생성합니다.
등록여부	정책서버에 등록된 노드를 기반으로 그룹을 생성합니다.
등록일자	ZTNA에 등록된 노드의 시간을 기반으로 그룹을 생성합니다.
센서	네트워크 센서 및 센서에 등록된 노드를 기반으로 그룹을 생성합니다.
시간	시간 객체를 기준으로 현재시간 기반에 그룹을 생성합니다.
에이전트	ZTNA 에이전트의 설치/동작 기반에 그룹을 생성합니다.
인증사용자	ZTNA의 사용자 인증기능 사용 시 인증된 사용자 기반에 그룹을 생성합니다.
장비소유자	노드에 설정된 장비소유자 정보를 기반으로 그룹을 생성합니다.
정책그룹	정책그룹을 포함하는 정책그룹을 생성합니다.(정책그룹을 조건으로 생성하는 레벨은 1단계만 가능)
태그	노드에 설정된 태그 정보를 기반으로 그룹을 생성합니다.

일반 노드그룹 생성 조건 확인하기

일반 노드그룹은 노드 상태 및 관련 조건 결과에 의해 측정된 노드 상태를 기반으로 하는 그룹입니다.

Note: 일반 노드그룹은 노드정책 전용 노드그룹에 설정조건을 모두 포함하고 있지만 노드정책에서는 사용할 수 없습니다.

분류	설명	항목
정책	ZTNA에서 정의한 정책을 기반으로 그룹을 생성합니다.	IP관리, 노드그룹, 노드정책, 인증사용자, 태그, 호스트명 제한
		트래픽, 플랫폼, 호스트/도메인명
에이전트 정보	에이전트에서 수집한 정보를 기반으로 그룹을 생성합니다.	USB 장치정보, WMI 정보수집, 가동시간, 계정비밀번호검증, 네트워크, 백신정보
		소프트웨어, 시스템, 시스템사용자 계정, 에이전트 상태, 에이전트 액션, 운영체제 업데이트
장비정보	장비에 설정한 정보를 기반으로 그룹을 생성합니다.	장비명, 장비설명, 제조일, 구입처, 내용연수 시작일, 내용연수 만료일
		일련번호, 구입가격, 책임자, 책임부서, 메모
추가설정정보	GPI 연동정보 및 추가필드에 설정한 정보를 기반으로 그룹을 생성합니다.	GPI 점수, GPI 검사결과
미분류	분류로 정의되지 않은 조건들을 기반으로 그룹을 생성합니다.	등록여부, IPv6주소, IP주소, MAC+IP주소, MAC주소, NAT, 등록일자, 서약동의, 시간, 위험감지

4.3 IP 주소 모니터링

네트워크센서 는 IP 주소를 모니터링하고 직관적인 매트릭스보기를 통해 실시간으로 IP 주소의 사용 상태를 표시합니다. (*C Class* 서브넷 마스크)

4.3.1 센서 IP 상태 보기

네트워크센서를 통해 탐색 하고 IP관리 항목 에서 현재 상태를 볼 수 있습니다.

네트워크센서의 네트워크 별 전체 IP 사용 상태 보기

1. 상단 패널의 **관리 > IP주소** 로 이동 하십시오.
2. 왼쪽 IP주소 관리 항목에서 **네트워크센서** 이름을 클릭 하십시오.

4.3.2 매트릭스 뷰를 사용하여 IP 상태 찾아보기

직관적인 매트릭스 뷰 를 통하여 **IP 사용량** 과 **현재 상태** 를 볼 수 있습니다.

각 네트워크 별 IP 주소가 사용되는 방법 찾기

1. 상위 항목의 **관리 > IP주소** 로 이동 하십시오.
2. 왼쪽 IP주소 관리 항목에서 **네트워크센서** 이름을 클릭 하십시오.

세부 사항 찾기

1. 상위 항목의 **관리 > IP주소** 로 이동 하십시오.
2. 왼쪽 IP주소 관리 항목에서 **네트워크센서** 이름을 클릭 하십시오.
3. **IP 주소 블록** 위로 마우스 를 가져 가면 자세한 정보를 볼 수 있습니다.

4.4 스위치 모니터링

특정 스위치 포트의 연결 상태 (*up / down*), 포트 보안 상태 레벨, 802.1x 정보, 트래픽, 사용률 등 얼마나 많은 장치가 연결되어 있는지 확인 할 수 있습니다.

4.4.1 스위치 찾아보기

스위치 를 식별하기 위해 Genian ZTNA는 **SNMP 요청** 을 전송합니다. 요청에 대한 응답이 OID(dot1dBaseBridgeAddress(1.3.6.1.2.1.17.1.1.1))로 반환되는 경우 Genian ZTNA는 **MAC 주소** 를 **스위치** 의 라벨로 지정합니다. **스위치가 공용 커뮤니티 문자열에서 식별되지 않으면 커뮤니티 문자열 구성을 확인하거나, SNMPWALK 명령어를 실행하여 스위치가 제대로 응답하는지 확인하십시오.**

네트워크센서에서 노드 스캔 주기 설정

1. 상위 항목에 있는 **시스템** 으로 이동
2. 왼쪽 시스템 관리에서 **시스템 목록 > 센서** 로 이동 하십시오.
3. **네트워크센서 IP** 를 클릭 하십시오.

설정 탭에서 다음을 수행:

1. **센서설정** 을 클릭 하십시오.

서브넷 노드스캔 에서

1. **수행주기** 의 시간 간격을 수정합니다. (*10* 분 - *1* 년)
2. **수정** 버튼을 클릭하여 업데이트합니다.

SNMP 검사를 위한 SNMP 설정하기

1. 상단 항목의 **설정** 으로 이동 하십시오.
2. 왼쪽 설정 메뉴에서 **환경설정 > 노드관리** 로 이동합니다.

아래에서 **SNMP 검색**:

1. SNMP 설정에 대해 **추가** 를 클릭합니다.

1. **SNMP 버전** 의 경우 `Version 2c` 또는 `Version 3` 을 선택합니다.
2. Version 2 의 경우 **Community** 에 read/write 커뮤니티 문자열을 설정합니다. (예: *public,private*)
3. Version 3 의 경우 **Username** 과 적절한 **Security Level** 을 선택합니다.
4. **Security Level** 에는 `NoAuth/NoPriv`, `Auth/NoPriv`, and `Auth/Priv` 가 있습니다.

1. **네트워크 정보 수집** 이 필요한 경우 **On** 설정. (*SNMP* 정보를 *Off* 로 설정하면 수집되지 않습니다)
2. **검색주기** 의 수행 시간을 수정합니다. (*5* 분 – *1* 년)
3. 특정 시간에 수행하기 위한 **시간객체** 를 설정합니다.
4. SNMP를 즉시 검색하려면 **지금시작** 버튼을 클릭 하십시오.

Windows 단말에서 SNMPWALK를 사용하여 스위치 응답 확인

Note: 스위치 목록에 스위치 정보가 없다면 먼저 스위치의 커뮤니티 문자열을 확인 한 다음 SNMPWALK를 실행하십시오.

---

1. **스위치** 에 로그인하고 SNMP 커뮤니티 문자열을 확인 하십시오.
2. Genian ZTNA 에 올바른 **SNMP 커뮤니티 문자열** 이 설정되어 있는지 확인 하십시오.
3. Windows 단말과 Net-SNMP를 사용하여 다음을 수행 하십시오.
    - Windows 용 **Net-SNMP** 다운로드 (기본 폴더 위치를 *C: Net-SNMP*로 설정하여 쉽게 찾을 수 있음)
    - 명령 프롬프트를 열고 디렉토리를 변경 하십시오. (이동 경로: **cd /Net-SNMP/bin**)
    - 다음 명령을 사용하여 snmpwalk를 실행하십시오. snmpwalk -Os -c public -v 2c "Switch-IP".1.3.6.1.2.1.17.1.1 (예 : *snmpwalk-Os -c public -v 2c 192.168.50.5 .1.3.6.1. 2.1.17.1.1*)

- **mib-2.17.1.1.0 = Hex-STRING: XX XX XX XX XX XX** 이 표시 되어야합니다. (스위치가 *SNMP* 요청에 올바르게 응답 함을 표시합니다)

읽기 / 쓰기 커뮤니티 설정

1. 상단 항목에서 **관리 > 스위치** 로 이동 하십시오.
2. 왼쪽 스위치 관리 창에서 **스위치관리** 폴더를 찾아 클릭 하십시오.
3. 전체 스위치 창에서 원하는 **스위치** 이름을 찾아 클릭 하십시오.
4. **SNMP 커뮤니티** 문자열을 **읽기/쓰기 커뮤니티** 필드에 입력 하십시오.
5. **수정** 버튼을 클릭 하십시오.

4.4.2 스위치 포트

스위치 포트 찾아보기

스위치 포트 목록은 네트워크에서 감지된 모든 **스위치 포트** 에 대한 자세한 정보를 제공합니다. **스위치 포트 목록** 은 왼쪽 상단에 있는 **스위치 관리 항목** 으로 이동한 후 스위치 포트를 클릭하면 볼 수 있습니다.

스위치 관련 정보

1. **관리 > 스위치** 로 이동 하십시오.
2. 원하는 **스위치 이름** 을 찾아 클릭합니다.
3. 다음과 같은 정보를 찾습니다.
    - **스위치** - 스위치 호스트명
    - **이름** - 스위치 포트 번호
    - **설명** - 스위치 포트 설명
    - **접속사용자** - 연결 된 스위치 포트를 통해 인증 된 사용자의 전체 이름
    - **접속호스트** - 연결된 스위치 포트를 통해 확인 된 단말의 호스트명
    - **IP / MAC** - 스위치 포트를 통해 연결 된 IP / MAC 정보
    - **노드** - 스위치 포트를 통해 연결 된 노드의 수
    - **MACs** - 스위치 포트를 통해 연결 된 MAC 의 수
    - **연결방식** - 스위치 포트를 통해 연결 된 연결 방식
    - **연결** - 스위치 포트 링크의 UP/Down 상태
    - **관리자 Down** - 관리자에 의한 포트 셧다운
    - **Duplex** - 링크 전이중/반이중 설정 정보
    - **속도** - 포트 속도 정보
    - **트래픽** - 스위치 포트 트레픽(byte/s)
    - **Utilization** - 스위치 포트 이용률 %
    - **VLAN ID** - 포트에 할당 된 VLAN ID

- **Trunk Port** - 트렁크 포트 설정의 활성화 여부 표기: `trunk` or 공란
- **포트보안** - Port Security 설정 상태: `On` or `Off`
- **802.1x 설정** - 802.1x 설정 상태: `Enable` or 공란
- **허용MAC개수** - 인증 MAC Address 개수

노드바구니에 담기

1. 상위 항목의 **관리 > 스위치** 로 이동 하십시오.
2. 추가할 **스위치 포트** 를 찾아 **체크박스** 클릭합니다. (포트에 노드가 하나 이상 연결되어 있는지 확인)
3. **작업선택 > 노드바구니에 담기** 를 클릭합니다.
4. **확인** 클릭합니다. (노드가 노드바구니에 추가 되면 관리 > 노드뷰에 표기 됩니다)

노드바구니로 부터 삭제

1. 상단 항목의 **관리 > 노드** 로 이동 하십시오.
2. 왼쪽 항목의 **센서 탭 > 노드바구니** 로 이동 하십시오.
3. **노드 바구니** 창에서 **노드** 를 찾으십시오. **체크박스** 클릭합니다.
4. 오른쪽 상단에 있는 **선택 노드바구니 비우기** 버튼을 클릭합니다. (노드바구니 전체를 삭제하려면 전체 노드바구니 비우기를 클릭 하십시오)

스위치 포트 검색

관리 뷰 상단에 있는 **검색 입력창** 을 사용하여 **스위치** 및 해당 정보를 검색할 수 있습니다. 검색할 수 있는 세부 정보는 스위치, 이름, 설명, 접속사용자, 접속호스트 또는 MAC/노드 수입니다.

스위치 포트 설명 변경

1. 상단 항목에 있는 **관리 > 스위치** 로 이동 하십시오.
2. **이름** 열에서 **스위치 포트** 을 찾아 클릭합니다.

기본정보 탭에서

1. **설명 입력란** 에서 설명을 입력합니다.
2. **수정** 을 클릭합니다.

스위치 포트 VLAN ID 변경

1. 상단 항목에 있는 **관리 > 스위치** 로 이동 하십시오.
2. **이름** 열에서 **스위치 포트** 을 찾아 클릭합니다.

기본정보 탭에서

1. **VLAN ID** 에서 설정하고자 하는 VLAN ID를 입력합니다.
2. **수정** 을 클릭합니다.

Note: 설명, VLAN ID를 변경하려면, 해당 스위치에 대한 쓰기 권한이 있는 read/Write Community 값 또는 SNMPv3 Username을 지정해야합니다.

4.4.3 스위치 현황정보 설정 및 확인하기

스위치로 탐지된 대상에 정보 수집을 설정할 수 있으며 수집된 정보를 확인할 수 있습니다.

Note:

1. SNMP Read Community 를 사용하여 정보수집을 진행할 수 있습니다.
2. SNMP Write Community 를 사용할 경우 스위치의 설정을 변경할 수 있습니다.

스위치 정보 확인하기

시스템에 의해 스위치로 분류된 대상에 대해서 수집된 정보를 확인할 수 있습니다. 수집되는 정보는 다음과 같습니다.

항목	설명
스위치 ID	스위치의 MAC을 나타냅니다.
스위치명	스위치의 이름을 나타냅니다.
IP주소	스위치에 설정된 관리 IP를 표시합니다.
가용/전체 포트	스위치 포트 중 사용하는 포트의 개수와 전체 포트의 개수를 표시합니다.
포트보안	특정 포트에 특정 MAC 주소를 지정하는 포트보안 지원 여부를 나타냅니다.
802.1x	802.1x 지원 여부와 현재 사용 여부를 나타냅니다.
갱신시각	스위치 정보를 갱신한 시각을 나타냅니다.
동작시간	스위치의 동작 시간을 나타냅니다.
시리얼넘버	스위치의 시리얼넘버 표시합니다.
모델명	스위치의 모델명을 표시합니다.
설명	스위치에 대한 설명을 표시합니다.

스위치 포트 정보 확인하기

스위치의 포트마다 설정된 항목을 확인할 수 있습니다. 확인할 수 있는 정보는 다음과 같습니다.

1. 상단 패널에 **관리 > 스위치** 로 이동합니다.
2. 왼쪽 메뉴에서 **전체스위치포트** 를 선택합니다.
3. 확인하고 싶은 포트의 **이름** 을 클릭합니다.

항목	설명
스위치명	스위치를 구분하는 이름이 표시됩니다.
이름	스위치 포트의 이름이 표시됩니다.
포트#	포트 번호를 표시합니다.
설명	ZTNA에서 임의의 값을 설정할 수 있습니다.
타입	포트의 타입(전화라인, 파워라인 등등)을 표시합니다.
연결상태	현재 포트 사용 여부를 표시합니다.
Duplex	인터페이스의 Duplex 모드가 표시됩니다.
속도	포트에 설정된 속도가 표시됩니다.
트래픽	SNMP 검색주기 동안의 트래픽량을 1초당 트래픽량(bps)으로 나누어 표시됩니다.
Utilization	트래픽 사용률을 나타내며, 사용률이 높을 경우 과부화가 일어날 수 있습니다.
수신	수신 누적 트래픽량이 표시됩니다.
전송	전송된 누적 트래픽량이 표시됩니다.
노드	포트에 연결된 시스템에서 관리하는 노드수가 표시됩니다.
Trunk Port	포트의 Trunk Port 설정 유무가 표시됩니다.
포트보안	포트보안 설정 유무가 표시됩니다.
포트보안상태	포트보안이 설정되었을 때 포트보안의 상태가 표시됩니다.
802.1x 설정	802.1x의 설정 유무가 표시됩니다.
802.1x 상태	802.1x가 설정되었을 때 802.1x의 상태가 표시됩니다.
허용 MAC 개수	해당 포트로 연결할 수 있는 MAC 개수가 표시됩니다.
MACs	포트에 연결된 MAC 수가 표시됩니다.
기본 VLAN	VLAN Tag가 설정되지 않은 VLAN ID가 표시됩니다.
VLAN ID	포트가 속한 VLAN ID가 표시됩니다.
관리자 Down	관리자에 의한 포트 Down 여부가 표시됩니다.

스위치 정보 수집 설정하기

스위치에서 정보를 수집하기 위한 SNMP 설정을 할 수 있습니다.

스위치 설정사항 중 Write Community 값을 설정할 경우 다음에 항목에 설정을 변경할 수 있습니다.

Note:

1. 스위치 포트에 설정된 기본 Vlan ID
2. 스위치 포트에 할당된 Vlan ID
3. 스위치 포트에 대한 관리자 Down 상태 변경

항목	설명
SNMP 정보수집	스위치 정보수집을 비활성화 할 수 있습니다.
SNMP 버전	SNMP 통신을 위해 SNMP 버전을 선택 할 수 있습니다.
Read Community	SNMP의 RO 권한의 Community를 설정 할 수 있습니다.
Write Community	SNMP의 RW 권한의 Community를 설정 할 수 있습니다.
Write Memory 설정	스위치의 설정값 저장 기능을 사용할지 여부를 설정합니다.

4.5 무선랜 모니터링

내장 무선 어댑터가 있는 네트워크센서는 네트워크를 검색하여 모든 내부 및 인접 무선 SSID를 탐지합니다. 정책 서버는 엔드포인트에 설치된 에이전트와 통신하여 내장 무선 어댑터를 활용하여 SSID 정보를 수집하고 내부 SSID와 인접 SSID를 검색할 수 있습니다. **관리 > 무선랜** 항목을 통해 정책을 모니터링, 관리 및 적용하기 위한 그룹을 생성합니다. (무선 어댑터가 없으면 *WLAN SSID*를 감지할 수 없습니다)

4.5.1 무선랜 AP 탐지

무선 네트워크를 지원하는 단말을 찾아 **무선랜 AP** 상태(*SSID* 사용 여부, 보안 상태, 주파수, *802.11* 프로토콜, 신호 강도, 감지 날짜, 연결된 무선 장비 등) 정보를 확인할 수 있습니다. 무선랜 모니터링을 위해서는 네트워크센서에 무선NIC가 있거나 엔드포인트에 무선랜제어 플러그인이 활성화된 에이전트가 설치되어 있어야합니다.

네트워크에서 탐지된 모든 SSID보기

1. 상단 항목에서 **관리 > 무선랜** 으로 이동 하십시오.

테이블 열의 사용자 지정

1. 무선랜 노드 목록 왼쪽 위의 **작업선택** 을 클릭합니다.
2. **관리뷰 편집** 을 선택합니다.
3. 열 제목을 **사용 가능** 에서 **선택** 항목으로 이동하여 목록에 추가 하십시오.
4. 드래그앤드롭으로 순서 변경이 가능합니다.
5. 수정 버튼을 클릭 하십시오.

SSID 검색

관리 > 무선랜 기본 항목 상단에 있는 검색창를 사용하여 SSID 및 해당 정보를 검색 할 수 있습니다. 검색할 수 있는 항목은 **SSID, MAC 주소, 제조업체** 입니다.

무선랜 현황 및 필터

무선랜은 현황 & 필터 항목에서 미리 정의된 필터로 필터링 할 수 있습니다.

무선 접속정보 보기

Station 는 **STA** 라고도 하며 802.11 프로토콜을 사용 할 수 있는 기능을 가진 장비입니다.

접속 세부정보 보기

1. 상단 항목의 **관리 > 무선랜** 으로 이동합니다.
2. 메인 **무선랜** 목록에서 **접속(전체)** 열을 클릭하여 정렬합니다.(각 MAC 주소에 대한 여러 접속 현황 기반으로 열을 정렬합니다)
3. **원하는 단말의 접속(전체) 열 에서 숫자 를 클릭합니다.**
    - 이제 MAC 주소에 대한 모든 접속정보를 보고 **외부/내부** 보기를 변경할 수 있습니다.
    - **검색창** 을 사용하여 특정 **접속정보** 를 볼 수 있습니다. (외부/내부 또는 내부 검색 간에 검색을 필터링할 수 있습니다)

SSID 물리적 위치 찾기

BYOD 환경에서 많은 장비들이 불특정 시간에 나타나며 이를 추적하는 것은 상당히 어려운 일입니다. 어떤 장비가 네트워크 내부 또는 외부에 있는지 알아 내려면 해당 장비의 실제 위치를 찾기 위해 여러 단계가 필요합니다.

장비와 연결된 SSID를 확인

악성 장비가 네트워크에 나타나면 이를 추적하는 첫 번째 단계는 연결된 SSID를 찾는 것입니다.

1. 상단 항목에 있는 **관리 > 노드** 로 이동합니다.
2. 원하는 노드의 **IP 주소** 를 클릭합니다.
3. **기본정보** 아래 **접속AP** 에 표시되는 **SSID** 를 클릭합니다.

이제 해당 SSID와 관련된 모든 정보가 메인 항목에 표시 됩니다

장비의 신호 강도 보기

단말의 상대적 위치는 신호의 강도를 모니터링하여 어느 방향과 어느 정도 가까운지 파악 할 수 있습니다. 신호가 강할수록 단말의 위치는 가까워집니다.

신호 강도는 두 가지 방법으로 표기 됩니다.

- **색상 / 아이콘** : 빨간색은 약한 것을 의미하고, 주황색은 이상 신호를 의미하고 녹색은 강한 신호 연결을 의미합니다.
- **dBm** : 신호의 데시벨 강도입니다. 수치가 낮을수록 신호가 강해지고 단말의 위치가 가까워집니다.

이제 장비를 상대적 위치까지 추적 할 수 있습니다. 그런 다음 장비를 찾거나 찾을 때까지 직원에게 해당 단말에 대해 문의할 수 있습니다.

4.5.2 내부 SSID 탐지

SSID는 **내부 AP** 에서 **인접 AP** 로 구분 됩니다.

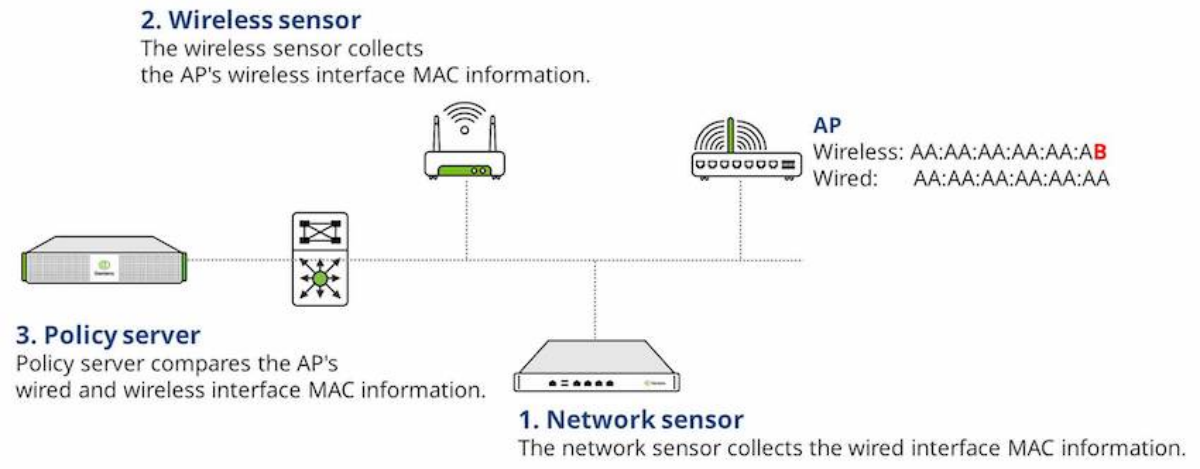
내부 SSID 표시

1. 상단 항목에서 **관리 > 무선랜** 으로 이동 하십시오.
2. 기본 무선랜 창에서 **내부** 컬럼명 열을 찾아 클릭하십시오. 모든 내부 AP는 이 컬럼에서 확인 표시로 식별됩니다.

내부 AP 찾는 방법

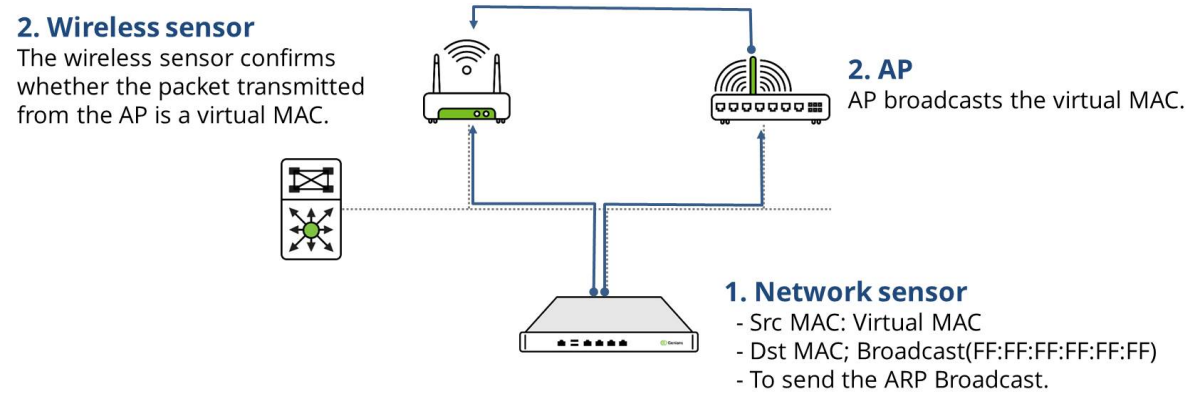
Agent와 무선센서에 의해 탐지된 AP는 내부적으로 연결된 AP에 의해 여러 기준에 의해 구별될 수 있습니다. 내부 AP 감지 방법은 다음과 같습니다.

MAC 유사성 검사



1. 네트워크센서는 내부적으로 연결된 AP의 유선 인터페이스 MAC 정보를 수집합니다.
2. 무선센서는 AP의 무선 인터페이스 MAC 정보를 수집하여 이를 정책서버로 보냅니다.
3. 정책서버는 AP의 유선 및 무선 인터페이스 MAC 정보를 비교하여 유사성이 확인되면 AP가 내부 네트워크에 연결되어 있다고 판단합니다.

Packet broadcasting



1. 네트워크센서는 가상 MAC을 네트워크에 브로드 캐스팅합니다.
2. 이때 내부 네트워크에 연결된 AP는 네트워크센서에서 수신한 가상 MAC을 AP의 무선 대역으로 브로드 캐스팅합니다.
3. 무선센서는 무선 네트워크를 모니터링하고 무선 센서가 AP로부터 가상 MAC을 수신하면 AP를 내부 AP로 판단합니다.

에이전트

1. 에이전트는 사용자 단말에서 탐지된 모든 무선 네트워크 인터페이스 정보를 수집합니다.
2. 알려진 무선 네트워크 인터페이스 MAC 주소와 SSID MAC 주소를 매칭 시킵니다.

무선 컨트롤러가 포함된 SNMP

1. SNMP를 사용하여 무선 컨트롤러에서 정보를 수집합니다.
2. 무선 컨트롤러의 알려진 MAC 주소와 SSID MAC 주소를 매칭 시킵니다.

4.5.3 무선 그룹 생성

무선 그룹 은 식별자로 설정된 조건 또는 속성으로 인해 함께 그룹화된 **SSID** 의 감지된 수량입니다. 이는 네트워크 관리자가 대량의 SSID를 처리할 때 특정 **SSID** 또는 **카테고리** 로 신속하게 이동 할 수 있도록 하기 위한 것입니다.

무선랜 그룹 생성

무선랩 그룹을 생성하여 SSID 를 더 효율적으로 분류 할 수 있습니다.

1. 상단 항목에서 **정책** 로 이동 하십시오.
2. **그룹 > 무선랜** 으로 이동 하십시오.
3. **작업선택 > 생성** 을 클릭 하십시오.

아래 **기본정보** 에서:

1. **그룹ID** 를 생성하기 위한 고유의 이름을 입력합니다.
2. **설명** 의 경우 이 그룹을 구성하는 내용에 대해 입력합니다.
3. **적용모드** 의 경우 드롭다운에서 **사용함** 을 선택합니다.
4. **감사로그** 의 경우, SSID가 그룹에 추가 될 때 로그를 생성하려면 **On** 을 설정합니다.

그룹조건 에서 다음을 수행합니다.

1. **조건연산** 의 경우 모든 조건을 일치하기 위해 **AND** 를 선택하고, 특정 조건에 일치하기 위해서는 **OR** 를 선택 하십시오.
2. **조건설정** 에서 **추가** 를 클릭하여 조건을 추가합니다.

조건설정 에서 다음을 수행:

다음은 SSID 를 식별 할 수 있도록 해주는 조건부 설정입니다.

1. **항목** 의 경우 MAC, 프로토콜, SSID, 보안 설정, 태그 등을 선택 할 수 있습니다.
2. **조건** 의 경우 다음과 같거나, 같거나, 포함하지 않거나, 포함하지 않는 등의 항목을 선택 할 수 있습니다.
3. **설정** 의 경우 검색한 값과 일치하는 값을 입력합니다.
4. **설정메모** 의 경우 이 그룹이 수행하는 작업 설명을 입력합니다.

5. **추가** 버튼을 클릭 하십시오.
6. **생성** 버튼을 클릭 하십시오.

무선랜 태그 할당

SSID에 태그를 지정하여 분류하고 다음 태그를 사용하여 정책을 생성 할 수 있습니다.

1. 상단 패널의 **관리 > 무선랜** 으로 이동합니다.
2. 원하는 **SSID 의 체크박스** 를 찾아 클릭 하십시오.
3. **작업선택 > 무선랜 태그설정** 을 클릭 하십시오.

아래와 같이 **무선랜 태그 할당** :

1. 드롭 앤 다운 항목에서 **선택한 태그 추가** 선택합니다.
2. **설정** 버튼을 클릭 하십시오.

무선랜 그룹 할당

태그, SSID 이름, 벤더, 보안 설정, 프로토콜 등을 기반으로 서로 유사한 SSID를 그룹화 할 수 있습니다.

1. 상단 항목의 **관리 > 무선랜** 으로 이동합니다.
2. 원하는 **SSID** 의 **체크박스** 를 찾아 클릭합니다.
3. **작업선택 > 무선랜 그룹할당/해제** 선택합니다.

아래 **무선랜 그룹** 을 할당합니다.

1. 동작선택에서 **무선랜그룹 지정** 또는 **무선랜그룹 해제** 를 선택 하십시오.
2. 무선랜 식별에서 **SSID, MAC** 또는 **MAC+SSID** 를 선택 하십시오.
3. **무선랜 그룹** 의 경우 연관 된 그룹입니다.
4. **설정** 을 클릭합니다.
5. **변경정책적용** 을 클릭합니다.

무선랜 센서 별 그룹

무선랜 센서가 많은 경우 하나의 목록에서 모든 센서를 관리하기가 어렵습니다. 여기에서 그룹을 만들고 무선랜 센서 를 할당 할 수 있습니다.

1. 상단 항목에서 **관리 > 무선랜** 으로 이동 하십시오.
2. 오른쪽 상단의 **트리 편집 아이콘** 을 클릭 하십시오.
3. **전체 무선랜 AP** 또는 **전체 무선랜 클라이언트** 에서 마우스 오른쪽 버튼을 클릭하고 **생성** 을 선택 하십시오.(새 노드 그룹이 나타나 이름을 변경합니다)
4. 새로 생성 된 그룹을 마우스 오른쪽 버튼으로 클릭하고 **할당** 을 클릭 하십시오.
5. **무선 센서** 를 검색하고 이 그룹에 추가 할 각 **체크박스** 를 선택합니다.
6. **선택확인** 을 클릭 하십시오.

Note: 전 세계에 사업장이 있는 경우 국가 **그룹** 을 만들고 해당 **국가** 에 있는 **무선랜 센서** 를 추가 할 수 있습니다 .

4.5.4 무선랜 그룹 세부 설정하기

무선랜을 제공하는 AP(Access Point)에 대해서 별도의 조건을 기반으로 무선랜그룹을 생성할 수 있습니다.

Note: 무선랜 그룹을 조건으로 노드그룹을 생성하여 정책에 사용할 수 있습니다.

조건항목	설명
802.11 프로토콜	무선접속에 대한 기본 프로토콜을 조건으로 설정합니다.
MAC+SSID	AP의 MAC과 AP의 SSID 값을 매칭하여 조건으로 설정합니다.
MAC주소	AP의 MAC을 조건으로 설정합니다.
SSID	AP에서 전송하는 SSID를 조건으로 설정합니다.
무선랜그룹	기존 생성된 무선랜그룹을 포함하는 조건을 설정합니다.
보안설정	무선랜의 인증방식과 프로토콜을 조건으로 설정합니다.
상태 및 속성	무선랜의 연결 상태값을 조건으로 설정합니다.
인가상태	AP로 등록된 노드의 차단상태를 조건으로 설정합니다.
태그	AP에 등록된 태그 정보를 조건으로 설정합니다.

무선랜 그룹 세부 항목값

무선랜 그룹 생성 시 설정값을 간략하게 설명합니다.

+=============+===========+==============================+=====================================
| 조건 | 항목 | 설정값 | 설명 |+=============+===========+==============================+=====================
| 보안설정 | 인증방법 | PSK (Pre-Shared Key) | 무선 네트워크를 사용하기 위하여 정의된 암호화 Key 사용하는
방식 | + + +----------------------------+---+ | | | 801.1x (EAP
프로토콜) | 무선 네트워크를 사용하기 위해 세션별 암호화 key 사용하는 방식 | + +-----------+-----------------
-----------+---+ | | 프로토콜 | Open, WEP, WPA, WPA2 |
무선 네트워크를 사용하기 위한 Key의 암복호화 방식 | +-------------+-----------+----------------------------+------
---+ | 상태 및 속성 | | ADHOC | Device(LAN Card)에서 다른
Device(AP) 없이 네트워크 망을 구성하는 형태 | + + +----------------------------+-----------------------------------
---------------------------------+ | | | SoftAP | 무선랜 Client를 Software로 AP 역할을 수행하도록 구성하는 형태
| + + +----------------------------+---+ | | | 내부망 | AP에서
제공하는 네트워크 대역이 ZTNA에서 관리하는 내부망일때의 속성값 | +-------------+-----------+-------------------
---------+---+

4.5.5 무선랜 현황 확인하기

무선랜 네트워크 AP와 Client 정보를 수집하여 현황 정보를 확인하거나, 필요없는 서비스를 제공하는 AP와 Client 접속 현황을 확인할 수 있습니다.

Note:

1. 무선랜 제어 플러그인 **AP 정보 수집 대상** 설정을 사용하여 무선랜 AP 정보를 수집할 수 있습니다.
2. 무선랜 제어 플러그인 **무선 연결 이력 정보 수집** 설정을 사용하여 무선랜 Client 정보를 수집할 수 있습니다.
3. 무선랜 제어 플러그인 설정은 다음에 무선랜 제어 참고하시기 바랍니다.

무선랜 AP 현황 확인하기

무선랜 관리 > 전체 무선랜 AP 에서 AP 정보 수집 대상이 설정된 단말에서 수집된 정보를 확인할 수 있습니다.

항목	설명
내부	수집된 AP의 정보가 내부 네트워크에 연결되는지 여부를 표시합니다.
접속(내부)	해당 AP를 사용하는 내부 네트워크에 등록된 Client 갯수
접속(전체)	해당 AP를 사용하여 무선랜을 사용하는 Client 전체 갯수
동작	AP의 동작상태를 표시합니다.
SSID	AP가 전송하는 SSID(Service Set IDentifier)를 표시합니다.
MAC	서비스를 제공하는 AP의 BSSID(Basic Service Set Identifier)를 표시합니다.
제조업체	OUI를 기반으로 AP 제조업체명을 표시합니다.
암호화방식	무선랜 접속에 사용되는 암호화 방식을 표시합니다.
규약	무선랜 접속 시 IEEE 802.11에서 정의한 전송방식 표준 값이 표시됩니다.
채널	무선랜 주파수에 사용되는 채널을 표시합니다.
신호강도 (dBm)	값의 차이를 Log로 나타낸 (상대적) 스케일의 dBm 신호강도를 표시합니다.
위치	AP가 연결된 네트워크를 관리하는 네트워크 센서 이름을 표시합니다.
등록시각	AP가 최초로 등록된 시각을 표시합니다.

무선랜 접속 Client 현황 확인하기

무선랜 관리 > 전체 무선랜 Client 에서 무선 네트워크 접속 정보가 수집된 대상에 정보를 확인할 수 있습니다. (Windows OS 한정)

항목	설명
MAC	무선랜 인터페이스의 MAC 정보가 표시됩니다.
NIC 벤터	OUI(Organizationally Unique Identifier) 값을 기반으로 제조사 정보가 표시됩니다.
접속 AP	무선 네트워크 접속 지점을 표시합니다.
IP	무선 네트워크 접속 시 할당 받은 IP가 표시됩니다.
상태	무선 네트워크 접속 상태가 표시됩니다.
호스트명	단말에 호스트명이 표시됩니다.
인증사용자	ZTNA 사용자 인증 시 인증된 사용자 이름이 표시됩니다.
부서명	ZTNA 사용자 인증 시 인증된 사용자가 소속된 부서명이 표시됩니다.
위치	접속된 네트워크를 관리하는 네트워크 센서가 표시됩니다.
최근 접속 일자	무선 네트워크에 접속된 최근 시간이 표시됩니다.
등록시각	무선 네트워크 접속 정보가 최초 수집된 시각이 표시됩니다.

4.6 대시보드 관리

대시보드는 위젯의 집합입니다. 대시보드는 사용자에게 가장 중요한 보고서와 메트릭스의 개요를 제공합니다. 위젯을 사용자 정의하여 대시보드를 개인화 할 수 있습니다. 기본적으로 Genian ZTNA는 146개의 위젯을 제공합니다.

4.6.1 대시보드 추가

요구 사항에 따라 대시보드를 추가, 삭제 및 사용자 지정할 수 있습니다.

1. 메인화면 탭 우측 항목의 **탭추가** 를 클릭하십시오.
2. 대시보드 탭 추가 창에서 **탭 이름** 을 입력하십시오.
3. **확인** 버튼을 클릭하십시오.

4.6.2 대시보드 삭제

1. 삭제하고자 하는 탭의 이름에 마우스를 올려주십시오.
2. 이름 옆의 **삭제** 버튼을 클릭하십시오.
3. 확인창에서 **확인** 버튼을 클릭하십시오.

4.6.3 대시보드 위젯을 추가

1. 메인화면 상단 우측 항목의 **대시보드 설정** 으로 이동합니다.
2. **설정 > 위젯 추가** 를 클릭하십시오.
3. 위젯 추가 창에서 **위젯 카테고리** 항목을 찾습니다. **카테고리** 를 선택합니다.
4. 위젯 추가 창에서 **위젯** 항목을 찾습니다.
5. 원하는 위젯에서 **대시보드에 추가** 버튼을 클릭하십시오.

4.6.4 위젯 정렬

위젯은 제목 표시 줄에서 마우스 왼쪽 버튼으로 잡아서 원하는 위치로 끌 수 있습니다.

4.6.5 위젯 설정 사용자 정의

위젯 위에 마우스를 올리면 위젯의 오른쪽 상단에 기어 아이콘이 표시됩니다. 톱니바퀴 아이콘을 클릭하면 해당 위젯의 설정이 표시됩니다. 완료되면 저장을 클릭하여 설정 변경 사항을 위젯에 적용 할 수 있습니다.

4.6.6 위젯 삭제

1. 메인화면 상단 우측 항목의 **대시 보드 탭** 로 이동하십시오.
2. **위젯** 을 찾아 제목 표시 줄 위로 마우스를 가져갑니다.
3. **X** 버튼을 클릭하십시오.
4. **확인** 버튼을 클릭하십시오.

4.6.7 센서 맵 만들기

Google Maps를 사용하여 전 세계에 센서 배치를 모니터링하고 사용자 정의합니다.

- 센서 맵을 사용하기 위해 Google Maps API Key를 발급받아야 합니다.
- 사용을 위해 API Key 발급 안내 를 따라해주세요.
    1. 메인화면 탭 우측 항목의 **탭추가** 를 클릭하십시오.
    2. 대시보드 탭 추가 창에서 **탭 이름** 을 입력하십시오.
    3. **센서 맵** 을 활성화 시키십시오.
    4. **확인** 버튼을 클릭하십시오.
    5. 발급받은 **API Key** 를 입력하십시오.
    6. **확인** 버튼을 클릭하십시오.

4.6.8 센서 맵에 센서 배치

1. Sensor Map (센서 맵) 탭으로 이동합니다.
2. 화면 오른쪽 위 모서리에 있는 메뉴 찾기 아이콘을 클릭하십시오.
3. 센서 풍선 아이콘을 찾아 마우스를 통해 원하는 위치로 이동 시킵니다.

4.6.9 대시보드 내보내기

대시보드를 다음과 같은 여러 형식으로 내보낼 수 있습니다.

1. 메인화면 상단 우측 항목의 **대시보드 탭** 으로 이동하십시오.
2. 내보 낼 **대시보드 탭** 을 선택합니다.
3. **내보내기 아이콘** 를 클릭하면 팝업창이 출력됩니다.
4. 내보내기 파일 타입을 선택합니다.
5. 리포트 제목 페이지 표시 여부를 선택합니다.
6. 페이지 크기를 설정합니다.
   - A4,A3,A2,B4,B3,B2,LETTER 사이즈를 PORTRAIT/LANDSCAPE 별로 선택할 수 있습니다.
   - Custom 가로, 세로 크기 설정을 통해 대시보드에 출력되는 모든 위젯을 한 페이지로 출력할 수 있습니다.
7. **내보내기** 를 클릭합니다.

모바일 플랫폼 기반 사용자 정의 위젯 생성하기

모바일 플랫폼별 현황을 대시보드에서 모니터링할 수 있도록 설정할 수 있습니다. 모바일 플랫폼별로 노드그룹 생성 후, 위젯에 관심노드그룹으로 할당하여 사용할 수 있습니다. Android와 IOS 플랫폼의 노드를 모니터링하는 위젯 생성 방법을 안내합니다.

Step 1. 모바일 플랫폼 노드그룹 생성하기

노드그룹 생성 방법은 노드 그룹 관리 문서를 참고해주시기 바랍니다.

Android 노드그룹 생성하기

- 노드그룹 구분 : 노드그룹
- **그룹 조건**
  - 항목 : 운영체제유형
  - 설정 : Android

IOS 노드그룹 생성하기

- 노드그룹 구분 : 노드그룹
- **그룹 조건**
  - 항목 : 운영체제유형
  - 설정 : iPhone OS

Step 2. 위젯에 노드그룹 할당하기

1. 메인화면 상단 우측 항목의 **대시보드 설정** 으로 이동합니다.
2. **설정 > 위젯 추가** 를 클릭하십시오.
3. 위젯 추가 창에서 **위젯 카테고리** 항목을 찾습니다. **노드/장비** 항목을 선택합니다.
4. 위젯 추가 창에서 **노드그룹** 혹은 **노드그룹 카운트** 항목을 찾습니다.
5. **대시보드에 추가** 버튼을 클릭합니다.
6. 좌측 노드그룹 목록에서 생성한 노드그룹을 찾아 **관심노드그룹** 으로 이동시킵니다.
7. 타이틀, 화면갱신주기, 카운트사이즈, 이름사이즈를 설정합니다.
8. **저장** 버튼을 클릭합니다.

4.7 클라우드에서 노드 관리

Genian ZTNA Cloud Collector는 클라우드 환경에서 IP 지원 노드에 대한 정보를 수집하도록 활성화할 수 있습니다. 설정된 수행 주기로 Cloud Collector는 Cloud Service provider에게 쿼리하여 지정된 환경의 노드와 검색된 노드의 기타 중요한 클라우드 관련 세부 정보를 식별합니다.

4.7.1 클라우드 환경 구성

Cloud Provider 추가

클라우드와 관련한 다양한 작업을 위해, 클라우드 계정을 등록하고 관리하는 설정 화면 입니다.

1. 상단 메뉴에서 시스템 > Cloud Provider로 이동합니다.
2. 작업 선택을 클릭한 다음 생성을 클릭합니다.
3. 설정명 입력(예: 'AWS Cloud')
4. Cloud에 대해 "AWS", "AZURE", "NHN", "NAVER", "LINODE" 중 하나를 선택하십시오.
5. 아래 'Cloud 종류별 입력방법'을 참고하여 정보를 넣어주십시오.
6. 생성 클릭

Cloud 종류별 입력방법

- **AWS의 크리덴셜 정보**
  1. Access Key : AWS Console > 오른쪽 상단의 사용자 이메일 선택 > Security credentials(보안 자격 증명) 선택 > 'Access key' 확인 후 입력합니다.
  2. Secret Key : Access key 생성할 때 show(표시) 선택 > 'Secret key' 확인 후 입력합니다.
  - **AWS 계정의 IAM관련 활성화 되어야하는 정책**
  - 설정 경로 : AWS Console > IAM > Users > 사용자 아이디 > Permissions > Policy name
  - AdministratorAccess : AWS 서비스 및 리소스에 대한 전체 액세스를 제공합니다.
  - AmazonEC2FullAccess : AWS Management Console을 통해 Amazon EC2에 대한 전체 액세스를 제공합니다.

- AmazonRoute53FullAccess : AWS Management Console을 통해 모든 Amazon Route 53에 대한 전체 액세스를 제공합니다.
- AmazonS3FullAccess : AWS Management Console을 통해 모든 버킷에 대한 전체 액세스를 제공합니다.
- AWSMarketplaceFullAccess : AWS Marketplace 소프트웨어를 구독 및 구독 취소할 수 있는 기능을 제공하고, 사용자가 Marketplace '귀하의 소프트웨어' 페이지에서 Marketplace 소프트웨어 인스턴스를 관리할 수 있도록 하며, EC2에 대한 관리 액세스를 제공합니다
- AWSSupportAccess : 사용자가 AWS 지원 센터에 액세스할 수 있도록 허용합니다.
- CloudFrontFullAccess : CloudFront 콘솔에 대한 전체 액세스 권한과 AWS Management Console을 통해 Amazon S3 버킷을 나열하는 기능을 제공합니다.
- CloudWatchEventsFullAccess : Amazon CloudWatch Events에 대한 전체 액세스를 제공합니다.
- CloudWatchFullAccess : CloudWatch에 대한 전체 액세스를 제공합니다.
- SecurityAudit : 보안 감사 템플릿은 보안 구성 메타데이터를 읽을 수 있는 액세스 권한을 부여합니다. AWS 계정의 구성을 감사하는 소프트웨어에 유용합니다.

- **AZURE의 크리덴셜 정보**

1. Client ID : Azure Portal > Azure Active Directory > App registrations(앱 등록) > 'Application ID' 확인 후 입력합니다.
2. Client Secret : Home > Azure Active Directory > App registrations(앱 등록) > Certificates & secrets(인증서 및 암호) > 'Value' 확인 후 입력합니다.
3. Subscription ID : Home > Subscriptions > 'Subscription ID' 확인 후 입력합니다.
4. Tenant ID : Home > Azure Active Directory > App registrations(앱 등록) > 'Directory ID' 확인 후 입력합니다.
5. Resource Group Name : Home > Subscriptions > Subscription Name > Resource groups > 'Name' 확인 후 입력합니다.

- **Azure 계정의 IAM관련 활성화 되어야하는 정책**
- 설정 경로 : Access control(IAM) > View my access > Current role assignments > Role 항목
- Contributor : 모든 리소스를 관리할 수 있는 전체 액세스 권한을 부여하지만 Azure RBAC에서 역할을 할당하거나, Azure Blueprints에서 할당을 관리하거나, 이미지 갤러리를 공유할 수는 없습니다.
- User Access Administrator : Azure 리소스에 대한 사용자 액세스를 관리할 수 있습니다.
- Managed Application Operator Role: 관리형 애플리케이션 리소스에 대한 작업을 읽고 수행할 수 있습니다.

- **NHN의 크리덴셜 정보**

1. User Name : NHN Console 로그인 'ID'를 입력한다.
2. Tenant ID : Compute > Instance > 관리 페이지 > API 엔드포인트 설정 버튼 클릭 > 'Tenant ID' 확인 후 입력한다.
3. Password : Compute > Instance > 관리 페이지의 API 엔드포인트 설정 버튼 클릭 > 원하는 API 'Password' 지정 후 입력한다.

- **NHN 계정의 IAM관련 설정해야 할 프로젝트의 역할**
- 경로 : 해당 콘솔 로그인 > 맴버 관리 > IAM 맴버
- 프로젝트의 역할 설정은 ADMIN으로 한다.

  - 프로젝트 기본 정보, 멤버, 역할, 서비스 등 프로젝트 전체에 대한 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)가 가능하다.

- **NAVER의 크리덴셜 정보**

  1. Access Key : NCloud Console > 우측 상단 사용자 ID > 계정 관리 > 비밀번호 및 인증 > 인증키 관리 > 신규 API 인증키 생성 > 'Access Key ID' 확인 후 입력한다.
  2. Secret Key : API 인증키 생성 후 'Secret Key' 확인 후 입력한다.

  - **Naver 계정의 IAM관련 활성화 되어야하는 정책 항목**
  - 설정 경로 : 우측 상단 사용자 ID > 권한보기
  - 권한의 정책명은 NCP_ADMINISTRATOR(포털과 콘솔에 접근할 수 있는 권한이 메인 계정과 동일한 권한)로 설정한다.
  - 권한설정은 관리자 전용 메뉴로 좌측 상단에 서비스 환경 설정 > 구성원/권한 관리에서 설정한다.

- **LINODE의 크리덴셜 정보**

  1. Token : Linode Console > My Profile > API Tokens > Add a Personal Access Token > 'Key' 확인 후 입력한다.

  - **Linode 계정 관련 활성화 되어야하는 정책**
  - API Token 생성시 생성/삭제 등 모든 권한을 가지도록 설정한다.
  - 좌측 Account > User & Grants > 해당 유저의 User Permissions > Full Account Access로 설정한다.

클라우드 사이트 생성

SASE 구성을 설정하기 위한 설정 화면 입니다. 사이트 생성 및 관리를 통해 Cloud에 Service Edge(ZTNA Gateway, Hub)를 만들고 Service Edge에 연결할 Branch를 구성 할 수 있습니다.

1. 상단 메뉴에서 시스템 > 사이트로 이동합니다.
2. 작업을 클릭한 다음 생성을 클릭합니다.
3. 사이트명 입력 (예: '기업 hub' 또는 'VPC-XXXXXXXX')
4. 인프라의 경우 Cloud 선택
5. Cloud Provider의 경우 이전 단계에서 생성한 Cloud Provider를 선택합니다.
6. Region 의 경우 목록에서 원하는 AWS 리전을 선택합니다.
7. VPC ID의 경우 목록에서 원하는 VPC를 선택합니다.

Note: VPC가 나열되지 않으면 이전 단계와 로그를 확인하여 Cloud Provider를 추가할 때 문제가 없었는지 확인하십시오.

---

1. 타입에 대해 hub 또는 branch를 선택하십시오.
2. 네트워크 주소에 7단계에서 입력한 VPC에 해당하는 서브넷을 입력합니다(예: 172.31.16.0/20).
3. Collector 상태를 사용으로 설정(프록시 설정을 기본값으로 두고 원하는 수행 주기 설정)
4. 저장 클릭

클라우드 노드 감지 확인

센서에 의해 등록된 노드를 다양한 현황 및 필터를 사용하여 검색할 수 있는 페이지 입니다.

1. 상단 메뉴에서 관리 > 노드로 이동합니다.
2. 왼쪽 창에서 이전 단계에서 만든 사이트 이름을 클릭합니다.
3. 이전에 지정된 VPC 및 서브넷의 모든 AWS EC2 인스턴스는 노드로 나열되어야 합니다.
4. 검색된 노드에 대한 AWS 세부 정보는 노드 세부 정보를 볼 수 있습니다. 노드 세부 정보는 관리 > 노드로 이동하여 노드 IP를 클릭하고 AWS 섹션까지 아래로 스크롤하여 볼 수 있습니다.

Note: 노드 검색, 그룹화 및 모니터링에 대해서는 네트워크 노드 모니터링 를 참조 하십시오.

AWS Connector 설치

1. 상단 항목에서 **시스템 > 업데이트 관리 > 소프트웨어 > 정책서버 플러그인** 으로 이동 하십시오.
2. 작업선택 메뉴에서 플러그인 업로드를 선택하십시오.
3. 파일선택을 클릭하여 내컴퓨터에 다운로드 받은 AWS Connector를 업로드하십시오.
4. **시스템 > 업데이트 관리 > 소프트웨어 > 정책서버 플러그인** 메뉴의 목록에서 AWS Connector의 상태가 설치됨으로 변경되었는지 확인하십시오.

AWS Connector 설정

1. 상단 항목에서 **설정 > 환경설정 > AWS Connector** 으로 이동 하십시오.
2. AWS Connector 의 사용여부를 **주기적 수행** 또는 **지정시각 수행** 으로 변경하십시오.
3. AWS계정옵션의 **추가** 버튼을 클릭하십시오.
4. AWS의 계정정보(Access Key, Access Secret Key, Region)와 이 설정을 지정할 이름(Account Name)을 입력하십시오.
5. **추가** 버튼을 클릭 하십시오.
6. AWS Instance정보를 가져오는 수행주기를 설정하십시오.
7. 하단의 **수정** 버튼을 클릭하십시오.

AWS Instance 정보 확인

1. 상단 항목에서 **관리 > 노드** 으로 이동하십시오.
2. 좌측 트리 항목에서 AWS Connector 계정 설정시 지정한 이름을 선택하십시오.
3. 우측 보기 창에서 AWS EC2 서비스에서 생성한 Instance정보를 노드로 등록되었는지 확인하십시오.

Note: 검색, 그룹화 및 노드들을 모니터링을 위해서 네트워크 노드 모니터링 페이지를 참고하십시오.

4.8 네트워크 트래픽

4.8.1 Netflow Agent 기능 활성화

Genian ZTNA는 센서의 Netflow Agent 기능을 활용하여 네트워크 트래픽을 모니터링할 수 있습니다 이 연결된 장치의 흐름 정보는 ZTNA 정책을 시행하기 위한 중요한 구성 요소인 향상된 네트워크 가시성을 제공합니다. 활성화되면 Netflow Agent는 센서를 통해 흐르는 모든 트래픽의 Flow를 기록합니다. 로그인된 정보 흐름에는 다음이 포함되지만 이에 국한되지는 않습니다.

- **소스 IP 주소**
- **대상 IP 주소**
- **프로토콜(UDP/TCP)**
- **소스 포트**
- **목적지 포트**
- **신청**
- **지리적 위치 데이터**
- **사용자(Flow 연결된 사용자)**
- **패킷 수**
- **바이트 수**
- **흐름 시작(날짜/시간)**
- **흐름 종료(날짜/시간)**

Note: Netflow Agent를 활용하는 Flow를 보려면 엔드포인트의 트래픽이 네트워크 센서를 통해 흘러야 합니다. 센서를 통해 트래픽을 라우팅하려면 아래 지침에 따라 클라우드 게이트웨이 및 ZTNA 클라이언트를 배포합니다

클라우드에서 노드 관리

클라우드 리소스에 대한 접근 제어

네트워크 센서에서 Netflow 에이전트를 활성화하려면:

1. 상단 패널에서 **시스템 > 센서** 로 이동합니다.
2. tap_1 센서 인터페이스의 **센서 설정** 을 클릭합니다.
3. 트래픽 모니터링 설정 화면까지 아래로 스크롤하고 **Netflow Agent** 를 **On** 로 전환합니다.
4. 페이지 하단의 **수정** 를 클릭합니다.

Flow 데이터가 수집되고 기록되는지 테스트하고 확인하려면 다음을 수행합니다.

1. 상단 패널에서 **감사 > Flow** 로 이동합니다.
2. 네트워크 센서를 통한 모든 트래픽 라우팅에 대한 가시성을 제공 합니다.

Note: 연결된 ZTNA 클라이언트에 대한 Flow만 기록됩니다.

연결된 ZTNA 클라이언트를 보려면:

1. 상단 패널에서 **시스템 > 사이트** 로 이동합니다.

2. ZTNA - 클라이언트 열 아래에서 **(*)** 링크를 클릭하여 연결된 클라이언트를 봅니다.
3. 이러한 클라이언트의 트래픽은 Flow에 표시되어야 합니다.

Flow에 대한 요약 정보를 보려면 다음을 수행합니다.

1. 상단 패널의 **대시보드** 로 이동합니다.
2. 대시보드에서 **설정** 을 클릭 후 **Flow 위젯** 을 추가 합니다.
3. Source IP, Destination IP, User 등의 Top Traffic을 포함한 다양한 위젯을 볼 수 있습니다.

CHAPTER

FIVE

네트워크 접근제어

Note: 이 기능을 사용하려면 Professional 또는 Enterprise Edition이 필요합니다.

네트워크센서 및 에이전트를 통해 수집 된 정보를 기반으로 정책을 설정하여 미준수 단말의 네트워크 사용을 제한 할 수 있습니다. 제어 정책은 다양한 방식으로 적용될 수 있습니다. Genian ZTNA는 다음과 같은 방법을 제공합니다.

5.1 접근제어 정책의 이해

Genian ZTNA는 크게 4가지(**IP/MAC 정책, 노드정책, 제어정책, 무선랜정책**)의 네트워크 접근제어 정책을 사용합니다.

5.1.1 IP/MAC 정책

IP/MAC 정책은 관리자가 수동 또는 자동으로 장치의 IP사용을 제어할수 있습니다. 또한 IP와 MAC을 기반으로 네트워크 엑세스를 제어합니다.

ZTNA에서 위 기능을 사용하려면 반드시 네트워크센서 운영모드를 Enforcement 모드로 변경하고 IP관리정책을 활성화 해야합니다. 본 문서에서는 IP관리 정책을 활성화하고, IP 충돌과 변경을 방지하는 방법, IP를 할당하는 방법을 설명합니다.

IP관리를 사용하여 네트워크접근 제어 준비

IP관리에 의해 거부 된 IP관리 정책을 변경하여 적용이 가능하도록 설정하고 개별 네트워크센서 IP관리 정책을 변경 할 수 있습니다.

IP관리 차단정책 활성화

기본적으로 IP관리 제어정책은 활성화되어 있지 않습니다. 정책을 사용하여 노드를 제어하기 전에 "IP관리 차단" 에 대한 제어 정책을 활성화 해야합니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목의 **제어정책** 으로 이동합니다.
3. 제어정책 창에서 **IP관리 차단** 정책명을 클릭합니다.
4. **기본설정 > 적용모드** 를 찾아 **사용함** 으로 변경합니다.

5. **수정** 버튼을 클릭합니다.
6. 오른쪽 우측 상단에 **변경정책적용** 을 클릭합니다.

IP 관리 신규노드정책 변경

각 네트워크센서에는 IP 관리 신규노드정책이 있습니다. 네트워크센서에 의해 신규 노드가 감지되거나 네트워크에 IP 또는 MAC 주소가 처음 탐지되는 경우 신규노드정책이 자동으로 적용됩니다.

- **MAC 차단**: MAC 주소를 차단합니다.
- **IP 차단**: IP 주소를 차단합니다.
- **IP/MAC 차단**: IP 와 MAC 주소 모두 차단합니다.
- **허용모드**: IP 와 MAC 주소 모두 허용합니다. (기본옵션)
- **변경금지모드**: 노드의 MAC에 변경금지 모드를 설정합니다.
- **충돌보호모드**: 노드의 IP에 충돌보호 모드를 설정합니다.

네트워크센서의 IP 관리 신규노드정책 변경

각 네트워크센서의 설정에서 신규노드정책을 변경 할 수 있습니다.

1. 상단 항목의 **시스템** 으로 이동 하십시오.
2. 좌측 **시스템 > 센서관리** 로 이동 하십시오.
3. 설정할 센서의 **IP 주소** 를 클릭 하십시오.
4. 우측 상단의 **...** 을 클릭하여 **센서설정** 으로 이동합니다.
5. 하단 **IP 관리** 항목에서 **신규노드정책** 을 변경 하십시오.
6. **수정** 버튼을 클릭 하십시오.

IP관리 정책 변경

Genian ZTNA는 노드목록 및 IP 매트릭스 뷰를 이용하여 노드의 차단하거나 허용할 수 있습니다.
노드 리스트 및 IP 매트릭스 뷰에서는 다음과 같은 IP관리 정책을 사용할 수 있습니다.

네트워크센서의 IP 관리 신규노드정책 변경

(*IP*관리 정책은 각 센서의 설정에서 변경 할 수 있습니다)

1. 상단 항목의 **시스템** 으로 이동 하십시오.
2. 시스템 관리 왼쪽 항목의 **시스템 > 센서관리** 로 이동 하십시오.
3. 원하는 센서의 **IP 주소** 를 클릭 하십시오.
4. **설정** 탭 그리고 **센서설정** 을 클릭 하십시오.
5. **IP 관리** 항목에서 **신규노드정책** 메뉴를 찾아 적용모드를 변경 하십시오.
6. **수정** 버튼을 클릭 하십시오.

노드목록에서 IP관리 허용 및 차단

1. 상단 **관리 > 노드** 로 이동합니다.
2. **작업할 노드에 체크박스** 선택을합니다.
3. 상단 **작업선택 > IP/MAC 정책** 에서 아래 옵션을 선택합니다.
4. IP관리 정책 항목
    - **IP 차단:** IP를 차단상태로 변경합니다.
    - **IP 허용 - 충돌보호 해제:** IP를 허용합니다.(IP 충돌보호설정을 해제합니다.)
    - **IP 허용 - 충돌보호 (지정MAC):** IP를 허용하고 노드의 MAC주소가 IP를 점유합니다.(노드상세화면 정책탭에서 추가 MAC주소를 설정할 수 있습니다.)
    - **IP 사용 호스트명제한 설정:** 노드의 호스트명 정책을 설정합니다.
    - **IP 사용 호스트명제한 해제:** 노드의 호스트명 정책을 해제합니다.
    - **IP 사용시간 제한/해제 설정:** IP사용 허용시간을 설정하거나 해제합니다.
    - **IP 사용 신규노드정책 설정:** 노드의 IP를 사용하는 신규노드에 정책을 설정/해제합니다.(MAC 허용, 충돌보호 설정, 변경금지 설정, 충돌보호/변경금지)
    - **IP 용도설정:** IP 사용 형태를 지정합니다.(선택안함, 유동IP 사용, 지정IP 사용, 임시사용 중 선택합니다.)
    - **MAC 차단:** MAC을 차단합니다.
    - **MAC 허용 - 변경금지 해제:** MAC을 허용하고 변경금지설정이 존재하면 해제합니다.
    - **MAC 허용 - 변경금지 (지정 IP대역):** MAC을 허용하고 해당 MAC은 노드의 지정된 IP만 사용하도록합니다.(지정 IP대역은 노드의 관리센서 대역내에서는 지정한 IP만 사용이 가능합니다.)
    - **MAC 허용 - 변경금지 (모든 IP대역):** MAC을 허용하고 해당 MAC은 노드의 지정된 IP만 사용하도록합니다.(모든 IP대역은 ZTNA관리범위 전체에서 지정된 IP만 사용가능합니다.)
    - **MAC 사용시간 제한/해제 설정:** MAC사용 허용시간을 설정하거나 해제합니다.
    - **IP 및 MAC 차단:** IP 와 MAC을 차단합니다.
    - **IP 및 MAC 허용:** IP 와 MAC을 허용합니다.
    - **IP 충돌보호 및 변경금지 설정:** 노드에 IP 충돌보호 설정과 변경금지 설정을합니다.

매트릭스 뷰의 IP관리 차단 및 허용

1. 상단 항목의 **관리 > IP주소** 로 이동합니다.
2. 좌측 트리에서 원하는 **네트워크센서** 의 이름을 클릭합니다.
3. 작업할 **IP주소 네모칸** 을 클릭합니다.
4. 상단 **작업선택** 버튼을 클릭 하십시오.
5. 원하는 **옵션** 을 선택 하십시오.
6. 옵션 종류:
    - **노드등록:** 수동으로 노드를 등록합니다.
    - **노드삭제:** 선택한 IP를 사용하고 있는 노드를 삭제합니다.
    - **IP차단:** IP를 차단상태로 변경합니다.

- **IP(모든MAC) 허용 - 충돌보호해제:** IP를 허용합니다.(IP 충돌보호설정을 하지 않습니다.)
- **IP(지정MAC) 허용 - 충돌보호설정:** IP를 허용하고 노드의 MAC주소가 IP를 점유합니다.(노드상세화면 정책탭에서 추가 MAC주소를 설정할 수 있습니다.)
- **IP 충돌보호 및 변경금지 설정:** 노드에 IP 충돌보호 설정과 변경금지 설정을합니다.
- **IP사용 신규노드정책 설정:** 선택한 IP에 신규노드에 정책을 설정/해제합니다.(MAC 허용, 충돌보호 설정, 변경금지 설정, 충돌보호/변경금지 설정에서 선택합니다.)
- **IP사용시간 제한/해제 설정:** 노드의 IP를 사용하는 신규노드에 정책을 설정/해제합니다.(MAC 허용, 충돌보호 설정, 변경금지 설정, 충돌보호/변경금지)
- **IP소유부서설정:** IP의 소유부서를 설정합니다.(IP소유부서설정은 노드그룹의 조건항목으로 사용가능합니다.)
- **IP용도설정:** IP용도를 설정합니다.(고정IP 사용, 유동IP사용, 임시사용)

Note: 차단 된 IP / MAC 주소는 연한 빨간색으로 강조 표시되고 IP 주소의 텍스트에는 취소선이 있습니다

IP 변경 금지

사용자가 자신의 IP 주소를 변경하지 못하게 할 수 있습니다. IP를 변경하면 사용자가 의도하지 않은 권한을 얻을 수있는 충돌이나 손상 문제가 발생할 수 있습니다. 예를 들어, 관리자는 인터넷 액세스를 허용하도록 지정된 IP 주소를 설정하고 다른 모든 주소는 차단할 수 있습니다. 해당 직원이 IP를 사용 할 수 없을 때 IP를 지정 된 주소로 변경 할 수 있는 경우, 인터넷에 접속 할 수 있습니다.

IP 변경 금지 동작 원리

센서는 각 단말에서 전송되는 패킷을 감시하고 분석합니다. 신규 노드가 감지되면 센서가 Gratuitous ARP(GARP) 요청을 보냅니다. 단말은 자신과 일치하는 소스 IP가 포함된 ARP 요청을 수신하면 IP 충돌이 있음을 알 수 있습니다.

IP 변경금지 설정

1. 상단 항목에 있는 **관리 > 노드** 로 이동합니다.
2. 원하는 **IP** 주소를 클릭합니다.
3. **정책** 탭을 클릭합니다.
4. **MAC 정책** 항목을 찾아 **MAC허용 - 변경금지** 박스를 선택합니다.(변경금지는 2가지가 있으며 IP변경을 현재 대역에서만 금지할지 모든 대역에서 금지할지 선택합니다.)
5. 선택한 장비에서 사용할 IP를 하단 드롭다운항목에서 선택하거나 수동 작성을 한뒤 추가버튼을 클릭합니다.
6. 상단 **수정** 버튼을 클릭합니다.

IP 변경금지 해제

1. 상단 항목에 있는 **관리 > 노드** 로 이동합니다.
2. 원하는 **IP** 주소를 클릭합니다.
3. **정책** 탭을 클릭합니다.
4. **MAC 정책** 항목을 찾아 **MAC허용 - 변경금지해제** 를 클릭합니다.
5. 상단 **수정** 버튼을 클릭합니다.

IP 충돌보호

지정된 IP는 지정한 MAC을 가진 장비만 사용할 수 있도록 설정하는 기능입니다.

예를 들어 IP별로 방화벽 정책이나 네트워크 엑세스 권한이 다른 경우 IP별 장비를 제한할때 사용합니다.

IP 충돌보호 동작 원리

네트워크센서는 네트워크에서 전송되는 패킷을 감시하고 분석합니다. IP 충돌보호정책을 위반한 노드가 네트워크에 접근하면 hello packet, Gratuitous ARP(GARP) 패킷이 발생하고 이에 대한 응답을 보냅니다. 단말은 자신과 일치하는 소스 IP가 포함된 ARP 응답을 수신하면 IP 충돌로 판단하고 네트워크 접근을 스스로 제한합니다.

IP 충돌보호 설정 방법

1. 상단 **관리 > 노드** 로 이동합니다.
2. 설정할 노드의 **IP** 를 클릭합니다.
3. **정책** 탭을 클릭합니다.
4. **IP 정책** 항목에서 **IP허용 - 충돌보호(지정 MAC)** 를 선택합니다.
5. 선택한 IP에서 사용할 MAC을 하단 **드롭다운항목에서 선택하거나 수동 작성을 한뒤 추가** 버튼을 클릭합니다.
6. **수정** 버튼을 클릭 하십시오.

IP 충돌보호 해제

1. 상단 **관리 > 노드** 로 이동합니다.
2. 설정할 **IP** 주소를 클릭합니다.
3. **정책** 탭을 클릭합니다.
4. **IP 정책** 항목을 찾아 **IP허용 - 충돌보호해제** 를 선택합니다.
5. **수정** 버튼을 클릭합니다.

시간 기준의 IP/MAC 허용

지정된 시간(날짜, 시간) 동안 IP 주소를 허용하여 임시적으로 네트워크 접근이 허용되도록 할 수 있습니다. 허용 시간이 만료 되면 IP 주소는 차단되거나 추가 허용 허용설정이 될 때까지 네트워크 차단 됩니다.

IP 사용 기간 설정 방법

1. 상단 **관리 > 노드** 를 클릭 하십시오.
2. 설정할 **IP 주소** 를 클릭 하십시오.
3. **정책** 탭을 클릭 하십시오.
4. **IP정책** 항목에서 **IP사용 시작** OR **IP사용 종료** 를 클릭하여 날짜 및 시간 설정을 편집합니다.
5. **수정버튼** 을 클릭합니다.

MAC 사용 기간 설정 방법

1. 상위 항목에서 **관리 > 노드** 를 클릭 하십시오.
2. 원하는 **IP 주소** 를 클릭 하십시오.
3. **정책** 탭을 클릭 하십시오.
4. **MAC정책** 항목에서 **MAC사용 시작** OR **MAC사용 종료** 를 클릭하여 날짜 및 시간 설정을 편집합니다.
5. **수정버튼** 을 클릭합니다.

IP 관리 사전설정하기

IP 신청시스템과 IP관리 기능을 사용하기 위해서는 다음에 항목을 사전 설정해야 합니다.

항목	설명
IP 사용신청서	IP 신청시스템을 사용하기 위한 항목을 설정합니다.
IPM 정책	IP/MAC 기반에 차단 기능을 사용하기 위한 항목을 설정합니다.
IP 신청시스템 화면설정	IP 신청시스템을 사용하기 위한 관리화면 항목을 설정합니다.

1. IP 신청시스템 사전설정하기

IP 신청시스템을 사용하기 위해서는 다음에 항목들이 최소한 사전에 설정되어야 합니다.

항목	세부사항	설명
IP사용신청서	IP사용신청	CWP 페이지에서 **IP사용신청** 버튼에 대한 표시부분을 설정합니다.
	IP신청서 거부처리	IP 신청서에 대한 자동으로 거부처리하는 기간을 설정합니다.
	할당대상 IP	승인 시 할당할 수 있는 IP 대상을 설정합니다.
	할당 IP 대여기준	승인 시 할당할 수 있는 IP 범위를 설정합니다.
	임시사용자 신청허용	사용자 계정이 없는 대상에게 신청서 등록 권한을 할당할지 여부를 설정합니다.
	승인번호 인증	승인번호 인증을 사용하여 승인된 IP 사용권한을 할당할지 여부를 설정합니다.
	IP신청서 등록권한	신청서 등록 권한을 할당할 대상을 설정합니다.
	IP 다중신청서 양식	다수의 신청서를 신청할 경우 사용할 수 있는 신청서 양식을 업로드 합니다.
	IP신청서 처리결과 자동알람	신청자에게 처리결과를 전송하는 방법을 선택합니다.
IP신청시스템 화면설정	신청시스템 메뉴	신청시스템에서 사용할 수 있는 메뉴를 설정합니다.

2. IP 관리기능 사전 설정하기

IP 관리 기능을 사용하기 위해서는 네트워크 센서의 **IP관리** 항목과 **설정>환경설정>IP관리>IPM정책** 을 사전에 설정해야 합니다.

Note: 네트워크 센서의 **IP관리** 부분과 제어설정은 다음에 *IP관리 정책 변경* 참고하시기 바랍니다.

항목	설명	참고
IP/MAC 사용만료 처리방법	사용시간이 만료된 IP/MAC에 대한 노드 삭제여부를 설정합니다.	시간 기준의 *IP/MAC* 허용
특수정책 우선	특수정책(시간제한, 충돌보호, 변경금지)에 대한 우선순위를 설정합니다.	1. *IP* 변경 금지 2. *IP* 충돌보호

5.1.2 노드정책

노드정책은 주로 노드로부터 정보를 수집하고 정책을 만족하고 있는 상태에 있는 네트워크를 확인 및 관리할 수 있습니다. 노드정책을 사용하면 노드의 사용자 인증방법에 따라 인증정책을 수립할 수 있고 단말의 정책준수를 위한 기본설정을 할 수 있습니다.

노드정책을 설정하기 위해서는 생성되어 있는 노드그룹을 사용하거나 신규로 생성해야합니다.

그 다음 **관리 WebUI > 정책 > 노드정책 > 작업선택 > 생성** 으로 이동합니다.

정책생성 절차에 따라 정책에 그룹을 할당하고 세부 옵션을 설정합니다.

참고: | 사용자 인증 옵션 설정 | 노드정책의 에이전트 설정 | 노드 관리 | node-policy-detail

5.1.3 제어정책

노드정책이 노드의 정보를 수집하는 것이라면, 제어정책은 노드가 네트워크에 엑세스하는 것에 대해 허용/차단하고 추가적인 조치를 하는데 사용됩니다. 이 추가 조치는 정책준수를 위해 CWP로 리다이렉션하거나 에이전트를 통한 단말 제어를 포함합니다.

노드그룹을 생성해놓고(노드 그룹 관리) 제어정책을 생성하면 단말 제어에 대한 밑그림이 완성됩니다. 그 다음 제어정책에 노드그룹을 할당하여 그룹에 포함된 노드에 정책을 적용합니다.

권한 생성하기

권한 이해하기

권한을 사용하면 네트워크, 서비스 및 시간을 포함하는 다양한 객체 조합을 기반으로 노드 엑세스를 정의 할 수 있습니다. Genians는 사전 정의된 제어 정책에 사용되는 2개의 사용 권한을 가집니다. 이것은 **PERM-ALL** 및 **PERM-DENY** 입니다. **PERM-DENY** 객체는 시스템에서 자동으로 생성되며 정책에 할당된 권한이 없을 경우 **PERM-DENY** 권한을 부여 받게 됩니다.

- **PERM-ALL**: 모든 네트워크와 서비스를 허용합니다.
- **PERM-DENY**: 모든 네트워크에서 오직 DNS 서비스만 허용합니다. (CWP Redirection을 위해 DNS 프로토콜을 허용합니다.)

(사용자 지정 권한을 만들 수 있지만 먼저 네트워크, 서비스 및 시간 객체와 편집 및 생성 방법을 이해해야합니다.)

Note: 권한은 *ARP* 제어, 미러 제어, *Windows* 방화벽 제어 에 적용됩니다.

- **네트워크** - 특정 네트워크를 식별하고 IP/Netmask 또는 IP 범위 그리고 FQDN 을 기반으로 제어를 정의 할 수있게 해주는 규칙입니다.
- **서비스** - 여러 프로토콜 및 포트를 통해 제어를 정의 할 수 있도록 서비스를 식별하는 규칙입니다.
- **시간** - 특정 요일과 시간에 허용하거나 특정 요일이나 시간에 거부 할 수 있도록 여러 제어 시간을 만드는데 사용되는 규칙입니다.

(제외 확인란은 ***NOT* 연산자* 로 사용됩니다. 예를 들어 정의된 네트워크의 경우 제외 확인란을 선택하면 노드가 이 네트워크 이외의 모든 네트워크에 제어 할 수 있습니다.*)

Note: 객체에 세부적인 정보는 다음에 object-detail 참고하시기 바랍니다.

1단계. 사용자 지정 네트워크 객체를 만듭니다.

1. 상단 항목에서 **정책** 로 이동합니다.
2. 왼쪽 정책 항목에서 **객체 > 네트워크** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 다음을 입력합니다.
    - **ID**: 고유 이름 (예 : 게스트 네트워크)
    - **포함그룹**: 네트워크 객체에 적용할 그룹을 선택합니다.
    - **네트워크주소**: IP/Netmask or Range and FQDN

5. **생성** 버튼을 클릭합니다.
6. **변경정책적용** 버튼을 클릭합니다.

기본 네트워크 객체

- **@LOCAL** - 각 센서 인터페이스의 로컬 네트워크를 나타내는 객체입니다. 로컬 서버는 로컬 네트워크의 모든 사용자가 액세스 할 수 있지만 외부 접속은 차단 됩니다.
- **@MANAGED** - 모든 네트워크센서의 결합 된 네트워크입니다. 새 네트워크센서가 추가되면 해당 네트워크가 자동으로 추가되어 @MANAGED 그룹에 포함됩니다.

예제:

네트워크센서	IP 주소
센서 1	192.168.10.10
센서 2	192.168.20.10
센서 3	192.168.30.10

노드에 연결 된 IP: 192.168.10.100

노드가 허용되고 네트워크 객체가 LOCAL인 경우입니다. 그룹: A(192.168.10.100) Perm Destination Network: Local 노드는 네트워크 범위 192.168.10.0/24에만 연결할 수 있습니다.

노드가 허용되고 네트워크 객체가 관리 됩니다. 그룹:A(192.168.10.100) Perm Destination Network: Manage 노드는 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24의 네트워크 범위에만 연결 할 수 있습니다.

2단계. 사용자 지정 서비스 객체를 생성

1. 상단 항목에서 **정책** 로 이동합니다.
2. 왼쪽 정책 항목에서 **객체 > 서비스** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 다음을 입력합니다.
   - **ID**: 고유 이름 (예 : *80 port*)
   - **포함그룹**: Select Group or Groups to apply to this Network Object
   - **서비스 포트**: 서비스 포트로 선택 할 프로토콜과 연산자를 선택합니다.(예: 포트 *80*의 경우: *TCP/ = 80, TCP/ = 8080*) 입니다.
5. **생성** 버튼을 클릭합니다.
6. **변경정책적용** 버튼을 클릭합니다.

3단계. 사용자 지정 시간 객체 생성

1. 상단 항목에서 **정책** 로 이동합니다.
2. 왼쪽 정책 항목에서 **객체 > 시간** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 다음을 입력합니다.
   - **ID**: 고유 이름 (예 : 방문자의 업무시간)
   - **Group**: 네트워크 객체에 적용할 그룹을 선택합니다.
   - **시간객체**: 특정 날짜 또는 일 및 시간의 범위입니다. (예. 시간: *0800-1800,* 일: 월요일-금)
5. **생성** 버튼을 클릭합니다.
6. **변경정책적용** 버튼을 클릭합니다.

4단계. 권한 생성

1. 상단 항목에서 **정책** 로 이동합니다.
2. 왼쪽 정책 항목에서 **객체 > 권한** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 다음을 입력합니다.
   - **ID**: 권한 명
   - **설명**: 권한의 기능을 이해하는 데 도움이 되는 설명입니다.
   - **조건설정**: 네트워크, 서비스 및 시간을 선택하고 편집합니다.
   - **Exclude 체크 박스**: NOT 연산자로 사용 됩니다.
5. **생성** 버튼을 클릭합니다.
6. **변경정책적용** 버튼을 클릭합니다.

노드 그룹에 대한 제어 정책 생성

제어 정책 은 우편 실에서의 분류와 비슷한 방식으로 작동합니다. 모든 노드는 **제어 정책** 의 우선 순위 목록을 통하여 허용되는 접근노드 수 및 적합한 그룹을 결정합니다. (사용자 정의 제어 정책을 만들거나 제어 정책 목록을 다시 정렬할 때 두 개의 제어 정책이 있어야 현재 위치에 유지됩니다)

- **예외 허용** : 예외 허용 정책 위에 사용자 정의 제어 정책을 배치할 수 없거나 예외가 제대로 적용되지 않습니다.
- **기본 정책** : 기본 정책 아래에 사용자 정의 제어 정책을 배치 할 수 없습니다. 이 정책은 제어정책의 기본값입니다.

제어 정책 만들기

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 제어정책** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **정책선택** 탭에서 **다음** 을 클릭합니다.
5. **정책 기본설정** 탭에서는 **ID** 와 간단한 **설명** 을 입력하여 정책이 수행하는 것 들을 정의합니다.(우선 순위는 기본값으로 유지되며 상태는 사용 가능 이어야합니다). **다음** 을 클릭 하십시오.
6. **노드 그룹 할당** 탭에 생성 된 노드 그룹 을 선택하고 선택한 부분으로 이동 한 후 **다음** 을 클릭 하십시오 .
7. **권한 할당** 탭에서 **사용 가능한 권한** 을 **선택** 하고 **선택 항목** 으로 이동 한 후 **다음** 을 클릭 하십시오 .
8. **제어옵션 설정** 탭은 **CWP** 및 **스위치포트 차단** 을 설정하는 옵션입니다. **다음** 을 클릭 하십시오 .
9. **제어액션 설정** 탭은 **에이전트 액션** 을 추가 할 때의 **옵션** 입니다.
10. **완료** 를 클릭 하십시오.

제어 상태 관리

제어 정책 페이지에는 제어과 관련 된 정보를 제공하는 위젯이 표시됩니다. 이러한 정보는 상단 항목에서 정책을 클릭 한 다음 왼쪽 정책 항목에서 정책 > 제어 정책을 선택하여 볼 수 있습니다. 표시되는 두 위젯은 다음과 같습니다.

- **센서 운영모드 현황** : Enforcement 또는 Monitoring 동작모드의 네트워크센서 수를 표시합니다.
- **제어정책 적용 현황** : 탐지 된 모든 노드에서 차단 된 노드를 % 로 표시합니다.

노드 관리 페이지에서 제어정책 상태 보기

노드의 제어정책 적용 상태 는 **노드관리** 페이지에서 확인 할 수 있으며, 상단 항목에서 **관리 > 노드** 를 클릭하면 볼 수 있습니다.

- **제어 정책 컬럼**: 해당 노드에서 차단 중인 정책을 표시합니다. 노드에 **주황색** 으로 나열 된 정책이 있는 경우 해당 노드는 관련 정책을 준수하지 않으므로 현재 **차단** 된 상태입니다.

제어정책 그룹

노드관리 페이지의 왼쪽 아래에 있는 상태 & 필터로 이동합니다. 아래 항목 중 **제어정책** 을 선택합니다.

제어정책에 제어액션 설정

제어정책의 제어액션은 설치된 에이전트를 이용하여 네트워크 차단 외에 추가 동작이 가능합니다. PC 전원 제어, 사용자 알림메시지 등 다양한 에이전트 플러그인을 지원합니다.

제어액션 생성

1. 상단 항목의 **정책** 을 클릭합니다.
2. 좌측 항목에서 **제어정책 > 제어액션** 을 클릭합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **제어액션** 에서 **액션 수행설정** 을 설정합니다.
5. **생성** 을 클릭합니다.
6. 오른쪽 화면 상단의 **변경정책적용** 을 클릭합니다.

사용 가능한 플러그인 항목

제어액션에 사용할 수 있는 플러그인은 다음과 같습니다.

OS 종류	플러그인	설명
Windows	*Windows 방화벽 제어*	Windows 방화벽을 사용하여 사용자 네트워크를 제어합니다.
	사용자 알림메시지	사용자에게 알림메시지를 표시합니다.
	시스템 종료	지정된 시각에 Windows 시스템의 절전, 재시작, 종료를 수행합니다.
	인터페이스 제어	인터페이스를 사용안함으로 바꾸는 기능을 제공합니다.
	프로그램 제거	제어판의 프로그램 제거에 등록된 프로그램중 제거 가능한 특정 프로그램을 제거합니다.
	프로세스 강제종료	액션 검사조건에 설정된 프로세스에 대해서 강제종료 기능을 수행합니다.
Linux	없음	
macOS	사용자 알림메시지	사용자에게 알림메시지를 표시합니다.

제어정책에 제어액션 할당

1. 상단 항목에서 **정책** 을 클릭합니다.
2. 좌측 항목에서 **제어정책** 을 클릭합니다.
3. 설정을 원하는 **제어정책** 의 정책명을 찾아 클릭합니다.
4. 하단 **제어액션 설정** 을 찾아 **할당** 을 클릭합니다.
5. **사용가능** 항목에서 **제어액션** 을 찾아 **선택** 항목으로 이동합니다.
6. **추가** 를 클릭합니다.
7. 수정 버튼을 클릭합니다.
8. 우측 상단의 **변경정책적용** 을 클릭합니다.

제어액션 할당 해제

1. 상단 항목에서 **정책** 을 클릭합니다.
2. 좌측 항목에서 **제어정책** 으로 클릭합니다.
3. 설정을 원하는 **제어정책** 의 정책명을 찾아 클릭합니다.
4. **제어액션 설정** 에서 삭제하고자 하는 **제어액션** 을 찾아 **삭제** 를 클릭합니다.
5. 수정 버튼을 클릭합니다.
6. 우측 상단의 **변경정책적용** 을 클릭합니다.

제어액션 삭제

1. 상단 항목에서 **정책** 을 클릭합니다.
2. 좌측 항목에서 **제어정책 > 제어액션** 을 클릭합니다.
3. 삭제할 **제어액션** 을 찾아 **체크박스** 를 클릭합니다.
4. **작업선택 > 삭제** 를 클릭합니다.
5. 우측 상단의 **변경정책적용** 을 클릭합니다.

5.1.4 무선랜 정책

무선랜 정책은 프로파일(Client)을 배포하는데 사용됩니다.

무선랜 정책에서 접근제어 기능을 사용하기 위해서는 AGENT와 무선랜제어 플러그인이 필요합니다.

무선랜 정책 설정하기

무선랜 정책을 통해 단말에 적용할 Client 프로파일을 관리할 수 있으며, 무선 네트워크 사용 대상에 대한 접근 제어를 적용할 수 있습니다.

기본정보 설정하기

무선랜 정책이 적용받기 위한 기본 항목을(SSID, 타입, 설명, 사용유무) 설정합니다.

항목	세 부 항목	설명	비고
기본 정보	SSID	무선연결을 위한 SSID(Service Set IDentifier)를 설정합니다.	Client 모두 적용
	타입	SSID에 대한 패턴 사용유무를 설정합니다.	패턴은 Client 프로파일만 사용

RADIUS 정책 설정하기

무선 네트워크 사용을 위한 사용자 인증을 수행할 수 있는 대상을 지정합니다.

항목	세부항목	설명	비고
RADIUS 정책	인증허용 사용자 그룹	무선연결 시 사용자 인증을 받을 수 있는 대상을 설정합니다.	WPA2 Enterprise, 802.1X 대상

Client 정책 설정하기

무선연결관리자 를 대상으로 동작하는 정책을 설정합니다.

항목	세부항목	설명	비고
Client 정책	Client 프로파일	무선연결관리자가 적용할 Client 프로파일을 지정합니다.	무선접속을 위한 *Client* 프로파일 사용자 단말에 적용하기
	허용 MAC 목록	무선연결이 가능한 NIC의 MAC을 지정합니다.	

5.1.5 RADIUS 정책

RADIUS 정책은 무선 및 유선으로 RADIUS로 인증을 시도한 사용자인증을 승인/거부하고 추가적인 조치를 하는데 사용됩니다.
이 추가 조치는 네트워크에 접근이 허용된 노드가 연결된 스위치의 포트에 ACL, VLAN, Session timeout, Filter 설정을 포함합니다.

정책을 설정하기 위해서는 생성되어 있는 사용자그룹을 사용하거나 신규로 생성해야합니다.

그 다음 **관리 Web콘솔 > 정책 > RADIUS 정책 > 작업선택 > 생성** 으로 이동합니다.

정책 생성 절차에 따라 정책에 사용자그룹 을 할당 하고 조건을 추가한뒤 세부 정책설정을합니다.

RADIUS 정책 설정

RADIUS 정책을 설정하는데 필요한 조건설정과 정책설정에 대한 안내입니다.

조건설정

조건설정은 정책을 적용하는 대상에 대해 설정하는 항목입니다.
접속 정보를 활용하여 정책적용 대상을 지정할 수 있습니다.

속성으로 사용가능한 항목들

속성항목	설명
User-name	인증사용자명
Calling-Station-Id	접속요청한 단말의 MAC
Called-Stastion-Id	접속한 장비(AP)의 MAC

continues on next page

Table 1 – continued from previous page

속성항목	설명
Called-Station-SSID	접속한 장비(AP)의 SSID
Framed-IP-Address	접속한 장비의 IP
NAS-Port	접속한 장비의 물리적 포트번호
NAS-Identifier	접속한 장비의 호스트명
Service-Type	요청하거나 제공할 서비스 유형(login, callback login, authentication 등)
Fiter-Id	접속한 사용자에 대한 필터목록의 이름
Login-IP-Host	로그인서비스 속성을 사용할때 연결할 시스템
Class	
Vendor-Specific	접속한 장비의 제조사명
NAS-Port-Type	접속한 포트의 종류(wireless-802.11, ethernet, adsl 등)
Connect-Info	
NAS-Port-ID	접속한 장비의 포트
Aruba-User-Role	Aruba AAA프로파일의 사용자역할명
Aruba-Essid-Name	Aruba ESSID(동일한 SSID를 사용하는 하나 이상의 AP로 구성된 네트워크)

정책설정

인증한 사용자에게 적용할 정책을 설정하는 항목입니다.
기본적으로 인증한 사용자를 허용/거부가 기본으로 설정이 됩니다.
인증된 사용자에게 추가속성을 부여할 수 있습니다.

추가 속성

속성항목	설명	예시
VLAN 번호/이름(Tunnel-Private-Group-Id)	VLAN 할당	1~4092 숫자
Cisco-AVPair(ip:inacl)	Inbound 패킷에 대한 ACL 설정	permit ip host 192.168.1.203 any
Cisco-AVPair(ip:outacl)	Outbound 패킷에 대한 ACL 설정	deny ip host 192.168.1.203 any
Cisco-AVPair(security-group-tag)	보안 그룹 태그	
Cisco-AVPair(url-redirect-acl)	Cisco 장비에 생성된 ACL명	
Cisco-AVPair(url-redirect)	Redirect 주소	http(s)://IP or DOMAIN
Cisco(AVPair)	Cisco AVPair 속성	문자열
Filter-ID	접속장비에 설정된 ACL명	
NAS-Filter-Rule	ACL 리스트 설정	permit in tcp from any to any

continues on next page

Table 2 – continued from previous page

속성항목	설명	예시
Session-Timeout	인증 후 세션종료 값	초
Termination-Action	세션만료 후에 동작	1(재인증), 0(종료)
직접입력	세부속성값 직접입력	문자열

기본설정, 조건설정, 정책설정을 완료하고 하단 수정버튼을 클릭합니다.

속성 항목에 대해서는 RFC2865 문서를 참고하시기 바랍니다.

5.2 제어 방법

조직에서 정의한 네트워크 접근제어 정책을 위반하는 장치를 제어하는 방법이 필요합니다. Genian ZTNA는 Layer 2 계층에서 Application 계층까지 다양한 계층의 제어방법을 제공합니다. 네트워크 환경 또는 보안 수준 요구 사항에 따라 다음 옵션들을 사용할 수 있습니다.

5.2.1 ARP 제어

내부 네트워크의 단말 상태에 따라 네트워크 접근 제어는 어려움이 많습니다. 내부 네트워크 내의 접근을 제어하기 위해 라우터에 ACL을 설정하면 간단한 액세스 제어만 제공할 수 있습니다.

단말이 자주 이동하거나 단말의 IP가 자주 변경되는 DHCP 환경에서는 ACL을 적용하기 어렵습니다. 또한 동일한 서브넷에 연결된 여러 단말 간의 접근 제어가 가장 어려운 작업이며 솔루션이 많지 않습니다.

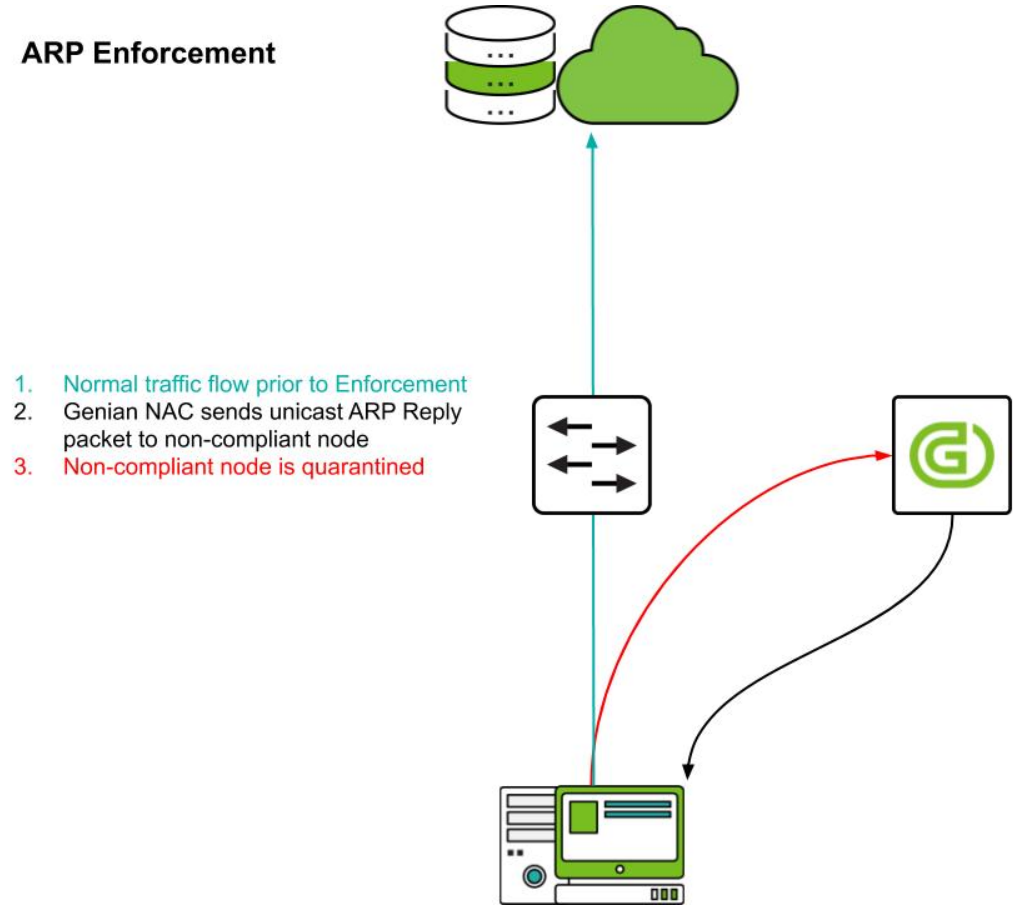
802.1x를 사용하여 장치가 연결된 스위치 포트에 포트 기반 접근 제어 기능을 적용할 수 있습니다. 그러나 802.1x는 비용이 많이 들며 지원되는 장치로 바꾸고 같은 제조업체의 제품으로 교체하는 등 대규모 네트워크 구성 변경이 필요합니다.

또한 모든 네트워크 장비가 802.1x를 지원하지 않기 때문에 연결된 각 스위치 포트에 수동 구성이 자주 필요합니다. 거대한 엔터프라이즈 네트워크에서 각 스위치 포트에 대한 802.1x에 대한 예외 또는 MAC 주소를 설정하면 매우 큰 관리 문제가 야기되어 배포 및 관리에 매우 오랜 시간이 걸릴 수 있습니다.

또 다른 옵션은 ARP 변조와 함께 네트워크 접근 제어를 사용하는 것입니다. ARP 변조는 상대방이 ARP Request를 통해 MAC주소를 얻을 때 상대방으로 가장하여 생성된 패킷을 가로채어 단말에 접근 제어를 적용 할 수 있도록 ARP 프로토콜의 특성을 사용합니다.

Genian ZTNA는 다음 절차를 통하여 ARP 제어를 수행합니다.

- 차단될 단말이 ARP Request를 수행합니다.
- 네트워크센서의 MAC으로 해당 요청에 응답합니다.
- 차단된 단말은 네트워크센서로 패킷을 전송합니다.
- 네트워크센서는 접근제어 정책에 따라 패킷을 Drop하거나 실제 목적지 대상으로 Redirection합니다.



정적 ARP가 설정된 차단 단말의 ARP 변조 우회를 방지하기 위해 게이트웨이 등의 통신 대상에서 생성된 응답 패킷을 제어하기 위한 양방향 변조 기능을 제공하며 에이전트를 통해 정적 ARP 설정을 차단할 수 있습니다.

Static ARP 사용단말 제어하기

단말에서 ARP Table의 MAC주소를 정적(Static)으로 설정하여 사용하면 정책을 위반한 단말이 네트워크접근 통제를 우회하여 통신이 가능합니다.

Note: ARP를 이용한 제어방법에서, 네트워크센서는 정책을 위반한 단말에게 ARP 제어패킷을 전송하여 네트워크를 제어합니다.

해결방법

Static ARP 사용 단말을 제어하기 위해 Genian ZTNA에서는 아래 네 가지 제어 방법을 제공합니다.

Static ARP 설정 방지 기능 적용(Agent)

- 에이전트가 단말 ARP Table의 정적 설정 여부를 실시간으로 모니터링하여 동적으로 변경함
- 정책 > 노드정책 > 노드액션 > ARP 관리 > Static ARP 차단 On
- ARP 관리 노드액션을 노드정책에 할당하여 단말에 정책적용

802.1x 구성을 통한 제어

802.1x 포트기반 접근제어는 네트워크 환경에서 적용 할 수있는 가장 강력한 접근제어 방법입니다. 사용자 기반 인증을 사용하여 사용자별 권한을 스위치포트에 부여하여 역할별 접근제어를 수행할 수 있습니다.

유무선 802.1x 구성

- RADIUS서버 기능을 활성화하고 네트워크장비(Switch, AP)와 연동합니다.
- 에이전트 유선인증관리자 플러그인을 네트워크환경에 맞게 설정 한뒤 단말에 적용합니다.
- RADIUS 정책 설정을 활용하여 스위치 포트기반 네트워크 제어를 수행합니다.

RADIUS 제어 설정, *RADIUS 정책 설정* 문서를 참고바랍니다.

Mirror 구성을 통한 제어

- Static ARP 단말의 상단 네트워크에 네트워크센서(Mirror Mode)를 추가 구성하여 HTTP Redirection으로 제어
- 시스템 > 센서관리 > 센서설정 > 차단방법 > HTTP Redirection Drop(Reject)

Note:

HTTP Redirection의 두 가지 옵션

- Drop : 차단된 패킷을 drop 후 추가 동작 없음
- Reject : TCP인 경우 RST 패킷 전송, UDP인 경우 ICMP Unreachable 패킷 전송

Strict Mode를 통한 제어(네트워크센서)

- 정책위반 단말을 고립시키는 형태로써 보안에 위반된 단말이 목적지로 패킷 전송 시 응답패킷을 네트워크센서로 유도하여 네트워크통신을 제어하는 방법
- 시스템 > 센서관리 > 센서설정 > 센서 운영모드 > ARP Strict Mode

Note:

Strict Mode의 세 가지 옵션

- Normal : Strict Mode 적용하지 않음

- Strict : Strict Mode 적용
- Strict (without Gateway) : Strict Mode 적용 (게이트웨이는 제어하지 않음)

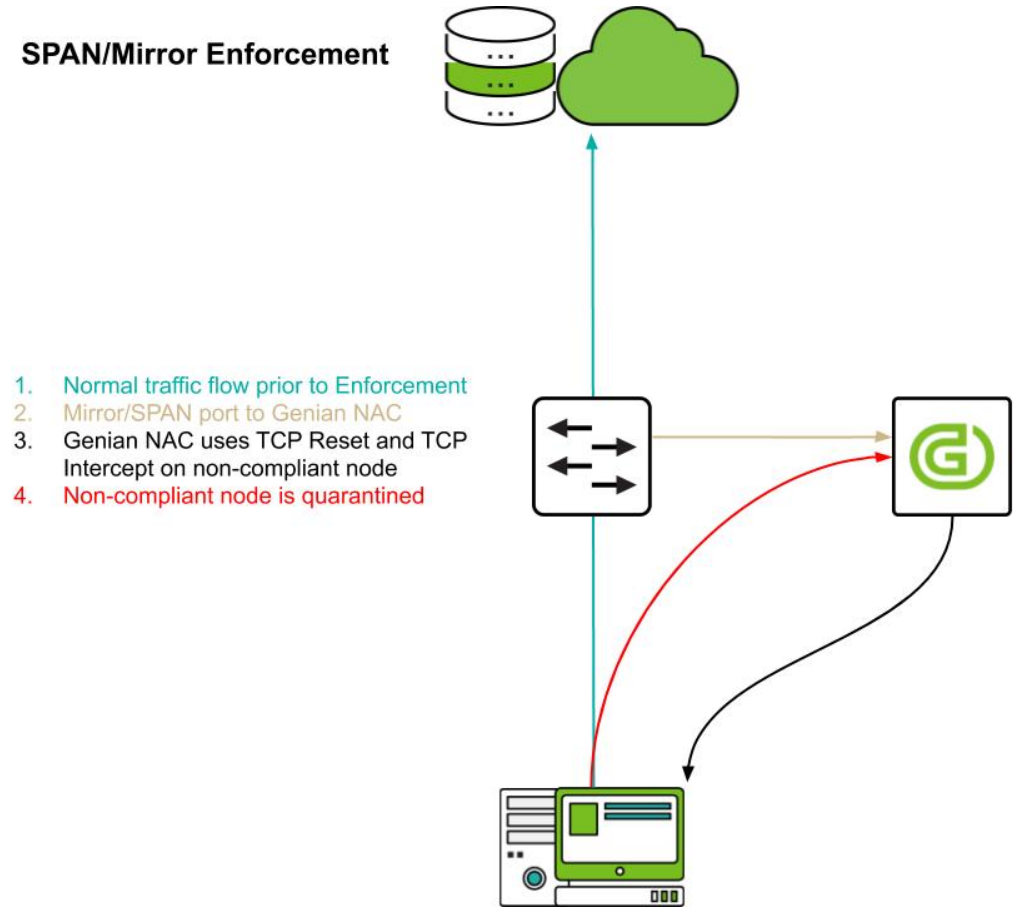
Genian ZTNA에는 RADIUS 서버가 내장되어 있어 802.1x 및 ARP 변조를 통해 패킷을 센서로 경유시키고, 사용자는 네트워크 환경에 따라 이를 선택 할 수 있습니다.

5.2.2 포트 미러링 (SPAN)

Genian ZTNA는 최소한의 네트워크 구성 변경으로 접근 제어를 제공하는 방법으로 포트 미러링 (Cisco의 SPAN)을 사용합니다. 미러링 포트를 통해 새로 연결된 세션을 모니터링하고 TCP RST 또는 ICMP Destination Unreachable 패킷을 전송하여 연결을 차단합니다.

이렇게 하려면 Port Mirroring 지원 스위치 또는 네트워크 TAP 장비를 사용하여 Genian ZTNA에 트래픽을 전송해야합니다.

Genian ZTNA는 두 가지 유형의 포트 미러링 모드를 제공합니다.



글로벌 미러 센서

글로벌 미러 센서는 Genian ZTNA에 등록 된 모든 노드에 대한 정보를 가지고 있으며 정보 수집 및 접근 제어를 수행할 수 있습니다. 일반적으로 인터넷에 연결된 구간 네트워크에 위치하며 모든 내부 트래픽을 모니터링하면서 접근 제어가 수행 됩니다.

네트워크에서 생성된 모든 트래픽을 모니터링 하면서 모든 노드를 제어하므로 네트워크센서와 별도의 전용 고성능 하드웨어를 사용하는 것이 좋습니다.

로컬 미러 센서

ARP 변조와 달리 로컬 미러 센서는 해당 위치의 특정 네트워크 세그먼트를 통과하는 패킷만 제어 할 수 있습니다. 이 문제를 해결하기 위해 각 최종 네트워크에 설치된 네트워크센서에 미러링 포트를 추가 할 수 있습니다. 이를 통해 로컬 네트워크 내에서 발생하는 연결을 제어 할 수 있습니다.

로컬 미러 센서는 네트워크센서 장비에서만 감지되고 기존 노드에 대한 제어만을 수행하기 때문에 글로벌 미러 센서와 비교할 때 상대적으로 낮은 사양의 하드웨어에서 작동 할 수 있습니다.

5.2.3 802.1x (RADIUS)

802.1x 포트 기반 접근 제어는 엔터프라이즈 무선랜 환경에 적용 할 수있는 가장 이상적인 접근 제어 방법입니다. 사용자 기반 인증을 사용하면 권한이 부여 된 사용자 만 네트워크에 액세스 할 수 있습니다. 또한 단말의 보안준수 상태에 따라 특정 VLAN에 연결하거나 연결 된 상태를 강제로 해제 할 수 있습니다.

802.1x를 지원하는 사용자 단말, 802.1x 지원 액세스 포인트(AP) 또는 스위치와 같은 네트워크 액세스 장비 및 RADIUS 서버가 필요합니다. Genian ZTNA는 내장형 RADIUS 서버를 제공하며 다음과 같은 접근 제어 기능을 제공합니다.

사용자 인증

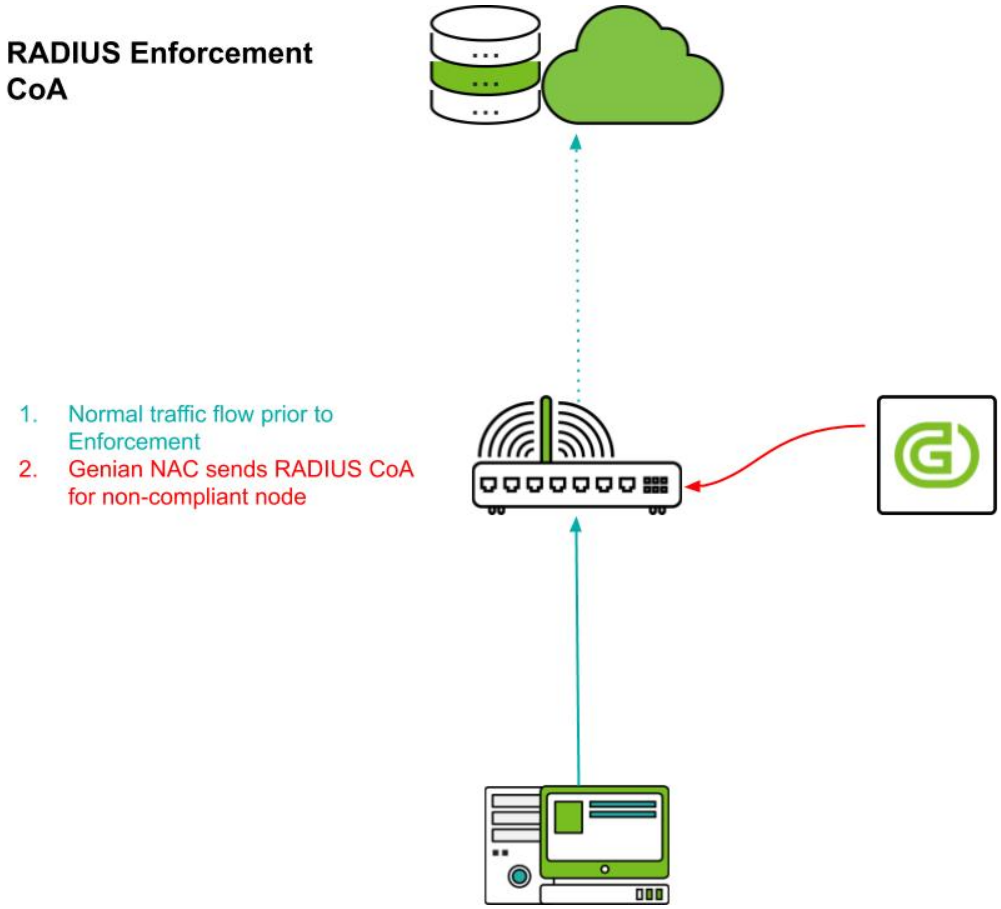
802.1x에서는 공유 암호와 같은 취약한 인증 방법 대신 사용자 기반 인증을 통해 네트워크에 액세스할 수 있습니다. 사용자 인증에 대한 자세한 내용은 *802.1x 설정* 을 참조 하십시오.

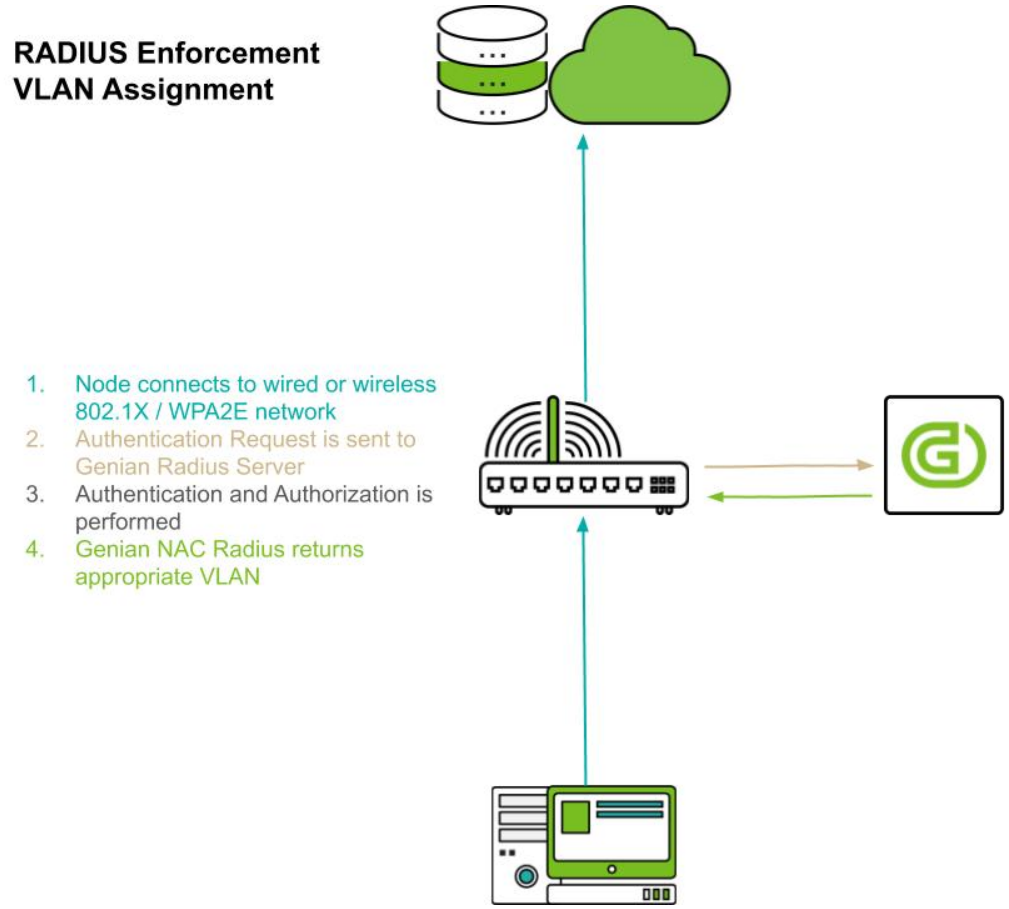
격리 VLAN

802.1x 가 가능한 액세스 포인트(AP) 또는 스위치가 RADIUS *Tunnel-Private-Group-ID* 속성을 지원하면 장치의 상태에 따라 특정 VLAN에 대한 액세스를 제어 할 수 있습니다. RADIUS 서버가 사용자 인증 성공 결과를 전송하면이 속성이 추가되어 전송되고 액세스 포인트 또는 스위치는 VLAN ID를 수신하고 해당 VLAN ID를 액세스 포트에 할당합니다.

Change of Authorization(CoA)

단말 상태 변경으로 인해 네트워크 접근를 제한 해야하는 경우 RADIUS CoA (권한 변경)를 사용하여 단말의 접속상태를 종료 시 킬 수 있습니다. 연결이 끊긴 단말는 새 연결을 시도하고 이 때 분리 된 VLAN에 연결하여 단말을 네트워크에서 안전하게 분리합니다. 이렇게 하려면 액세스 지점 또는 스위치가 RADIUS에 대한 표준 (*RFC 5176 - Dynamic Authorization Extensions*) 을 지원 해야합니다.


RADIUS Enforcement
CoA
1. Normal traffic flow prior to Enforcement
2. Genian NAC sends RADIUS CoA for non-compliant node

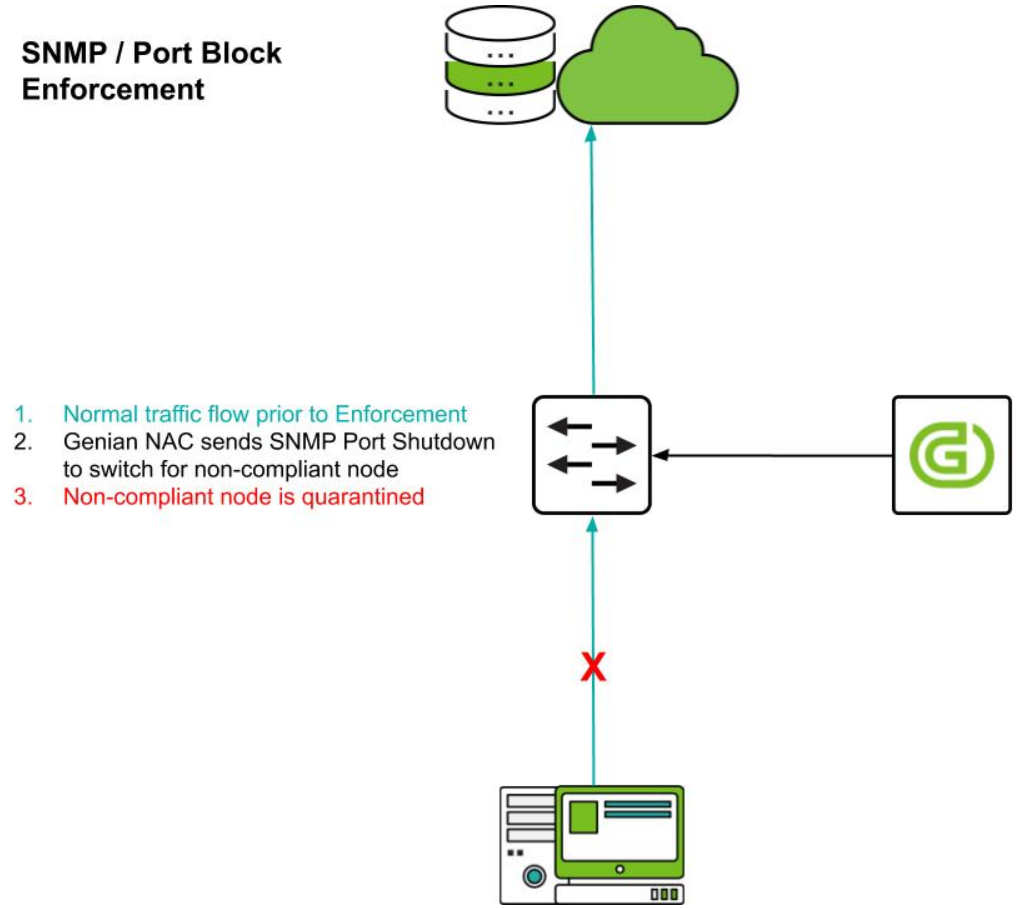


5.2.4 DHCP

Genian ZTNA는 내장된 DHCP 서버를 통해 IP/MAC 정책에 따라 IP를 할당하거나 할당하지 않습니다. 이렇게 하면 권한이 없는 단말이 네트워크에 접근하는 것을 방지하거나 특정 MAC 주소가 있는 단말에 고정 IP 주소를 할당 할 수 있습니다.

5.2.5 스위치 포트 차단

SNMP를 지원하는 스위치를 사용하는 경우 Genian ZTNA는 SNMP를 수집하고 각 노드에 연결된 스위치 정보 및 포트 정보를 수집합니다. 이 정보는 장치의 보안 정책에 따라 스위치 포트를 종료하는 데 사용할 수 있습니다. 스위치는 쓰기 가능한 *SNMP MIB-2 ifAdminStatus* 등록 정보를 제공해야합니다.

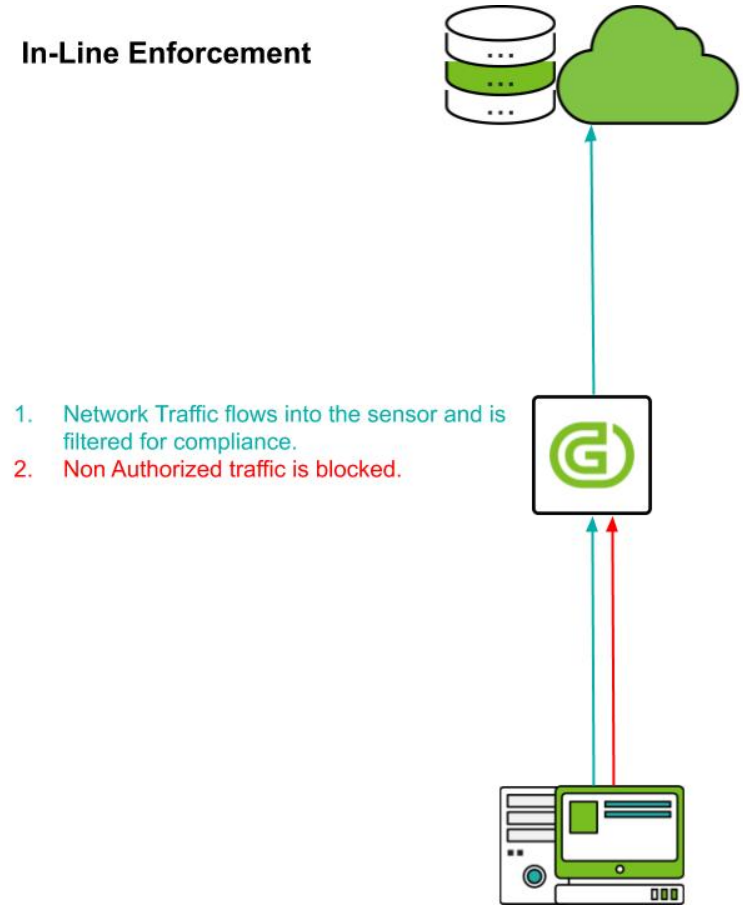


5.2.6 인라인 패킷 필터링

적용 정책에 따라 지정 된 제어 정책을 적용하려면 두 네트워크간에 양방향 패킷 필터링 장치를 사용할 수 있습니다. 이것은 일반적으로 방화벽과 동일한 방식으로 작동합니다. 두 네트워크 인터페이스는 각 네트워크에서 게이트웨이로 작동하며 패킷을 전달하는 과정에서 정책을 확인하고 승인되지 않은 패킷을 삭제합니다.

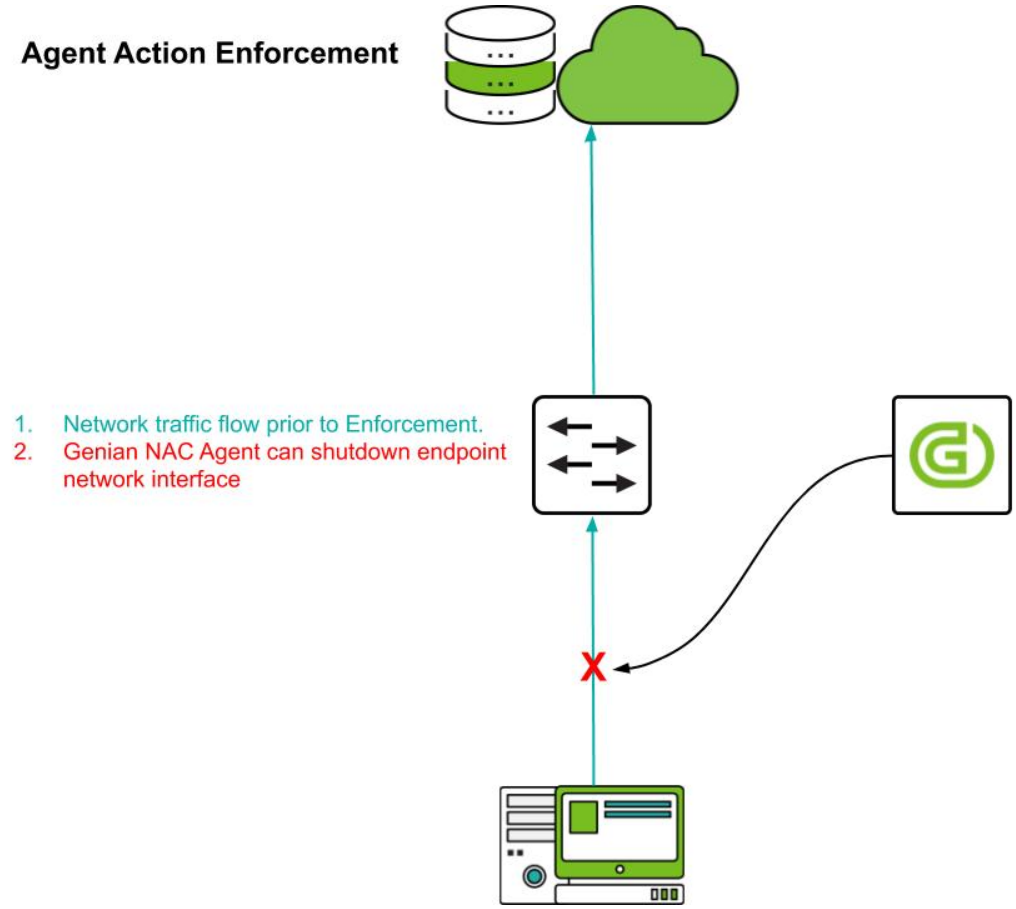
ARP 또는 포트 미러링 방법과 같은 대역 외 방법과 달리 통과하는 모든 패킷에 대해 보안 정책을 확인하고 허용 된 패킷 만 전송하기 때문에 보안이 강화 됩니다 그러나 인라인 장비는 통과하는 모든 패킷에 대해 보안 정책 검사를 받아 패킷 전송 지연을 유발 할 수 있습니다. 또한 인라인 장비를 통과하지 않는 패킷에는 접근 제어 정책을 적용 할 수 없습니다. 따라서 배포하기 전에 설치 위치를 주의해야합니다.

인라인 패킷 필터링의 경우 네트워크센서 소프트웨어는 두 개 이상의 네트워크 인터페이스가있는 하드웨어에 설치해야합니다. 설정을 통해 센서 작동 모드가 'Inline'으로 설정되면 보안 정책이 수신 된 패킷에 적용 된 다음 라우팅 테이블에 따라 시스템의 다른 인터페이스로 전달 됩니다.



5.2.7 에이전트 액션

에이전트는 네트워크 인터페이스 종료, 무선 연결 차단, PC 종료 및 알림 플러그인을 제공하여 단말을 직접 제어 할 수 있습니다.



5.3 ARP 제어 설정

네트워크센서는 기본적으로 네트워크의 트래픽을 수신하도록 구성되어 있으며 정책 서버로 전달되는 정보를 수동으로 수집합니다. 수집 된 정보는 단말의 IP, MAC, 플랫폼, 호스트명 및 동작상태 등을 식별하고 요구 사항에 따라 정책을 생성하는데 도움이 됩니다. 네트워크센서 운영 모드를 Monitoring에서 Enforcement로 변경해야 정책 서버가 정책을 적용하고 단말의 네트워크에 대한 접근을 제어 할 수 있습니다.

자세한 정보는 제어 방법 에서 참고 하십시오.

5.3.1 ARP 제어 설정 방법

네트워크센서 를 활성화하여 정책을 시행할 수 있습니다. 네트워크센서에는 두 가지 유형의 **센서 운영모드** 가 있습니다.

1. 상단 항목에 있는 **시스템** 으로 이동합니다.
2. 왼쪽 시스템 관리 항목의 **시스템 > 센서관리** 로 이동합니다.
3. 제어를 활성화 하기 위해 원하는 센서의 **IP 주소** 를 선택합니다.
4. 우측상단의 ••• 버튼을 클릭하십시오.
5. **센서 설정** 을 클릭합니다.

6. **센서 운영 모드** 를 **Enforcement** 로 변경합니다.
7. **수정** 을 클릭합니다.

5.4 미러 모드 설정

미러링 포트를 통해 새로 연결된 세션을 모니터링하고 TCP RST 또는 ICMP Destination Unreachable 패킷을 전송하여 연결을 차단합니다.

미러 모드에는 NIC가 두 개 이상 필요합니다. 첫 포트는 센서를 관리하기 위해 IP를 할당하고, 다른 포트는 패킷 모니터링을 위한 포트로 IP 할당 없이 사용됩니다.

자세한 정보는 제어 방법 을 참조합니다.

5.4.1 글로벌 미러(Global Mirror)

미러 센서는 모든 노드에 동작합니다.

1. 상단 항목에 있는 **시스템** 으로 이동합니다.
2. 왼쪽 시스템 관리 항목의 **시스템 > 센서관리** 로 이동합니다.
3. 미러 설정에 대해 원하는 센서의 **IP 주소** 를 선택합니다.
4. **설정 탭 > 센서 설정** 를 클릭합니다.
5. 미러 모드에서 사용 할 인터페이스를 클릭합니다. **eth1** 이 인터페이스에 할당된 IP가 없습니다.
6. **센서 동작 모드** 에서 **Mirror** 를 선택합니다.
7. **미러 동작범위** 에서 **Global** 을 선택합니다.
8. **센서 운영모드** 의 경우 **Enforcement** 로 변경합니다.
9. **수정** 버튼을 클릭합니다.

Note: 글로벌 미러를 사용 할 경우 노드가 등록되지 않으므로 엔드 포인트에 에이전트를 설치해야합니다.

5.4.2 로컬 미러(Local Mirror)

Monitoring 모드 센서 와 함께 사용하면 더 많은 정보를 수집 할 수 있습니다 . **Monitoring** 모드 센서 와 동일한 장비에서 사용 할 수 있습니다.

1. 상단 항목에 있는 **시스템** 으로 이동합니다.
2. 왼쪽 시스템 관리 항목의 **시스템 > 센서관리** 로 이동합니다.
3. 미러 설정에 대해 원하는 센서의 **IP 주소** 를 선택합니다.
4. **설정 탭 > 센서 설정** 를 클릭합니다.
5. 미러 모드에서 사용 할 인터페이스를 클릭합니다. **eth1** 이 인터페이스에 할당된 IP가 없습니다.
6. **센서 동작 모드** 에서 **Mirror** 를 선택합니다.
7. **미러 동작범위** 에서 **Local** 을 선택합니다.
8. **센서 운영모드** 의 경우 **Enforcement** 로 변경합니다.

9. **수정** 버튼을 클릭합니다.

Note: 로컬 미러는 트래픽 모니터링 기능을 추가로 사용 할 수 있습니다.

1. **트래픽 모니터링** 항목을 찾습니다.
2. **수집주기** 0 은 사용 안함, 최소 10 **초**, 최대 1 **일** 입니다.
3. **평균계산 시간** 은 최소 10 **초**, 최대 1 **일**, 초기값은 5 **분** 입니다.
4. **업데이트 최소값** 은 KB/s 단위이며, 트래픽 정보를 업데이트하는 최소값의 기본 설정값은 30 KB/s입니다.
5. **업데이트 변동폭** 은 % 단위이며, 최소 변동 백분율의 기본 설정값은 30 %입니다.
6. **목적지별 현황수집** 은 **On** 또는 **Off** 를 선택하고 대상에 따라 트래픽 정보를 수집합니다.

5.5 RADIUS 제어 설정

Genian ZTNA에는 무선 및 유선 802.1x 인증(인증서 또는 클라이언트 인증서)에 사용할 수 있는 RADIUS 서버가 내장되어 있습니다.

Genian ZTNA RADIUS 서버가 RADIUS 클라이언트/인증자(스위치, 컨트롤러, 엑세스포인트 등)의 인증 요청을 승인하기 위해서는 RADIUS 서버에 RADIUS 클라이언트로 추가해야 합니다. RADIUS 서버에 RADIUS 클라이언트를 추가하려면 하단 지침을 참조하시기 바랍니다.

또한 RADIUS 서버는 장비 정보를 정책서버 데이터베이스에 등록할 수 있으며 IP주소 및 기타 정보를 인증하는 RADIUS 계정을 통해 수집할 수 있습니다.

5.5.1 자체 RADIUS 서버 활성화

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 항목의 **서비스 > RADIUS 서버** 로 이동합니다.

RADIUS Secret 설정

1. **추가** 를 클릭하고 RADIUS 클라이언트(인증자)를 추가합니다.
2. **이름** 은 RADIUS 클라이언트(인증자)를 대표할 이름을 입력합니다.
3. **IP/Subnet** 은 허용할 RADIUS 클라이언트(인증자) 의 IP 주소를 입력합니다(여러 개일 경우 줄 바꿈을 통해 입력).
4. **CoA 포트번호** 는 CoA패킷을 수신할 RADIUS 클라이언트(인증자) 의 포트번호를 입력합니다(CoA 사용 참조).
5. **인증키** 의 경우, RADIUS 인증자(스위치, 컨트롤러, 엑세스포인트 등)를 인증하기 위해 미리 공유된 비밀키를 입력합니다.

RADIUS Authentication Server 설정

1. **포트번호** 에 RADIUS 인증 포트 번호(*Default is 1812*)를 입력합니다.
2. **인증대체** 의 경우 RADIUS 계정 패킷을 통해 자동으로 ZTNA 사용자에 대해 인증처리를 하려면 **On** 을 선택합니다.
3. **패킷타입** 의 경우 **Start** 및 **Stop** 체크박스를 선택합니다.
4. **노드검색방법** 의 경우 **MAC 또는 IP** 를 선택하고 노드와 일치시킬 속성을 선택합니다.

5. **적용대상** 에 대해 **모든 노드** 를 선택합니다.
6. **수정** 을 클릭합니다.

외부 RADIUS서버의 RADIUS Accounting 정보는 *RADIUS Accounting* 를 참조합니다.

5.5.2 802.1X 인증

IEEE 802.1X는 포트 기반의 네트워크 접근제어(*PNAC: port-based Network Access Control*)를 위한 IEEE 표준입니다. LAN 또는 Wireless LAN 에 연결하려는 단말에 인증 메커니즘을 제공합니다.

802.1X 인증에 필요한 구성요소는 아래와 같습니다. - supplicant (요청자) - authenticator (인증자) - authentication server (인증 서버)

요청자는 LAN / WLAN에 연결하려는 클라이언트 장치(예 : 노트북) 입니다. '요청자'라는 용어는 인증자에게, 자격 증명을 제공하는 단말에서 실행되는 소프트웨어를 나타내기 위해 서로 바꿔서도 사용합니다.

인증자는 이더넷 스위치 또는 무선 AP와 같은 네트워크 장비입니다. 인증자는 보호된 네트워크에 대한 보안 감시 역할을 합니다. 요청자는 신원이 확인되고 승인될 때까지 네트워크에 접근할 수 없습니다.

802.1X 포트 기반 인증을 사용하면 요청자는 사용자 이름 / 암호 또는 디지털 인증서와 같은 자격증명을 인증자에게 제공하고 인증자는 인증을 위해 자격증명을 인증 서버에 전달합니다. 인증 서버가 자격 증명이 유효하다고 판단하면 요청자(사용자 단말)는 네트워크의 보호된 쪽에 있는 리소스에 액세스 할 수 있습니다.

802.1x 설정

EAP 설정

사용자 자격증명을 어떤 데이터베이스에서 하는지에 따라 다른 설정이 필요합니다.

Active Directory or Genian 로컬 데이터베이스

1. 상단 항목의 **설정** 으로 이동합니다.
2. 좌측 메뉴의 **서비스 > RADIUS서버** 로 이동합니다.
3. **RADIUS Authentication Server** 항목으로 이동합니다.
4. **EAP 인증 > Protected EAP(PEAP) On** 선택합니다.
5. **기본 EAP 유형(PEAP)** 항목에 **MSCHAPv2** 를 선택합니다.
6. **수정** 을 클릭합니다.

LDAP (or 다른 데이터베이스)

1. 상단 항목의 **설정** 으로 이동합니다.
2. 좌측 메뉴의 **서비스 > RADIUS서버** 로 이동합니다.
3. **RADIUS Authentication Server** 항목으로 이동합니다.
4. **EAP 인증 > Protected EAP(PEAP)** 항목에 **On** 을 선택합니다.
5. **기본 EAP 유형(PEAP) 항목에 EAP-GTC 를 선택합니다.**
    - 원본 암호화 알고리즘이 *NT-HASH* 가 아닌 경우 GTC 인증서를 사용
    - GTC 인증서는 OS기본 제공사항이 아니기 때문에 Genian ZTNA 에이전트가 필요
6. **수정** 을 클릭합니다.

EAP-TLS

스마트 카드 또는 인증서가 있는 TLS와 같이 강력한 EAP 유형을 사용하는 경우, 클라이언트와 서버 모두 인증서를 사용하여 서로의 ID를 확인합니다.

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 항목의 **서비스 > RADIUS서버** 로 이동합니다.
3. **RADIUS Authentication Server** 메뉴 하단에서 확인합니다.
4. 아래 **EAP 인증 > EAP-TLS** 옵션의 **On** 설정을 선택합니다.
   - **CA 인증서** 오른쪽에 있는 **업로드** 버튼을 클릭하여 **CA 인증서** 를 업로드합니다.
   - **CA 인증서** 업로드 팝업창의 **+** 버튼을 클릭하여 CA의 인증 파일을 선택합니다.
   - **CA 인증서 정보** 항목에서 인증서의 정보를 확인 할 수 있습니다.
5. **서버인증서** 오른쪽에 있는 **서버인증서 생성** 버튼을 클릭합니다.
   1. 호스트명에 `ztna.genians.com`, FQDN(정규화된 도메인 이름) 또는 IP와 같은 **일반 이름** 을 입력합니다. (웹 브라우저에서 입력한 내용과 정확히 일치하지 않으면 오류가 발생합니다.)
   2. 국가 코드를 **국가** 로 입력하세요. `KR`, 두 글자 ISO 국가 코드입니다.
   3. 조직의 이름을 `Genians Inc.` 처럼 **조직** 으로 입력합니다.
   4. 이메일을 `admin@genians.com` 처럼 **전자메일** 로 입력합니다. 이메일 주소는 당신의 조직에 문의하는 데 사용됩니다.
   5. **서명요청서(CSR) 생성** 을 클릭합니다.
   6. 상자의 모든 텍스트가 **서명요청서(CSR)** 오른쪽에 복사 됩니다.
   7. CA 서버에 요청을 보내 서버 인증서를 발급하고, BASE64 인코딩된 파일을 열어, 상자에 있는 텍스트를 **인증서** 의 오른쪽에 복사하여 붙여 넣습니다.
   8. **등록** 버튼을 클릭합니다.
6. 인증서 해지 목록을 **CRL 배포 지점** 으로 입력합니다.. CRL을 확인하지 않으면 입력 할 필요가 없습니다.
7. 온라인 인증서 상태 프로토콜 응답자 URL 을 **OCSP 응답자 URL** 로 입력합니다. OCSP를 사용하지 않으면 입력 할 필요가 없습니다.
8. **수정** 버튼을 클릭합니다.

Note:

- EAP-TLS를 사용하려면 사용자는 서버에 인증서를 발급 한 동일한 CA 서버 또는 신뢰할 수있는 CA 서버에서 인증서를 얻어야합니다.
- 서버 인증서 및 사용자 인증서의 발급, 해지 및 관리는 외부 CA 서버를 통해 관리 됩니다.

Cisco 네트워크장비 기본 RADIUS 설정 방법

1. 스위치 AAA 설정

- 스위치에서 AAA 서버(RADIUS)를 등록하여 등록한 서버에서 인증을 수행할 수 있도록합니다.

```
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. 인터페이스 설정

- 각 인터페이스 802.1x 설정을 하여 포트에 장비가 연결되면 인증을 수행하도록합니다.

```
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: Cisco IOS 버전 별로 명령어가 다를 수 있습니다.

Note: 포트에 설정하는 타이머 및 인증 모드에 대한 자세한 내용은 Cisco 설명서를 참조하시기 바랍니다.

5.5.3 MAC Authentication Bypass (MAB)

일부 장치는 802.1X 인증을 지원하지 않습니다. 예를 들어 네트워크 프린터, 환경 센서, 카메라 및 무선 전화와 같은 이더넷 기반 전자 장치가 있습니다. 이러한 장치가 보호된 네트워크 환경에서 사용 되려면 해당 장치를 인증하기 위한 대체 메커니즘이 제공되어야합니다.

포트에 MAB가 구성되어 있으면 해당 포트는 먼저 연결된 디바이스가 802.1X를 준수하는지 확인하고 연결된 디바이스에서 응답이 없으면 연결된 디바이스의 MAC 주소를 사용자 이름 및 암호로 사용하여 RADIUS 서버에서 인증을 시도합니다. MAC 인증만 수행하도록 스위치 포트를 설정 할 수 있고 인증 순서 변경 옵션도 사용할 수 있습니다. 이것들은 스위치 제조사에 따라 다를 수 있습니다.

무선 네트워크의 경우 인증 방법은 일반적으로 SSID 단위로 설정되며 802.1X/WPA2E 또는 MAC 인증이지만 이 두가지가 아닌 경우도 있습니다.

MAC 인증 설정(MAB)

Genian ZTNA는 지정된 노드그룹을 통하여 네트워크 사용이 허용되는 MAC주소를 선택할 수 있습니다. 인증 요청된 MAC주소가 노드그룹에 포함되어 있는 경우 인증이 허용되고 그렇지 않으면 인증이 거부됩니다.

MAC 인증 설정 방법

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 패널의 **서비스 > RADIUS 서버** 로 이동합니다.
3. **RADIUS Authentications Server** 메뉴 아래에 설정이 있습니다.
4. **MAC 인증** 의 경우 MAC 인증 바이패스(MAB)를 사용하려면 **On** 을 선택합니다.
5. **노드 그룹** 의 경우 MAC 인증을 허용하려면 노드 그룹을 선택합니다.
6. **수정** 을 클릭합니다.

5.5.4 Authorization

AAA는 Authentication, Authorization, Accounting 을 의미합니다. 단말이 네트워크에 인증(authenticate)되면 수행하는 권한 허가(Authorization)는 선택적 사항입니다.

권한 허가는 한정된 접근 수준(VLAN or ACL)이나 장비의 연결 측면(QoS 속성 등)을 제어하는 장비 속성을 적용하는 방법입니다.

Genian ZTNA RADIUS 서버는 인증 후 VLAN을 할당합니다. RADIUS 서버 외부의 Genian ZTNA에서도 추가적인 접근제어가 가능합니다.(ACLs, ARP Enforcement, etc)

Authorization 설정

인증요청에 포함된 AD/LDAP 그룹 멤버십 또는 RADIUS 속성을 기준으로 초기인증을 완료할 수 있습니다. 또한 RADIUS CoA(Change of Authorization)는 노드그룹, 정책 미준수, 상태 변경 등과 같은 다른 기준에 따라 인증이 완료된 후 권한이 서로 다르게 부여합니다.

초기 Authorization 설정

Genian ZTNA는 네트워크에 연결할 때 장치의 속성을 지정할 수 있는 기능이 제공합니다. 사용자 이름과 같은 노드 인증 특성을 기반으로 VLAN, ACL 또는 기타 속성을 할당하는 데 사용할 수 있습니다. 추가로 이기능을 사용하여 인증 요청을 선택적으로 거부할 수 있습니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴의 **정책 > RADIUS 정책** 으로 이동합니다.
3. **작업선택 > 생성** 을 선택합니다.
4. 기본 설정인 **이름, 우선순위, 적용모드** 를 입력합니다.
5. **조건설정** 에서 **속성** 을 선택합니다.
6. **조건설정** 에서 **조건과 값** 을 입력합니다.
7. **조건설정** 을 **추가** 합니다.
8. **정책설정** 에서 정책 대상자에 대한 **접근정책** 을 선택합니다.
9. **생성** 을 클릭합니다.

Note: *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* 등의 RADIUS 속성을 사용 할 수 있습니다.

Attention: RADIUS 클라이언트 장치는 클라이언트 인증에 RFC2868 IEEE 802.1X 표준을 지원해야합니다.

CoA (Change of Authorization) 사용

네트워크 사용 중에 단말이 정책을 위반하는 등 네트워크에 인증된 후 상태가 변경되면 다양한 RADIUS 속성을 사용하여 장치에 대한 네트워크 접근을 제한 하거나 거부할 수 있습니다. 이것은 CoA(Change of Authorization, RFC 5176 - RADIUS 표준에 대한 동적 인증 확장) 라는 표준을 통해 제공 됩니다.

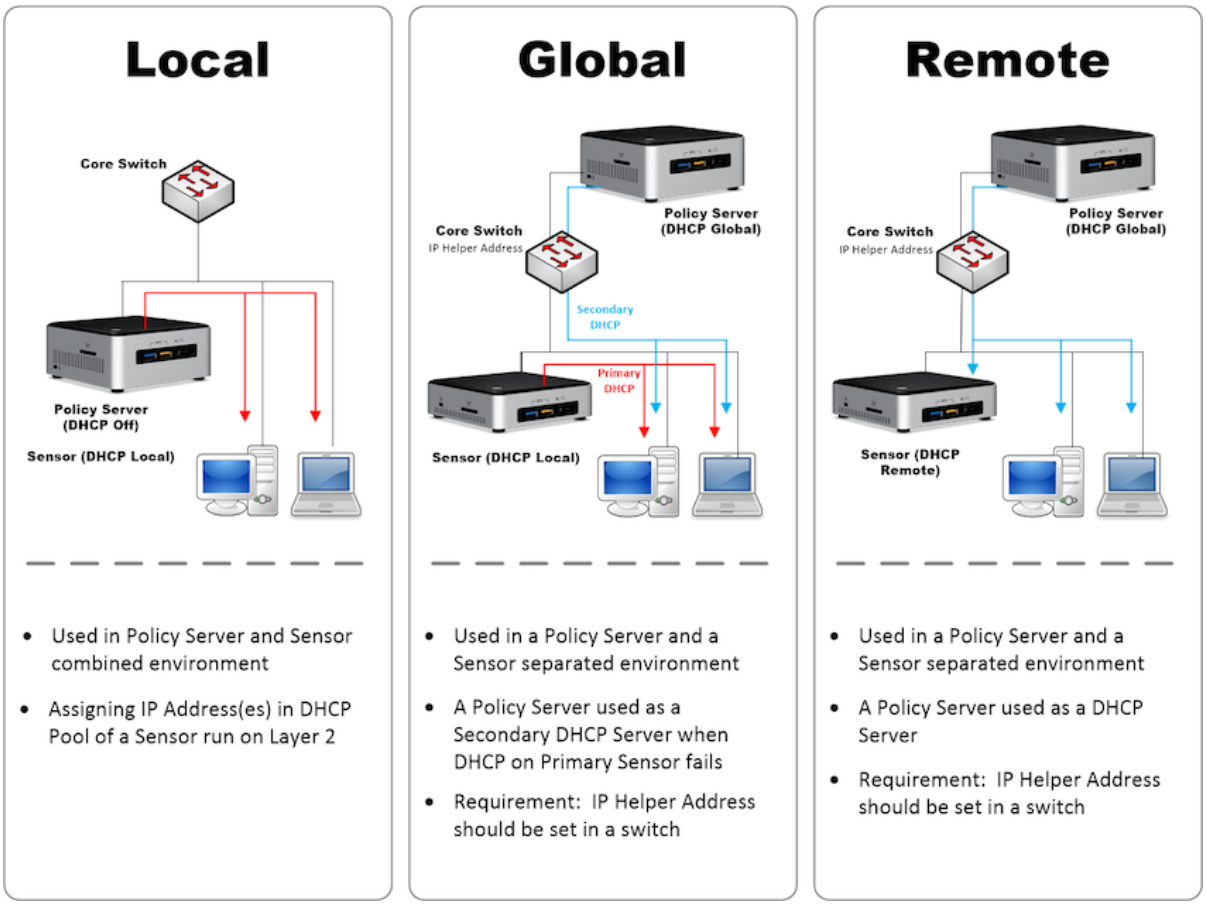
CoA는 제어 정책이 변경된 단말에 대한 현재 연결을 끊습니다. 연결이 끊어진 단말은 다시 연결을 시도한 다음 VLAN 할당을 통해 격리 된 VLAN으로 이동합니다.

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 항목에서 **정책 > 제어정책** 으로 이동합니다.
3. 연결을 끊을 제어 정책의 이름을 클릭합니다.
4. **제어 옵션 > RADIUS 제어** 에서 옵션을 선택합니다.
5. **RADIUS CoA** 에 옵션에 대해 **On** 을 선택합니다.
6. **CoA Command** 의 경우 표준 속성에 대해 **Terminate-Session** 을 선택하거나 다른 Generic-CoA를 선택하여 VSA(Vendor Specific Attribute) 를 입력합니다.
7. **Vendor-Specific-Attribute** 에 VSA 값(예: `Nas-filter-Rule='permit in tcp from any to any 23'`)을 입력합니다.
8. **수정** 을 클릭합니다.
9. 오른쪽 상단에 있는 **변경정책적용** 을 클릭합니다.

5.6 DHCP 서버 구성

DHCP (Dynamic Host Configuration Protocol)는 IP 네트워크에서 사용되는 표준화 된 네트워크 프로토콜입니다. DHCP는 IP 주소와 같은 네트워크 구성 매개 변수를 동적으로 배포하는 정책 서버 / 네트워크센서에 의해 제어됩니다. 자체적으로 제공하는 DHCP 옵션을 설정 관리하고 정책 서버 / 네트워크센서를 구성하여 세 가지 DHCP 서비스(로컬, 리모트, 로컬 과 리모트)를 활용할 수 있습니다.

요구 사항에 따라 DHCP에 대한 세 가지 옵션이 있습니다. (**로컬**, **리모트**, **로컬 과 리모트**)



5.6.1 DHCP 서비스 구성하기

- 네트워크센서 *DHCP* 서비스 설정하기

5.6.2 단말에 고정된 IP 할당하기

Genian ZTNA는 많은 환경들을 분석하여 DHCP 환경의 일부단말에는 고정적인 IP를 할당해야하는 상황을 지원하기 위하여 고정형 DHCP IP할당을 지원합니다.

1. Web콘솔 관리 > 노드로 이동합니다.
2. 고정적인 IP를 할당할 단말 좌측 체크박스에 체크합니다.
3. 작업선택 > IP/MAC 정책 > IP 충돌보호 및 변경금지를 클릭합니다.

- 충돌보호 및 변경금지를 설정하면 해당 IP는 설정단말에게만 할당됩니다.

5.6.3 DHCP Leases 관리

DHCP 서버가 단말에 할당 한 DHCP IP를 조회하고 삭제하는 기능입니다. 이 기능은 CLI (Command Line Interface)를 통해서만 사용 할 수 있습니다.

DHCP Lease 상태 보기

```
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
```

DHCP Lease 상태 지우기

```
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
```

5.7 스위치 포트 제어 설정

제어 정책 또는 수동 종료를 위한 스위치 포트 차단 및 VLAN 설정은 SNMP의 구성으로 시작되며, 포트 차단 및 VLAN설정에 필요한 정보와 액세스를 제공합니다. 기본 스위치 설정은 다음을 참고합니다. 스위치 찾아보기

5.7.1 제어정책의 스위치포트 차단 설정

스위치포트 차단대상은 제어정책에 따라 결정 됩니다. 특정 노드의 스위치 포트를 차단하려면 해당 노드를 대상으로 하는 제어정책을 생성한 다음 스위치포트 차단 옵션을 설정해야합니다.

1. 상위 항목의 **정책** 으로 이동합니다.
2. 왼쪽 항목의 **정책 > 제어정책** 으로 이동합니다.
3. 스위치포트 차단을 적용 할 제어정책의 원하는 **ID** 를 클릭합니다.

제어옵션 > 스위치포트 제어 에서 아래와 같이 설정합니다.

1. **스위치포트 제어** 옵션을 **포트차단** 으로 선택합니다.
2. **SNMP Community** 의 경우 기본 Community 문자열 또는 SNMPv# 사용자 및 비밀번호를 입력합니다. 이 설정이 비어 있으면 스위치 자체 설정을 사용합니다.
3. **차단포트 MAC 개수** 의 경우 스위치 포트의 MAC 수가 이 개수를 초과하면 차단되지 않습니다.
4. **Port Description** 의 경우 스위치 포트의 기존 설명에 추가할 텍스트를 입력합니다.
5. **수정** 버튼을 클릭합니다.

5.7.2 스위치 포트 종료

웹 UI에서 수동으로 **스위치 포트** 를 종료 할 수 있습니다.

1. 상위 항목의 **관리 > 스위치** 로 이동합니다.
2. **전체 스위치포트** 관리 뷰에서 **이름** 을 클릭합니다.
3. **관리자 Down** 옆의 **체크박스** 를 클릭합니다.
4. **수정** 버튼을 클릭합니다.

5.7.3 제어정책의 스위치 VLAN 설정

스위치포트 VLAN설정 대상은 제어정책에 따라 결정 됩니다. 특정 노드의 스위치 포트에 대한 VLAN을 설정하려면 해당 노드를 대상으로 하는 제어정책을 생성한 다음 스위치 VLAN설정 옵션을 설정해야합니다.

노드의 스위치 포트 이동에 따른 VLAN설정을 하기 위해서는 설정 > 환경설정 > 감사기록 > SNMP Trap 수신 설정이 필요하며, 스위치에서 MAC-Notification Trap 설정이 필요합니다.

1. 상위 항목의 **정책** 으로 이동합니다.
2. 왼쪽 항목의 **정책 > 제어정책** 으로 이동합니다.
3. 스위치포트 차단을 적용 할 제어정책의 원하는 **ID** 를 클릭합니다.

제어옵션 > 스위치포트 제어 에서 아래와 같이 설정합니다.

1. **스위치포트 제어** 옵션을 **VLAN설정** 으로 선택합니다.
2. **SNMP Community** 의 경우 기본 Community 문자열 또는 SNMPv# 사용자 및 비밀번호를 입력합니다. 이 설정이 비어 있으면 스위치 자체 설정을 사용합니다.
3. **수정** 버튼을 클릭합니다.

5.8 외부 시스템 연동

Note: 이 기능을 사용하려면 Enterprise Edition 이 필요합니다.

Genan ZTNA는 다양한 보안 벤더와 통합되어 보안 인텔리전스를 구축 할 수 있습니다.

5.8.1 Cisco VPN 연동 가이드

이 가이드는 CISCO VPN제품과 네트워크 접근제어 시스템인 Genian ZTNA의 연동을 위한 설정 방법에 대한 가이드입니다.

가이드 개요

CISCO VPN은 VPN 접속용 소프트웨어 AnyConnect를 사용자에게 제공하여, VPN 게이트웨이로 접속하여 인증과정을 거친 후, 내부네트워크로 접속할 수 있도록 합니다.

Genian ZTNA는 내부보안 관리를 위해 내부네트워크에 존재하는 단말에 대하여 가시성확보, 사용자 권한별 네트워크 접근제어, 단말의 보안정합성 제어방안을 제공합니다.

각각의 솔루션이 제공하는 기능을 연동하여, VPN 접속자에게 Genian ZTNA의 기능으로 구현된 보안정책에 만족하는지 체크 후 VPN 접속을 허용하기 위하여 본 연동을 진행하였습니다.

연동의 목적

Genian ZTNA와 CISCO VPN의 연동은 다음을 목적으로 합니다.

VPN 접속단말의 보안정합성 체크

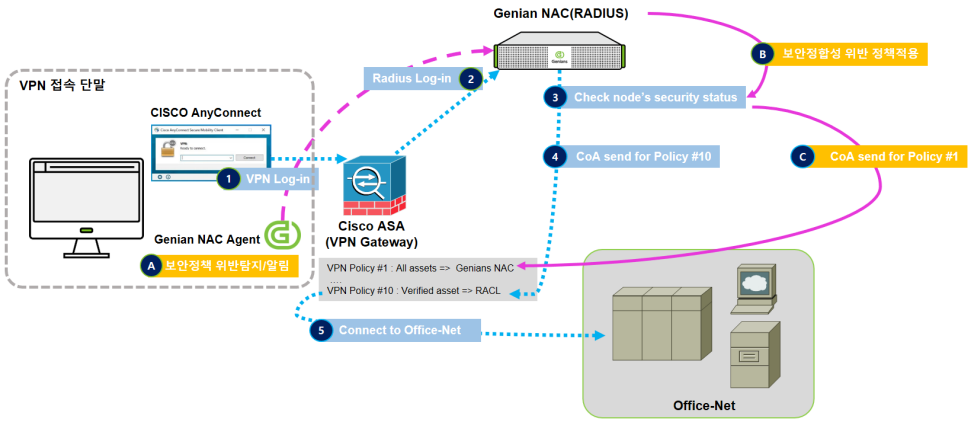
- VPN 접속단말은 VPN-Gateway가 제공하는 부분에만 한정하여 정보가 수집됩니다. 그러나 Genian ZTNA와 연동시, Genian ZTNA가 접속단말의 정합성 정보를 제공합니다.

VPN 접속단말의 보안정합성 결과에 따른 제어

- CISCO VPN과 Genian ZTNA의 연동으로 VPN 접속단말이 내부 네트워크로 진입하기 이전에 보안정합성을 판단하여 위협이 존재할 시, 네트워크 접속을 차단합니다.

  접속 당시 보안정합성이 통과되어 접속한 단말에 대해서도 정합성 위반시, 정합성을 다시 확보 할 수 있도록 네트워크를 차단 후, 보안정합성을 확보하도록 합니다.

연동의 시나리오 소개



[최초 접속 시]

(1) 사용자가 CISCO AnyConnect 를 이용하여 CISCO VPN Gateway 로 접속 시도

(2) CISCO VPN Gateway 는 사용자 인증서버로 Genian ZTNA 의 RADIUS 로 지정 및 차단정책적용(접속단말은 CWP 만 접속가능)

(3) Genian ZTNA 는 접속단말에 ZTNA Agent 설치시도 및 단말의 보안정합성 만족여부 체크

(4) 보안정합성 만족 시, AllowAll 정책을 부여할 것을 CISCO VPN Gateway 로 전송(CoA)

=> VPN 접속단말의 네트워크 진입

[접속중인 단말이 보안정합성 위반시]

(A) Genian ZTNA 의 Agent 가 접속단말의 보안정합성 체크 및 Genian ZTNA Policy-Center 로 위반정보 전송

(B) Genian ZTNA 는 정합성위반에 따른 차단정책적용

(C) 차단정책을 적용할 것을 CISCO VPN Gateway 로 전송(CoA)

=> 세션이 종료되며, 최초 접속시의 (3) 단계로 이동하여 이 후 과정을 거치게 됨

사전준비 사항

Genian ZTNA RADIUS 와 CISCO VPN Gateway 간 Secret Key 정하기

본 가이드에서 제시하는 연동의 구성은 CISCO VPN Gateway 의 인증서버가 Genian ZTNA(RADIUS) 가 되어 접속을 시도하는 모든 VPN User 는 Genian ZTNA RADIUS 로 인증을 받도록 구성됩니다.

두 장비 간의 안전한 연결을 위해 Secret Key 를 활용하도록 합니다.

CISCO VPN Gateway 사전준비

Change of Authorization(CoA) 가 지원되는 VPN 버전을 확인합니다.

권장버전은 다음과 같습니다.

장비 명	버전	참고
CISCO ASA	9.12(4) 이상	VPN Gateway
CISCO ASDM	7.13(1) 이상	CISCO 관리도구

Networking 사전 준비사항

Genian ZTNA Policy Center 와 CISCO VPN Gateway 간의 통신을 확인합니다.

기본 포트는 다음과 같습니다.

서비스명	Port	용도
RADIUS	1812(UDP)	Authentication protocol
RADIUS	1813(UDP)	Accounting protocol
CoA	3799(UDP)	CoA(change of authorization)

연동을 위한 CISCO VPN 설정

(CISCO VPN Gateway 의 설정은 Adaptive Security Device Manager(ASDM) 을 이용하였습니다)

Step 1: 정책 만들기

ASDM에서 Configuration > ACL Manager로 이동하여, Add를 클릭하여 다음과 같은 2개의 정책을 생성합니다.

정책이름	출발지	목적지	허용서비스
AllowAll	VPN 접속단말중, Genian ZTNA 인증을 거친 단말	업무용 네트워크, 인프라	업무용 서비스 포트
Redirect	모든 VPN 접속자	Genian ZTNA의 안내페이지만 접속가능	http, https

AllowAll 정책: VPN 접속단말이 Genian ZTNA에 설정된 보안정합성을 준수하면 해당정책(Allow)을 부여 받습니다.

Redirect 정책: VPN 최초 접속 시와 보안정합성 위반시 적용될 Redirect 룰입니다. 이 정책에 의해서 VPN으로 접속한 단말과 보안정합성을 위반한 단말은 모든 접속시도가 Redirect되어 Genian ZTNA의 CWP(사용자 안내페이지)로만 접속됩니다.

Step 2: 외부 인증서버(Authentication Server) 연동 설정

Configuration > Remote Access VPN > Network(Client) Access > AnyConnect Connection Profiles로 이동하여 Access interfaces 지정합니다.

설정 항목	설정 값	참고
Access interfaces	Enable CISCO AnyConnect VPN Client	
Outside	SSL Access Enable	

순서대로, Basic 메뉴에서 Authentication에서 다음과 같이 설정합니다.

설정 항목	설정 값	참고
Method	AAA	
AAA Server Group	ZTNA	

Advanced 메뉴에서 Accounting에서 Server Group은 ZTNA으로 설정합니다.

Step 3: CoA (Change of Authorization) 설정

Configuration > Remote access VPN > AAA/LocalUsers > AAA Server Groups로 이동하여, ZTNA서버 그룹을 만들어 줍니다. 다음과 같이 설정 해 줍니다.

설정 항목	설정 값	참고
Server Group	ZTNA	고정 값
Protocol	RADIUS	고정 값
Accounting Mode	Single	Single 선택
Reactivation Mode	Depletion	Depletion 선택
Dead Time	10	'10' 입력
Max Failed Attempts	3	'3' 입력
Enable dynamic authorization	체크	체크
• dynamic Authorization Port	3799	ISE Policy Enforcement

연동을 위한 Genian ZTNA 설정

Step 1: VPN 접속단말 관리를 위한 노드그룹 만들기

정책 > 그룹 > 노드 로 이동하여, **생성** 을 클릭하여, 다음 **3개** 의 노드그룹을 만들어 줍니다.

VPN을 통해서 접속하는 단말을 상태별로 관리하기 위한 노드그룹을 만듭니다.(Genian ZTNA에서 노드그룹은 노드의 관리단위입니다.)

(1) VPN으로 접속한 노드그룹(VPN access policy) 노드그룹 만들기

VPN을 통해서 접속한 모든단말을 대상으로 지정하는 그룹입니다. 다음과 같은 조건으로 만들어 줍니다.

설정 항목	설정 값	참고
조건연산	'(AND) 아래의 모든조건을 만족하면' 선택	
조건설정 > 추가 > 접속장치/접속포트	'연결방식이 같으면', '가상 IF' 각각 선택	
조건설정 > 추가 > 인증사용자	'인증타입', 'RADIUS 인증' 각각 선택	

(2) VPN 접속노드용 보안정합성을 충족하는 노드그룹(VPN Compliance) 만들기

VPN 접속단말을 대상으로 적용할 보안정합성 점검요소를 확인하기 위한 노드그룹으로 본 가이드에서는 Genian ZTNA의 에이전트 동작상태와 백신정보 존재여부를 예)로 들어 설명합니다. 보안정합성 요건은 각사의 VPN 접속사용자에 대한 보안정책의 요건들을 추가하시기 바랍니다.

설정 항목	설정 값	참고
조건연산	'(AND) 아래의 모든조건을 만족하면' 선택	
조건설정 > 추가 > 노드그룹	'속하면', 'VPN access policy' 각각 선택	
조건설정 > 추가 > 에이전트상태	'동작상태', 'Up' 각각 선택	보안정합성 점검요소 1
조건설정 > 추가 > 백신정보	'백신정보 존재여부', '존재함' 각각 선택	보안정합성 점검요소 2

(3) VPN 접속단말용 보안정합성을 충족하지않는 노드그룹(VPN NonCompliance) 만들기

VPN 접속단말 중, 보안정합성에 위배되는 단말을 제어하기 위한 그룹을 만들어 줍니다.

설정 항목	설정 값	참고
조건연산	'(AND) 아래의 모든조건을 만족하면' 선택	
조건설정 > 추가 > 노드그룹	'속하면', 'VPN access policy' 각각 선택	
조건설정 > 추가 > 노드그룹	'속하지 않으면', 'VPN Compliance' 각각 선택	

Step 2: VPN 접속단말 관리를 위한 제어정책 만들기

정책 > 제어정책 으로 이동하여, **생성** 을 클릭하여, 다음 **2개** 의 노드그룹을 만들어 줍니다.

Genian ZTNA는 접속단말의 네트워크 사용권한을 할당하기 위해서 제어정책을 활용합니다. VPN 보안정합성에 따라 다른 권한을 부여하기 위해서 각각의 제어정책을 생성해 줍니다. (Genian ZTNA의 정책은 순서대로 적용받습니다)

(1) 보안정합성 미검증 제어정책 만들기

VPN으로 접속한 최초접속자와 접속중이던 사용자가 보안정합성에 위배되는 행위를 하였을 때, 적용받는 정책으로 Genian ZTNA의 안내페이지(CWP)로만 접속이 허용됩니다.

다음과 같이 설정해 줍니다.(보안정합성이 확보된 단말 정책보다 상단에 설정합니다)

설정 항목	설정 값	세부 설정
노드그룹 설정	VPN Non-Compliance	다음 2 개의 조건을 모두만족 해야함.(1.VPN access policy 노드그룹에 속함 2.VPN Compliance 그룹에 속하지 않음)
권한설정	PERM-DNS	Genian ZTNA CWP 만 접속허용 권한
RADIUS CoA 설정	'On' 선택	CoA 사용
CoA Commands	Reauthenticate host(CISCO VSA)	재인증 요청

(2) VPN 보안정합성 검증 제어정책 만들기

VPN으로 접속한 단말의 보안정합성 검증이 완료된 후, 정상적인 네트워크 활용을 위한 정책을 만들어줍니다.

아래와 같이 설정해 줍니다.

설정 항목	설정 값	세부 설정
노드그룹 설정	VPN Compliance	다음 3 개의 조건을 모두만족 해야함.(1.VPN access policy 노드그룹에 속함 2.ZTNA 에이전트가동작중이어야 함 3. 백신정보 존재함)
권한설정	PERM-ALL	네트워크 접근권한 설정
RADIUS CoA 설정	'On' 선택	CoA 사용
CoA Commands	Use vendor-specific-attribute(VSA)	참고. CoA 는 제조사에 따라 다름
Vendor-SpecificAttribute	Cisco-AVPair=ACS:CsicoSecure-Defined-ACL=AllowAll	참고. 앞서 CISCO ASA 에 정의한 AllowAll 을 적용하도록 함

참고: 보안적합성이 검증되어 아래정책을 적용받는 단말이 보안위배 사항이 발생하면, 다시 보안정합성 미검증 정책이 부여됩니다.

Step 3: RADIUS 정책 만들기

정책 > RADIUS 정책 으로 이동하여, 기본설정이 적용된 적용을 활용합니다.

VPN 접속시, 사용자의 인증을 위한 RADIUS서버를 설정하는 과정입니다.

연동기능을 활용하기 위해서는 기본제공하는 RADIUS 정책 중에서 **VPN_NonCompliant** 정책과 **VPN_Compliant** 정책의 두개만 설정하면 됩니다.

(1) RADIUS 정책: VPN_NonCompliant 정책 수정하기

최초로 접속한 VPN 사용자와 VPN 사용자중 보안정합성을 위반한 사용자를 위한 RADIUS 정책을 기본 제공되는 정책을 아래와 같이 수정/추가해 줍니다. (권장설정은 입력되어있음)

다음과 같이 조건을 설정합니다.

속성	조건	값	참고
NAS-Port-Type	속성값이 같으면	Virtual	
Calling-Station-id	노드그룹에 포함되면	컴플라이언스 위반노드	기본 제공 노드그룹
조건연산		'(AND) 모든조건을 만족하면' 선택	

다음과 같이 정책을 설정합니다. (조건에 부합하는 경우에 해당정책의 적용을 받습니다)

정책이름	값	참고
Cisco-AVPair (url-redirect-acl)	속성값이 같으면	
Cisco-AVPair (url-redirect)	https://a.b.c.d/CWP2 (정책서버 ip/cwp2)	해당정책으로 인해 접속단말의 기본접속 URL 은 Genian ZTNA 의 CWP 로 지정됨

(2) RADIUS 정책: VPN_Compliant 정책 수정하기

보안정합성을 조건을 만족하는 사용자의 RADIUS 정책을 아래와 같이 기본 제공되는 정책을 수정합니다. (권장설정은 입력되어있음)

다음과 같이 조건을 설정합니다.

속성	조건	값	참고
NAS-Port-Type	속성값이 같으면	Virtual	
Calling-Station-id	노드그룹에 포함되지 않으면	컴플라이언스 위반노드	조건에 주의
조건연산		'(AND) 모든조건을 만족하면' 선택	

다음과 같이 정책을 설정합니다. (조건에 부합하는 경우에 해당정책의 적용을 받습니다)

정책이름	값	참고
Filter-id	AllowAll	보안정합성이 확보된 접속단말을 네트워크 사용 허용

Step 4: RADIUS 서비스 만들기

정책 > 서비스 > RADIUS 서버 로 이동하여 설정합니다.

VPN 접속시, 사용자의 인증을 위한 RADIUS서비스를 설정하는 과정입니다.

- RADIUS Secret 설정

  클라이언트 설정 > 추가를 클릭하여 다음과 같이 설정합니다. (RADIUS 서버 접속 사전 설정)

설정 항목	설정 값	참고
이름	CISCO-VPN	CISCO VPN 접속 Client
IP/Subnet	192.168.50.0/24	접속 IP 주소/서브넷
CoA 포트번호	3799	기본 값은 3799(변경가능)
인증키	Secret-key	CISCO ASA 와 공유키

본 가이드에서는 CISCO ASA VPN을 통해서 접속하는 구성이므로 CISCO VPN, Network Access Server(NSA) 에 대한 설정을 합니다.

이하 RADIUS 서버에 대한 설정은 기본설정 값을 활용해도 됩니다.

CISCO VPN과 Genian ZTNA의 연동설정 완료

CISCO VPN과 Genian ZTNA의 연동을 위한 설정이 완료되었습니다.

정상 동작여부의 테스트를 위해서,

VPN 접속단말이 최초 접속시의 노드그룹과 보안정합성 검증여부 확인 시의 **노드그룹** 이 **변경** 된 것을 확인하도록합니다. 노드그룹이 변경된다면 연동설정이 정상적으로 적용되어 있는 상태입니다.

확인 방법은

1) **정책 > 제어정책** 에서 VPN 접속단말이 **적용받는 제어정책** 을 확인하셔도 되고,

2) **관리 > 노드** 에서 **VPN 접속단말의 그룹** , **적용받는 정책** 이 변경된 것을 확인할 수 있습니다.

작업이 완료되었습니다.

5.8.2 Infoblox-DDI 연동 가이드

이 가이드는 Genian NAC와 Infoblox DDI 연동에 대한 정보를 제공합니다.

가이드 개요

이 가이드는 Genian NAC와 Infoblox-DDI를 연동하여 Infoblox-DDI가 악성 사이트에 접속을 시도하는 노드를 탐지하고, 해당 노드를 Genian NAC의 접근제어 기능을 활용하여, 자동화된 대응이 가능함을 보여줍니다. 또한, 두 제품간의 연동으로 infoblox-DDI의 Secure-DNS를 전사 노드에 활용할 수 있도록 Genian NAC를 이용하여 네트워크 전체를 대상으로 모든 노드의 DNS 설정 정보 확인/교정 기능을 제공합니다.

연동의 목적

Genian NAC와 infoblox-DDI를 연동하여, 다음과 같은 장점 및 효과를 IT관리자와 사용자에게 제공합니다.

관리대상 노드의 자동판단

- Genian NAC는 네트워크 상의 모든 장치들에 대해서 정보를 수집하고, 이 것을 기반으로 자동 분류하고 그룹을 생성합니다.
- infoblox-DDI는 Genian NAC로 IP를 전달하면, Genian NAC 는 이 IP에 대해서 추가적인 정보를 활용하여, 제어대상 여부를 자동으로 판단하여 제어합니다.

이상단말의 빠른 식별과 교정시간의 단축

- Infoblox-DDI에서 GenianNAC로 IP 및 로그 정보를 보내면, Genian NAC는 Infoblox-DDI의 정보와 Genian NAC가 직접 수집한 이 노드에 대한 정보를 관리자에게 신속하게 제공한다.
- 그리고 이 비정상적인 노드는 Genian NAC를 통해서, 네트워크 격리 등 즉시 대응할 수 있습니다.

관리범위의 확대

- Genian NAC는 L2-네트워크 계층에서 네트워크 접속 제어를 수행합니다.
- Genian NAC는 관리대상 네트워크에 존재하는 모든 IP를 가지는 노드를 찾아내고, 해당노드의 추가적인 정보를 수집/분석하여 특성에 따라 노드를 자동분류, 그룹화합니다.
- 관리자는 Genian NAC, infoblox-DDI가 제공하는 정보를 통하여 관리해야 할 대상과 범위를 더 잘 이해할 수 있습니다.

연동을 위한 infoblox-DDI 설정

Step 1: RPZ(Response Policy Zones) Policy 추가(또는 설정)**

Data management > DNS > Response Policy Zones로 이동합니다.

- RPZ 정책을 만듭니다(기존의 black-rule에 추가하셔도 됩니다)

  (본 가이드에서는 기존의 Black 룰과 별도의 다른 이름으로 만들어서 테스트 했습니다.)

Step 2: Syslog 전송설정

RPZ monitoring에서 Genian NAC로 전달하기 위한 설정입니다.

'Grid > Grid Manager > setting icon(Grid properties icon)을 선택합니다.

- 'Monitoring'을 선택하여, Genian NAC-policy 정책서버의 IP를 설정합니다.
- External Syslog 설정에서 RPZ-rule에만 적용하여 전송하도록 선택합니다. (다중으로도 구현 가능합니다.)

연동을 위한 Genian NAC 설정

Step 1: Syslog 수집설정

infoblox-DDI가 전송한 이벤트를 받기 위한 설정입니다.

설정 > 환경설정 > 감사기록 > Syslog 감사기록 저장으로 이동하여 필터를 추가합니다.

설정 항목	설정 값	참고
필터이름	infoblox-filter	program,host,match,netmask 중 선택
필터타입	host	정책의 설명을 작성.
필터값	172.29.52.3	infoblox-DDI 장비 IP
IP 키값	SRC=	IP정보를 읽을 키값을 설정
문자셋	유니코드(UTF-8)	일반적으로 UTF-8을 사용

Step 2: 제어를 위한 Tag 추가하기

Genian NAC는 타 장비와 연동 등에서 유연하고 다양하게 활용하기 위하여, Tag 기능을 제공합니다.

Infoblox DDI와의 연동 시에는, infoblox의 로그에서 제공하는 위험 등급에 따라 3종류의 Tag를 생성, 적용하였습니다.

(infoblox-DDI의 RPZ 정책의 위험도에 따라서 나누었습니다)

- 설정 > 속성관리 > 태그 관리 > 작업선택 > 생성으로 이동합니다.
- 태그를 생성합니다. (태그의 이름, 설명 등을 입력 후, 'Save'합니다.)
- 본 가이드에서는 이해를 돕기 위해 'Infoblox-DDI-Isolation'으로 설명합니다.

Step 3: 제어정책 적용을 위한 로그필터 생성과 Tag 적용정책 만들기

Genian NAC는 유용한 로그필터 기능을 제공합니다.

로그의 값들을 이용하여 원하는 형태로 필터링하여 필터링된 정보를 기반으로 정책화할 수 있는 구조로 만들어져 있습니다.

1. 로그필터 생성하기

로그 필터를 만들기 위해, '감사 > 로그'로 이동합니다.

infoblox의 로그에서 제공하는 정보 검색필터 조건은 다음과 같이 작성합니다.

설정 항목	설정 값	참고
설명	passthru-major	구분을 위해 중복이름은 피해서 작성합니다.
로그 타입	알림	제어 방식을 선택합니다.
로그 ID	Syslog	infoblox에서 활용하는 RPZ-policy의 구성요소 이름

필터를 만든 후, 우측의 '저장' 버튼을 눌러서 저장하면, 로그 필터의 생성은 완료됩니다.

2. 로그필터를 통해 추출된 로그에 Tag 적용하기

로그필터 설정 창에서 추출된 노드에게 Tag를 적용하여, Infoblox-DDI가 제어할 수 있도록 설정합니다.

설정 항목	설정 값	참고
태그 (Tag)	할당	Tag의 상태를 설정합니다.
검색 대상	노드	검색의 대상을 지정합니다.
할당 대상	노드	태그(Tag)의 할당 대상을 노드로 합니다.
태그 (Tag) 추가	Infoblox-DDI-Isolation	연동을 위한 Genian NAC 설정에서 정해 둔 태그(Tag) 명을 설정합니다.

연동을 위한 설정이 완료되었습니다.

5.8.3 FireEye의 연동 가이드

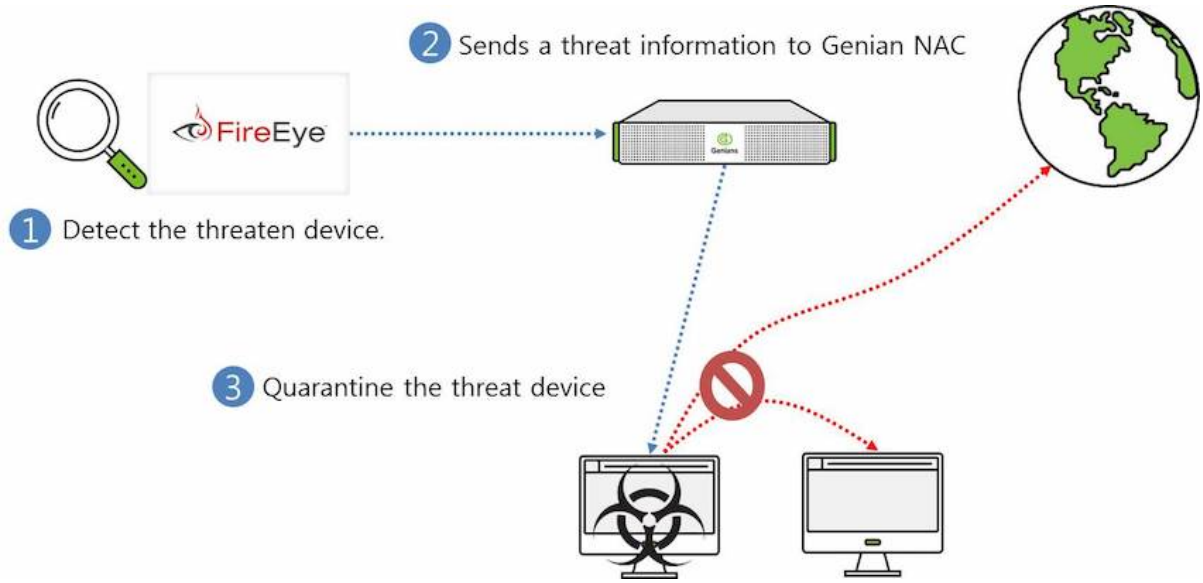
본 가이드에서는 Genian ZTNA와 FireEye와 연동하는 방법을 안내합니다.

가이드 개요

FireEye에 의해 특정 이상 징후가 감지되면 FireEye는 SYSLOG를 통해 Genian ZTNA에 이상 징후 정보를 전송합니다.

Genian ZTNA는 이상 징후 대상을 격리하여 이상 징후가 확산되는 것을 방지 할 수 있도록합니다.

FireEye를 이용한 Genian ZTNA 구축 구성



1. FireEye가 위협 단말을 감지합니다.
2. FireEye는 이상 정보를 SYSLOG를 통해 Genian ZTNA로 전송합니다.
3. Genian ZTNA는 위협 단말을 격리하여 위협 단말이 다른 네트워크에 연결 할 수 없습니다.

SYSLOG를 통한 FireEye 연동 구성

Genian ZTNA의 설정

Genian ZTNA는 FireEye에서 위협 단말에 대한 알림메시지를 SYSLOG로 수신하기 때문에 관련 설정 추가가 필요합니다.

CEF(Common Event Format, 공통 이벤트 포맷)를 사용하여 FireEye로부터 데이터를 수신하려면 다음 단계를 완료해야합니다.

1. 관리자 계정으로 Genian ZTNA에 로그인
2. 상단 항목의 **설정** 탭으로 이동
3. 왼쪽 항목의 **환경설정 > 감사기록** 이동
4. **Syslog 감사기록 저장** 옵션 에 필터 **추가**
5. 정보를 입력합니다.

필터이름	FireEye
필터타입	host
필터값	[FireEye의 IP]
IP 키값	src=
MAC 키값	smac=

6. 하단 **추가** 버튼을 클릭 하고 **수정** 버튼을 클릭

FireEye 설정

FireEye 어플라이언스는 알림 출력과 관련하여 매우 유연하며 다음 형식을 지원합니다.

- CEF
- LEEF
- CSV

본 가이드에서는 CEF를 사용합니다. CEF를 사용하여 Genian ZTNA에 데이터를 보내려면 다음 단계를 수행해야합니다.

1. 관리자 계정으로 FireEye 어플라이언스에 로그인합니다.
2. 상단 항목의 **Settings** 탭으로 이동합니다.
3. 왼쪽 항목의 **Notifications** 로 이동합니다.
4. 가운데에 있는 **rsyslog** 를 클릭합니다.
5. 확인란에 있는 "Event type" 을 확인합니다.
6. **Rsyslog setting** 이 있는지 확인합니다.

```
Default format: CEF
Default delivery: Per event
Default send as: Alert
```

7. 아래에 **Add Rsyslog server** > Genian ZTNA **Name** 입력 > **Add Rsyslog Server** 버튼을 클릭합니다.
8. IP 주소 필드에 Genian ZTNA의 IP 주소를 입력합니다.
9. 아래의 **Update** 버튼을 클릭합니다.

검증

위의 단계를 완료하게 되면 Genain ZTNA는 FireEye로부터 SYSLOG 메시지를 수신 할 수 있습니다.

1. 상단 항목의 **감사** 로 이동합니다.
2. 로그 메시지가 표시되면 **LogID** 는 FireEye입니다.

FireEye 데이터를 기반으로 Genian ZTNA 정책 적용

Genian ZTNA가 FireEye에서 SYSLOG 데이터를 수신하면 로그 파일에 포함 된 장치 정보를 사용하여 개별 노드에 태그를 자동으로 적용 할 수 있습니다. 이러한 태그를 사용하여 조직 또는 정책 목적으로 노드를 그룹화 할 수 있습니다.

감사로그 태그를 통해 정책을 적용하려면 태그를 이용한 정책 적용 을 참조하십시오.

5.8.4 Genian GPI 연동 가이드

이 가이드는 Genian ZTNA와 Genian GPI 간의 연동에 대한 정보를 제공합니다.

가이드 개요

본 가이드는 사용자 PC의 정보보안 수준 진단, 평가를 통해 PC의 보안성 확보 및 사용자의 보안 의식을 강화하기 위한 Genians의 솔루션, Genian GPI(Genian Policy Inspector)와 네트워크 접근제어 시스템인 Genian ZTNA의 연동 기능을 수행하기 위한 설정방법 및 연동 기능의 테스트 방법을 안내하는 문서입니다.

Genian GPI는 보안성이 확보된 PC에 한하여 네트워크 사용을 허가하도록 Genian ZTNA와의 연동 설정을 Web콘솔에서 제공합니다. (별도의 기능 추가/설정 불필요)

연동 기능이 설정되면, Genian GPI는 수치화한 PC의 정보보안 수준 정보를 Genian ZTNA로 전송하고, Genian ZTNA는 정보보안 수준이 미흡 단계의 PC를 네트워크에서 차단한 후, 사용자에게 PC의 교정을 위한 안내페이지에만 접속할 수 있도록 하여, 정보보안 수준이 확보된 PC만을 네트워크에 접속할 수 있도록 동작합니다.

권장 버전

제품명	버전	비고
Genian GPI	V4.0.12 이상	정책서버 버전 (2020.10 이후 버전)
Genian ZTNA	V6.0 이상	정책서버 버전 (2022.5 이후 버전)

연동의 목적

Genian ZTNA와 Genian GPI의 연동은 다음의 효과를 제공합니다.

1. **취약 PC의 강제조치, 자동제어 수행**

- Genian GPI가 진단한 점수를 기준으로 Genian ZTNA에서 네트워크 격리, 강제 수행 등의 정책이 자동으로 적용되어 관리자의 개입없이 강제화 수행이 가능합니다.

2. **조치 대상의 사용자에게 조치에 대한 사유 및 차등 안내페이지 자동 연결**

- Genian GPI에서 진단한 점수에 따라 Genian ZTNA가 조치한 PC의 초기 접속페이지를 차등 적용하여 차단된 사유 안내 및 차단된 사유를 해소하여 정상적으로 네트워크 사용을 위한 조치 방법에 대한 안내 페이지를 제공합니다. (예, GPI 지수 70~80 구간: 에이전트를 통한 단순 안내, 40점 미만: 네트워크 차단 및 강제 조치 수행, 안내페이지만 접속 가능 등)

사전준비 사항

Genian GPI Agent 배포대상, 설치여부 확인 및 공용 PC의 담당자 선정 확인
Genian GPI는 PC의 정보보안 점검을 위해 Agent를 이용합니다.

배포대상에 Genian GPI Agent가 설치되었는지 확인하고, 특정 사용자가 존재하지 않는 공용 PC는 담당자를 선정하시기 바랍니다. 만약 Genian GPI Agent가 설치되어있지 않거나 담당자를 선정하지 않은 경우 관리 대상에서 제외됩니다.

(Agent 설치 유무 확인 방법은 각 제품 별 Web콘솔에서 확인 가능합니다.)

Networking 사전 준비사항
두 제품간의 통신은 TCP/443, TCP/3306을 이용하여 통신합니다.

(Genian ZTNA 의 접속 포트정보는 Web콘솔에서 **시스템 > 서비스 관리 > 접속포트** 에 있습니다.)

연동을 위한 Genian GPI 설정

PC 보안점검 설정

1. Genian GPI Web콘솔에서 **보안점검 > 점검정책 관리** 메뉴로 이동
2. **사이버보안 진단의 날 > (우측) 관리** 에서 **정책점검 수정(연필모양)** 아이콘 클릭
3. 점검 대상자 설정

설정 항목	설정 값	참고
대상자	항목: IP주소 / 조건: IP가 같으면 / 대상자: 점검대상자	셀렉트 박스를 통해 설정 값 입력
설정	192.168.100.40	대상자 값에 따른 설정 값 입력
점검일시	x일 후 xx시 xx분 부터	점검 일시 입력 (정책 설정 시간 이후부터 적용)

4) 우측 상단 **저장** 버튼 클릭하여 저장

Genian ZTNA와 연동 설정

1. Genian GPI Web콘솔에서 **환경설정 > 보안점검 > 보안점검 결과 점수 > 보안점검 점수를 NAC와 연동하는 옵션** 항목으로 이동
2. **NAC** 텍스트 좌측 체크박스에 체크
3. 보안점검 점수를 수신할 Genian ZTNA 정책서버의 IP주소 입력

연동을 위한 Genian ZTNA 설정

본 가이드에서 다루는 Genian ZTNA 의 설정 부분은 Genian GPI 와 연동을 위해 최소한의 부분만을 소개합니다. 본 과정은 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: GPI 점검 미수행 그룹 제어를 위한 노드그룹 생성
정책 > 그룹 > 노드 메뉴로 이동하여 다음과 같이 1 개의 노드그룹을 설정 후 생성합니다.

설정 항목	설정 값	참고
기본정보 > ID	GPI_사이버보안 진단의 날_미수행 그룹	노드그룹 이름 입력
기본정보 > 설명	GPI 사이버보안 진단의 날 규제정책을 수행하지 않은 그룹입니다.	노드그룹 설명 입력
기본정보 > CWP 메시지	귀하의 PC는 사이버보안 진단의 날 규제정책을 수행하지 않아 네트워크가 차단되었습니다. 네트워크 접속을 원하시면 사이버보안 진단의 날 규제정책을 수행하시기 바랍니다.	CWP 페이지에 표시될 메시지 입력
기본정보 > 적용모드	사용함	사용함 선택
기본정보 > 감사로그	Off	On, Off 중 선택
그룹조건 > 조건연산	AND	AND, OR 중 선택
그룹조건 > 조건설정	항목: 노드타입 / 조건: 감지된 노드타입이 같으면 / 설정: PC	노드타입 조건 추가
	항목: GPI 점수 / 조건: 규제정책이 존재하지 않으면 / 설정: 사이버보안 진단의 날	GPI 점수 조건 추가. (설정 부분에서 GPI 정책명 입력)

Step 2: GPI 점검 미수행 그룹 격리를 위한 제어정책 생성
정책 > 제어정책 메뉴로 이동 한 후 **작업선택 > 생성** 셀렉트박스를 클릭 하면 제어정책 마법사가 실행됩니다. **제어정책 마법사** 에서 제공하는 순서에 따라 제어정책을 생성합니다.

설정 항목	설정 값	참고
정책 선택	신규생성	신규생성 선택
정책 기본설정 > ID	GPI_사이버보안 진단의 날_미수행_격리 정책	제어정책 이름 입력
정책 기본설정 > 설명	GPI의 사이버보안 진단의 날 규제정책을 수행하지 않은 노드를 격리하기 위한 정책입니다.	제어정책 설명 입력
정책 기본설정 > 순서	2	제어정책 순서 입력
정책 기본설정 > 적용모드	사용함	사용함 선택
노드그룹 할당	GPI_사이버보안 진단의 날_미수행 그룹	Step 1 에서 생성한 그룹선택
권한 할당	PERM-DNS	격리를 위해 PERM-DNS 선택
제어옵션설정 > 사용자 메시지		CWP 페이지에 표시될 메시지 입력
제어액션		제어액션 할당

Note:

- **제어옵션설정 > 사용자 메시지** 는 Step 1의 사용자 메시지와 중복되므로 공백 처리
- 본 가이드에서는 격리 과정만 수행하므로 **제어액션** 은 공백 처리

Step 3: GPI 점검 점수 70점 미만 격리를 위한 노드그룹 생성

정책 > 그룹 > 노드 메뉴로 이동하여 다음과 같이 1개의 노드그룹을 설정 후 생성합니다.

설정 항목	설정 값	참고
기본정보 > ID	GPI_사이버보안 진단의 날_70점 미만 그룹	노드그룹 이름 입력
기본정보 > 설명	GPI 사이버보안 진단의 날 규제정책 70점 미만 그룹	노드그룹 설명 입력
기본정보 > CWP 메시지	귀하의 PC는 보안점수가 70점 미만이므로 네트워크가 차단되었습니다. 네트워크 접속을 원하시면 PC 조치 후 상태 재검사를 수행하시기 바랍니다.	CWP 페이지에 표시될 메시지 입력
기본정보 > 적용모드	사용함	사용함 선택
기본정보 > 감사로그	Off	On, Off 중 선택
그룹조건 > 조건연산	AND	AND, OR 중 선택
그룹조건 > 조건설정	항목: 노드타입 / 조건: 감지된 노드타입이 같으면 / 설정: PC	노드타입 조건 추가
	항목: GPI 점수 / 조건: 점수가 보다 낮으면 (점수,GPI정책) / 설정: 설정: 70, 사이버보안 진단의 날	GPI 점수 조건 추가. GPI 점수 조건 추가 (설정 부분에서 점수와 GPI 정책명 입력, 점수 '70' 입력 시 70점 미만으로 설정됨.)

Step 4: GPI 점검 점수 70점 미만 그룹 격리를 위한 제어정책 생성

정책 > 제어정책 메뉴로 이동 한 후 **작업선택 > 생성** 셀렉트박스를 클릭 하면 제어정책 마법사가 실행됩니다. **제어정책 마법사** 에서 제공하는 순서에 따라 제어정책을 생성합니다.

설정 항목	설정 값	참고
정책 선택	신규생성	신규생성 선택
정책 기본설정 > ID	GPI_사이버보안 진단의 날_70점 미만_격리 정책	제어정책 이름 입력
정책 기본설정 > 설명	GPI의 사이버보안 진단의 날 규제정책 점수가 70점 미만인 노드를 격리하기 위한 정책입니다.	제어정책 설명 입력
정책 기본설정 > 순서	3	제어정책 순서 입력
정책 기본설정 > 적용 모드	사용함	사용함 선택
노드그룹 할당	GPI_사이버보안 진단의 날_70점 미만 그룹	Step 3 에서 생성한 그룹선택
권한 할당	PERM-DNS	격리를 위해 PERM-DNS 선택
제어옵션설정 > 사용자 메시지		CWP 페이지에 표시될 메시지 입력
제어액션		제어액션 할당

Note:

- **제어옵션설정 > 사용자 메시지** 는 Step 3의 사용자 메시지와 중복되므로 공백 처리
- 본 가이드에서는 격리 과정만 수행하므로 **제어액션** 은 공백 처리

연동 결과 확인

연동을 위한 설정 작업 완료 후, 진단을 수행한 PC의 보안점검 점수가 기준 미달일 경우의 동작 테스트 과정입니다. (본 테스트 과정은 Genian ZTNA와 Genian GPI의 Agent가 설치되어 있는 상태에서 진행하였습니다.)

Step 1: 192.168.100.40 PC에서 Genian GPI 보안점검 수행

1. 우측 하단 **Tray 메뉴 - Genian GPI** 에서 **열기** 항목 클릭
2. 우측 상단 **점검시작** 버튼 클릭 후 점검 수행
3. 점검 수행 후 점수 70점 미만 확인

Step 2: Genian GPI Web콘솔 "보안점검 > 개인별 점검결과(월별)" 에서 점수 확인

- 192.168.100.40 IP에 사이버보안 진단의 날 점수 70점 미만 확인

Step 3: Genian ZTNA Web콘솔 "감사 > 로그" 에서 이벤트 발생 확인

- 192.168.100.40 IP에 **GPI 점수 추가 감지됨** 이벤트 확인

Step 4: Genian ZTNA Web콘솔 "정책 > 제어정책" 에서 "GPI_사이버보안 진단의 날_70점 미만_격리 정책" 에 포함되었는지 확인

- 192.168.100.40 IP에 70점 미만 격리 정책 할당 확인

Step 5: 192.168.100.40 PC에서 네트워크 접속 시도 테스트

- 네트워크가 차단되며, 안내페이지에서 차단된 메시지 확인
- 안내페이지 메시지: 귀하의 *PC*는 보안점수가 *70*점 미만이므로 네트워크가 차단되었습니다. 네트워크 접속을 원하시면 *PC* 조치 후 상태 재검사를 수행하시기 바랍니다.

5.8.5 Paloalto PAN-OS Single Sign On(SSO) 연동 가이드

이 가이드는 Genian NAC와 Paloalto PAN-OS 제품간의 Single Sign On(SSO) 연동에 대한 정보를 제공합니다.

가이드 개요

이 문서는 Next Generation Firewall(NGFW) 시스템인 Paloalto의 PAN-OS와 네트워크 접근제어 시스템인 Genian NAC의 연동을 위한 설치와 설정 방법에 대한 가이드입니다.

두 제품간 사용자 인증정보를 연동하여 Genian NAC에서 인증한 사용자는 Paloalto PAN-OS에서 추가적으로 인증하지 않더라도 내부 시스템에 접근 할 수 있도록 하며, Paloalto PAN-OS가 Genian NAC의 사용자-노드의 결합된 정보를 이용하여, 사용자 기반의 접근제어 정책을 활용할 수 있도록 도움을 줍니다.

연동의 목적

Genian NAC와 PAN-OS의 연동은 다음의 효과를 제공합니다.

Single-Sign-On(SSO)

- Genian NAC는 사용자가 노드를 사용하려 하거나 회사의 네트워크에 접속하기 위해서 필수적으로 로그인 절차를 거치도록 합니다. 이 로그인 정보를 이용하여 PAN-OS에서는 별도로 인증하는 불편함을 해소하며, 사용자 기반의 보안 정책을 구현하는데 도움을 줍니다.

사용자기반 정책구현, 정보불일치 해소

- 실제 노드의 사용자 정보를 보유하고 있는 Genian NAC의 사용자 정보를 이용하여, 신규 입사자, 부서이동, 근무위치의 변경 등의 사유로 인한 노드와 실제 사용자 정보의 불일치 되는 문제를 해결할 수 있습니다.

<연동시의 인증/사용자 접근제어 프로세스>

1. Genian NAC에서 사용자 인증
2. Genian NAC가 인증정보(IP, User-ID)를 Paloalto PAN-OS로 전송 (XML API, syslog)
3. 등록된 노드(IP) 정보와 사용자정보의 조합: PAN-OS
4. 사용자정보가 확인된 IP에 태그 할당: PAN-OS
5. 사용자 기반의 제어: PAN-OS

사전준비 사항

networking 사전 준비사항

- Genian NAC Policy Center와 Paloalto PAN-OS간의 통신을 확인합니다.
- 본 가이드에서는 XML API (http, https) 방식과 syslog방식의 두가지 방법을 제시하고 있으므로 활용하고자 하는 방법에 따라 확인바랍니다.

구현방식	권장설정(보안수준 높음)	간편설정(연결성 높음)
XML API	https (8443)	http (80)
Syslog	TLS (6514)	UDP (514)

Genian NAC의 접속 포트정보는UI에서 '시스템 > 서비스 관리 > 접속포트'에 있습니다.

XML API를 이용한 연동

XML API 연동을 위한 paloalto PAN-OS 설정

본 문서에서 다루는 PAN-OS의 설정에 대한 설명은 Genian NAC와의 연동을 위한 부분에 한합니다.

Step 1: 사용자인증정보의 처리를 위한 관리자 역할 생성하기

Device >Admin roles 으로 이동한 후, Add를 선택하면, Admin Role Profile창이 나타납니다.

Admin Role Profile 창에서의 입력 값은 다음과 같습니다.

설정 항목	설정 값	참고
Name	Genian_NAC_SSO	Admin role의 이름 설정
Description	Admin role의 용도를 서술	생략 가능
XML API탭	모든 항목을 Enable 해줍니다. (본 가이드의 기능만을 활용할 경우는 Report, Export, Import의 기능은 생략가능)	Report, Log, Configuration, Operational Requests, Commit, User-ID Agent, Export, Import 모두를 enable 함

Step 2: 사용자 인증정보 처리를 위한 관리자 계정 생성하기

Device >Administrators 로 이동한 후, Add를 선택하면, Administrator 추가 창이 나타납니다.

Administrator 창에서의 입력 값은 다음과 같습니다

설정 항목	설정 값	참고
Name	Genian_NAC	계정의 이름 설정
Authentication Profile	None	별도 설정하지 않음
Use only client certification authentication (Web)	설정 안함	계정의 Password를 이용하여 접근권한을 확인하므로 별도로 설정하지 않음 (API-Key를 확인하는 경우에 설정)
Use Public Key Authentication(SSH)	설정 안함	
Administrator Type	Role Based 선택	Step 1에서 생성된 권한을 상속함
Profile	Genian_NAC_SSO	Admin Role과 동일하게 설정
Password Profile	None	별도 설정하지 않음

Step 3: 사용자 인증정보를 전송하기 위한 API-Key 생성하기

웹브라우저를 이용하여, *[https://PAN-OS IP/api/?type=keygen&user=[username]&password=[password]]* 를 입력하여 API-Key를 생성합니다.

웹브라우저에 위와 같이 입력하면, 다음의 결과를 얻을 수 있습니다.

```
#Script
<response status='success'>
<result>
<key>
↪LUFRPT1KbW80SU1hRXJuNk5XNHBudUhCNGMydE0rSUk9RFIzdEJ5RGcwWkRCVlhYMXl0Q1FPdz09
</key>
</result>
</response>
```

여기서 생성된 API-Key를 이용하여, Genian NAC가 인증정보를 PAN-OS로 전송합니다.

Step 4: Genian NAC로부터 사용자 인증정보 수신시 SSO동작을 위한 구성하기

Network > *Zone* 으로 이동하여, Enable User Identification 선택 후 'OK' 클릭 (인증된 사용자는 사용권한을 할당 받습니다)

XML API 연동을 위한 Genian NAC 설정

Genian NAC에서 사용자가 인증시 발생하는 로그를 활용하여, PAN-OS로 XML API(webhook)를 전송하도록 설정하는 과정에 대한 설명입니다.

Step 1: 사용자가 Genian NAC에 인증시 발생하는 로그에 대한 검색필터 만들기

검색필터를 만들기 위해 감사 > 로그검색 으로 이동합니다.

사용자 인증시 PAN-OS로 전송해야 하므로 다음과 같이 로그 검색조건을 적용합니다.

설정 항목	설정 값	참고
로그ID	인증	셀렉트박스에서 선택
설명	사용자가 인증됨	사용자 인증시의 로그 중, 키워드 설정

위의 조건으로 로그 검색시, 사용자 인증과 관련한 로그가 존재하는 지 확인 후, 저장합니다.

Step 2: 검색필터 이벤트 발생시, PAN-OS로 이벤트 전송설정하기

Step1에서 만든 검색필터의 '저장'을 클릭하면, 검색필터를 설정화면이 나타납니다.

여기에서 다음과 같이 설정합니다.

설정 항목	설정 값	참고
이름	사용자 로그인 정보 전송	검색필터의 이름
설명	사용자가 로그인 시의 로그를 PAN-OS로 전송하기 위함	
Webhook	선택, 로그인 이벤트 발생시 API 호출을 위함	XML API
태그	할당, 검색대상:사용자, 할당대상:노드, 태그:인증사용자	

Webhook 설정: 다음과 같이 입력합니다.

설정 항목	설정 값	참고
방식	POST	
URL	https://XXX.XXX.XXX.XXXX/api/?type=user-id&action=set&key	PAN-OS의 IP
CHARSET	UTF-8	
POST 데이터	아래 POST 데이터 입력값 참고	
데이터 전송 타입	multipart/form-data	
API-Key	팔로알토 PAN-OS 설정 Step3 에서 만든 API-Key 입력	

POST 데이터 입력값

```
<uid-message>
  <version>1.0</version>
  <type>update</type>
  <payload>
      <login>
        <entry name="{ID}" ip="{_IP}" timeout="20" />
      </login>
  </payload>
</uid-message>
```

Syslog를 이용한 연동

Syslog 연동을 위한 paloalto PAN-OS 설정

본 문서에서 다루는 PAN-OS의 설정에 대한 설명은 Genian NAC와의 연동을 위한 부분에 한합니다.

Step 1: 사용자 인증정보의 수신을 위한 Syslog 설정하기

1. *Device* > *User Identification* > *User Mapping* 으로 이동한 후, User-ID Agent Setup 탭에서 Edit 버튼을 선택합니다.
2. Syslog filter를 선택하고 Add를 클릭하면 Syslog Parse profile 설정 창에 다음과 같이 설정 값을 작성합니다.

설정 항목	설정 값	참고
Syslog Parse Profile	Genian_NAC	Syslog Parse의 이름 설정
Description		생략가능
Type	Field Identifier	Syslog의 Type을 지정합니다.
Event String	USERAUTH	Genian NAC에서 전송시의 메시지 구분 값
Enter a Username Prefix	ID=	Genian NAC에서 인증한 사용자의 ID
Enter a Username Delimiter	, (comma)	구분자
Enter a Address Prefix	IP=	Genian NAC에서 인증한 사용자 노드의 IP
Enter a Address Prefix	, (comma)	구분자

Step 2: 사용자 인증정보의 Syslog 송신자 지정하기

Device > *User Identification* > *User Mapping* 으로 이동한 후, Server Monitoring 부분에서 Add 를 클릭하여 User Identification Monitored Server 설정 창에 다음과 같이 작성합니다

설정 항목	설정 값	참고
Name	Genian_NAC	계정의 이름 설정
Description		생략가능
Enabled	Enabled 선택	동작 선택
Type	Syslog Sender 선택	
Network Address	Genian NAC IP	Genian NAC의 정책서버 IP
Connection Type	UDP	SSL(default) 와 UDP중 선택
Filter	Genian_NAC 선택	Genian NAC에서 전송하는 정보 중 특정정보만 받기 위한 Filter선택

Step 3: Syslog Listener 서비스 활성화

Network > *Network Profiles* > *Interface Mgmt* 로 이동한 후, ADD를 클릭하면, syslog Listener New profile이 나타납니다.

- 다음과 같이 설정 값을 작성합니다.
  1. Network Profile: Allow Genian NAC
  2. User-ID SYSLOG Listener-SSL 또는 User-ID SYSLOG Listener-UDP 선택

설정을 완료하고, 'OK'를 클릭하면 the interface management profile로 이동합니다.

Step 4: Interface Management에 Genian NAC의 접근 허용하기

Network > *Interfaces* 를 선택한 후, 해당 인터페이스의 설정을 확인, 설정합니다. (UDP를 이용하는 경우 UDP/514, SSL을 이용하는 경우는 TCP/6514 입니다)

Advanced > *Other info* > *Interface Management Profile* 로 가서 Allow Genian NAC를 선택한 후, 'OK'를 클릭합니다.

설정을 반영하기 위해, 'Commit'을 클릭합니다.

Syslog 연동을 위한 Genian NAC 설정

Genian NAC에서 사용자가 인증시 발생하는 로그를 PAN-OS로 Syslog로 전송하도록 설정하는 과정에 대한 설명입니다.

Step 1: 사용자가 Genian NAC에 인증시 발생하는 로그에 대한 검색필터 만들기

검색필터를 만들기 위해 '* 감사 > 로그검색* '으로 이동합니다.

사용자 인증시 PAN-OS로 전송해야 하므로 다음과 같이 로그 검색조건을 적용합니다.

설정 항목	설정 값	참고
로그ID	인증	셀렉트박스에서 선택
설명	사용자가 인증됨	사용자 인증시의 로그 중, 키워드 설정

위의 조건으로 로그 검색시, 사용자 인증과 관련한 로그가 존재하는 지 확인 후, 저장합니다.

Step 2: 검색필터 이벤트 발생시, PAN-OS로 이벤트 전송 설정하기

Step1에서 만든 검색필터의 '저장'을 클릭하면, 검색필터를 설정화면이 나타납니다, 다음과 같이 설정합니다.

설정 항목	설정 값	참고
이름	사용자 로그인 정보전송	검색필터의 이름
설명	사용자가 로그인 시의 로그를 PAN-OS로 전송하기 위함	
SYSLOG 전송	선택, 사용자로그인시 Paloalto PAN-OS로 Syslog 전송	아래 Syslog 설정 입력값 참고
태그	할당, 검색대상:사용자, 할당대상:노드, 태그:인증사용자	

Syslog 설정 입력값

설정 항목	설정 값	참고
서버주소	Paloalto PAN-OS의 IP입력	
전송방법	UDP	UDP, TLS 중 선택
전송포트	514	UDP(514), TLS(6514)
포맷	Default	Default, CEF 중 택1
Syslog 메세지	USERAUTH, ID={ID}, IP={_IP}	
CHAER-SET	UTF-8	일반적으로 UTF-8

연동 동작 테스트: Paloalto PAN-OS에서 Genian NAC에서 전송한 사용자 로그인 이벤트 수신 확인하기

연동구성 완료 후, 다음과 같이 동작 테스트를 합니다.

1. Command Line Interface(CLI) 에서 확인하기

'*show user ip-user-mapping all*' 을 입력하여 수신된 정보를 확인합니다.

```
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
```

위와 같이, 수신된 정보가 확인되면, 정상적으로 설정이 된 것입니다.

2. WEB User-interface(UI) 에서 확인하기

Monitor > *Logs* > *User-ID* 로 이동하면, Genian NAC의 인증을 통해 전달된 인증목록을 확인할 수 있습니다

5.8.6 Paloalto PAN-OS에서 탐지한 위협노드 격리를 위한 연동 가이드

이 가이드는 Genian NAC와 Paloalto PAN-OS 제품간의 위협노드 탐지에 따른 노드의 격리를 위한 연동관련 정보를 제공합니다.

가이드 개요

이 문서는 Next Generation Firewall(NGFW) 시스템인 Paloalto의 PAN-OS와 네트워크 접근제어 시스템인 Genian NAC의 연동을 위한 설치와 설정 방법에 대한 가이드입니다.

이 문서에서 설명드릴 태그를 이용한 Paloalto PAN-OS와 Genian NAC의 연동은 Paloalto PAN-OS에서 탐지한 위협정보의 노드를 이용하여 Genian NAC가 위협노드가 네트워크로 진입하기 이전에 차단하여 회사의 네트워크를 위협에 최소화 하며, Genian NAC가 사용자용 노드에게 보안교정도구의 제공 및 노드 사용자를 위한 차단안내가이드를 적용할 수 있도록 태그를 적용하는 과정에 대한 것입니다.

연동의 목적

Genian NAC와 PAN-OS의 연동은 다음의 효과를 제공합니다.

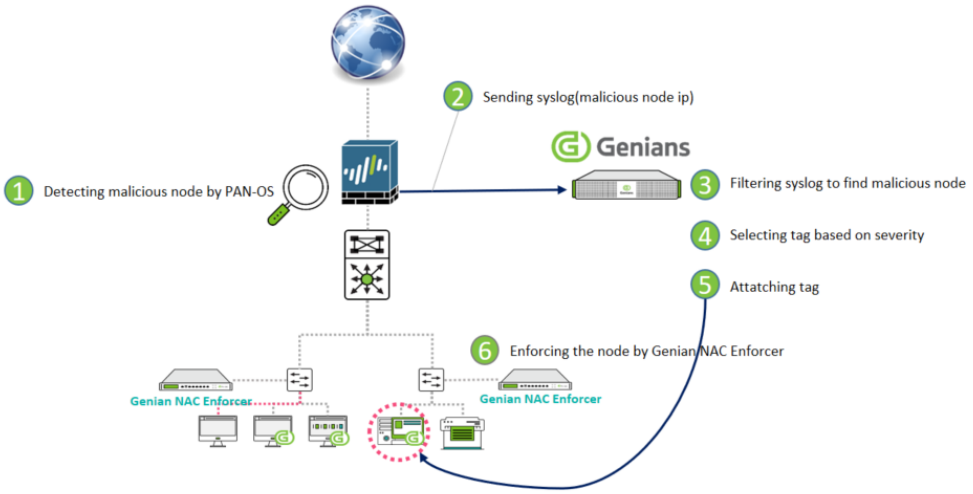
위협의 범위를 최소화하여 노드의 네트워크 차단 수행

- Genian NAC의 차단용 센서는 사용자 노드와 동일한 네트워크 레벨에 설치되어 동작합니다. 노드의 네트워크 접근을 차단하는 동작지점이 위협의 노드와 동일한 네트워크에서 수행하므로, 상대적으로 확산을 최소화 하여 노드를 격리합니다.

노드의 위험 수준에 따른 격리, 교정, 알림정책 적용

- Genian NAC는 노드의 정보 수집을 위해 사용자 노드에 Agent를 설치하여 운영합니다. 그러므로, Genian NAC의 관리서버가 어떤 노드에서 위협이 탐지되었다는 정보를 PAN-OS로부터 수신한 후, 탐지된 위험의 수준에 따라 네트워크 격리, 노드의 특정 서비스 중단 또는 어플리케이션의 삭제와 같은 제어 그리고 사용자가 네트워크 사용을 위한 접속 시도 시, 격리된 사유와 해결방법등을 제시하는 방식의 적용 등의

노드의 위험 수준에 따른 제어방법을 선택적으로 적용할 수 있습니다(예. 태그 생성 시, high, medium, low로 생성)



<접근제어 연동프로세스>

1. 위협노드 탐지: PAN-OS
2. IP정보 전송 (syslog): PAN-OS
3. Malicious node에 대한 syslog 추출: Genian NAC 정책서버
4. 위험도, 위험의 카테고리에 따른 선별: Genian NAC 정책서버
5. Tag 적용: Genian NAC 정책서버
6. Tag에 따른 노드의 제어: Genian NAC 센서

사전준비 사항

networking 사전 준비사항

- Genian NAC Policy Center와 Paloalto PAN-OS간의 Syslog 통신을 확인합니다.

구현방식	TCP	UDP
Syslog	TLS (6514):TLSv 1.2	UDP (514)

Genian NAC의 접속 포트정보는UI에서 '시스템 > 서비스 관리 > 접속포트'에 있습니다.

(TLS 이용 시, Paloalto PAN-OS가 TLSv 1.2만 지원합니다.)

연동을 위한 paloalto PAN-OS 설정

본 문서에서 다루는 PAN-OS의 설정에 대한 설명은 Genian NAC와의 연동을 위한 부분에 한합니다.

Step 1: Syslog Server profile 생성하기

Device > *Server Profiles* > *Syslog* 로 이동한 후, Add를 선택합니다.

(만약, PAN-OS 제품이 여러 개일 경우, Location을 선택합니다)

- *Syslog server Profile* 창에서의 입력 값은 다음과 같습니다.

설정 항목	설정 값	참고
Name	Genian_NAC_Tag	존재하는 Tag 중, 유일한 이름을 설정
Syslog Server	IP주소 또는 도메인 이름(FQDN)	Genian NAC의 정책서버 IP를 입력합니다.
Transport	TCP, UDP, SSL 중에서 선택합니다.	SSL일 경우 TLSv1.2만 지원합니다.
Port	통신포트를 지정합니다.	TLS, TCP는 6414, UDP 514로 입력합니다.
Format	BSD, IETF, IETF(SSL,TLS) 중 선택	기본 값은 BSD입니다.

Step 2: 트래픽, 위협 정보, Wildfire를 위한 Syslog 전송 설정하기

트래픽 정보, 위협 정보, 그리고 보안 위협에 자동대응 하도록 만들어진 WildFire의 전송을 위한 설정입니다.

(기존에 존재하던 Log Forwarding Profile을 선택하셔도 되고, 신규로 만들어 주셔도 됩니다.)

Objects > *Log Forwarding* 을 선택하면 나타나는 *Log Forwarding Profile* 설정 창 에 다음과 같이 입력합니다.

1. Profile의 이름을 정해줍니다.
2. 각 로그 별로 type을 지정하고 위험도를 정하고 Syslog Server의 Profile을 선택합니다. (Genian_NAC_Tag 선택)

연동을 위한 Genian NAC 설정

Syslog 연동을 위한 paloalto PAN-OS 설정

Paloalto PAN-OS가 위협노드 정보를 syslog로 Genian NAC으로 전송 시, Genian NAC에서의 처리를 위한 설정에 대한 안내입니다.

Step 1: paloalto PAN-OS가 전송한 정보를 수신하기 위한 syslog 서버 설정하기

설정 > 환경설정 > 감사기록 으로 이동합니다.

Syslog 감사기록 저장에서 추가 를 클릭한 후, 다음의 설정 값을 입력합니다.

설정 항목	설정 값	참고
필터 이름	PANOS_critical	
필터 타입	host	Program, Host, Match, netmask중 택1
필터 값	xxx.xxx.xxx.xxx	PAN-OS 장비의 IP
IP키 값	src=	노드의 IP
MAC 키 값	입력하지 않음	
User 키값	입력하지 않음	
문자셋	유니코드(UTF-8)	

작성 후, 추가 를 클릭합니다.

Step 2: 제어를 위한 Tag 추가하기

Genian NAC는 타 장비와 연동 등에서 유연하고 다양하게 활용하기 위하여, Tag 기능을 제공합니다. PAN-OS와의 연동 시에는, PAN-OS의 로그에서 제공하는 위험 등급에 따라 제어정책을 적용하기 위하여 3종류의 Tag를 생성, 적용하였습니다. (원래 PAN-OS는 Critical, High, Medium, Low, Informational을 제공하지만, 위험도가 높은 3가지에 대해서만 작성했습니다)

설정 > 속성관리 > 태그 관리 *로 이동한 후, *작업선택 > 생성 을 클릭하여 태그를 생성합니다.

Step 3: 제어정책 적용을 위한 로그필터 만들기 및 위협노드에 태그적용하기

Genian NAC는 유용한 로그필터 기능을 제공합니다.

로그필터기능은 로그의 값들을 사용자가 자유롭게 검색한 정보를 기반으로 정책화 할 수 있는 구조로 만들어져 있습니다. 다시 말하면, 필터링 가능한 정보가 담긴 로그라면 Genian NAC는 대상노드를 제어할 수 있다는 의미입니다.

본 연동가이드에서는 PAN-OS의 로그의 설명 중, 'Severity:critical'+ 'category:malicious' 가 포함된 것을 검색하여, 필터를 만들고, 이 필터에 해당하는 로그의 노드에 태그를 적용하는 것을 예로 설명합니다.

로그필터 만들기

1. 감사 > 로그 로 이동합니다.
2. 로그검색창에서 Add Filters를 클릭하면 필터 설정화면 이 열립니다.
3. 설정화면 중, 설명 란에 *'Severity:critical'+ 'category:malicious'* 를 적용하여 검색합니다.
4. 필터를 만든 후, 우측의 *'Save'* 버튼을 눌러서 저장하면, 로그필터가 만들어 집니다.
5. 원하는 정보만 남았는지 확인하여 필터에서 잘못된 정보가 나타나지 않도록 설정을 완료합니다.

위험도에 따른 태그적용 설정하기

로그필터에서 가려낸 노드에 태그를 적용하기 위하여, 필터 하단부의 태그를 *NONE* > 할당 으로 변경하고 다음과 같이 입력합니다.

설정 항목	설정 값	참고
검색대상	노드	
할당대상	노드	
태그 추가	PANOS-Critical	아래의 Threat Log Fields 참고하여 설정합니다.

이렇게 설정하면 PAN-OS에서 탐지된 위협의 수준(severity)와 분류(category)에 따라 노드에 태그가 적용됩니다.

참고: PAN-OS의 로그 중, 위험도, 분류와 같이 유용한 필터정보는 PAN-OS Threat log field 를 참조바랍니다.

Step 4: 제어정책 만들기

Genian NAC는 정책을 생성할 때 그룹단위로 적용합니다. 그러므로 노드를 그룹에 추가해 주어야합니다.

태그가 적용된 노드그룹 만들기

정책 > 그룹 > 노드 로 이동한 후, 작업선택 > 생성 을 클릭합니다.

설정 부분의 기본정보를 작성 한 후, 하단 부의 '그룹조건'에서 다음과 같이 설정합니다.

설정 항목	설정 값	참고
조건 연산	OR	AND 또는 OR 선택
조건 설정 > 항목	태그	
조건 설정 > 조건	존재하면	설정유무, 존재하면, 존재하지 않으면 중 택1
조건 설정 > 설정	PANOS-critical	

작성 후 '생성'을 클릭합니다.

태그가 적용된 제어정책 만들기

정책 > 제어정책 으로 이동한 후, 작업선택 > 생성 을 클릭합니다.

정책생성 마법사를 이용하여 정책을 생성합니다. 다른 과정은 모두 동일하며, 노드그룹할당 부분에서 *PAN-OS critical* 을 선택하여 적용합니다.

정책을 생성한 후, 우측 상단부의 '변경정책적용'을 클릭하면 연동작업은 완료됩니다.

5.8.7 Paloalto Networks Firewall의 연동 가이드

이 가이드에서는 Palo Alto 방화벽을 통한 연동에 대한 내용을 제공합니다.

가이드 개요

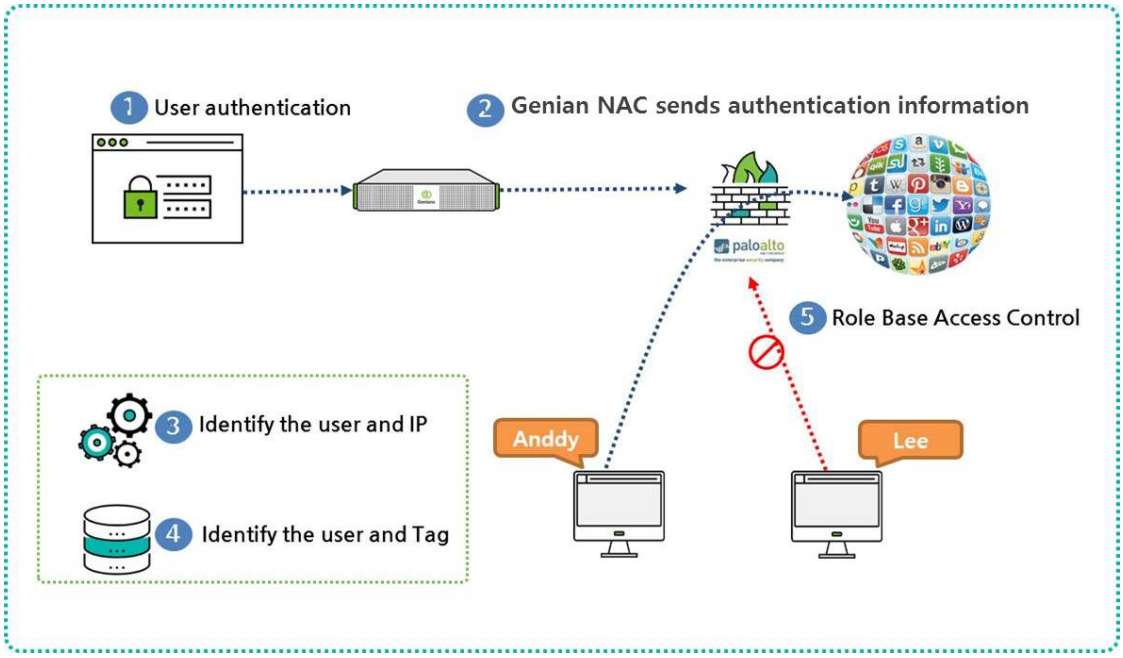
이 가이드는 Genian NAC 엔지니어 및 기업 운영자가 Genian NAC 및 PAN 방화벽과 협력하여 PAN 인증 방화벽에 사용자 인증 정보를 보내는 방법에 대해 설명합니다.

PAN 방화벽은 일반적으로 사용자가 부서 나 위치를 변경 할 때 IP 정보가 변경되고 이에 따라 할당 된 권한이 수정 되도록 요구합니다. IP 기반 방화벽 정책은 누가 IP를 사용하고 있는지 알지 못하지만 Genian NAC와 협력하여 IP에 대한 사용자 정보를 얻을 수 있습니다.

이 정보를 바탕으로 사용자의 부서 또는 위치가 이동되고 IP 정보가 변경 되더라도 사용자는 방화벽의 규칙을 수정하지 않고 각 사용자에게 할당 된 권한을 적용 할 수 있습니다. 관리자의 내부 인프라 운영 및 보안을 효율적으로 향상시킵니다.

PAN Firewall을 이용한 Genian NAC 구축

Genian NAC는 인증 연동을 제공합니다. PAN 방화벽은 Genian NAC에서 제공하는 IP 및 사용자 인증 정보를 참조하여 정보에 태그를 할당하고 PAN 방화벽에서 생성 된 USER-ID 및 매핑을 수행하여 PAN 방화벽의 사용자 역할에 의한 액세스 제어를 가능하게합니다.



인증 프로세스는 다음과 같습니다.

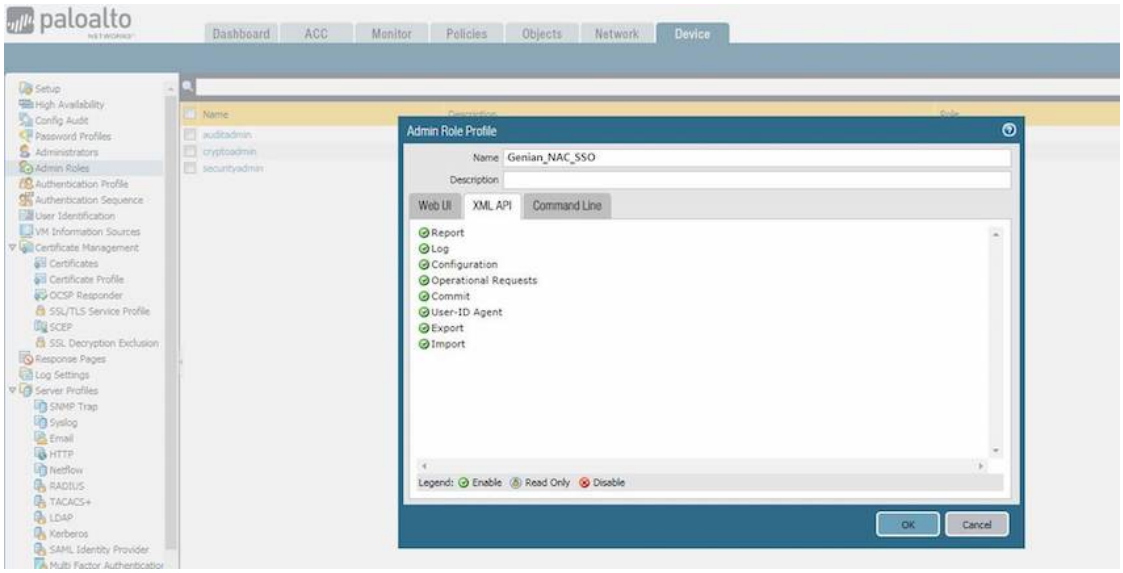
1. Genian NAC의 사용자 인증
2. Genian NAC는 인증 사용자 및 IP 정보를 PAN 방화벽에 보냅니다.
3. PAN 방화벽은 인증 사용자와 Genian NAC에서받은 IP 정보를 자체 사용자 ID 테이블과 비교합니다.
4. PAN은 User-ID에 할당 된 태그를 확인합니다.
5. 각 사용자에게 할당 된 태그를 기반으로 역할 별 액세스 제어 정책이 수립됩니다.

XML API를 통해 연동을 위한 PAN Firewall 구성

1. PAN 방화벽에서 관리자 역할 생성

먼저 웹에서 관리자 역할을 생성

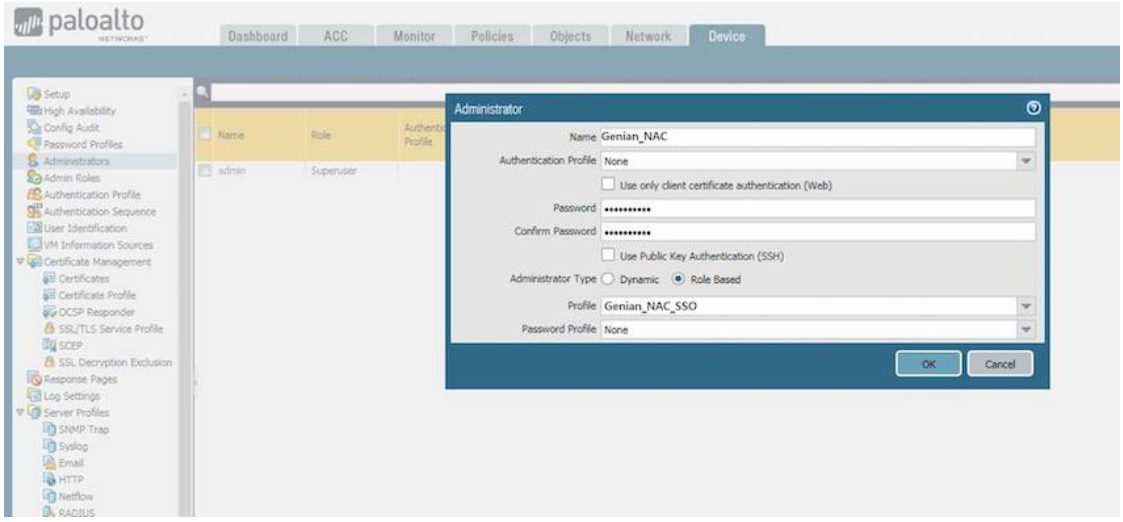
- **Device > Admin Roles > Add** 으로 이동합니다.
- Genian_NAC_SSO 의 role **Name** 을 만들고 **XML API** 탭 아래를 설정합니다.
- 모든 것을 활성화하고 **OK** 를 사용하여 확인합니다.



2. PAN 방화벽에서 Genian NAC 계정 생성

계정에 SSO 역할을 할당합니다.

- **Name** 입력: Genian_NAC
- **Administrator Type** 선택: Role Based
- **Profile** 선택: Genian_NAC_SSO



3. PAN 방화벽에서 XML 키를 생성

다음 URL로 이동: **https://[IP of PAN firewall]/api/?type=keygen&user=[username]&password=[password]**
아래에서 생성된 키를 볼 수 있습니다.

```
Script
<response status = 'success'>
<result>
<key>
↪LUFRPT1KbW80SU1hRXJuNk5XNHBudUhCNGMydE0rSUk9RFIzdEJ5RGcwWkRCVlhYMXl0Q1FPdz09
</key>
</result>
</response>
```

4. Genian NAC에서 SYSLOG 전송을 위한 설정

Genian NAC는 감사 로그의 필터를 사용하여 XML과 연동합니다.

- 상위 항목의 **감사** 로 이동합니다.
- 왼쪽 로그 항목에서 **로그 > 검색 > 고급검색 > 로그 ID > 인증 > 검색** 버튼을 클릭합니다.
- 사용자 인증 로그가 표시되고 **다른이름으로 저장** 버튼을 클릭합니다.

(가) 로그필터 생성 및 감사로그 전송설정

- **이름** 입력: SSO_PaloAlto
- **Webhook URL** 설정:

```
Call the PAN firewall XML
https://[IP of PAN firewall]/api/?type=user-id&action=set&
↪key=LUFRPT1KbW80SU1hRXJuNk5XNHBudUhCNGMydE0rSUk9RFIzdEJ5RGcwWkRCVlhYMXl0Q1FPdz09
```

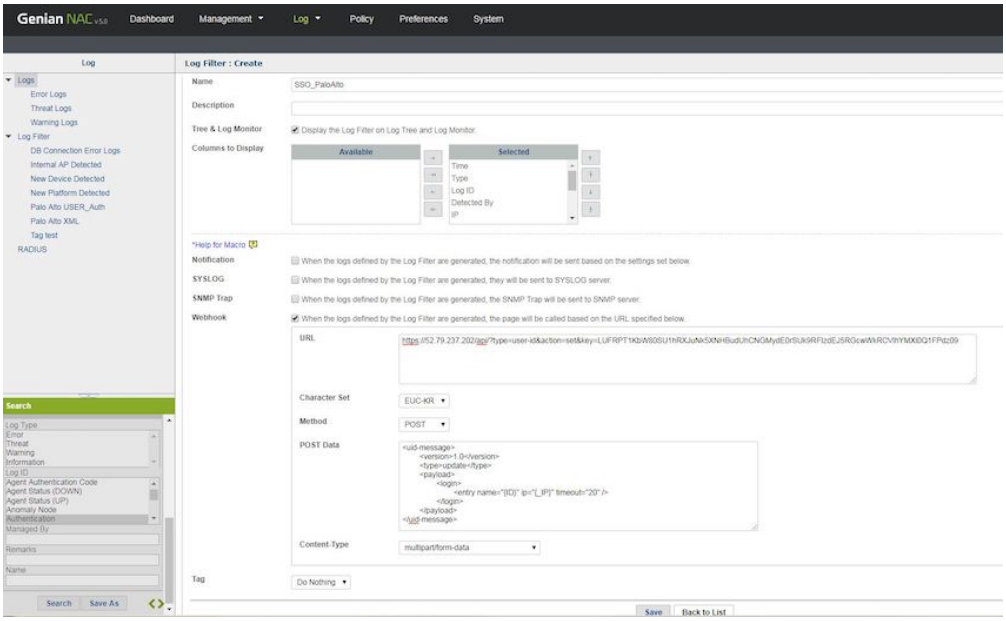
(나) 로그필터 문자셋 및 전송내용 설정

- **character Set** 선택: EUC-KR
- **방식** 선택: POST
- **POST 데이터** 입력:

```
Script
<uid-message>
<version>1.0</version>
<type>update</type>
<payload>
   <login>
      <entry name="{ID}" ip="{_IP}" timeout="20" />
</login>
</payload>
</uid-message>
```

(다) 로그필터 데이터 전송타입 설정

- **데이터전송타입**: multipart/form-data



5. PAN 방화벽에서 보안 영역에 사용자 식별 구성

PAN 방화벽 정책 규칙은 보안 영역을 사용하여 영역 내에서 자유롭게 흐르는 데이터 트래픽을 식별합니다. 허용된 보안 정책 규칙을 정의하기 전에는 다른 영역 간에 자유롭게 흐르지 않습니다. 사용자 ID를 적용하려면 최종 사용자 트래픽으로 전달되는 인바운드 및 아웃바운드 영역 모두에서 사용자 ID를 사용하도록 설정 해야합니다.

사용자 ID를 사용하도록 설정

- **Network > Zone** 로 이동
- **Enable User Identification** 선택 및 **OK** 클릭.

6. PAN 방화벽에서 SSH 및 웹 콘솔에서 로그인 이벤트를 수신하고 있는지 확인

```
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
```

PAN 방화벽 WebConsole

- **Monitor** 로 이동합니다.
- 왼쪽 Monitor 항목의 **Logs > User-ID** 로 이동합니다.
- Genian NAC를 통해 인증 목록을 볼 수 있습니다.

SYSLOG를 통해 연동을 위한 PAN Firewall 구성

1. PAN 방화벽에서 필터 생성

Palo Alto 방화벽은 Genian NAC와 Syslog 메시지를 수신할 때 인증 관련 메시지를 구분하는 로그 필터를 생성합니다.

- 상단 항목의 **Device** 로 이동합니다.
- 사용자 **Identification** > **User Mapping** > PAN 방화벽 **User-ID Agent Setup** 탭에서 **기어** 와 같은 모양의 버튼을 클릭합니다.
- Syslog **Filters** > **Add** 로 이동합니다

```
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: ,
```

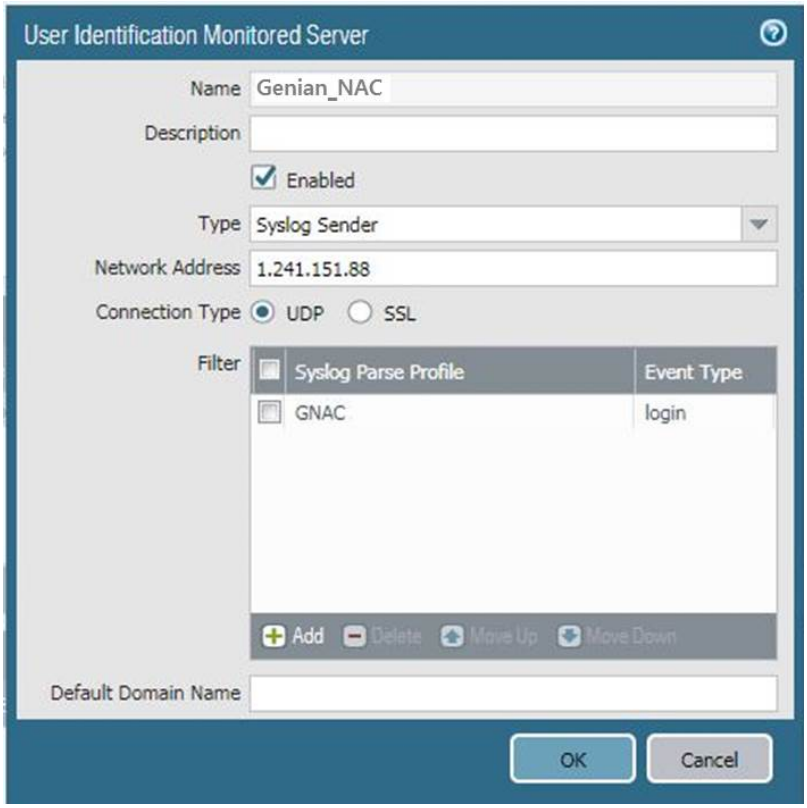
2. PAN 방화벽이 모니터하는 SYSLOG 송신자 지정

Device > **User Identification** > **User Mapping** 및 **ADD** (서버 모니터링 목록에 대한 항목을 추가)

```
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: UDP 프로토콜은 암호화되지 않은 데이터이므로 스푸핑이 될 수 있어 SSL 프로토콜을 사용하는 것이 좋습니다.

The listening ports(514 for UDP and 6514 for SSL)



4. PAN 방화벽에서 SYSLOG Listener 서비스 활성화

Genian NAC의 SYSLOG를 받을 수 있습니다.

- **Network > Network Profiles > Interface Mgmt > ADD** 새 프로파일로 이동합니다.

```
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
```

5. PAN 방화벽에서 인터페이스 관리 프로파일을 인터페이스에 할당

- **Network > Interfaces** 로 이동하여 인터페이스를 편집합니다.
- **Advanced > other info > Interface Management Profile** 선택 > **Allow Genian NAC** 선택 > **Ok** 를 클릭합니다.

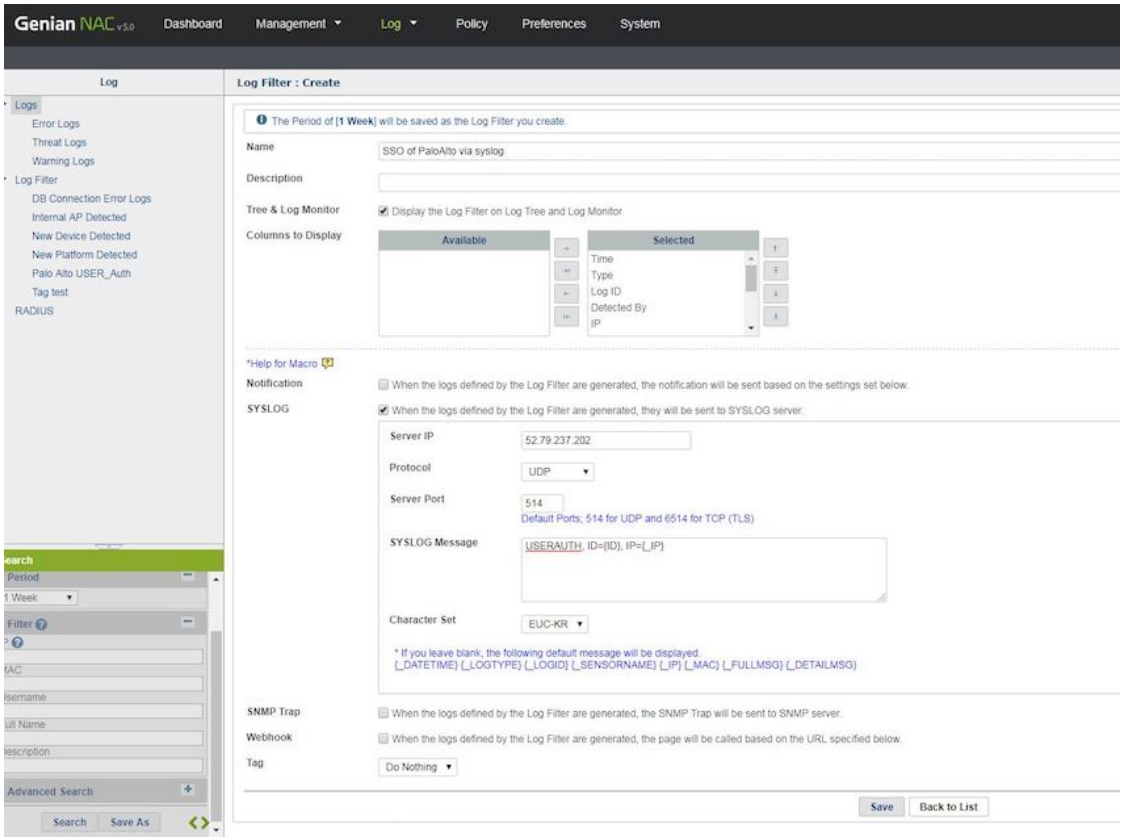
- **Commit**

6. Genian NAC에서 SYSLOG를 전송하도록 설정

Genian NAC는 감사 로그의 필터를 사용하여 SYSLOG 와 연동합니다.

- 상위 항목의 **감사** 로 이동합니다.
- 왼쪽 로그 항목에서 **로그 > 검색 > 고급검색 > 로그 ID > 인증 > 검색** 버튼을 클릭합니다.
- 사용자 인증 로그가 표시되고 **다른이름으로 저장** 버튼을 클릭합니다.

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

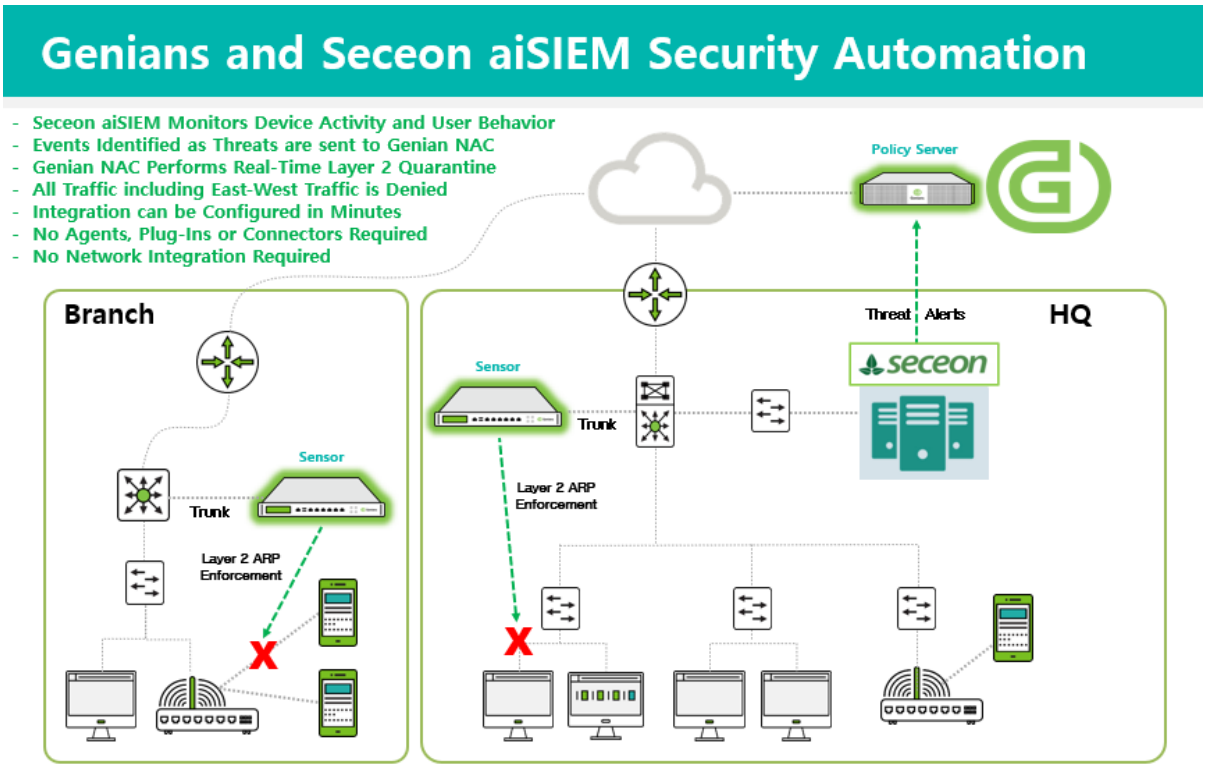


7. PAN 방화벽에서 사용자가 로그인하거나 로그아웃할 때 사용자가 매핑되는지 확인

```
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
```

5.8.8 Seceon aiSIEM 연동

이 가이드는 Syslog를 이용하여 Genian NAC와 Seceon aiSIEM과 연동방법에 대한 정보를 제공합니다. Seceon aiSIEN의 위협 탐지 기능을 Genians NAC의 강력한 제어 기능으로의 확장을 제공합니다. 데모영상을 통하여 연동하는 방법을 비디오 웨비나로 함께할 수 있습니다. Seceon



연동의 주요 단계는 다음과 같습니다.

1. Seceon APE에서 Remediator를 구성합니다.
2. APE Remediator가 보낸 syslog 이벤트를 이용하여 해당 노드에 정책을 적용할 수 있도록 Genian NAC를 설정합니다.

APE Remediator 설정

Seceon APE UI에 로그인:

1. **Administration > Remediator > Add** 에서 Genian NAC를 방화벽 장치유형으로 선택하고 Genian NAC 정책서버의 IP를 입력합니다.
2. 사용자명, 패스워드, 패스워드 확인 항목은 필수이지만 연동을 하는데 필요치 않으므로 아무런 값이나 입력합니다.

Genian NAC Syslog 설정

Syslog를 수신하기 전에 서버에 syslog 패턴 설정을 추가해야합니다. 차단할 장치에 대한 정보를 추출하기 위해 Seceon aiSIEM 메시지 형식에 따라 서버 규칙을 설정합니다. 이 연동에서는 IP주소를 사용하여 차단할 장치를 식별합니다.

1. Web콘솔 **설정 > 환경설정 > 감사기록** 으로 이동합니다.
2. **Syslog 감사기록 저장** 항목에서 필터 **추가** 버튼을 클릭합니다.
3. 팝업창에서 **필터이름** 을 입력하고 **필터타입** 을 선택합니다. 이 항목은 syslog 또는 지정된 호스트의 메시지를 허용하는 부분입니다.
4. **필터값** 을 입력합니다. 수신한 syslog의 filter 변수가 필터 설정값과 일치하게 되면 syslog 메시지가 정책서버 로그에 표시됩니다. 여기에서는 **Seceon CCE IP** 를 입력합니다.
5. **IP 키값** 은 syslog에서 IP정보를 읽을때 사용할 키값입니다.
6. **문자셋** 은 수신한 syslog 처리시 적용할 인코딩값입니다. seceon과 매칭합니다.
7. 하단 **추가** 버튼을 클릭합니다.
8. 하단 **수정** 버튼을 클릭합니다.

이제 Seceon aiSIEM의 시스템 메시지는 Genian NAC가 감지 한 노드와 상호 연계됩니다.

Genian NAC 노드태그와 정책 설정

다음 위치로 이동합니다. **설정 > 속성관리 > 태그 관리**

1. **Seceon-Threat-Detected 라는 태그를 생성한 다음 저장을 클릭합니다.**
   이 태그는 감사로그 필터와 연결되고 그다음 노드에 제어정책이 할당될 것입니다.
2. 상단 **감사** 를 클릭합니다.
3. **Add filters** 라고 써있는 로그 검색창을 클릭합니다.
4. **설명 부분에 THREAT so performing 을 입력하고 검색을 클릭합니다.**
   위 메시지는 Seceon aiSEIEM의 syslog 메시지내용입니다.
5. 검색창 우측 **저장** 버튼을 클릭합니다.
6. **이름, 설명 을 입력하고 하단 태그 항목에서 할당 을 선택합니다.**
   검색대상, 할당대상 을 노드나 MAC, IP, 무선랜, 사용자를 선택할 수 있지만 **노드** 를 선택합니다.
7. **추가** 버튼을 클릭하여 앞에서 생성한 **Seceon-Threat-Detected** 태그를 체크하고 설정을 클릭합니다.

정책 > 그룹 으로 이동합니다.

1. **작업선택 에서 생성 을 클릭합니다.**
   이 노드그룹은 제어정책에 할당 예정입니다.
2. ID, 설명, CWP메시지 등 기본정보를 입력합니다.
3. 그룹조건에서 **추가** 버튼을 클릭하고 항목란에서 **태그** 를 선택합니다.
4. 조건항목에서는 **존재하면** 을 선택합니다.
5. 설정항목에서는 **Seceon-Threat-Detected** 태그를 선택하고 **추가** 버튼을 클릭합니다.
6. **생성** 버튼을 클릭합니다.

정책 > 제어정책 으로 이동합니다.

1. **작업선택** 에서 **생성** 을 클릭합니다.

2. 정책생성 절차대로 진행하고 노드그룹 선택에서 **Seceon-Threat-Detected** 그룹을 할당합니다.
3. 할당할 **권한** 을 선택하고 제어된 사용자에게 표시될 CWP메시지를 입력합니다.
4. **완료** 버튼을 클릭하여 정책을 생성합니다.

검증 테스트

1. Seceon Integrated Genian NAC 시스템의 네트워크센서에서 관리하는 테스트단말을 선택합니다.
2. 테스트단말에서 Seceon에서 탐지되는 Malware사이트로 접속합니다.
3. 약 1~3분(Seceon에서 위협처리에 필요한 시간) 안에 Seceon은 Genian NAC로 위협탐지 syslog 경고를 발송합니다.
4. Genian NAC에서 Seceon이 보낸 syslog를 수신했다면 테스트노드에 태그가 할당되야 합니다.
5. 태그가 할당된 노드는 위협 제어정책이 할당되고 네트워크격리가됩니다. 단말에서는 Gateway로 Ping이 실패하고 단말이 격리되었음을 나타내는 CWP가 표시됩니다.

5.8.9 모니터랩 AISWG 연동 가이드

이 가이드는 Genian NAC와 모니터랩 AISWG 간의 연동에 대한 정보를 제공합니다.

가이드 개요

본 가이드는 시큐어 웹게이트웨이 시스템인 모니터랩의 Application Insight Secure Web Gateway (이하, **AISWG** 로 표기함) 와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위해 설정방법 및 연동테스트에 대한 가이드입니다.

Genian NAC의 사용자인증 정보와 에이전트를 통한 실시간 정보 수집 기능을 활용하여, 사용자정보 및 인증서 설치 현황 정보를 AISWG 관리자 페이지에 실시간으로 자동 갱신되도록 연동됩니다.

AISWG는 Genian NAC와 연동을 통해 신규 사용자 추가, 인증서 설치 현황에 대해 자동으로 업데이트하여, 인증서 미설치 사용자는 AISWG 정책에 의해 웹서비스 이용을 차단하고, 인증서 설치 유도를 위해 안내페이지를 제공합니다.

권장 버전

제품명	버전	비고
AISWG	V3.0.2 이상	
Genian NAC	V5.0 이상	2020.05 이후 버전

연동의 목적

Genian NAC와 모니터랩 AISWG의 연동은 다음의 효과를 제공합니다.

인증서 설치 현황에 대한 실시간 탐지

- Genian NAC는 단말에 설치된 에이전트를 통해 인증서 설치 현황 정보를 실시간으로 수집하고, 이에 대한 이벤트 발생 시 연동을 통해 정보 전달이 가능합니다.
- 모니터랩 AISWG는 인증서 설치 현황에 대해 최초 1회만 업데이트하여 PC 변경이나 초기화 시 인증서 설치 현황이 업데이트되지 않기 때문에, 실시간 탐지가 가능한 Genian NAC와의 연동을 통해 인증서 설치 현황을 계속 업데이트 할 수 있게 됩니다.

인증서 미설치 사용자에 대한 안내페이지 제공

- 모니터랩 AISWG는 Genian NAC와 연동을 통해 인증서 설치 현황에 대한 정보를 실시간으로 전달받아 인증서가 설치된 사용자는 정상적인 웹서비스 이용이 가능하고, 미설치 사용자는 인증서 설치 안내페이지를 제공하며, AISWG 정책에 의해 웹서비스 이용이 차단됩니다.

신규 사용자 자동 추가

- AISWG Web콘솔에 신규 사용자는 수동으로 추가하여 인증서 설치 현황 업데이트를 하였지만, Genian NAC와 연동을 통해 별다른 조작없이 AISWG Web콘솔에 자동으로 사용자 추가를 할 수 있고, 기존에 존재하는 사용자의 경우에는 인증서 설치 현황만 업데이트 됩니다.

사전준비 사항

Networking 사전 준비

SYSLOG 수신을 위한 NAC 연동 설정 을 참고하여 AISWG Web콘솔에 설정한 포트에 대해 Genian NAC 정책서버와 모니터랩 AISWG 서버 간의 통신을 확인하기 바랍니다.

- Genian NAC와 AISWG에서 SYSLOG 설정 시 사용되는 기본 포트는 UDP/514 입니다. (AISWG와 연동 시 UDP 통신만 지원하며, TCP/TLS 통신은 추후에 지원 예정입니다.)
- AISWG에서 SYSLOG 수신 시 사용되는 포트는 설정하는 값에 따라 다를 수 있습니다.
- Genian NAC의 접속 포트정보는 UI에서 **시스템 > 서비스 관리 > 접속포트** 에 있습니다.

연동을 위한 AISWG 설정

본 항목에서 다루는 모니터랩 AISWG의 설정 부분은 Genian NAC와 연동을 위해 설정하는 최소한의 부분만을 소개합니다. 본 과정은 연동 이후 최초 1회만 작업해주시면 이후엔 자동으로 적용됩니다.

SYSLOG 수신을 위한 NAC 연동 설정

AISWG 관리자 페이지 **정책 설정 > 기본 설정** 으로 이동 후 **NAC 연동** 항목에서 다음과 같이 설정합니다.

설정 항목	설정 값	참고
사용 여부	'사용' 체크	'사용', '사용안함' 중 '사용' 라디오버튼 선택
서비스	514	Genian NAC 로부터 SYSLOG 수신 시 사용될 포트번호 입력 (포트번호는 변경 가능하고, 설정되는 포트번호는 자동으로 OPEN 됩니다.)
구분자	셀렉트박스: | / 개수: 1	Genian NAC 로부터 SYSLOG 수신 시 메시지의 내용 구분을 위한 구분자('|', 버티칼바)와 개수 설정

이 과정을 통해서 모니터랩 AISWG는 Genian NAC로부터 SYSLOG를 수신할 수 있는 환경이 구성됩니다.

연동을 위한 Genian NAC 설정

본 항목에서 다루는 Genian NAC의 설정 부분은 모니터랩 AISWG와 연동을 위해 최소화해서 설정하는 부분만을 소개합니다. 본 과정은 최초 1회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 인증서 설치 현황 검사를 위한 노드액션 생성

정책 > 노드정책 > 노드액션 으로 이동하여 다음과 같이 2개의 노드액션을 설정 후 생성합니다.

1) 인증서 설치 검사를 위한 노드액션 설정

설정 항목	설정 값	참고
기본설정 > 액션명	인증서_설치_노드액션	노드액션 이름 입력
기본설정 > 설명	인증서 설치 노드액션	노드액션 설명 입력
기본설정 > CWP 메시지	Certificate installed	CWP 페이지에 표시될 메시지 입력
액션 수행설정 > OS 종류	Windows	Windows, macOS 중 선택
액션 수행설정 > 조건연산	AND	AND, OR 중 선택
액션 수행설정 > 조건설정	항목: 파일 / 조건: 존재하면 / 설정: C:Readme_check_certificate.txt	설정 부분에는 인증서 설치 현황를 체크하기 위한 txt 파일 경로와 파일명 (확장자 포함) 입력
액션 수행설정 > 플러그인선택	수행조건만 검사	수행조건만 검사 선택
액션 수행설정 > 수행주기	항상수행	항상수행 선택

2) 인증서 미설치 검사를 위한 노드액션 설정

설정 항목	설정 값	참고
기본설정 > 액션명	인증서_미설치_노드액션	노드액션 이름 입력
기본설정 > 설명	인증서 미설치 노드액션	노드액션 설명 입력
기본설정 > CWP 메시지	Certificate not installed	CWP 페이지에 표시될 메시지 입력
액션 수행설정 > OS 종류	Windows	Windows, macOS 중 선택
액션 수행설정 > 조건연산	AND	AND, OR 중 선택
액션 수행설정 > 조건설정	항목: 파일 / 조건: 존재하지 않으면 / 설정: C:Readme_check_certificate.txt	설정 부분에는 인증서 설치 현황를 체크하기 위한 txt 파일 경로와 파일명 (확장자 포함) 입력
액션 수행설정 > 플러그인선택	수행조건만 검사	수행조건만 검사 선택
액션 수행설정 > 수행주기	항상수행	항상수행 선택

Note: AISWG의 실제 인증서가 설치되는 위치는 운영체제마다 상이하며, 인증서가 PC에 설치될 때 인증서의 존재 유무를 파악하기 위해 'C:' 경로에 **Readme_check_certificate.txt** 파일이 자동으로 생성됩니다.

Genian NAC는 **txt** 파일을 통해 인증서의 설치 현황을 체크하게 됩니다.

Step 2: 인증서 설치 현황에 대한 노드그룹 생성

정책 > 그룹 > 노드 로 이동하여 다음과 같이 2개의 노드그룹을 설정 후 생성합니다.

1) 인증서가 설치된 그룹 분류를 위한 노드그룹 설정

설정 항목	설정 값	참고
기본정보 > ID	인증서_설치_노드그룹	노드그룹 이름 입력
기본정보 > 설명	인증서 설치 그룹	노드그룹 설명 입력
기본정보 > CWP 메시지	Certificate installed	CWP 페이지에 표시될 메시지 입력
기본정보 > 적용모드	사용함	사용함 선택
기본정보 > 감사로그	On	On 선택
그룹조건 > 조건연산	AND	AND, OR 중 선택
그룹조건 > 조건설정	항목: 에이전트액션 / 조건: 특정 액션을 만족하면(수행전 포함) / 설정: 인증서_설치_노드액션	설정 부분은 *Step 1* 에서 생성한 노드액션(인증서_설치_노드액션) 선택

2) 인증서가 미설치된 그룹 분류를 위한 노드그룹 설정

설정 항목	설정 값	참고
기본정보 > ID	인증서_미설치_노드그룹	노드그룹 이름 입력
기본정보 > 설명	인증서 미설치 그룹	노드그룹 설명 입력
기본정보 > CWP 메시지	Certificate not installed	CWP 페이지에 표시될 메시지 입력
기본정보 > 적용모드	사용함	사용함 선택
기본정보 > 감사로그	On	On 선택
그룹조건 > 조건연산	AND	AND, OR 중 선택
그룹조건 > 조건설정	항목: 에이전트액션 / 조건: 특정 액션을 만족하면(수행전 포함) / 설정: 인증서_미설치_노드액션	설정 부분은 *Step 1* 에서 생성한 노드액션(인증서_미설치_노드액션) 선택

Step 3: 인증서 설치 및 미설치 시 발생하는 로그에 대한 검색필터 조회

감사 > 로그 > 로그검색 으로 이동하여 인증서 설치 여부에 대한 검색필터를 조회합니다.

1) 인증서 설치 시 발생하는 로그에 대한 검색필터 조회

설정 항목	설정 값	참고
설명	RESULT=SUCCESS, ACTION=인증서_설치_노드액션	인증서가 설치된 로그 분류를 위한 키워드 설정
로그ID	에이전트액션	에이전트액션 선택 필수

2) 인증서 미설치 시 발생하는 로그에 대한 검색필터 조회

설정 항목	설정 값	참고
설명	RESULT=SUCCESS, ACTION=인증서_미설치_노드액션	인증서가 미설치된 로그 분류를 위한 키워드 설정
로그ID	에이전트액션	에이전트액션 선택 필수

위의 조건들로 로그 검색 후 Step 4 과정을 진행합니다. (노드 그룹 수립 직후 로그 검색 시, 그룹화 작업이 진행 중이므로 검색 내용에 나타나지 않을 수 있습니다.)

Step 4: 검색필터 로그 발생 시, AISWG 로 SYSLOG 전송 설정하기

Step 3 에서 검색필터 조회 후 우측 상단 **저장** 버튼을 클릭하면, 검색필터 설정화면이 자동으로 나타납니다. 여기에서 다음과 같이 설정 후 저장합니다.

1) 인증서 설치 로그 발생 시 검색필터 및 SYSLOG 전송 설정

설정 항목	설정 값	참고
이름	인증서_설치_SYSLOG 전송	검색필터 이름 입력
설명	인증서 설치 PC의 로그를 AISWG로 전송	검색필터 설명 입력
SYSLOG 전송	체크박스에 체크	아래 SYSLOG 전송 설정 참고

SYSLOG 전송 설정	설정 값	참고
서버주소	xxx.xxx.xxx.xxx	AISWG 서버의 IP 입력
전송방법	UDP	UDP만 지원 (TCP/TLS 추후 지원 예정)
전송포트	514	AISWG에 설정된 포트 입력
포맷	Default	Default 선택
SYSLOG 메시지	cert_success|{_DATETIME}|부서명|{_USERDEPT}|{_USERNAME}|{_IP}|{_USERID}	*3. 참고: SYSLOG 메시지 포맷 설명* 내용 참고
CHARSET	UTF-8	UTF-8 선택

2) 인증서 미설치 로그 발생 시 검색필터 및 SYSLOG 전송 설정

설정 항목	설정 값	참고
이름	인증서_미설치_SYSLOG 전송	검색필터 이름 입력
설명	인증서 미설치 PC의 로그를 AISWG로 전송	검색필터 설명 입력
SYSLOG 전송	체크박스에 체크	아래 SYSLOG 전송 설정 참고

SYSLOG 전송 설정	설정 값	참고
서버주소	xxx.xxx.xxx.xxx	AISWG 서버의 IP 입력
전송방법	UDP	UDP만 지원 (TCP/TLS 추후 지원 예정)
전송포트	514	AISWG에 설정된 포트 입력
포맷	Default	Default 선택
SYSLOG 메시지	cert_fail|{_DATETIME}|부서명|{_USERDEPT}|{_USERNAME}|{_IP}|{_USERID}	*3. 참고: SYSLOG 메시지 포맷 설명* 내용 참고
CHARSET	UTF-8	UTF-8 선택

Step 4까지의 과정을 통해서 Genian NAC는 인증서 설치 현황에 대해 실시간으로 정보를 수집하여 이벤트 발생 시 모니터랩 AISWG로 SYSLOG 전송이 가능한 환경이 구성됩니다.

3) 참고: SYSLOG 메시지 포맷 설명

본 가이드에서 사용되는 SYSLOG 메시지의 포맷은 Genian NAC와 모니터랩 AISWG제품 연동 시 약속된 포맷이기 때문에 임의적으로 변경하면 정상적으로 연동이 이루어지지 않을 수 있습니다.

SYSLOG 메시지의 각 포맷 별 구분자는 AISWG Web콘솔 내 NAC 연동 설정에서 설정한 구분자(e,g '|') 로 입력 해야합니다.

인증서 설치 현황에 대해 노드에 Genian NAC 사용자인증이 되어있지 않으면, 사용자 정보가 전달되지 않기 때문에 AISWG Web콘솔에 갱신되지 않습니다. 또한 AISWG Web 콘솔에서 같은 부서에 동일한 사용자명이 있는 경우 인증서 설치 현황이 갱신되지 않습니다.

SYSLOG 메시지 포맷에 대한 설명은 다음과 같습니다.

포맷	설명
'cert_success' or 'cert_fail'	AISWG는 Genian NAC로부터 SYSLOG 수신 시 메시지 맨 앞 구문을 보고 인증서 설치 여부를 판단하기 때문에, SYSLOG 전송 시 메시지 맨 앞에 **cert_success** or **cert_fail** 구문을 반드시 입력해야 합니다.
{_DATE-TIME}	이벤트 발생 시간
부서명	AISWG에 존재하는 최상단 부서 조직명을 입력합니다. (일반적으로 해당 고객사에서 사용되는 최상단 부서 조직명을 입력합니다.)
{_USERDEPT}	이벤트가 발생된 노드의 사용자인증에 사용된 계정의 부서명 (AISWG 관리자페이지에 해당 부서명이 최상단 부서 이하에 존재하면, 그 부서로 자동 분류되고, 존재하지 않으면 None 으로 분류됩니다.)
{_USER-NAME}	이벤트가 발생된 노드의 사용자인증에 사용된 계정의 사용자명 (AISWG 관리자페이지에 해당 사용자가 존재하지 않을 시 자동으로 추가되고, 사용자가 존재할 시 기존 사용자 명에 업데이트 됩니다.)
{_IP}	이벤트가 발생된 노드의 IP 주소
{_USERID}	이벤트가 발생된 노드의 사용자인증에 사용된 계정의 ID

연동 결과 확인

연동을 위한 설정 작업 완료 후, 인증서 미설치 동작에 대한 테스트 과정입니다.

Step 1: 단말에 인증서 삭제

- 인증서 미설치 동작 테스트를 위해 'C:' 경로에 *Readme_check_certificate.txt* 파일을 삭제합니다

Step 2: Genian NAC Web콘솔 **감사 > 로그** 메뉴에서 이벤트 발생 확인

- 인증서 미설치 이벤트 발생 확인

Step 3: AISWG Web콘솔에서 인증서 설치 현황 갱신 확인

- **모니터랩 > 인증서 설치 현황** 메뉴에서 사용자명 검색 후 인증서 설치여부 확인
  - 인증서 삭제 전 **설치 시간** 컬럼을 통해 인증서 존재 확인 이후에 인증서 삭제 후 **설치 시간** 컬럼이 변경됨 확인
- **정책설정 > 정책관리 > 정책 > 사용자관리** 메뉴에서 사용자명 검색 후 인증서 설치여부 확인
  - 인증서 삭제 전 **인증서** 컬럼을 통해 인증서 존재 확인 이후에 인증서 삭제 후 **인증서** 컬럼 *NO* 로 변경

Note: 인증서가 사용자의 PC에 존재하지 않을 시 AISWG의 정책에 의해 정상적인 웹서비스를 이용할 수 없게 되고, 인증서 설치 안내페이지가 제공됩니다.

5.8.10 수산INT eWalker SWG 연동 가이드

이 가이드는 Genian NAC와 수산INT eWalker SWG 연동에 대한 정보를 제공합니다.

가이드 개요

유해사이트 접속차단 제품인 수산INT의 eWalker SWG와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정방법 및 연동테스트을 안내합니다.

Genian NAC에서 IP변경이 감지되면, IP가 사용자 노드의 IP인지 확인한 후, eWalker SWG로 변경된 정보를 전송하여 eWalker SWG에서 정책에 따른 정책을 적용할 수 있도록 연동됩니다.

(본 가이드에서는 Genian NAC가 타사장비와 연동시 범용적으로 활용하도록 제공하는 Webhook(API)을 활용하였습니다.)

권장 버전

제품명 (구성요소)	버전	비고
eWalker SWG	V9.2.2 이상	2020.12 이후 버전
Genian NAC (정책서버)	V5.0 이상	2020.12 이후 버전

연동의 목적

본 연동은 eWalker SWG와 인사정보연동이 되어있지 않거나 인사정보 연동이 불가한 경우에 노드의 MAC 주소를 기준으로 IP가 변경되는 것을 Genian NAC가 탐지하여 eWalker SWG로 전달하여 IP가 변경되는 것에 대해 제어할 수 있도록 도움을 줍니다.

Genian NAC와 eWalker SWG 연동은 다음의 효과를 제공합니다.

단말의 IP변경시, 유해사이트 접근제어 정책의 자동적용

- eWalker SWG 사용고객 중, 일반 사용자의 IP가 다양한 이유로 변경된 경우, IP기반으로 운영중인 고객사에서는 관리자가 수동으로 확인하여, 사용자의 고유 IP와 비교하여, 적용된 정책을 변경하거나 사용자에게 IP를 변경하도록 요청하여야 합니다. 그러나 연동 설정을 해두면, IP변동 시 자동으로 인지하고 eWalker SWG로 정보가 전송되어, 자동으로 정책을 적용하도록 합니다.

IP를 고의적으로 변경한 사용자에게 네트워크 차단 등 조치

- 인사정보를 연동하지 않은 유해사이트 접속차단 제품은 사용자 IP를 기준으로 접근 가능한 사이트가 관리되기 때문에 사용자가 단말의 IP를 변경하여 접근하는 사용자에 대해서 제어가 필요합니다.
- 예) 사용자 기반으로 운영되는 Genian NAC는 내부사용자가 (인터넷 사용 등에 제한이 없는 방문사용자들의 IP로 변경하여, 사내에서 접근이 제한되는 사이트를 방문하려고 시도하는 경우, Genian NAC에서 네트워크 차단 등의 조치가 가능합니다.

사전준비 사항

Networking 사전 준비

- Genian NAC 정책서버와 수산INT eWalker SWG 서버 간의 통신을 확인합니다. http TCP/80, https TCP/8443,8501 이 API 통신의 기본 포트입니다.

수산INT eWalker SWG 의 서버정보 확인

- Genian NAC 에서 IP 변경을 탐지한 노드의 정보(MAC 주소 또는 IP 주소변경을 탐지한 차단서버 정보(IP 또는 차단서버 이름)를 전송할 eWalker SWG 서버의 정보를 사전에 수집합니다.

Note:

- eWalker SWG 서버의 API 접속 주소 예) https://{}eWalker SWG 서버 IP]:8501
- API 경로 예) https://{}eWalker SWG 서버 IP]:8501/ewalker/orgdb/dhcp/macid

연동을 위한 Genian NAC 설정

본 항목에서 다루는 Genian NAC의 설정 부분은 eWalker SWG와 연동을 위한 최소한의 부분만을 소개합니다. 본 과정은 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: IP 변경 태그 만들기
설정 > 속성관리 > 태그관리 으로 이동하여 **작업선택 > 생성** 버튼 클릭 후 **SWG_IP 변경** 태그를 생성합니다.

Step 2: 로그필터를 이용하여 IP 변경 노드그룹 만들기
감사 > 로그 > 로그검색 으로 이동하여 아래의 항목에 대한 검색필터 생성 과정을 진행합니다.

1) 팝업 된 필터 설정 창의 **설명** 부분에 **노드 IP 변경 추가 감지됨** 을 입력하고, 검색 버튼을 클릭하여 IP 변경노드 탐지정보가 출력되는지 확인합니다.

설정 항목	설정 값	참고
설명	노드 IP 변경 추가 감지됨	

2) 우측상단의 **저장** 을 클릭하면 추가설정 창이 나타납니다. 이름을 설정하고 하단부 태그의 NONE 을 **할당** 으로 변경한 후, 다음과 같이 입력하고 저장합니다.

설정 항목	설정 값	참고
검색대상	MAC	eWalker SWG의 관리기준: MAC
할당대상	MAC	eWalker SWG의 관리기준: MAC
태그	SWG_IP 변경	Step 1 에서 생성한 태그 이름

Step 3: IP 변경에 대한 관리대상 노드그룹 만들기
정책 > 그룹 > 노드 로 이동하여 **작업선택** 버튼을 클릭하여 노드정책을 생성합니다.

- 노드그룹의 조건은 다음과 같이 설정합니다

설정 항목	조건	설정 값	참고
태그	존재하면	SWG_IP 변경	조건 1) IP 를 변경한 노드
인증사용자	사용자부서에 속하면	회사직원	조건 2) 인증된 직원에 한함
조건연산	AND		위의 두 조건을 만족해야 함

Note: IP 가 변경된 노드에 대해서 그룹을 생성하였으나 IP 가 변경된 것만으로 제어하는 것은 운영상의 위험이 따르므로 조건을 추가적용하여 신뢰도를 높여야 합니다. 본 가이드에서는 위의 2가지 조건을 적용하여 관리대상을 지정했습니다

Step 4: 관리대상 노드 정보를 eWalker SWG로 전송하기 위한 설정
감사 > 로그검색 으로 이동 후 상단의 검색 바를 클릭하면 검색옵션을 설정하는 부분이 팝업 됩니다.

팝업 된 필터 설정 창의 **설명** 부분에 **제어정책 변경됨. NEW='IP 임의 변경단말 네트워크 차단'** 을 입력하고 **검색** 버튼을 클릭하여 정보가 출력되는지 확인합니다.

올바르게 정보가 출력되면, 우측 상단의 **저장** 을 클릭하여 검색필터 설정창으로 이동합니다. 필터의 이름을 정해주고, 하단 부의 **Webhook** 을 선택하여 다음의 정보를 입력합니다.

- Webhook 전송 설정

설정 항목	설정 값	참고
방식	POST	Data 전송
URL 설정	https://{}eWalker SWG 서버 IP]:8501/ewalker/orgdb/dhcp/macid	변경될 수 있음
CHARSET	UTF-8	
POST 데이터	아래의 코드 참조	reqip는 참고용 이므로 관리자가 식별이 용이한 정보로 대체 가능 (ex. 정책서버 IP)
데이터 전송 타입	application/json	

- POST 데이터 설정 값

```
{
   "cmd": "update",
   "reqip": "{_SENSORIP}",
   "reqtime": "{_DATETIMEZ}",
   "list": [
       ["{_MAC}", "{_IP}"]
   ]
}
```

연동을 위한 eWalker SWG 설정

본 항목에서 다루는 eWalker SWG의 설정 부분은 Genians NAC 연동 시의 운영 방법에 대한 부분으로, eWalker SWG에서 사용되는 조직도의 사용자 ID를 MAC 주소로 대체하여, Genian NAC에서 전달 받은 {MAC+IP 주소} 를 eWalker SWG 정책에 적용하기 위한 설정입니다.

Step 1: MAC 기반등록 사용자그룹만들기

MAC 주소를 이용하여 정책을 생성하기 위해서, 사용자 그룹을 먼저 만들어 줍니다.

정책 > 사용자 제어 정책 > 사용자 그룹 으로 이동하여, 우측 상단의 **ADD** 버튼을 클릭하여 사용자 그룹을 추가합니다.

- 정책 적용 대상인 **사용자 그룹** 은 등록 시 IP 를 제외한 모든 조합이 가능 합니다. IP 정보는 정책 적용을 위해 사용되며, 이는 IP 변경에 따라 자동으로 변경되는 구조가 아닌 사용자, MAC 주소를 기준으로 IP 가 추가되는 형태로 구현됩니다.

Step 2: MAC 기반등록 정책만들기

MAC 주소를 이용하여 정책을 생성하는 단계입니다.

정책 > 사용자 제어 정책 > 정책 설정 으로 이동하여, 우측 상단의 **ADD** 버튼을 클릭하여 정책을 추가합니다.

- 사용자, 카테고리 그룹, 시간 그룹에 대해서도 사용자 그룹과 동일한 방식으로 생성 또는 기존에 활용 중이던 그룹정책을 활용하여 설정해 줍니다. 하단부의 설정 값은 기본 값을 활용하셔도 됩니다.

여기까지 설정 시, 내부사용자가 IP 를 변경하면, Genian NAC 에서 탐지하여 내부사용자만을 가려내어 eWalker SWG의 MAC 기반 IP 등록 정책에 자동 적용됩니다.

정상 동작 테스트 방법

Step 1: Genian NAC의 감사 > 로그 메뉴에서 확인

1. 사용자 노드의 IP 변경 시, 이벤트 발생 및 전송 여부 확인 가능

Step 2: eWalker SWG의 정보/실시간 로그 > 시스템 로그 메뉴에서 확인

1. eWalker SWG Web콘솔 접속 후, (https://{[}eWalker SWG 서버 IP]:8500) 내용을 확인합니다.
2. Genian NAC 에서 정보 (MAC:IP) 변동 정보를 받을 경우 처리 내역 확인. (로그)
3. 사용자 "00:11:22:33:44:55" MAC의 IP 가 "192.168.100.100" 으로 변경되었음을 확인 후 수신 적용 확인

(Genian NAC 에서 전송한 IP 가 하나의 MAC 주소로 추가되어 다수의 IP 가 존재하는 것이 확인되면 정상적으로 동작하는 것으로 볼 수 있습니다.)

5.9 클라우드 리소스에 대한 접근 제어

Genian ZTNA Cloud Sensor는 Cloud Gateway로 배포하여 제어할 수 있습니다. 클라우드 리소스에 접근 할 수 있습니다. Genian ZTNA Agent에 내장된 ZTNA Client 기능과 결합하면 원격 엔드포인트와 Cloud Gateway 간에 보안 연결이 설정됩니다. 사용자가 성공적으로 인증되면 관리자가 정의한 접근 권한만 사용할 수 있습니다. 다른 모든 연결 시도는 Cloud Gateway에 의해 삭제 됩니다.

5.9.1 Cloud Sensor 배포

Note: 현재 Cloud Sensor는 Genian ZTNA UI에서만 AWS Cloud 환경에 배포할 수 있습니다. AWS가 아닌 다른 환경에 Cloud Sensor를 배포 하려면 Genians에 문의 바랍니다.

Note: 아래 단계를 수행하기 전에 Cloud Provider와 클라우드 사이트를 이미 추가했는지 확인하십시오. 참조: 클라우드에서 노드 관리

5.9.2 클라우드 사이트에서 ZTNA Client 활성화

1. 상단 메뉴에서 시스템 > 사이트로 이동합니다.
2. 원하는 사이트명 클릭
3. ZTNA 클라이언트에서 상태를 '사용함'으로 설정합니다.
4. Cloud Gateway에 연결하는 Client에 대한 IP 대역 자동 할당을 위해 클라이언트 할당 네트워크 필드를 비워 둡니다.
5. 저장 클릭

5.9.3 노드 정책에 ZTNA 연결 관리자 추가

1. 노드 정책을 선택합니다(특정 노드 정책을 생성하려는 경우가 아니면 기본 노드 정책을 사용할 수 있습니다.)
2. 상단 메뉴에서 정책 > 노드 정책으로 이동하여 원하는 노드 정책을 클릭합니다.
3. 인증 정책에서 인증 방법을 비밀번호 인증에서 호스트 인증으로 변경 합니다.
4. 아래로 스크롤 하여 노드 액션 할당 부분으로 이동 후 , 할당을 클릭 합니다.
5. 사용 가능 창에서 'ZTNA 연결 관리자'를 선택 합니다. 선택한 'ZTNA 연결 관리자'를 사용가능 창에서 선택 창으로 이동 시킨 후 수정을 클릭 합니다.
6. 화면 좌측에 있는 노드정책 > 노드 액션을 클릭 합니다.
7. 아래로 스크롤하여 ZTNA 연결 관리자를 클릭합니다.
8. 플러그인 설정 화면에서 사이트 창 오른쪽에 있는 할당을 클릭합니다.
9. ZTNA 클라이언트를 사용하여 클라우드 센서를 통해 원격으로 연결할 사이트를 선택 합니다.
10. 수정을 클릭한 다음 오른쪽 화면 상단에서 깜박이는 적용하기를 클릭합니다.

5.9.4 Cloud Sensor 배포

1. 상단 메뉴에서 시스템 > 시스템 관리로 이동합니다.
2. 작업 선택을 클릭한 다음 ZTNA Gatway 추가를 선택합니다.
3. ZTNA Gatway를 배포할 원하는 사이트를 선택합니다.
4. Amazon 머신 이미지(AMI) 선택(권장 AMI가 표시됨)
5. 원하는 EC2 Instance Type을 선택합니다(t2.medium 권장).
6. ZTNA Gatway가 배포될 서브넷에 대해 원하는 서브넷 ID를 선택합니다.
7. ZTNA Gatway EC2에 대한 원격 CLI 액세스를 위해 원하는 키 쌍을 선택하십시오.

Note: 일반적으로 Cloud Sensor에 대한 CLI 액세스는 필요하지 않지만 AWS EC2 생성 프로세스에는 필수입니다. 지정된 지역에 대해 생성된 모든 유효한 키 쌍을 사용 할 수 있습니다. 원격 EC2 접근을 위한 키쌍을 생성하는 방법에 대한 자세한 내용은 AWS 설명서를 참조 하십시오.

---

1. Check Init 클릭
2. 선택한 모든 정보가 EC2 생성에 성공하는지 확인하기 위해 Terraform 초기화 테스트가 수행됩니다.
3. Check Init 프로세스 중에 오류가 표시되면 계속 진행하기 전에 AWS 환경의 문제를 해결하십시오.

Note: Cloud Sensor를 배포하는 지역에서 하나 이상의 탄력적 IP를 사용할 수 있어야 합니다.

---

1. Create 클릭
2. 적용 완료 메시지가 표시되면 Cloud Sensor가 성공적으로 배포되었음을 의미합니다.
3. 닫기를 클릭하여 창을 닫습니다.
4. 이제 Cloud Sensor가 시스템 목록에 표시됩니다.

Note: Cloud Sensor가 완전히 초기화되고 Cloud Policy Server와 통신하는 데 최대 15분이 소요될 수 있습니다. Cloud Sensor EC2의 상태를 확인하려면 AWS EC2 콘솔에 로그인합니다.

5.9.5 Cloud Sensor를 Cloud Gateway 모드로 설정

1. 상단 메뉴에서 시스템으로 이동 합니다.
2. Cloud Sensor IP를 클릭합니다.
3. 센서 설정 탭을 클릭합니다.
4. eth0 인터페이스의 경우 맨 오른쪽 설정 열에서 센서 설정을 클릭합니다.
5. 센서 설정에서 센서 동작모드를 Host에서 Inline으로 변경하고 동작범위를 Local에서 Global로 변경합니다.
6. 아래로 스크롤하여 수정을 클릭합니다.

5.9.6 Genian ZTNA 클라이언트 설치 및 클라우드 액세스 확인

1. 관리 > 사용자 > 작업 > 사용자 추가에서 원격 접근를 위한 테스트 계정을 만듭니다.
2. https://정책서버IP/agent 로 이동합니다.
3. 다운로드 버튼을 클릭하여 에이전트를 설치 하십시오.
4. 설치가 완료되면 에이전트 아이콘을 마우스 오른쪽 버튼으로 클릭하고 네트워크 액세스를 선택하고 연결을 클릭합니다.
5. 위 단계에서 생성한 사용자 이름과 비밀번호를 입력하세요.
6. ZTNA 클라이언트는 현재 연결되었음을 나타내는 메시지를 표시하고 연결을 위한 IP를 제공해야 합니다.
7. 엔드포인트의 모든 트래픽은 이제 Cloud Gateway를 통해 라우팅됩니다.
8. 원격 세션 정보는 시스템 > 사이트 > ZTNA Client Sessions 에서 볼 수 있습니다.

CHAPTER

SIX

네트워크 연결 프로세스

Note: 이 기능을 사용하려면 Professional 또는 Enterprise Edition이 필요 합니다.

네트워크 연결 프로세스 항목에서 사용자 정의를 통해 Captive Web Portal 및 게스트 관리를 할 수 있습니다.

6.1 CWP(Captive Web Portal) 설정

CWP(Captive Web Portal)는 사용자가 네트워크에 접속할때 표시되는 첫 페이지입니다. 사용자의 현재 보안상태 또는 로그인 페이지 역할을합니다. 다양한 인증 및 정의된 페이지로 리다이렉션 가능합니다.

6.1.1 디자인 템플릿

접속인증페이지 디자인에 도움을 주고자 표준템플릿을 포함해서 유용한 디자인 템플릿을 제공하고 있습니다. 또한 기존 템플릿을 이용해서 새로운 사용자 정의 템플릿을 제작할 수도 있습니다.

6.1.2 CWP(Captive Web Portal) 설정

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목의 **제어 정책** 으로 이동합니다.
3. **원하는 제어 정책** 을 선택합니다.
4. **기본설정 > 적용모드** 에서 **사용함** 을 선택합니다.
5. **제어 옵션 > Captive Web Portal** 아래에서 다음과 같이 진행합니다.
6. **CWP 페이지** 메뉴에서 **표준 CWP 페이지** 를 선택합니다.
7. **수정** 버튼을 클릭합니다.
8. **변경정책적용** 버튼을 클릭합니다.

6.1.3 CWP 사용자 정의 메시지

관리자가 CWP 메세지를 정의하여 사용자의 네트워크가 차단되었을때 차단사유에 대한 충분한 정보를 제공할 수 있습니다. 필수 소프트웨어 다운로드 및 업데이트 등 사용자에게 알려야 하는 정보를 제공하십시오.

CWP 사용자 정의 메시지 추가

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목의 **제어 정책** 으로 이동합니다.
3. **원하는 제어 정책** 의 이름을 선택합니다.
4. **제어 옵션 > Captive Web Portal** 메뉴를 찾습니다.
5. **CWP 페이지** 에서 원하는 옵션을 선택합니다.
6. **CWP** 에 표시 할 **사용자 메시지** 를 입력합니다.(이 메시지는 접속이 차단 될 때 표시됨)
7. **수정** 을 클릭합니다.

6.1.4 공지사항 설정

공지사항은 직원이나 고객이 중요한 업데이트, 이벤트 또는 네트워크 관련 요소를 알 수 있도록하는 게시판 스타일의 메시지입니다. 공지 사항은 일반적으로 하나 이상의 항목을 설명하는 긴 문장이지만, 메시지는 사용자가 차단 된 이유 또는 네트워크에 액세스하기 위해 수행해야하는 작업에 대한 간략한 짧은 설명으로 사용 됩니다.

공지사항 생성

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 항목의 **접속인증페이지(CWP) > 공지사항** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **공지 기간** 이 필요한 경우 **체크박스** 를 클릭하고 **날짜** 및 **시간** 을 설정합니다.
5. **제목** 을 입력합니다.
6. **내용** 을 작성합니다.
7. **타입** 을 선택합니다. (*HTML, Text, or Markdown*)
8. **생성** 을 클릭합니다.

공지사항 삭제

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 항목의 **접속인증페이지(CWP) > 공지사항** 으로 이동합니다.
3. 삭제 할 **공지사항** 의 **체크박스** 를 선택합니다.
4. **작업선택 > 삭제** 를 클릭합니다.
5. **확인** 을 클릭합니다.

Note: 공지사항 설정에 세부사항은 다음에 notice-detail 참고하시기 바랍니다.

6.1.5 사용자 정의 버튼 관리

Captive Web Portal 페이지에 삽입되는 **Custom Buttons** 를 생성하여 웹페이지 리다이렉션, 필수 소프트웨어 다운로드 등 여러가지 동작을 수행할 수 있습니다.

버튼 타입	설명
하이퍼링크	CWP 페이지 버튼 선택 시 입력된 URL 주소 페이지로 이동합니다.
팝업 윈도우	CWP 페이지 버튼 선택 시 별도의 브라우저 창을 이용하여 입력된 URL 주소 페이지를 표시합니다.
에이전트 트레이 메뉴	에이전트 트레이 항목 선택 시 브라우저 창을 이용하여 입력된 URL 주소 페이지를 표시합니다.
정보수집	CWP 페이지 버튼 선택 시 정보수집 페이지로 이동합니다.
다운로드	CWP 페이지 버튼 선택 시 업로드된 파일을 다운로드 합니다.

버튼 생성

1. 상단의 **설정** 으로 이동합니다.
2. 좌측의 **접속인증페이지(CWP) > 사용자정의 버튼** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 기본설정의 **이름** 및 **설명** 을 작성합니다.
5. 이미지URL은 **이미지 업로드** 버튼을 통해 이미지를 업로드합니다.
6. 버튼타입 **하이퍼링크** 를 설정합니다.
7. 버튼표시 **항상 출력** 을 설정합니다.
8. **생성** 을 클릭합니다.

버튼 삭제

1. 상단의 **설정** 으로 이동합니다.
2. 좌측의 **접속인증페이지(CWP) > 사용자정의 버튼** 으로 이동합니다.
3. **체크박스** 를 클릭하고 **작업선택 > 삭제** 를 클릭합니다.

버튼 재정렬

1. 상단의 **설정** 으로 이동합니다.
2. 좌측의 **접속인증페이지(CWP) > 사용자정의 버튼** 으로 이동합니다.
3. **작업선택 > 순서 일괄수정** 을 클릭합니다.
4. 정렬후에 **저장** 을 클릭합니다.

사용자 정의버튼 기능 활용하기

1. 사용자 정의 버튼으로 특정 정보 입력받기

정보수집 기능을 사용하여 사용자에게 특정 정보를 입력받아 노드/장비/사용자 추가필드에 저장하는 기능을 사용할 수 있습니다.

Note: 추가필드를 설정하는 부분은 다음에 추가필드 관리하기 참고하시기 바랍니다.

6.1.6 관리자 정의 페이지 생성

다양한 상황에서 사용할 관리자 정의 CWP 레이아웃을 생성할 수 있습니다.

사용자정의 페이지 디자인

접속인증페이지(CWP) 기본 페이지를 편집하거나 새로운 사용자 정의 페이지를 만들 수 있고, 회사의 로고 등을 CWP에 추가 할 수 있습니다. **설정 > 접속인증페이지(CWP) > 디자인 템플릿** 에서 설정이 가능합니다.

컴포넌트 설정

사용자등록 버튼, 사용자 인증 버튼 등 다양한 컴포넌트에 대해 설정이 가능합니다.

1. 필요한 구성 요소의 추가 또는 삭제 버튼을 클릭합니다.
2. 웹 콘솔의 오른쪽에 있는 기본 페이지에 페이지 미리보기가 표시 됩니다.
3. **수정** 버튼을 클릭합니다.

수정

Javascript를 활용하여 실제 Web 소스 수정이 가능합니다.

1. CWP 페이지는 html 코드 형태로 표시 됩니다.
2. **페이지를 html 코드 형식으로 제공합니다.**
    - 코드에 컴포넌트의 기능를 활성화 하거나 비활성화하여 페이지의 옵션을 수정합니다.
    - html 코드를 사용하여 수정 할 수 있습니다.
3. **수정** 을 클릭합니다.
4. 웹 콘솔의 오른쪽에 있는 기본 페이지에 페이지 미리보기가 표시 됩니다.

레이아웃

Html 코드를 사용하여 페이지 레이아웃을 수정할 수 있습니다.

```
<?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"
   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>
</body>
</html>
```

CSS 스타일

CSS Style 클래스를 정의하고 수정 탭 또는 레이아웃 탭에서 사용 할 수 있습니다.

1. "CSS 스타일" 탭에 CSS 스타일 코드를 입력합니다

```
.test {color:red;}
```

2. "수정" 탭에서 정의 된 CSS 스타일을 사용합니다.

```
<div class="test">
TEST
</div>
```

3. **수정** 버튼을 클릭합니다.
4. 웹 콘솔의 오른쪽에 있는 기본 페이지에 페이지 미리보기가 표시 됩니다.

이미지 업로드

접속 인증 페이지에 사용할 이미지를 직접 업로드할 수 있습니다.

Note: 영문 알파벳 문자 파일 이름 "jpg / gif / png" 확장자 파일만 지원합니다.

정의된 CWP 템플릿 적용

1. 상단 항목에 있는 **정책** 으로 이동합니다.
2. 왼쪽 항목의 **노드정책** 으로 이동합니다.
3. 적용하려는 **노드정책 이름** 을 찾아 클릭합니다.
4. **관리정책 > Design Template** 옵션을 찾습니다.
5. CWP에서 사용할 디자인 항목을 선택합니다.
6. **수정** 을 클릭하고 화면 우측 상단의 **변경정책적용** 을 클릭합니다.

6.1.7 시스템 정의 메시지 변경

CWP 페이지에서 표시되는 시스템 정의 메시지에 대한 변경 기능을 제공합니다.

메시지 변경 기능을 사용하여 고객사 환경에 맞는 단어와 문구를 삽입하거나, 전체 메시지 문구를 변경할 수 있습니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **접속인증페이지(CWP)** 항목에 **메시지관리** 를 선택합니다.
3. 변경하고자 하는 **메시지 ID** 를 클릭합니다.
4. 변경하고자 하는 **언어** 에 해당하는 **메시지 내용** 을 수정합니다.
5. **수정** 버튼을 클릭합니다.

메시지 분류 확인

메시지의 분류로는 시스템 메시지와 적용모드 설정 메시지로 나눌수 있으며 각각 다음과 같이 사용할 수 있습니다.

분류	설명
시스템 메시지	사용 여부를 선택할 수 없으며, 메시지 내용만 변경가능
적용모드 설정 메시지	사용 여부를 선택할 수 있으며, 메시지 내용도 변경가능

6.2 방문자 관리 설정

Genian ZTNA는 네트워크에 정해진 사용 기간 동안 임시로 접속할 수 있는 방문자 계정을 발급 및 관리할 수 있습니다. 생성된 방문자 계정은 계정사용만료 시 처리방법을 설정할 수 있습니다. 방문자 계정 발급 방법은 관리자의 방문자 계정 추가와 방문자가 CWP페이지에서 신청하는 방법이 있습니다. 본 가이드 문서에서는 관리자의 방문자 계정 추가 및 삭제 방법을 안내합니다.

6.2.1 방문자 계정 추가

관리자가 직접 방문자 계정을 생성하여 ID와 비밀번호를 전달할 수 있습니다.

1. 상단 항목에 있는 **관리 > 사용자** 로 이동합니다.
2. **작업선택 > 사용자등록** 를 클릭합니다.
3. **기본설정 > 용도 > 임시계정** 을 클릭합니다.
4. 생성 버튼을 클릭합니다.

6.2.2 방문자 계정 기간만료 처리 설정

방문자 계정 사용기간만료 시 처리하는 방법을 설정할 수 있습니다.

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **속성관리 > 용도관리 > 사용자용도** 로 이동합니다.
3. 목록에서 **Guest** 를 선택합니다.
4. **용도별 처리 옵션 > 사용자계정 만료처리** 로 이동합니다.
5. 사용자계정 만료처리를 **사용중지, 계정삭제** 중 하나를 선택합니다.
6. 수정 을 클릭한 후, **정책적용** 버튼을 클릭합니다.

6.2.3 방문자 계정 삭제

1. 상단 항목에 있는 **관리 > 사용자** 로 이동합니다.
2. 삭제 할 **사용자ID** 를 찾아 **체크박스** 를 선택합니다.
3. **작업선택 > 사용자삭제** 를 클릭합니다.
4. 확인 버튼을 클릭합니다.

6.2.4 방문자 계정 신청 및 승인 프로세스 설정하기

방문자 계정 신청 및 승인 프로세스 설정하기

Genian ZTNA는 방문자 계정 발급을 통해 방문자 식별 및 관리를 할 수 있습니다. 방문자 계정 발급 방법은 관리자의 방문자 계정 추가와 방문자가 CWP페이지에서 신청하는 방법이 있습니다. 본 가이드 문서에서는 방문자가 계정을 직접 신청하고 승인받아 네트워크에 접속하는 프로세스를 안내합니다.

Note: 방문자는 신청한 방문자 계정의 승인이 완료될 때까지 해당 계정으로 로그인할 수 없습니다.

---

1. 방문자 계정 발급 신청 방법

방문자는 CWP 페이지에 접속하여 **사용자 등록** 항목을 통해 방문자 계정 발급을 신청할 수 있습니다.
방문자는 **CWP 페이지 > 사용자 등록 > 용도 > 임시계정** 을 선택해야 정상적으로 방문자 계정 발급신청이 완료됩니다.

CWP 사용자등록 버튼 활성화 방법

방문자가 CWP 페이지에서 방문자계정 발급 신청을 할 수 있도록, 관리자는 CWP 페이지의 사용자등록 버튼을 활성화 시켜야 합니다.

Note: 네트워크센서가 enforcement 모드로 동작 중이고, 노드 정책이 활성화되어 있는지 확인합니다. 네트워크센서에 enforcement 모드를 설정해야 정책을 적용하고 사용자 단말의 네트워크 접근을 제어할 수 있습니다.

---

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
3. 노드정책 창에서 원하는 **노드정책** 의 **정책명** 을 찾아 클릭합니다.
4. **세부설정 > 인증정책 > 사용자등록 페이지** 를 찾아 **On** 으로 선택합니다.
5. **사용자등록에 사용될 WEBPAGE 의 URL 을 설정** 합니다. (미입력시 기본 사용자등록페이지가 사용됩니다.)
6. 수정 을 클릭한 후, 정책적용 버튼을 클릭합니다.

방문자 CWP 접속 주소

```
http://(정책서버 IP)/cwp
```

2. 방문자 계정 발급 승인 방법

방문자 계정 발급 신청이 완료되면, 승인이 완료되어야 로그인이 가능합니다. 방문자 계정 발급 승인 방법은 관리자 직접승인, 이메일승인, 자동승인 총 세 가지 방법이 있습니다.

Case 1 : 관리자 직접 승인 방법

관리자는 WEB콘솔에서 방문자 계정 신청을 승인할 수 있으며, 미설정 시 해당 방식이 기본설정으로 되어있습니다.
방문자 계정 발급 승인 방법이 이메일 승인, 자동승인으로 설정되어있어도, 관리자는 신규등록 사용자 신청서 페이지에서 신규 방문자 계정 발급을 승인할 수 있습니다.

관리자 직접 승인 방법 설정하기

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **속성관리 > 용도관리 > 사용자용도** 로 이동합니다.

3. 목록에서 **GUEST** 를 선택합니다.
4. **용도별 처리 옵션 > 피방문자 이메일 승인** 을 **Off** 으로 설정합니다.
5. 자동승인을 **Off** 로 설정합니다.
6. 수정 을 클릭한 후, 정책적용 버튼을 클릭합니다.

관리자의 방문자 계정 발급 직접 승인/거절하기

1. 상단 항목의 **관리 > 신청** 으로 이동합니다.
2. 왼쪽 신청관리 항목에서 **사용자신청서 > 신규등록** 으로 이동합니다.
3. 계정정보를 확인한 후, 신청서처리 항목에서 **승인** 혹은 **거절** 을 선택합니다.

Case 2 : 이메일 승인 방법

신규 방문자계정 발급 신청을 이메일을 통해 승인할 수 있습니다. 사용자 등록 신청서가 승인자의 이메일로 수신되면, 신청내용을 확인한 후 발급 승인 할 수 있습니다. 이메일 승인자를 관리자, 피방문자(내부사용자), 모두 중 선택하여 설정할 수 있습니다.

임시 계정 이메일 승인자 설정

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **속성관리 > 용도관리 > 사용자용도** 로 이동합니다.
3. 목록에서 **GUEST** 를 선택합니다.
4. **용도별 처리 옵션 > 피방문자 이메일 승인** 을 **On** 으로 설정합니다.
5. 이메일 승인자를 **관리자**, **피방문자**, **모두** 중 하나를 선택합니다.
6. 수정 을 클릭한 후, 정책적용 버튼을 클릭합니다.

방문자 계정 발급 이메일 승인/거부 방법

1. 계정 알람정보에 설정한 이메일의 수신함에서 **'사용자 등록 신청서'** 를 확인합니다.
2. 신청서 내용을 확인하고 **승인/거부** 버튼을 클릭합니다.

> **Warning:** 'Failed to send email' 에러가 발생하는 경우, 외부 전송 이메일 서버 설정 과 관리자, 피방문자의 이메일 계정 확인이 필요합니다.

Note: 정책서버와 통신이 되지 않는 환경에선 메일의 승인 버튼을 클릭해도 승인 처리가 되지 않습니다.

Case 3 : 자동승인 방법

신규 방문자계정 발급신청을 자동으로 승인할 수 있습니다. 사용자 신규 신청완료와 동시에 승인이 이루어집니다.

방문자계정 자동승인 설정

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **속성관리 > 용도관리 > 사용자용도** 로 이동합니다.
3. 목록에서 **GUEST** 를 선택합니다.
4. **용도별 처리 옵션 > 피방문자 이메일 승인** 을 **Off** 으로 설정합니다.
5. 자동승인을 **On** 으로 설정합니다.
6. 수정 을 클릭한 후, 정책적용 버튼을 클릭합니다.

3. 방문자 계정 발급신청 결과 확인하기

방문자가 계정 발급 승인 결과를 확인하는 방법으로는 CWP페이지 신청결과조회와 이메일 확인이 있습니다.

Case 1 : CWP페이지에서 신청결과조회 하기

방문자 계정 신청자는 CWP 페이지의 신청결과조회 항목을 통해 승인 결과를 확인할 수 있습니다.

CWP 페이지 신청결과조회 버튼 활성화 방법

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **접속인증페이지(CWP) > 디자인템플릿** 으로 이동합니다.
3. 목록에서 해당하는 템플릿의 이름을 선택합니다.
4. **신청결과조회버튼** 을 활성화 시킵니다.
5. 수정 을 클릭하여 적용시킵니다.

Case 2 : 방문자계정 신청자의 발급신청 결과 수신 설정 방법

방문자 계정 신청자가 승인 결과를 메일로 수신받을 수 있도록 설정할 수 있습니다. 해당 기능 설정시 발급승인이 완료되면, 방문자 계정 신청자는 발급신청 결과 이메일을 수신하여 확인 가능합니다.

방문자계정 발급신청 결과 이메일 수신 설정 방법

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **속성관리 > 용도관리 > 사용자용도** 로 이동합니다.
3. 목록에서 **GUEST** 를 선택합니다.
4. **용도별 신청정보 > 사용자 신청 옵션 필드** 에서 **할당** 을 클릭합니다.
5. **전자우편** 항목을 우측 목록에 추가 후, **확인** 을 클릭합니다.

6. 수정 을 클릭한 후, 정책적용 버튼을 클릭합니다.

Note: 방문자는 계정 발급 신청 시, 이메일 필드에 값을 입력해야 승인 완료 알림을 받을 수 있습니다.

관리자의 발급신청 결과 확인 방법

관리자는 WEB콘솔에서 본인 혹은 피방문자가 승인/거절한 계정발급신청 결과를 확인할 수 있습니다.

1. 상단 항목에 있는 **관리 > 신청** 으로 이동합니다.
2. **사용자신청서 > 결과조회** 를 클릭합니다.
3. 처리 결과를 확인합니다.

6.3 CWP 기능을 활용한 보안서약 동의 받기

단말이 내부 네트워크에 접속 시 내부 네트워크 사용에 대한 보안약관을 공지하고 사용자에게 동의를 구할 수 있는 페이지를 제공할 수 있습니다.

보안서약에 동의여부, 동의기간 등의 설정을 통해 일정시간 동의를 수행하지 않는 단말을 제어하거나 재 동의를 수행하도록 할 수 있습니다.

6.3.1 보안서약 페이지 구성하기

사용자에게 표시할 보안서약 페이지 내용을 설정합니다. 보안서약 페이지는 사용자에게 표시할 약관과 사용자에게 수집할 정보를 설정하는 수집정보 항목으로 나눠집니다.

1. 상단 패널 **설정** 항목으로 이동합니다.
2. 왼쪽 접속인증페이지에서 **동의페이지 > 보안서약** 으로 이동합니다.
3. 작업선택에서 **생성** 을 클릭합니다.
4. **보안서약** 과 **수집정보** 를 할당 후 **생성** 을 클릭합니다.

6.3.2 보안서약 페이지 적용하기

보안서약 페이지는 Genian ZTNA에서 사용하는 접속인증페이지를 기능을 활용하여 사용자에게 표시합니다.

보안서약 페이지를 적용하기 위해서는 제어정책 을 생성하고, 세부 설정을 수행합니다.

일반적으로 보안서약은 네트워크를 사용하는 최초에 동의를 받아야 함으로 제어정책 생성 시 IP관리 정책 이후로 순서를 정의합니다.

1. 상단 패널 **정책** 항목으로 이동합니다.
2. 왼쪽 **제어정책** 으로 이동합니다.
3. 제어정책에 **ID** 를 클릭합니다.
4. **제어옵션 항목** 에서 CWP 페이지 입력값을 **보안서약 페이지** 로 설정합니다.

5. 세부항목을 설정 후 **수정** 버튼을 클릭합니다.
6. 오른쪽 화면 상단의 **변경정책적용** 을 클릭합니다.

6.4 CWP 페이지 Redirection 가능한 포트 추가하기

네트워크 보안을 목적으로 HTTP / HTTPS(웹서비스)를 기본 포트가 아닌 다른 포트로 변경하여 사용할 경우 Genian ZTNA에서 제공하는 CWP 페이지 Redirection 기능을 사용할 수 없음으로 변경된 포트를 추가해야 CWP 페이지 Redirection 기능을 사용할 수 있습니다.

6.4.1 HTTP, HTTPS 포트 변경 및 추가

HTTP는 기본 포트인 80,8080 이 설정되어 있으며, HTTPS 기본 포트인 443 이 설정되어 있습니다. 포트를 추가하기 위해서는 **,** 구분자를 입력해야 합니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 환경설정 항목에 **노드관리** 를 클릭합니다.
3. 차단설정 메뉴에서 **HTTP 포트** , **HTTPS 포트** 항목을 추가합니다.
4. 수정 버튼을 클릭합니다.

6.5 CWP가 아닌 다른 페이지로 리다이렉션 설정하기

단말의 네트워크가 차단되었을때 특정 페이지로 리다이렉션 되도록 설정하는 방법입니다. 관리자는 CWP 대신 특정 URL을 지정하거나, 사용자가 CWP의 확인 버튼을 클릭했을때 특정 URL로 리다이렉션 되도록 설정할 수 있습니다.

6.5.1 CWP가 아닌 특정 URL로 리다이렉션

단말의 네트워크가 차단되었을때 CWP 대신 관리자가 지정한 URL로 리다이렉션 설정합니다. 다만 새 URL에서 차단 사유에 대한 조치 방법이 충분히 제공이 되지 않는 경우 단말 네트워크 관리에 어려움이 있을 수 있습니다.

1. 상단 패널 **정책** 항목으로 이동합니다.
2. 좌측 **제어정책** 으로 이동합니다.
3. 제어정책 목록에서 설정을 변경할 정책을 클릭합니다.
4. **제어옵션** 의 **CWP 페이지** 를 **사용자정의 페이지** 로 변경합니다.
5. 리다이렉션 설정할 URL을 입력합니다.

6.5.2 CWP의 확인 버튼을 클릭했을때 특정 URL로 리다이렉션

사용자가 CWP의 확인 버튼을 클릭했을때 구글, 네이버, 사내 홈페이지 등 관리자가 지정한 URL로 리다이렉션됩니다.

1. 상단 패널 **설정** 항목으로 이동합니다.
2. 좌측 **접속인증페이지** 의 **디자인 템플릿** 으로 이동합니다.
3. 디자인 템플릿 목록에서 현재 사용중인 템플릿을 클릭합니다.
4. **컴포넌트 설정** 에서 **확인버튼** 을 클릭합니다.
5. 이미지 파일이 있는 경우 **아이콘이미지** 를 업로드합니다.
6. **확인버튼** 옵션에서 **항상사용** 또는 **모든조건 만족시 사용** 을 선택합니다.
7. URL을 입력하고 수정 버튼을 클릭합니다.
8. 수정 버튼을 클릭합니다.

6.6 무선접속을 위한 Client 프로파일 사용자 단말에 적용하기

무선 네트워크 접속을 위한 Client 프로파일을 무선연결관리자(WCM)을 사용하여 Windows OS의 사용자 단말에 자동으로 등록하는 기능을 적용합니다. 무선 네트워크 접속 설정이 Hidden 이거나 보안설정이 필요한 사항을 사용자가 수동으로 설정하지 않고 자동으로 등록과 관리를 수행할 수 있습니다.

프로파일을 단말에 배포하여 설정하기 위해서는 프로파일을 생성하고, 프로파일을 배포하는 무선랜 정책을 설정해야 합니다. 이후 프로파일이 배포되었다면 프로파일을 통해 무선랜을 접속하기 위한 무선연결관리자(WCM) 설정이 필요합니다.

Note: Client 프로파일에 상세 설정 부분은 client-profile-detail 참고하시기 바랍니다.

6.6.1 1. 단말에 적용할 무선 Client 프로파일 설정하기

Client 프로파일에서 설정할 수 있는 보안방식으로는 **Open, WEP, WPA2-Personal. WPA2-Enterprise, 802.1x** 가 있습니다.

1. 상단 패널에 **정책** 으로 이동합니다.
2. 왼쪽 **정책** 항목에 **무선랜정책 > Client 프로파일** 을 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. **Client 프로파일** 설정값을 입력합니다.
5. **생성** 버튼을 클릭합니다.

6.6.2 2. 단말에 적용할 무선랜 정책 설정하기

프로파일을 배포하는 무선랜 정책을 설정합니다. 무선랜 정책은 AP정책과 Client 정책으로 나눠지며 단말에 프로파일을 배포하기 위해서는 Client 정책만 설정하면 됩니다.

1. 상단 패널에 **정책** 으로 이동합니다.
2. 왼쪽 **정책** 항목에 **무선랜정책** 을 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. **Client 프로파일 정책** 에 생성된 **Client 프로파일** 을 할당합니다.
5. **생성** 버튼을 클릭합니다.

6.6.3 3. 무선연결관리자 노드액션과 노드정책 설정하기

노드액션과 노드정책 설정은 다음 무선 연결관리자 구성 을 참고하시기 바랍니다.

6.7 사용자 IP 신청 연동(With Google Form)

본 가이드는 Google Form(app script)을 활용하여 Genian NAC에 서비스중 하나인 IP신청시스템을 사용하는 방법을 안내합니다.

6.7.1 개요

Google Form의 Apps script와 Genian NAC의 RestFul API를 활용하여 Genian NAC를 사용하는 사용자가 네트워크 자원을 사용하기 전 보다 편리하게 IP와 MAC을 신청/승인 받고 비인가/인가 사용자에 대한 감사 증적을 남길 수 있습니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0.55 이상	

6.7.2 연동의 목적

Goole Form과 Genian NAC IP 신청 연동은 다음의 효과를 제공합니다.

사용자 친화적 IP 신청 프로세스

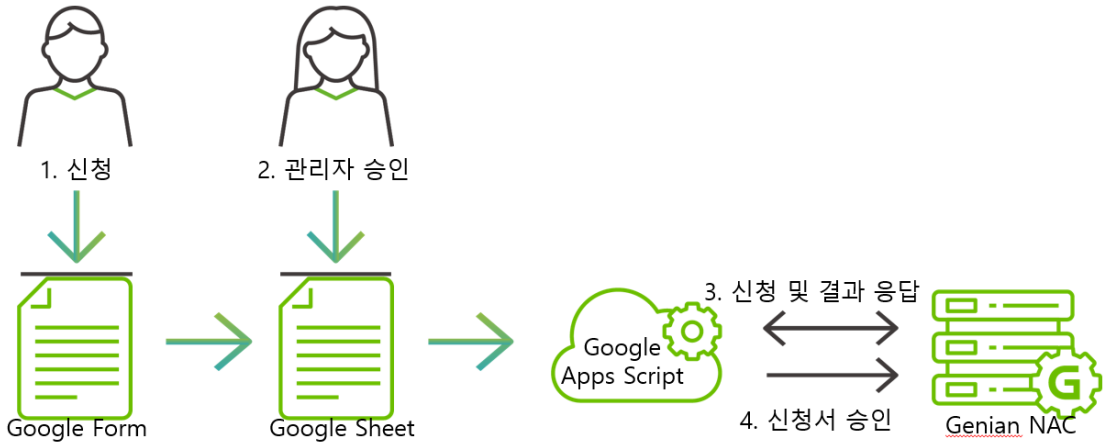
- 일정한 틀이 만들어져있는 기본 제공 IP 신청화면이 아닌 사용자측에서 개발한 UI를 사용하여 IP 신청 시스템을 구축할 수 있습니다.

관리자 친화적 IP 신청 프로세스

- 관리자가 원하는 IP 신청/승인 프로세스를 만들 수 있으며 언제든지 프로세스를 변경 할 수 있습니다.

6.7.3 IP신청 연동 시나리오

1. 사용자가 Google Form 으로 신청 내용 작성
2. Google Sheets 에 신청 내용 등록
3. 신청한 내용을 바탕으로 Genian NAC에 IP 신청
4. 관리자가 Google Sheets에서 승인으로 값 변경
5. 관리자가 승인한 IP 신청서 승인



6.7.4 사전 준비 사항

- 외부와 통신이 가능한 Genian NAC 정책 서버
- 관리자의 API 키
- 정책서버에 등록된 센서 장비 및 센서의 노드 아이디
- Google Form

1. Genian NAC

Google Apps Script에서 NAC의 API를 호출하기 위해서는 네트워크 접근이 가능해야하기 때문에 클라우드 기반의 NAC 환경이거나 NAC에 접근할 수 있도록 도메인 설정을 먼저 해야합니다. 여기서는 접근 편의성을 위해 Test용 Cloud NAC를 생성하여 진행합니다.

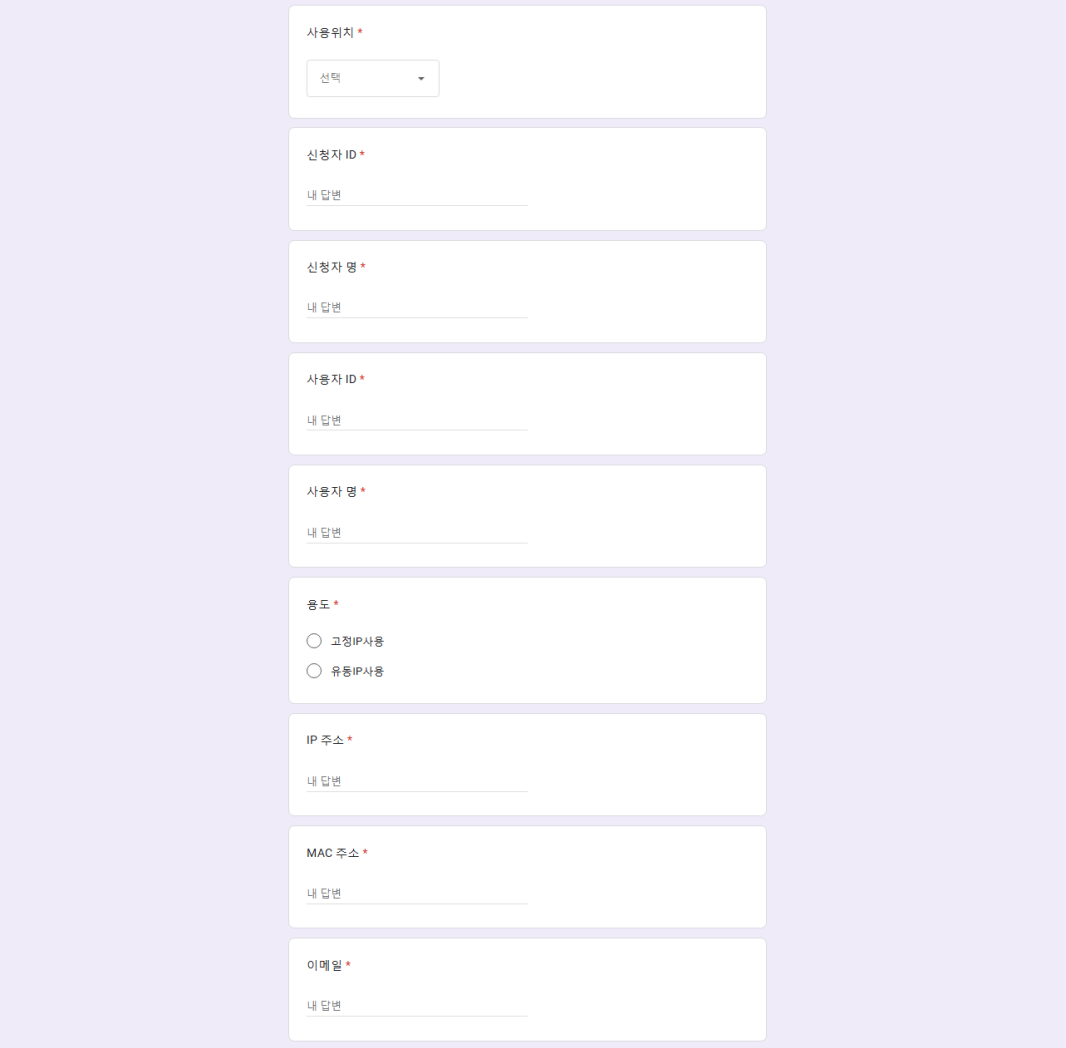
- Cloud NAC 사이트 생성
- genians(https://my.genians.co.kr/) 사이트에서 계정 생성 및 사이트 생성
- 센서 설정 및 API Key 발급
  - IP 신청을 하기 위해서는 관리하고 있는 네트워크에 NAC 센서를 연결하여 생성한 사이트에 등록해야합니다. NAC 센서 생성 및 설정은 네트워크센서 설치 를 참고하세요.
  - API 연동을 위해서는 관리자의 API Key를 생성해야합니다.
    - 관리 > 사용자 > 관리자의 상세화면에서 API Key를 생성합니다.

- 센서 Node ID 확인
- IP 신청을 할 때 사용하고자하는 IP대역을 선택하게 되는데 이때 센서를 선택하게됩니다. 선택하는 장비의 Key가 Sensor Node ID입니다.
- 시스템 > 센서설정 > 센서 상세화면의 Node ID를 확인합니다.

2. Google Form

- 사용자에게 IP 신청을 받을 수 있는 Google 설문지 폼을 설정합니다.
- Google Drive 메뉴에서 Google 설문지 메뉴를 선택합니다.
- IP 신청서 작성 시 필수 입력이 필요한 항목을 설정합니다.(※ 각 사이트마다 요구사항은 다를 수 있으며 환경에 맞게 구성합니다)
- 본 문서에서는 기본적인 항목을 기반하여 설정했으며 설정내용은 아래와 같습니다.

```
사용위치: 드롭다운
 - 사용하고 있는 센서를 추가합니다. 여러 항목중에 선택할 수 있도록 드롭다운을 사용하며 구분을
위해 IP 주소를 라벨로 지정했습니다.
사용자 ID: 단답형 텍스트
 - 사용자의 ID를 입력합니다.
사용자 명: 단답형 텍스트
신청자 ID: 단답형 텍스트
신청자 명: 단답형 텍스트
용도: 드롭다운
 - 유동, 고정 IP 사용인지 용도를 선택할 수 있습니다.
IP 주소: 단답형 텍스트
 - 고정 IP 용도인 경우 IP를 입력합니다.
MAC 주소: 단답형 텍스트
 - 고정 IP 용도인 경우 MAC 주소를 입력 받습니다.
이메일: 단답형 텍스트
 - 신청 결과를 받을 이메일 주소를 입력받습니다.
```



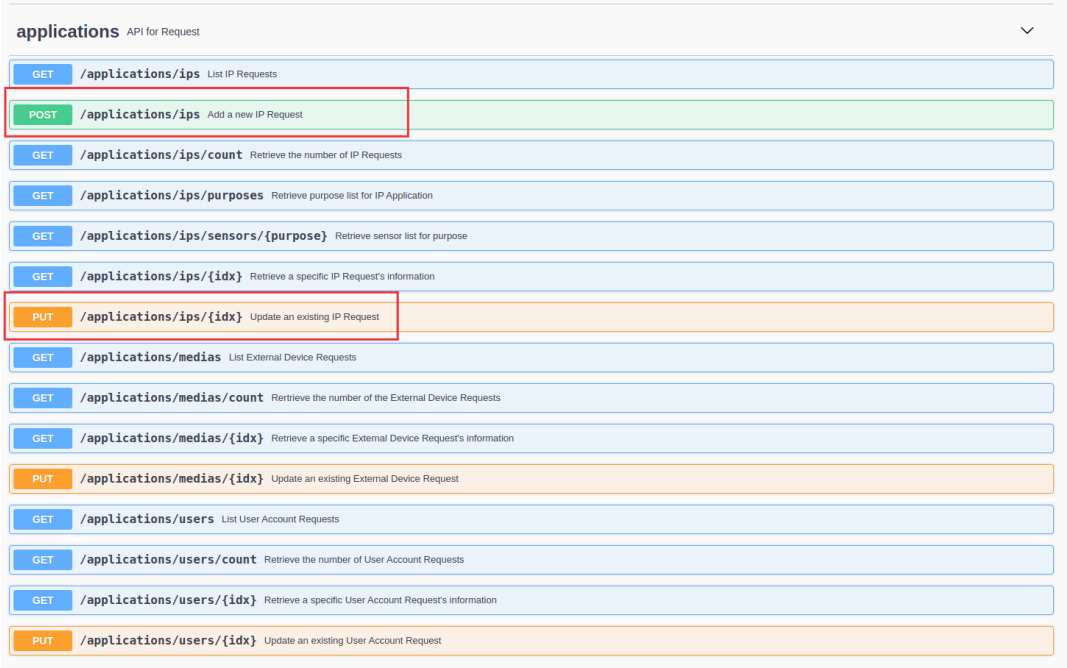
Note: 질문에 사용되는 항목명은 Apps script 에서 그대로 사용되는 값이므로 정확히 작성합니다.

- Sheets의 응답탭으로 이동하여 결과에 대한 Sheets를 생성합니다.
- 응답 > Sheets에서 보기 클릭
- Sheets 가장 마지막 열에서 컬럼 두개를 추가 합니다.
- 승인여부: 관리자가 승인 여부를 선택할 수 있도록 컬럼을 추가합니다.(드롭다운)
- idx: IP 신청 이후 정책서버에 등록되는 신청서의 index 값을 업데이트 할 컬럼입니다.

3. Apps Script

- 설문이 작성되어 시트에 내용이 저장될 때마다 실행될 스크립트를 작성합니다.
- 실행할 스크립트 종류는 두종류 입니다.
- 신청서 작성 시 신청서 등록 스크립트
- 관리자 승인 시 신청서 승인 스크립트
- Sheets 메뉴 > 확장 프로그램 > Apps Script를 선택합니다.

- 스크립트를 작성하기 전 NAC Swagger 페이지에서 사용할 API를 확인합니다.
- swagger는 Genian NAC에서 사용가능한 API를 문서화한 도구이며 {https://Domain/mc2/swagger/index.html} 에서 확인 가능합니다.
- 생성과 승인을 하기 위해 POST **/mc2/rest/applications/ips** (신청서 생성) 와 PUT **/mc2/rest/applications/ips/신청서idx** (신청서 상태 수정) API를 확인합니다.



- Google form이 작성될 때마다 실행될 스크립트를 작성합니다.
- IP 신청서 등록

```
function onFormSubmit(e) {
  const itemResponses = e.namedValues;

  // 관리자의 API Key를 생성한 뒤 api 호출 시 사용할 수 있도록 선언한다.
  const API_KEY = "관리자의 API KEY 값"
  // REST API 를 호출할 url
  const url = "https://[도메인]/mc2/rest/applications/ips";

    const applyResJson = applyIpApplication(url, API_KEY, itemResponses);
    if(applyResJson !== null) {
      const idx = applyResJson.ipApps[0].idx;
      const sheet = e.range.getSheet();
      const row = e.range.getRowIndex();
      sheet.getRange(row, 12).setValue(idx);
    }
  }

    /**
  * IP 신청서 신청 후 응답값을 json 객체로 반환
  */
  function applyIpApplication(_url, apiKey, itemResponses) {
    const url = _url + "?apiKey=" + apiKey;
    const payload = getApplicationPayload(itemResponses);
    // REST API 호출
```

(continues on next page)

(continued from previous page)

```
  const options = {
    "method": "POST",
    "contentType": "application/json;charset=UTF-8",
    "headers": {
      "accept": "application/json;charset=UTF-8"
    },
  "payload": payload
  };
  const response = UrlFetchApp.fetch(url, options);
  let resJson = null;
  try {
    resJson = JSON.parse(response.getContentText());
  } catch(e) {
    resJson = null;
  }
  return resJson;
}
/**
* IP 신청서 신청 시 입력된 값을 json string 으로 변환
*/
function getApplicationPayload(itemResponses) {
  // 센서의 nid을 가져올 수 있도록 객체로 미리 선언
  const sensorDatas = {'172.29.132.0/24': '[센서 Node ID]'
                       };
  // 용도의 value 값 선언
  const purposeDatas = {'유동IP사용': 'USERIP_VARIABLE',
                        '고정IP사용': 'USERIP_STATIC'};
  // 응답 데이터 가공
  const purposeType = itemResponses["용도"][0];
  const data = {};
  // 신규신청:1
  data["appType"] = 1;
  data["sensorNid"] = sensorDatas[itemResponses["사용위치"][0]];
  data["id"] = itemResponses["사용자 ID"][0];
  data["name"] = itemResponses["사용자 명"][0];
  data["applicantId"] = itemResponses["신청자 ID"][0];
  data["applicantName"] = itemResponses["신청자 명"][0];
  data["purposeCode"] = purposeDatas[itemResponses["용도"][0]];
  if(purposeType === '고정IP사용') {
  data["ipStr"] = itemResponses["IP 주소"][0];
  data["mac"] = itemResponses["MAC 주소"][0];
}
  data["alarmEmail"] = itemResponses["이메일"][0];
  const payload = JSON.stringify([
    data
  ]);
return payload;
}
```

- function 설명
- **onFormSubmit()**
  - Google form이 작성된 후 실행되는 진입점이 되는 function
- **applyIpApplication()**
  - 신청서 API를 호출하는 function. 작업이 완료되면 결과값을 json 형태로 리턴합니다.

- **getApplicationPayload()**
  - 신청서 API 호출 시 form에 입력된 정보를 바탕으로 파라미터를 생성합니다.
- 사전 정의한 정보

```
    const sensorDatas = {'172.29.50.xx': '센서 Node ID'};

// 용도의 value 값 선언
 const purposeDatas = {'유동IP사용': 'USERIP_VARIABLE',
                       '고정IP사용': 'USERIP_STATIC'};
```

  - IP 신청을 할 때 센서의 Node ID 값을 파라미터로 전송해야하는데 form에 Node ID를 노출하는것은 사용자가 인식하기 어려운 정보이기 때문에 해당 부분이 치환이 될 수 있도록 사전에 정의해놓습니다.

- IP 신청 승인

```
/**
* 시트에서 승인 컬럼 값이 변경되면 호출
* @param {e} 이벤트 객체
    */
  function onEdit(e) {
    const sheet = e.source.getActiveSheet();
    const targetColumn = 11; //  idx 컬럼, 0 시작 배열에서 가져오는 값이기 때문에
컬럼 인덱스 값 -1
    const editedRow = e.range.getRow();
    const val = e.range.getValue();
    // 수정된 셀의 ROW에 idx값이 있는 경우에만 처리
  if (val === '승인') {
    const record = sheet.getRange(editedRow, 1, 1, sheet.getLastColumn()).
↪getValues()[0];
    const idx = record[targetColumn];
    if(idx !== '') {
    approveIpApplication(idx);
    Logger.log("Value of val: " + idx);
    }
}
}
/**
* IP 신청서 승인
*/
function approveIpApplication(idx) {
// 관리자의 API Key를 생성한 뒤 api 호출 시 사용할 수 있도록 선언한다.
const API_KEY = "[관리자 API KEY값]"
const apiUrl = "[도메인]/mc2/rest/applications/ips/" + idx + "?apiKey=" +␣
↪API_KEY;
const options = {
    "method": "PUT",
    "contentType": "application/x-www-form-urlencoded",
    "headers": {
    "accept": "application/json;charset=UTF-8"
    },
    "payload": "cmd=approve"
};
    try {
    const response = UrlFetchApp.fetch(apiUrl, options);
} catch (err) {
    Logger.log("Error: " + err);
```

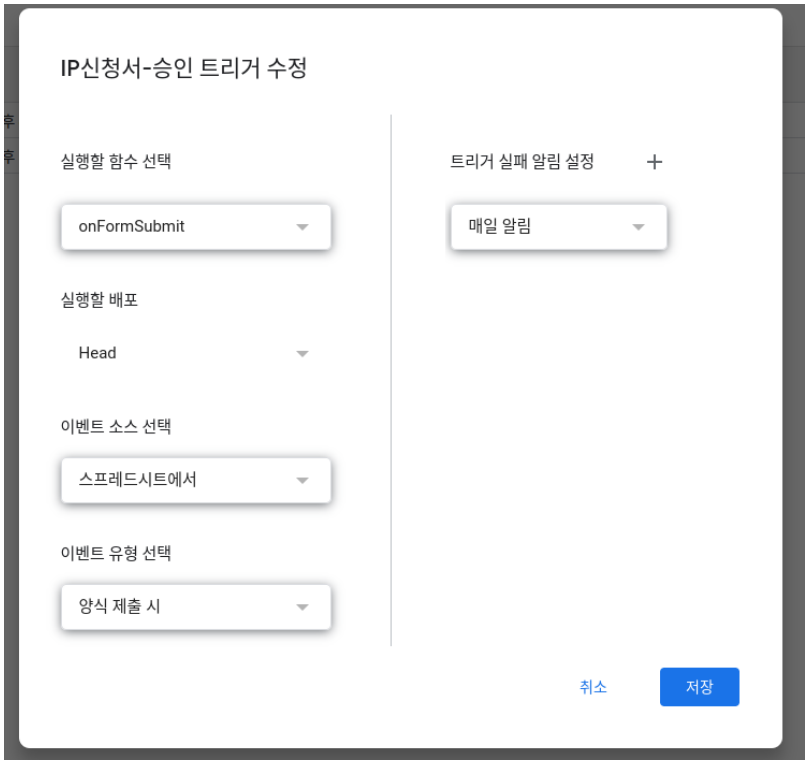
(continues on next page)

(continued from previous page)

```
}
}
```

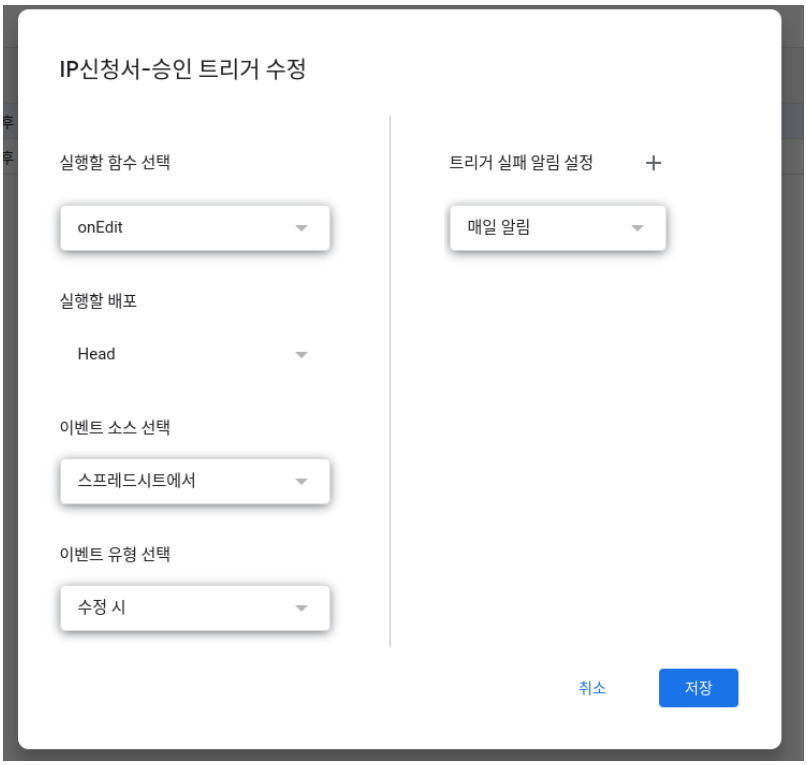
  - function 설명
  - **onEdit()**
    - 시트의 컬럼값을 관리자가 수정했을때 호출되는 function
    - 관리자가 수정한 컬럼이 승인여부 컬럼이면서 승인으로 값을 변경할 경우 approveIpApplication() function을 호출한다.
  - **approveIpApplication()**
    - 선택한 레코드의 IP 신청서를 승인한다.

- 트리거로 등록
- 트리거 메뉴로 이동합니다.
- 트리거 추가
  - IP 신청서 등록 트리거
    - 실행할 함수 선택: 스크립트에 작성한 onFormSubmit() 선택
    - 실행할 배포: Head
    - 이벤트 소스 선택: 스프레드시트에서
    - 이벤트 유형 선택: 양식 제출 시

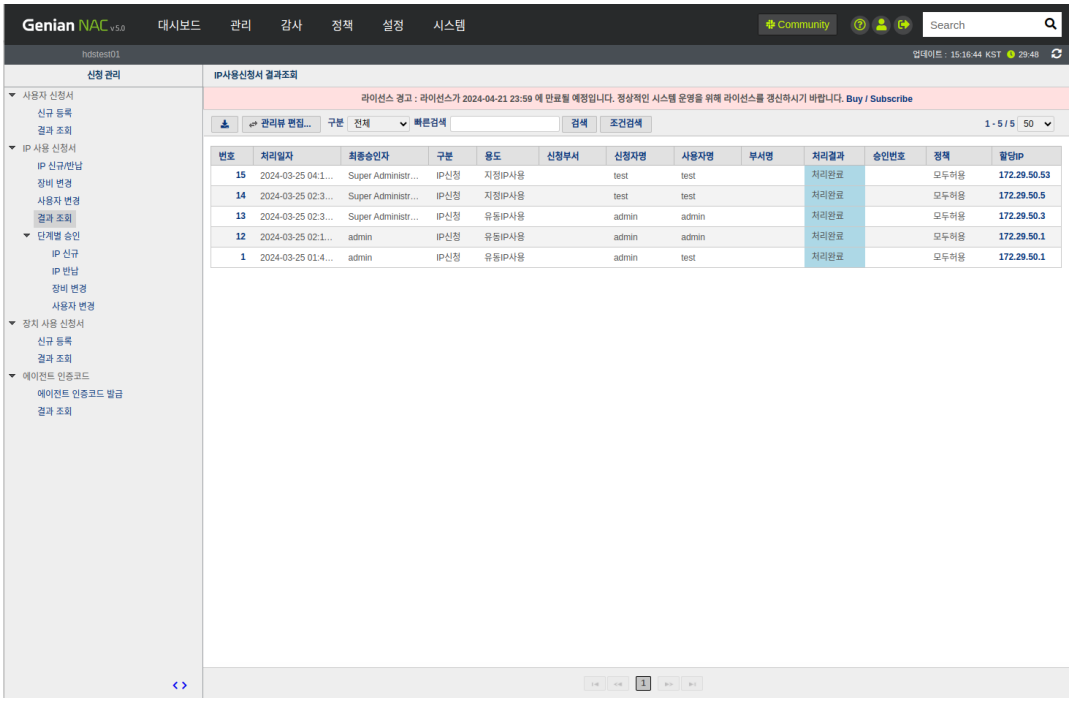


  - IP 신청서 승인 트리거
    - 실행할 함수 선택: 스크립트에 작성한 onFormSubmit() 선택

        * 실행할 배포: Head
        * 이벤트 소스 선택: 스프레드시트에서
        * 이벤트 유형 선택: 수정 시



- 설문 작성 및 실행 확인
    - 실행 확인
        * 설문을 작성 후 확인
        * 시트에서 승인 후 확인
        * Logger.log 로 확인할 내용을 작성해 놓으면 실행단계에서 확인이 가능합니다.
- NAC에서 IP 신청 결과 확인
    - 관리 > 신청 > IP 사용 신청서 > 결과조회 메뉴 이동
    - 승인된 신청서 확인



6.8 문제해결

6.8.1 차단단말이 CWP페이지 Redirection이 되지 않는 문제

Genian ZTNA는 회사의 보안 정책을 준수하지 않은 사용자가 브라우저로 네트워크 접속을 시도할 때 CWP를 통해 준수해야 하는 보안 정책을 보여 줍니다. 사용자에게 접속인증페이지를 표시하기 위해 Genian ZTNA은 사용자 PC가 네트워크 통신 프로세스를 모니터링하고 사용자가 액세스하려는 페이지 대신 Genian ZTNA의 CWP 페이지를 볼 수 있도록합니다.

Genian ZTNA가 제어하는 PC에서 CWP 페이지에 연결되어 있지 않습니다. 또는 웹브라우저에 "연결이 비공개입니다." 라는 문구만 표시되는 경우가 있습니다

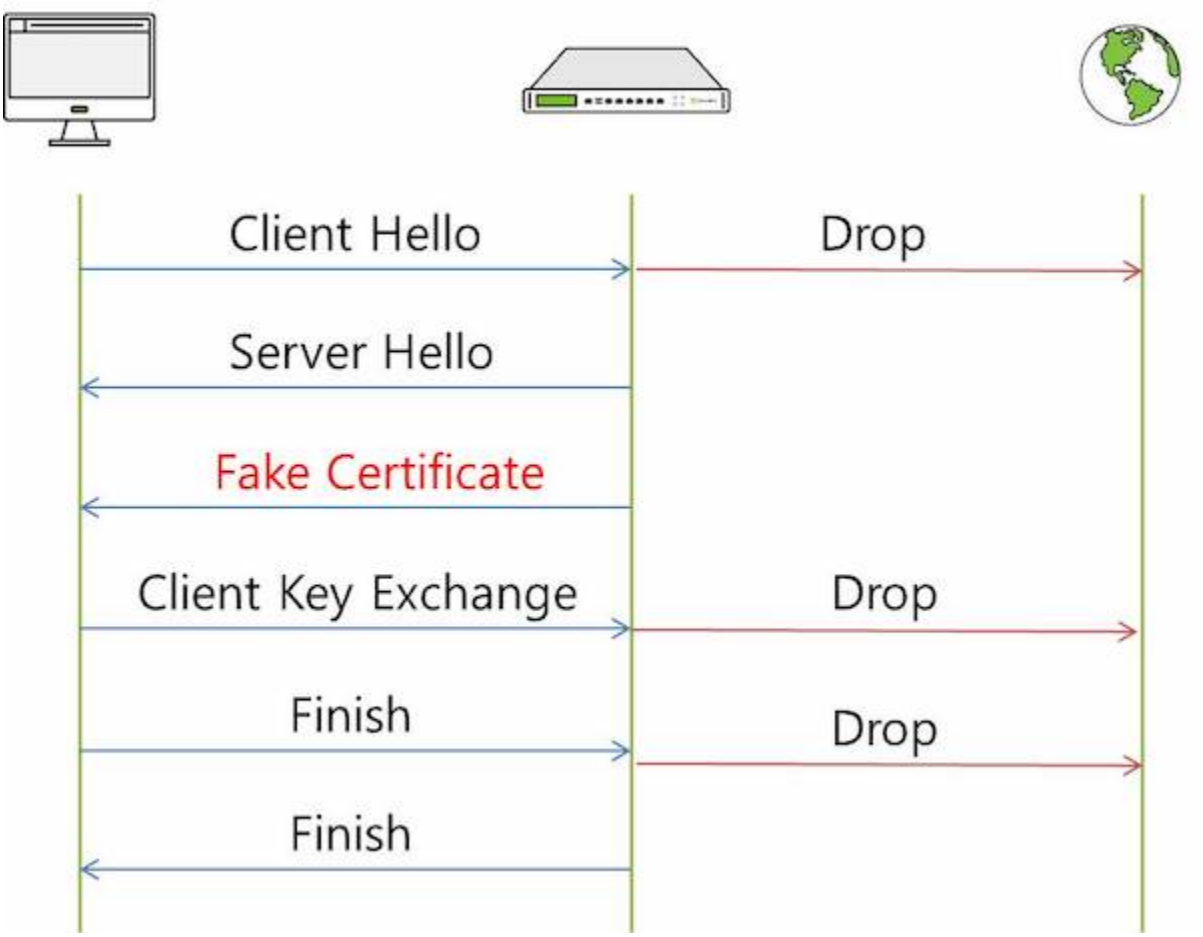
이 문제는 보안 정책을 준수하지 않는 사용자가 HTTPS 서비스를 사용하여 특정 사이트에 연결할 때 발생합니다. Genian ZTNA는 기본적으로 단말에서 발생하는 패킷을 우회시켜 사용자에게 CWP 화면을 표시하지만 HSTS 및 HPKP(브라우저의 인증서 확인)라는 브라우저의 기능으로 CWP 페이지 리다이렉션이 되지 않을 수 있습니다. 아래 내용들을 확인하여 ZTNA의 차단 페이지 동작방식을 이해할 수 있습니다.

HTTP 통신을 시도하는 PC에 CWP 페이지를 표시하는 방식

Genian ZTNA가 HTTPS 통신을 하려는 PC에 CWP 페이지를 표시하는 방법입니다. 차단된 단말이 WEB 브라우저로 통신을 시도할때 GENIAN ZTNA CWP 페이지가 표시되는 원리를 이해할 수 있습니다.

이 방법은 단말의 패킷을 가로채는 방법을 사용합니다.

보안 정책을 준수하지 않는 PC는 ARP 테이블이 변조된 상태에 있습니다. 모든 통신은 네트워크센서를 통해 이루어집니다. 웹 서버와 통신 할 때 네트워크센서는 웹 서버 대신 통신합니다.



여기서 중요한 점은 서버 인증서가 Genian ZTNA에서 생성한 CA 인증서(FAKE 인증서)로 전송되어 암호화된 통신이 웹 서버에 연결되지 않고 Genian ZTNA로 세션이 설정되므로 네트워크센서에서 통신 내용을 확인할 수 있습니다.
따라서 Genian ZTNA는 보안 정책을 준수하지 않은 PC에서 CWP 화면을 표시할 수 있습니다.
그러나 보안 정책을 준수하지 않은 사용자가 특정 웹 사이트에 액세스 할 때 브라우저 화면에서 "연결이 비공개로 설정되어 있지 않습니다"라는 메시지만 볼 수 있고 CWP 화면을 볼 수 없는 이유는 HSTS 및 HPKP 기능 때문입니다.

1. HSTS/HPKP 로 인한 CWP 페이지가 표시되지 않는 경우

증상

보안 정책을 준수하지 않는 사용자 PC가 특정 웹 사이트에 접속할 때 브라우저 화면에 **"연결이 비공개로 설정되어 있지 않습니다. (IE : 이 사이트는 안전하지 않습니다.)"** 라는 메시지가 나타납니다.

원인

Genian ZTNA가 CWP 페이지를 표시하지 못하는 경우와 보안 정책을 준수하지 않는 사용자를 제어하는 방법에 대해 설명 하겠습니다.

제어 대상 PC가 HTTPS 사이트에 액세스 할 때 Genian ZTNA는 자체 인증서를 특정 사이트 인증서 대신 제어 대상 PC에 전달합니다.

여기서 브라우저는 **Genian ZTNA에서 받은 인증서의 PIN 값을 사전 등록된 특정 사이트의 PIN 값과 비교** 합니다. PIN 값이 서로 다른 것으로 판단되면 Genian ZTNA는 제어 대상 PC와 암호화 대상 사이에 암호화 세션을 설정할 수 없으므로 사용자 PC에 CWP 페이지를 표시 할 수 없습니다.

따라서 특정 사이트에 액세스 할 때 제어 대상 사용자 PC가 CWP 화면으로 리다이렉션되지 않고 "사용자의 연결이 비공개가 아닙니다"라는 메시지만 표시되는 것입니다.

Note: HSTS(HTTP Strict Transport security) 란?

- 클라이언트가 요청하는 HTTP 패킷을 HTTPS로만 요청하도록 강제화 하는 설정
- 웹서버의 응답 헤더에 'Strict-Transport-Security' 를 삽입하여 최초 요청 시 부터 HTTPS로 강제화하는 설정
- 중간자 공격 MITM (Man In The Middle) 중 일부인 SSL Strip 공격을 방지할 수 있다.

HPKP(HTTP Public Key Pinning) 란?

- 클라이언트가 서버와 SSL/TLS 암호화 통신에 사용할 인증서를 최종 서버의 인증서로 고정(Pinning) 하는 설정
- 잘못된 PIN 값을 가진 인증서로 접속 요청 시 고정했던 인증서를 비교하여 다를 경우 접속을 거부
- 즉. 중간자 공격 MITM (Man In The Middle) 을 방지할 수 있다.

해결방법

리다이렉션 기능을 사용하는 모든 보안 솔루션에서 발생하는 문제이며 현재 다른 대책을 고려 중입니다.

2. Proxy 서버를 사용하여 CWP Redirection이 되지 않음

증상

네트워크를 제한하는 정책을 할당받은 노드가 WEB페이지 연결을 시도할때 CWP페이지로 Redirection 이 되지 않는 현상발생

원인

단말의 트래픽이 Proxy 서버를 거치면서 정상적으로 Redirection을 수행하지 못하는 문제로 발생

해결방법

Proxy 설정에서 정책서버의 IP를 예외처리합니다.

예외처리 방법은 하단을 참고하시기 바랍니다.

.pac 파일 수정 샘플

```
function FindProxyForURL(url, host) { if (isInNet(host, "[정책서버 IP]","255.255.255.255
↪"))
return "DIRECT"; else return "PROXY [프록시 서버 주소]"; }
```

.dat 파일 수정 샘플

```
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";
};
```

CHAPTER

SEVEN

사용자 인증

Note: 이 기능을 사용하려면 Professional 또는 Enterprise Edition이 필요합니다.

사용자 인증은 네트워크에 접근 하려는 사용자의 신원을 확인하고 ID 및 암호를 사용하여 책임추적을 가능하게 합니다.

ZTNA는 다양한 방법으로 사용자 인증 기능을 제공 합니다.

정책 서버에서 로컬로 사용자를 생성하거나 Active Directory, RADIUS, POP3, IMAP, SMTP, CSV 또는 기타 타사 사용자 관리 시스템에서 사용자 정보를 가져 오도록 정책 서버를 구성 할 수 있습니다.

로컬
: 사용자는 ZTNA 정책서버 내에 생성된 로컬 데이터베이스에 인증을 시도합니다. 자격 증명이 일치하면 사용자가 네트워크를 이용할 수 있습니다.

외부 (*Active Directory, RADIUS, IMAP, POP3, SMTP, CSV*)
: ZTNA는 외부 인증 시스템과 연동되어 로그인 시 적절한 자격 증명을 사용하여 사용자 액세스를 허용 할 수 있습니다.

7.1 사용자 인증 설정

접속인증페이지(CWP), 에이전트, 802.1x, AD(Active Directory) 및 RADIUS 를 사용하여 사용자 인증을 구성 할 수 있습니다.

7.1.1 접속인증페이지(CWP) 통한 인증

CWP는 사용자 인증, 게스트 관리, 사용자 알림에 사용됩니다. 관리자는 사용자 및 게스트 인증을 위해 접속인증페이지(CWP)를 구성할 수 있습니다. 사용자는 네트워크 사용을 위해 리다이렉션된 CWP에서 아이디/패스워드를 이용한 인증을 수행합니다. 정책서버는 인증된 사용자 정보를 바탕으로 사용자에게 정책 및 정보를 표시해 줍니다.

접속인증페이지(CWP) 를 통한 사용자 인증 설정 예:

"미인증 사용자" 상태그룹 편집

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목의 **그룹 > 노드** 로 이동합니다.
3. 노드그룹창에서 **미인증노드** 를 찾아 클릭합니다.
4. **기본정보 > 적용모드** 옵션을 찾아 **사용함** 을 선택합니다.
5. **수정** 버튼을 클릭합니다.
6. 우측 상단의 **변경정책적용** 버튼을 클릭합니다.

"미인증노드" 상태그룹을 "미인증차단" 제어정책에 적용

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목의 **제어정책** 으로 이동합니다.
3. **미인증차단** 제어정책을 찾아 클릭합니다.
4. **기본설정 > 적용모드** 옵션을 찾아 **사용함** 으로 선택합니다.
5. **노드그룹** 에 **미인증노드** 가 추가되었는지 확인합니다. (없을 경우 할당을 클릭하고 추가)
6. **수정** 버튼을 클릭합니다.
7. 우측 상단의 **변경정책적용** 버튼을 클릭합니다.

Note: 브라우저 주소창에서 '정책서버IP'/cwp2 로 이동하면 인증 아이콘 확인이 가능합니다.

7.1.2 에이전트를 통한 인증

에이전트 는 엔드포인트 단말의 상태를 확인하는 데 도움이 될 뿐만 아니라 시스템 정보 수집, 접근 제어 및 사용자 인증도 지원합니다. **Genian Agent** 플러그인을 사용하여 사용자를 인증하도록 정책 서버를 설정 할 수 있습니다 . 사용자가 인증되면 **에이전트** 는 2분 마다 정책 서버와 통신하여 엔드포인트 단말의 사용자를 계속 확인합니다.

1단계. 에이전트 인증을 위한 노드그룹 생성

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 정책 그룹 생성** 을 클릭합니다.
4. **ID** 를 **에이전트 인증** 으로 입력합니다.
5. 노드그룹 창에서 **그룹조건 > 조건설정** 메뉴을 찾습니다. **추가** 를 클릭합니다.
6. 다음을 입력합니다:
   - 항목: **에이전트**
   - 조건: **설치상태**
   - 설정: **설치됨**
7. **수정** 버튼을 클릭합니다.

8. 우측 상단의 **변경정책적용** 버튼을 클릭합니다.

2단계. 에이전트 플러그인을 통한 사용자 인증 설정

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. **에이전트 인증창** 을 찾아 클릭합니다.
4. **원하는 조건** 및 **에이전트 옵션 설정** 를 추가합니다.
5. **수정** 을 클릭합니다.
6. 우측 상단의 **변경정책적용** 버튼을 클릭합니다. 닫기를 클릭합니다.

3단계. 에이전트 인증을 위한 노드 정책을 생성

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다. **노드정책 마법사** 의 단계를 완료합니다.
4. **정책 기본설정** 탭에서 **ID** 를 **에이전트 인증** 으로 입력합니다.
5. **노드그룹 설정** 탭에서 **에이전트 인증** 노드 그룹을 선택하고 **선택** 위치로 이동합니다.
6. **정책 세부설정** 탭에서 **원하는 옵션** 을 입력합니다.
7. **노드액션 설정** 탭에서 **에이전트 인증창** 을 선택하고 **선택** 위치로 이동합니다.
8. **위험감지 설정** 탭 (이 탭에는 아무것도 필요하지 않습니다)
9. **완료** 를 클릭합니다.
10. 우측 상단의 **변경정책적용** 버튼을 클릭합니다. 닫기를 클릭합니다.

노드 정책에 에이전트 액션 할당

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 원하는 **노드정책** 명을 찾아 클릭합니다.
4. **노드액션 설정** 에서 **할당** 을 클릭합니다.
5. **에이전트 인증창** 액션을 **선택** 위치로 이동 시킵니다.
6. **추가** 를 클릭합니다.
7. **수정** 를 클릭합니다.
8. 우측 상단의 **변경정책적용** 버튼을 클릭합니다. 닫기를 클릭합니다.

Note: 새 노드 정책을 생성하지 않으려면 아래 단계를 선택하여 기존 노드 정책을 사용할 수 있습니다.

7.1.3 RADIUS(802.1x)를 통한 인증

Note: 이 기능을 사용하려면 Enterprise Edition이 필요합니다.

Genian ZTNA에는 802.1x 포트 기반 액세스 제어를 지원하는 자체 RADIUS 서버가 있습니다. 일반적으로 802.1x는 무선 네트워크에 접속하는 단말에 대해 향상된 사용자 인증을 제공하는데 널리 사용합니다. 유선 네트워크에서는 802.1x를 지원하는 스위치를 통해 네트워크에 연결된 단말에 대한 사용자 인증 기능을 제공할 수 있습니다.

먼저 RADIUS 서버를 활성화해야 합니다. *RADIUS 제어 설정* 를 참고하십시오.

외부 데이터베이스에 대한 RADIUS 인증의 경우 인증 연동을 구성해야 합니다. 외부 인증서버 설정 를 참고하십시오.

노드 정보에서 인증 결과를 업데이트하려면 RADIUS 계정 서버를 활성화해야 합니다. *RADIUS Accounting* 를 참고하십시오.

RADIUS AD 인증 연동

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **서비스 > RADIUS서버** 로 이동합니다.
3. **RADIUS서버 > ActiveDirectory 인증연동** 메뉴를 찾아 드롭다운에서 **On** 을 선택합니다.

Note: ※ 본 옵션은 EAP 인증 > 기본 EAP 유형(PEAP) 이 "MSCHAPv2" 인 경우 설정이 가능합니다.

4. 다음 항목들을 입력합니다.
   - **도메인 네임** : ActiveDirectory 서버의 도메인 네임을 입력합니다. (예: *genians.com*)
   - **Domain Admin 권한 계정 아이디** : ActiveDirectory 서버의 Domain Admin 권한이 있는 계정 아이디를 입력합니다.
   - **Domain Admin 권한 계정 비밀번호** : ActiveDirectory 서버의 Domain Admin 권한이 있는 계정 비밀번호를 입력합니다.
5. **수정** 버튼을 클릭합니다.

RADIUS URL 인증 연동

1단계.

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **서비스 > RADIUS서버** 로 이동합니다.
3. **RADIUS서버 > Webhook 인증연동** 메뉴를 찾아 드롭다운에서 **On** 을 선택합니다.

Note: ※ 아래 단계의 옵션들은 모두 EAP 인증 > 기본 EAP 유형(PEAP) 이 "GTC" 인 경우 설정이 가능합니다.

2단계.

1. 왼쪽 설정 항목에서 **서비스 > 인증연동 > Webhook 인증연동**
2. 다음 항목들을 입력합니다.

- **URL** : 인증을 수행할 외부 URL을 입력합니다. (예: *http://.com*)
- **방식** : 호출방식을 선택합니다. (GET / POST / PUT / DELETE)
- **결과검증 정규식** : 인증 성공을 판별할 수 있는 정규식을 입력합니다.

3. Click **Update**

RADIUS 이메일 인증 연동

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **서비스 > RADIUS서버** 로 이동합니다.
3. **RADIUS서버 > E-Mail 인증연동** 메뉴를 찾아 드롭다운에서 **On** 을 선택합니다.
4. 외부 인증서버 설정 의 IMAP/POP3/SMTP 사전 설정이 필요합니다.
5. **수정** 버튼을 클릭합니다.

RADIUS를 통한 사용자 단말(MAC) 인증

MAC 인증은 사용자 계정에 대한 인증과정을 통신을 시도하는 인터페이스의 MAC 정보로 대체하는 인증방식입니다. MAC 주소가 RADIUS 인증의 아이디, 패스워드를 대체합니다. 사용자는 네트워크에 접근하기 위해 특정 아이디, 패스워드를 제공할 필요가 없습니다.

- RADIUS 서버가 사용자의 MAC 주소를 검증할 수 없으면 인증이 실패합니다.

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **서비스 > RADIUS서버** 로 이동합니다.
3. RADIUS서버 화면에서 **RADIUS Authentication Server > MAC 인증** 옵션을 찾습니다.
   - **MAC 인증** 옵션 **On** 설정
   - **노드그룹** 옵션에서 MAC인증을 적용할 노드그룹을 선택합니다.
4. **수정** 버튼을 클릭합니다.

7.1.4 Single Sign-On(SSO)

Single Sign-On(SSO)은 하나의 인증매체를 이용하여 다른 여러 시스템의 인증을 대체하는 인증방식입니다.

Genian ZTNA가 타사의 인증을 활용한 SSO 구현가이드

AD Dommain Login

Genian ZTNA는 Windows 또는 macOS 에이전트를 이용하여 Active Directory 대체인증 하는데 사용할 수 있습니다.

AD를 통한 대체인증을 사용하려면 먼저 노드정책을 활성화해야 합니다.

1. 상단 항목에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
3. 활성화를 원하는 원하는 정책 이름을 클릭합니다.

인증정책 에서 다음을 수행합니다.

1. **인증대체정보** 에서 **Active Directory** 를 선택합니다.
2. **AD 허용 도메인명** 을 입력합니다.
3. **수정** 버튼을 클릭합니다.

Agent 기반 AD 대체인증 설정

- 에이전트를 설치합니다. (에이전트 설치)
- 에이전트 실행 / 설치 계정은 도메인관리자 계정이나 설치권한을 가진 계정으로 설정해야합니다. 에이전트가 로컬 계정에 설치되어 있으면 SSO가 작동하지 않습니다.

Agentless AD 대체인증 설정

- 아래 설정 추가 시 Agent를 설치하지 않은 노드에서도 인증대체 기능을 사용할 수 있습니다.
- 도메인 컨트롤러에 대한 WMI 쿼리를 통해 에이전트없는 SSO를 수행합니다 (도메인에 인증된 모든 노드 지원).
- 네트워크 센서는 AD서버에 발생한 도메인 로그인 이벤트 로그와 네트워크 센서가 Netbios를 통해 탐지한 단말의 호스트/도메인명을 비교하여 인증 대체를 수행합니다. 따라서 네트워크센서가 단말의 netbios, remote WMI 등 과의 통신이 원활한 상태여야합니다.

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자인증 > 인증연동 > AD인증대체** 로 이동합니다.

아래의 항목을 입력하여 **AD인증대체** 설정을 완료합니다.

1. **서버 접속 센서** : AD 서버에 접속할 센서를 선택합니다. (선택안함 설성시 정책서버에서 접속합니다.)
2. **서버주소** : AD 인증대체를 위한 서버시스템의 주소/도메인을 입력합니다. 노드가 도메인에 가입된 경우 노드의 사용자정보를 인증정보로 대체합니다.
3. **User ID** : 이벤트 로그 모니터링을 위한 AD 서버의 사용자 ID를 입력합니다.
4. **Password** : 이벤트 로그 모니터링을 위한 AD 서버의 사용자 Password를 입력합니다.
5. **Secondary AD 사용** : Secondary AD 사용여부를 선택합니다.
6. **수정** 버튼을 클릭합니다.

AD 환경설정

1. 입력한 AD 사용자 계정이 다음 그룹에 포함되는지 확인합니다.
   - Distributed COM Users
   - Event Log Readers
   - Domain Users
   - AD configuration
2. 명령 프롬프트에서 *wmimgmt.msc* 를 실행합니다.
3. WMI 제어 속성 보안탭에서 CIMV2 폴더를 선택합니다.
4. 보안을 클릭하고 추가를 누른 다음 ZTNA에 설정한 사용자 계정을 선택합니다.
5. 계정사용, 원격으로부터 사용가능을 허용으로 설정합니다.
6. 확인 버튼을 클릭하여 설정을 완료합니다.

단말의 AD도메인 가입여부 확인방법

1. **AD서버에서 확인하는 방법**
    - AD 서버에서 **제어판 > 관리도구 > Active Directory 사용자 및 컴퓨터** 를 실행합니다.
    - **도메인 > Computers** 를 클릭하여 우측의 가입된 컴퓨터 목록을 확인합니다.
2. **클라이언트 단말에서 확인하는 방법**
    - 클라이언트 단말의 CMD에서 `ping [AD 도메인]` 이 정상적인 IP로 해석되는지 확인합니다.

Genian ZTNA는 WMI쿼리를 통해 에이전트 없는 단말의 SSO를 수행합니다. 다음링크를 참고하여 WMI 구성을 설정해주시기 바랍니다.

원격 WMI 정보수집을 위한 환경 설정

WMI(Windows Management Instrumentation)는 웹 기반 엔터프라이즈 관리를 위한 Microsoft 도구입니다. WMI는 단말을 검사하고 단말에 정보를 수집하는데 사용할 수 있습니다.

기본 요구 사항

Windows 단말에서 WMI를 사용하려면 다음 설정이 필요합니다.

- 포트 135/TCP 를 사용할 수 있어야합니다.
- **다음 서비스가 단말에서 실행 중이어야합니다.**
    - Server
    - Windows Management Instrumentation(WMI)
- 방화벽에서 WMI 통신을 허용해야합니다.

추가 구성 및 문제 해결 옵션

원격 리모트 WMI 정보수집을 위해서는 다음 구성 설정을 확인 하시기바랍니다.

1. 다음과 같이 Active Directory 설정을 구성합니다. 그룹 정책을 사용하여 단말에 설정을 할 수 있습니다.

- Member of Domain Administrators or Local Administrators group
- **도메인 그룹의 구성원:**
    - Performance Log Users
    - Distributed COM Users
- **그룹의 구성원의 권한:**
    - Act as part of Operating System
    - Log on as a batch job
    - Log on as a service
    - Replace a process

2. dcomcnfg 유틸리티를 실행한다음 단말 권한을 설정합니다.

- Access Permissions: Enable all
- Launch and Activation Permissions: Enable all

3. wmimgmt.msc 유틸리티를 실행하고 WMI 도메인에 보안 설정을합니다. 도메인에 다음 위치에 대한 사용 권한을 할당합니다.

- root/CIMv2
- root/Default
- root/SecurityCenter
- root/SecurityCenter2

각 도메인에 다음 사용 권한을 할당합니다.

- Execute Methods
- Enable Account
- Remote Enable
- Read Security
- *FAQ* 의 Agentless 관련 항목을 참고해주시기 바랍니다.

RADIUS Accounting

RADIUS를 통한 사용자 인증이 네트워크에 적용되면 AP(Access Point)와 같은 RADIUS 클라이언트가 제공한 RADIUS ACCOUNT 패킷을 통해 사용자 인증을 자동으로 수행 할 수 있습니다. 정책서버는 외부 RADIUS ACCOUNT 패킷을 수신하여 감사 기록으로 저장하고 이를 사용자인증 정보로 대체사용합니다.

NAS(Network Access Server)가 사용자에게 네트워크 엑세스 권한을 부여하면 계정 시작(Acct-Status-Type 속성의 값이 "start" 인 RADIUS Account Request 패킷)이 NAS에서 RADIUS 서버로 전송되어 사용자의 네트워크 엑세스 시작을 알립니다.

"start" 레코드는 일반적으로 사용자의 식별, 네트워크 주소, 접속위치 및 고유한 세션 식별자를 포함합니다.

주기적으로 임시 업데이트 레코드("Acct-Status-Type 속성의 값이 "interim-update" 인 RADIUS Account Request 패킷)는 NAS가 RADIUS 서버로 전송하여 Active session의 상태를 업데이트합니다.

"Interim" 레코드는 일반적으로 현재 세션이 유지되는 시간과 현재 데이터 사용에 대한 정보를 전달합니다.

마지막으로 사용자의 네트워크 엑세스가 종료되면 NAS는 RADIUS 서버에 최종 사용량에 대한 정보, 패킷 전송량, 데이터 전송량, 연결 해제 사유, 기타정보를 제공하는 Accounting Stop 레코드를 보냅니다.

일반적으로 클라이언트는 Accounting-Response acknowledgement를 받을 때까지 Accounting-Request 패킷을 주기적으로 전송합니다.

Note: 대체인증이란 ZTNA가 아닌 다른 인증서버에서 인증한 결과를 가지고 ZTNA에 인증한 것으로 대체하는 인증방법입니다.

RADIUS 대체인증 설정

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **서비스 > RADIUS서버** 로 이동합니다.

아래를 통해 **RADIUS Accounting Server** 설정:

1. **포트번호** : RADIUS Accounting 수신포트를 설정합니다.(기본값: *1813*)
2. **인증대체** : RADIUS Accounting 수신시 인증 대체 여부를 설정합니다. (*On/Off*)

3. **수정** 버튼을 클릭합니다.

ESCARE PowerPack

본 가이드는 ESCARE PowerPack과 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다. (ESCARE PowerPack은 Symantec DLP 혹은 Symantec SEP 솔루션과 전용으로 연동되는 반출승인 및 매체사용승인 솔루션입니다.)

개요

Genian NAC와 PowerPack 제품 간 연동 전, 사용자는 제품별로 각각 사용자인증을 수행하는 불편함이 있지만, **연동 후 두 제품간의 SSO가 구현되어 사용자는 PowerPack의 사용자인증 수행 시 Genian NAC에는 사용자인증이 자동으로 처리됩니다.**

Genian NAC 에이전트에서 PowerPack의 인증을 대체하여 적용하도록 구성되어, 사용자의 인증을 위해 Genian NAC 에이전트가 PowerPack 에이전트를 경유하여, PowerPack 서버의 사용자 인증여부를 확인하며, 정상적인 인증상태에서 네트워크를 활용할 수 있도록 합니다.

이 과정을 통하여, 사용자에게는 단 한번의 로그인 과정으로 두 제품의 로그인 과정을 수행하는 편의성을 제공합니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V4.0	2019.06 이후 Release 버전
Genian NAC (에이전트)	V4.0	2019.06 이후 Release 버전
PowerPack		2019.06 이후 Release 버전

연동의 목적

Genian NAC와 ESCARE PowerPack 연동은 다음의 효과를 제공합니다.

SSO 환경 제공

- 사용자는 PowerPack에 먼저 사용자인증을 진행하고, Genian NAC 에이전트 플러그인 연동을 통해 Genian NAC 사용자인증이 자동으로 진행됩니다. Genian NAC는 PowerPack의 사용자인증 여부를 통해 Genian NAC에 사용자인증이 대체되어 SSO 환경이 구성됩니다.

PowerPack 미인증 사용자에게 네트워크 차단 사유 및 안내페이지 자동 연결

- Genian NAC는 PowerPack 미인증 사용자에게 네트워크 차단 사유를 안내하여 정상적인 네트워크 사용을 위한 조치 방법에 대한 안내페이지를 제공합니다.

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 준비

Genian NAC는 PowerPack와 SSO 구현을 위해 사용자인증 연동 구현에 별도 제작된 Genian NAC 에이전트용 플러그인이 활용되며, 플러그인 정보는 다음과 같습니다.

Genian NAC 에이전트 플러그인 파일명	비고
NAC-C_PowerPackSSO-R-89874-1.0.8.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V4.0 (2019.06 이후 Release 버전)

인증 정보를 호출하는 PowerPack 의 라이브러리 경로 및 파일명 확인

Genian NAC는 PowerPack과 연동 시 PowerPack의 인증 정보를 호출하는 라이브러리를 활용하여 사용자인증을 대체합니다. PowerPack의 라이브러리가 저장된 기본 경로는 **C:\ProgramData\scEscpp** 이고, 파일명은 **scEscppInfo.dll** 입니다.

PowerPack의 라이브러리 경로와 파일명은 Genian NAC의 별도 제작된 에이전트 플러그인에 기본으로 설정되어 있지만, 고객사에서 예외적으로 변경된 경우 경로와 파일명을 확인 후 연동을 위한 *Genian NAC 설정 > Step 2: 에이전트 플러그인 설정 > 3번* 항목에서 설정 값을 변경한 후에 진행하시기 바랍니다.

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 PowerPack과 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 업로드

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 에이전트 > 플러그인** 메뉴로 이동
2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **NAC-C_PowerPackSSO-R-89874-1.0.8.gpf** 플러그인 선택
3) **업로드** 버튼 클릭

Step 2: 에이전트 플러그인 설정

1) Genian NAC Web콘솔에서 **정책 > 노드정책 > 노드액션** 메뉴로 이동
2) **PowerPack 대체 인증** 플러그인 클릭
3) **액션 수행설정** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
라이브러리 경로	셀렉트박스 : `%SystemDrive%` 선택 / 입력 값 : *\ProgramData\scEscpp\scEscppInfo.dll*	PowerPack의 라이브러리 경로와 라이브러리 파일명 설정
변경된 사용자 정보 적용	`On`, `Off` 중 선택	`On` 옵션은 로그인 후, Genian NAC가 지속적으로 PowerPack에 인증정보와 인증여부를 확인하여, PowerPack에서 인증정보가 변경된 경우 변경된 인증정보를 반영하여 Genian NAC의 인증상태를 유지하고, 로그아웃된 경우 Genian NAC도 로그아웃 처리 함
		`Off` 옵션은 최초 SSO 로그인 이후, 추가적으로 PowerPack와 인증 정보를 공유하지 않고 Genian NAC의 인증갱신 주기를 따름

Step 3: 연동기능 적용을 위한 노드정책 설정

다음의 과정을 통해서 Genian NAC의 에이전트 플러그인을 이용하여, 사용자 PC와 서버간 인증을 위한 정상적인 통신 확인과 사용자인증 여부를 확인한 후, 네트워크 접속을 허가할 수 있도록 정책을 생성합니다.

1) Genian NAC Web콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 연동을 적용할 **노드그룹** (ex. 모든노드) 이 포함된 **노드정책** 클릭 (특정그룹에만 적용시, 별도의 노드그룹을 생성하여 활용)

3) **세부설정 > 인증정책 > 인증대체정보** 항목으로 이동 후 셀렉트박스에서 **연동API** 선택

4) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭

5) **PowerPack 대체 인증** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭

6) 하단부 **수정** 버튼 클릭

7) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

라톤테크 Rathon-SSO

본 가이드는 통합인증 보안플랫폼(SSO)인 라톤테크의 Rathon-SSO와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

Genian NAC와 Rathon-SSO 제품 간 연동 전, 사용자는 제품별로 각각 사용자인증을 수행하는 불편함이 있지만, **연동 후 두 제품간의 SSO가 구현되어 사용자는 Rathon-SSO의 사용자인증 수행 시 Genian NAC에는 사용자 인증이 자동으로 처리됩니다.**

Genian NAC 에이전트에서 Rathon-SSO의 인증을 대체하여 적용하도록 구성되어, 사용자의 인증을 위해 Genian NAC 에이전트가 Rathon-SSO 에이전트를 경유하여, Rathon-SSO 서버의 사용자 인증여부를 확인하며, 정상적인 인증상태에서 네트워크를 활용할 수 있도록 합니다.

이 과정을 통하여, 사용자에게는 단 한번의 로그인 과정으로 두 제품의 로그인 과정을 수행하는 편의성을 제공합니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2019.03 이후 Release 버전
Genian NAC (에이전트)	V5.0 이상	2019.10 이후 Release 버전
Rathon-SSO	V3.2 이상	2019.10 이후 Release 버전

연동의 목적

Genian NAC와 라톤테크 Rathon-SSO 연동은 다음의 효과를 제공합니다.

SSO 환경 제공

- 사용자는 Rathon-SSO에 먼저 사용자인증을 진행하고, Genian NAC 에이전트 플러그인 연동을 통해 Genian NAC 사용자인증이 자동으로 진행됩니다. Genian NAC는 Rathon-SSO의 사용자인증 여부를 통해 Genian NAC에 사용자인증이 대체되어 SSO 환경이 구성됩니다.

Rathon-SSO 미인증 사용자에게 네트워크 차단 사유 및 안내페이지 자동 연결

- Genian NAC는 Rathon-SSO 미인증 사용자에게 네트워크 차단 사유를 안내하여 정상적인 네트워크 사용을 위한 조치 방법에 대한 안내페이지를 제공합니다.

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 준비

Genian NAC는 Rathon-SSO와 SSO 구현을 위해 사용자인증 연동 구현에 별도 제작된 Genian NAC 에이전트용 플러그인이 활용되며, 플러그인 정보는 다음과 같습니다.

Genian NAC 에이전트 플러그인 파일명	비고
NAC-C_RathonSSO-R-89872-1.1.8.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상 (2019.10 이후 Release 버전)

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 Rathon-SSO와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 업로드

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인** 메뉴로 이동
2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **NAC-C_RathonSSO-R-89872-1.1.8.gpf** 플러그인 선택
3) **업로드** 버튼 클릭

Step 2: 에이전트 플러그인 설정

1) Genian NAC Web콘솔에서 **정책 > 노드정책 > 노드액션** 메뉴로 이동
2) **Rathon 대체 인증** 플러그인 클릭하여 확인

Note:

- Rathon 대체 인증 플러그인은 별도의 설정이 필요 없는 플러그인 입니다.
- Rathon-SSO의 연동 Library 경로나 파일명은 상호 협의된 기본값이 적용되어 있지만, 만일 변경된 경우 Rathon-SSO 관리자와 Genian NAC 관리자에게 문의하시기 바랍니다.

Step 3: 연동기능 적용을 위한 노드정책 설정

다음의 과정을 통해서 Genian NAC의 에이전트 플러그인을 이용하여, 사용자 PC와 서버간 인증을 위한 정상적인 통신 확인과 사용자인증 여부를 확인한 후, 네트워크 접속을 허가할 수 있도록 정책을 생성합니다.

1) Genian NAC Web콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 연동을 적용할 **노드그룹** (ex. 모든노드)이 포함된 **노드정책** 클릭 (특정그룹에만 적용시, 별도의 노드그룹을 생성하여 활용)
3) **세부설정 > 인증정책 > 인증대체정보** 항목으로 이동 후 셀렉트박스에서 **연동API** 선택
4) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭
5) **Rathon 대체 인증** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭
6) 하단부 **수정** 버튼 클릭
7) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

바이오닉스진 SafePC

본 가이드는 DLP 시스템인 바이오닉스진의 SafePC Enterprise (이하, **SafePC** 로 표기함)와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

Genian NAC와 SafePC 제품 간 연동 전, 사용자는 제품별로 각각 사용자인증을 수행하는 불편함이 있지만, **연동 후 두 제품간의 SSO가 구현되어 사용자는 SafePC의 사용자인증 수행 시 Genian NAC에는 사용자인증이 자동으로 처리됩니다.**

Genian NAC 에이전트 플러그인은 SafePC의 인증 정보를 호출하는 라이브러리를 활용하도록 구성되며, SafePC의 에이전트가 설치된 단말에서 사용자인증 시 라이브러리를 통해 SafePC 서버에서 인증 정보를 읽어와 Genian NAC에 인증이 대체되도록 적용됩니다.

이 과정을 통하여, 사용자의 인증 정보를 사용자의 PC에 보관하지 않은 상태에서 인증을 수행하여 사용자 계정의 안전을 보장하면서 사용자에게는 단 한번의 로그인 과정으로 두 제품의 로그인 과정을 수행하는 편의성을 제공합니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2019.03 이후 Release 버전
Genian NAC (에이전트)	V5.0 이상	2020.06 이후 Release 버전
SafePC Enterprise	V5.1 이상	2020.06 이후 Release 버전

연동의 목적

Genian NAC와 바이오닉스진 SafePC 연동은 다음의 효과를 제공합니다.

SSO 환경 제공

- 사용자는 SafePC에 먼저 사용자인증을 진행하고, Genian NAC 에이전트 플러그인 연동을 통해 Genian NAC 사용자인증이 자동으로 진행됩니다. Genian NAC는 SafePC 에이전트의 사용자인증 여부를 통해 Genian NAC에 사용자인증이 대체되어 SSO 환경이 구성됩니다.

SafePC 미인증 사용자에게 네트워크 차단 사유 및 안내페이지 자동 연결

- Genian NAC는 SafePC 미인증 사용자에게 네트워크 차단 사유를 안내하여 정상적인 네트워크 사용을 위한 조치 방법에 대한 안내페이지를 제공합니다.

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 준비

Genian NAC는 SafePC와 SSO 구현을 위해 사용자인증 연동 구현에 별도 제작된 Genian NAC 에이전트용 플러그인이 활용되며, 플러그인 정보는 다음과 같습니다.

Genian NAC 에이전트 플러그인 파일명	비고
NAC-C_SafePCSSO-R-89872-1.1.8.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상 (2020.06 이후 Release 버전)

인증 정보를 호출하는 SafePC의 라이브러리 경로 및 파일명 확인

Genian NAC는 SafePC와 연동 시 SafePC의 인증 정보를 호출하는 라이브러리를 활용하여 사용자인증을

대체합니다. SafePC의 라이브러리가 저장된 기본 경로는 **C:\Windows\Nics** 이고, 파일명은 **SUser.dll** 입니다.

SafePC의 라이브러리 경로와 파일명은 Genian NAC의 별도 제작된 에이전트 플러그인에 기본으로 설정되어 있지만, 고객사에서 예외적으로 변경된 경우 경로와 파일명을 확인 후 연동을 위한 *Genian NAC* 설정 > *Step 2:* 에이전트 플러그인 설정 > *3*번 항목에서 설정 값을 변경한 후에 진행하시기 바랍니다.

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 SafePC와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 업로드

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인** 메뉴로 이동
2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **NAC-C_SafePCSSO-R-89872-1.1.8.gpf** 플러그인 선택
3) **업로드** 버튼 클릭

Step 2: 에이전트 플러그인 설정

1) Genian NAC Web콘솔에서 **정책 > 노드정책 > 노드액션** 메뉴로 이동
2) **SafePC 대체 인증** 플러그인 클릭
3) **액션 수행설정** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
라이브러리 경로	셀렉트박스: `%WinDir%` 선택 / 입력 값 : *\Nics\SUser.dll*	SafePC의 라이브러리 경로와 라이브러리 파일명 설정
인증정보 소스	파일 , 레지스트리 중 선택	인증정보를 추출하는 대상 선택
변경된 사용자정보 적용	`On` , `Off` 중 선택	`On` 옵션은 로그인 후, Genian NAC가 지속적으로 SafePC에 인증정보와 인증여부를 확인하여, SafePC에서 인증정보가 변경된 경우 변경된 인증정보를 반영하여 Genian NAC의 인증상태를 유지하고, 로그아웃된 경우 Genian NAC도 로그아웃 처리 함
		`Off` 옵션은 최초 SSO 로그인 이후, 추가적으로 SafePC와 인증 정보를 공유하지 않고 Genian NAC의 인증갱신 주기를 따름

Step 3: 연동기능 적용을 위한 노드정책 설정

다음의 과정을 통해서 Genian NAC의 에이전트 플러그인을 이용하여, 사용자 PC와 서버간 인증을 위한 정상적인 통신 확인과 사용자인증 여부를 확인한 후, 네트워크 접속을 허가할 수 있도록 정책을 생성합니다.

1) Genian NAC Web콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 연동을 적용할 **노드그룹** (ex. 모든노드) 이 포함된 **노드정책** 클릭 (특정그룹에만 적용시, 별도의 노드그룹을 생성하여 활용)
3) **세부설정 > 인증정책 > 인증대체정보** 항목으로 이동 후 셀렉트박스에서 **연동API** 선택

4) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭

5) **SafePC 대체 인증** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭

6) 하단부 **수정** 버튼 클릭

7) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

이니텍 INISAFE Nexess

본 가이드는 통합인증 보안플랫폼(SSO)인 이니텍의 INISAFE Nexess와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

Genian NAC와 INISAFE Nexess 제품 간 연동 전, 사용자는 제품별로 각각 사용자인증을 수행하는 불편함이 있지만, **연동 후 두 제품간의 SSO가 구현되어 사용자는 INISAFE Nexess의 사용자인증 수행 시 Genian NAC에는 사용자인증이 자동으로 처리됩니다.**

Genian NAC 에이전트에서 INISAFE Nexess의 인증을 대체하여 적용하도록 구성되어, 사용자의 인증을 위해 Genian NAC 에이전트가 INISAFE Nexess 에이전트를 경유하여, INISAFE Nexess 서버의 사용자 인증여부를 확인하며, 정상적인 인증상태에서 네트워크를 활용할 수 있도록 합니다.

이 과정을 통하여, 사용자에게는 단 한번의 로그인 과정으로 두 제품의 로그인 과정을 수행하는 편의성을 제공합니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2019.03 이후 Release 버전
Genian NAC (에이전트)	V5.0 이상	2019.06 이후 Release 버전
INISAFE Nexess	V4.0 이상	2019.06 이후 Release 버전

연동의 목적

Genian NAC와 이니텍 INISAFE Nexess 연동은 다음의 효과를 제공합니다.

SSO 환경 제공

- 사용자는 INISAFE Nexess에 먼저 사용자인증을 진행하고, Genian NAC 에이전트 플러그인 연동을 통해 Genian NAC 사용자인증이 자동으로 진행됩니다. Genian NAC는 INISAFE Nexess의 사용자인증 여부를 통해 Genian NAC에 사용자인증이 대체되어 SSO 환경이 구성됩니다.

INISAFE Nexess 미인증 사용자에게 네트워크 차단 사유 및 안내페이지 자동 연결

- Genian NAC는 INISAFE Nexess 미인증 사용자에게 네트워크 차단 사유를 안내하여 정상적인 네트워크 사용을 위한 조치 방법에 대한 안내페이지를 제공합니다.

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 준비

Genian NAC는 INISAFE Nexess와 SSO 구현을 위해 사용자인증 연동 구현에 별도 제작된 Genian NAC 에이전트용 플러그인이 활용되며, 플러그인 정보는 다음과 같습니다.

Genian NAC 에이전트 플러그인 파일명	비고
NAC-C_NexessSSO-R-89872-1.1.8.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상 (2019.06 이후 Release 버전)

INISAFE Nexess의 인증 정보 API 호출을 위한 License Key 발급 및 연동 Library 확인

아래의 두개 항목은 연동을 위한 *Genian NAC 설정 > Step 2: 에이전트 플러그인 설정 > 3번* 항목 설정 시 활용됩니다.

1. INISAFE Nexess의 SSO 연동 Library 사용을 위한 License Key

- Genian NAC와 사용자인증 연동 시 INISAFE Nexess에 인증 정보 API 호출을 위해 INISAFE Nexess에서 별도로 제공되는 라이선스 키를 발급 받은 후 진행하시기 바랍니다.

2. 각 기관별 사용되는 연동 Library 확인

- INISAFE Nexess는 연동 시 사용되는 Library를 기본으로 제공하여 Genian NAC에 별도로 업로드를 하지 않아도 되지만, 각 기관별로 환경설정 혹은 세부설정이 다른 경우에는 INISAFE Nexess에서 별도로 제공하는 연동 DLL파일을 제공받은 후 진행하시기 바랍니다. (**NCApi.dll** 와 같은 형태로 배포)

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 INISAFE Nexess와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 업로드

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인** 메뉴로 이동

2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **NAC-C_NexessSSO-R-89872-1.1.8.gpf** 플러그인 선택

3) **업로드** 버튼 클릭

Step 2: 에이전트 플러그인 설정

1) Genian NAC Web콘솔에서 **정책 > 노드정책 > 노드액션** 메뉴로 이동

2) **Nexess 대체 인증** 플러그인 클릭

3) **액션 수행설정** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
License Key	*TEST-LICENSEKEY*	인증연동 Library 사용을 위해 각 기관마다 제공되는 키 입력
연동 DLL 업로드	**업로드** 버튼 클릭 후 `NCApi.dll` 파일 업로드	.dll 확장자 파일만 업로드 가능 (별도의 dll 사용시에만 업로드)
연동 범위	로그인, 로그인/로그아웃 중 선택	로그인/로그아웃 옵션은 로그인 후, Genian NAC가 지속적으로 Nexess로 인증여부를 확인하여, Nexess에서 로그아웃된 경우 로그아웃 처리함
		로그인 옵션은 최초 SSO 로그인 이후, 추가적으로 Nexess와 로그인 정보를 공유하지 않고 Genian NAC의 인증갱신 주기를 따름

Step 3: 연동기능 적용을 위한 노드정책 설정

다음의 과정을 통해서 Genian NAC의 에이전트 플러그인을 이용하여, 사용자 PC와 서버간 인증을 위한 정상적인 통신 확인과 사용자인증 여부를 확인한 후, 네트워크 접속을 허가할 수 있도록 정책을 생성합니다.

1) Genian NAC Web콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 연동을 적용할 **노드그룹** (ex. 모든노드)이 포함된 **노드정책** 클릭 (특정그룹에만 적용시, 별도의 노드그룹을 생성하여 활용)
3) **세부설정 > 인증정책 > 인증대체정보** 항목으로 이동 후 셀렉트박스에서 **연동API** 선택
4) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭
5) **Nexess 대체 인증** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭
6) 하단부 **수정** 버튼 클릭
7) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

유비앤티스랩 PassNI SSO

본 가이드는 통합인증 보안플랫폼(SSO)인 유비앤티스랩 PassNI SSO와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

Pass-Ni는 Genian NAC와 연동 구성시, 일반적인 동작프로세스는 Pass-Ni 로그인 > Genian NAC 로그인의 프로세스로 구성됩니다.

Genian NAC와 Pass-Ni 제품 간 연동 전, 사용자는 Pass-Ni로그인 이후 내부 네트워크 접근 시, Genian NAC로 별도의 로그인 과정이 필요하였지만, 연동 구성시 Pass-Ni로그인 만으로 Genian NAC까지 자동으로 로그인 되도록 구성됩니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2019.03 이후 Release 버전
Genian NAC (에이전트)	V5.0.17 이상	2019.03 이후 Release 버전
Pass-NI	4.0 이상	2019.03 이후 Release 버전

연동의 목적

Genian NAC와 유비앤티스랩의 Pass-Ni의 연동은 다음의 효과를 제공합니다.

SSO 환경 제공

- Genian NAC 에이전트가 Pass-Ni의 인증 정보를 활용하는 형태로 구성되어, 사용자 인증 여부를 Pass-Ni 서버에 확인하여 정상 인증된 사용자에 대해서 Genian NAC의 추가적인 인증없이 네트워크를 활용하도록 구성합니다.

Pass-Ni 미인증 사용자에게 네트워크 차단 사유 및 안내페이지 자동 연결

- Genian NAC는 Pass-Ni 미인증 사용자에게 네트워크 차단 사유를 안내하여 정상적인 네트워크 사용을 위한 조치 방법에 대한 안내페이지를 제공합니다. (새올시스템등과 추가 연동시, 안내페이지의 형태가 다를 수 있습니다)

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 준비

Genian NAC 는 Pass-Ni 와 SSO 구현을 위해 사용자인증 연동 구현에 별도 제작된 Genian NAC 에이전트용 플러그인이 활용되며, 플러그인 정보는 다음과 같습니다

Genian NAC 에이전트 플러그인 파일명	비고
NAC-C_PassNiSSO-R-89967-1.1.8.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상 (2020.08 Release 이후 버전)

Pass-Ni SSO 의 사용자용 API 호출도구 및 사용을 위한 License Key 발급

1. Pass-Ni 용 사용자 단말용 사용자 정보의 API 호출도구 (**SSO-CS-API-getUserInfo.zip** 와 같은 형태로 배포)
2. Pass-Ni SSO 연동 Library 사용을 위한 License Key (각 기관마다 Pass-Ni 가 별도로 제공하는 라이선스 키로 *3130312XXXXE352XXXX3* 와 같은 형식입니다.)

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC 의 설정 부분은 Pass-Ni 와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 업로드

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인** 메뉴로 이동
2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **NAC-C_PassNiSSO-R-89967-1.1.8.gpf** 플러그인 선택
3) **업로드** 버튼 클릭

Step 2: 에이전트 플러그인 설정

1) Genian NAC Web콘솔에서 **정책 > 노드정책 > 노드액션** 메뉴로 이동
2) **PassNi 대체 인증** 플러그인 클릭
3) **액션 수행설정** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
License Key	*3130312XXXXE352XXXX3* (입력값 예)	인증연동 Library 사용을 위해 각 기관마다 제공되는 키입력
연동범위	로그인, 로그인/로그아웃 중 선택	아래 **로그인/로그아웃** 옵션설명 참조

Note: 로그인/로그아웃 옵션

1) 로그인/로그아웃 옵션은 로그인 후, Genian NAC가 지속적으로 Pass-Ni로 인증여부를 확인하여, Pass-Ni 에서 로그아웃된 경우, 로그아웃 처리 함
2) 로그인 옵션은 최초 SSO 로그인 이후, 추가적으로 Pass-Ni 와 로그인 정보를 공유하지 않고 Genian NAC 의 인증갱신 주기를 따름

Step 3: 연동기능 적용을 위한 노드정책 설정

다음의 과정을 통하여, Genian NAC 의 에이전트 플러그인을 이용하여, 사용자 PC 와 서버간 인증을 위한 정상적인 통신확인과 사용자인증의 여부를 확인한 후, 네트워크 접속을 허가할 수 있도록 정책을 생성합니다.

1) Genian NAC Web 콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 연동을 적용할 **노드그룹** 이 포함된 **노드정책** 클릭 (ex. 노드그룹: 모든노드(특정그룹에만 적용시, 별도로 노드그룹을 생성하여 활용))
3) **세부설정 > 인증정책 > 인증대체정보** 항목으로 이동 후, 셀렉트박스에서 **연동 API** 선택
4) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭
5) **PassNi 대체 인증** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭
6) 하단 부 **수정** 버튼 클릭
7) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

정부OTP인증센터 GOTP

본 가이드는 모바일 OTP 시스템인 정부OTP인증센터의 GOTP와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

본 연동은 **Genian NAC 일반 사용자인증 진행 시 기존의 ID/PW 방식을 대체하여 GOTP(OTP) 인증으로 변경하기 위한 연동입니다.**

연동의 구성은 Genian NAC가 GOTP 전용 연동도구(정책서버 플러그인)를 제공하며, 사용자가 Genian NAC에 사용자인증 시도 시, GOTP 서버에서 사용자의 모바일 단말로 OTP(One Time Password)를 발행하게 하여, OTP 정보를 입력하는 방식의 인증 구성입니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2019.03 이후 Release 버전
GOTP		2018.03 이후 Release 버전

연동의 목적

Genian NAC와 GOTP 연동은 다음의 효과를 제공합니다.

사용자인증 시 로그인 보안을 위한 OTP 인증 환경 제공

- GOTP와 Genian NAC의 정책서버 플러그인 연동을 통해 사용자는 Genian NAC 사용자인증 진행 시, 기존의 ID/PW 방식 대신 GOTP(OTP)로 인증합니다.
- GOTP 연동으로 인해, 기존의 ID/PW 방식 대비 패스워드 도난, 계정 가로채기 등으로 인한 위협에 대해서 상대적으로 안전한 로그인 환경을 제공합니다.

미인증 사용자에게 네트워크 차단 사유 및 안내페이지 자동 연결

- GOTP를 Genian NAC와 연동하여 구성하므로 GOTP 인증과정을 거치지 않은 사용자 단말의 네트워크 접근 시 차단하며, 차단에 대한 사유 및 해결에 대한 안내페이지를 제공하여 관리자의 업무부담을 줄여줍니다.

사전준비 사항

GOTP 관련 사전준비

1. **GOTP 연계 신청 및 GPKI API(라이선스)와 GOTP API(API Key) 준비**
   API 호출 시 사용되는 GPKI API(라이선스)는 각 기관마다 다르기 때문에 기관 담당자는 GOTP 인증센터로 직접 GOTP 연계 신청 시 발급되는 **GPKI API(라이선스)** 와 **GOTP API(API Key)** 파일을 준비 한 후 연동 진행 시 지니언스 담당 엔지니어 혹은 기술지원팀에 제출합니다

2. **연동을 위한 기관 전용 Genian NAC 정책서버 플러그인 제작 요청**
   기관 담당자는 GPKI API(라이선스)와 GOTP API(API Key) 확인 후 **정책서버 플러그인 제작 요청** 을 해주시기 바랍니다.

   Note: 본 작업은 최초 1회에 한하며, 지니언스 담당 엔지니어 혹은 기술지원팀에 요청하시면 됩니다.

   ---

3. **GOTP 인증 서버로 API 호출을 위한 네트워크 접근허용 신청**
   Genian NAC에서 정부OTP 인증 서버로 접근이 가능하도록 하기 위해 기관 담당자는 국가정보자원관리원으로 네트워크 접근허가 신청을 하시기 바랍니다.

   Note:

   - 행정망 : www.gotp.go.kr, 8080 / 인터넷망 : www.gotp.go.kr, 80
   - 네트워크 접근허용 신청문의 : 국가정보자원관리원 서비스데스크(1577-0577)

   ---

4. **모바일 단말에 GOTP App 설치**
   일반 사용자는 Genian NAC 사용자인증 진행 시, 인증코드 발급을 위한 GOTP App을 모바일 단말에 설치하시기 바랍니다.

Genian NAC 사전준비

1. **연동을 위한 Genian NAC 정책서버 플러그인 준비**
   Genian NAC는 각 기관별로 지니언스가 제공하는 전용 Genian NAC 정책서버 플러그인(특수 목적을 위해 별도 제작된 Package)이 활용되며, 일반 정보는 다음과 같습니다.

Genian NAC 정책서버 플러그인 파일명	비고
GWP100006-5.0.gwp	별도 제작 시 라이선스와 API Key가 달라도 GWP100006-5.0.gwp 정책서버 플러그인 명칭은 동일하기 때문에 기관 담당자는 확인 후 업로드 하시기 바랍니다.

2. GOTP 기능 수행을 위한 라이브러리 준비

Genian NAC와 GOTP 연동 기능의 수행을 위해 Genian NAC 정책서버에 추가적인 라이브러리가 필요합니다. 정책서버 플러그인 제작 시 라이브러리 파일이 같이 제공, 업데이트 됩니다.

(라이브러리 압축 파일명: **lib.tar.gz**)

3. 인증코드 발급 시 활용되는 매체코드와 일련번호 간 정합성 보장을 위한 사용자 정보 최신화, 동기화

Genian NAC와 연동 후 GOTP 인증코드 발급 시 매체코드와 GOTP 일련번호가 활용됩니다. 두 정보는 Genian NAC에서 사용자 정보동기화를 통해 Custom 필드에 저장해야 합니다.

- CUSTOM08 필드: 매체코드 (H/W, Mobile, PC, 스마트폰 등 매체에 대한 코드 저장)
- CUSTOM09 필드: 기기일련번호 (각 기관별 정부OTP 매체의 고유한 일련번호 저장)

사용자 정보동기화 방법은 외부 사용자 정보 동기화 를 참고하시기 바랍니다.

Note:

- 기관 담당자는 해당되는 두 정보에 대한 제공 방식과 정보동기화를 위해 지니언스 담당 엔지니어 혹은 기술지원팀에 문의 후 협의하여 정보동기화를 진행하시기 바랍니다.

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 GOTP와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 정책서버 플러그인 업로드

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 정책서버 플러그인** 메뉴로 이동
2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **GWP100006-5.0.gwp** 플러그인 선택
3) **업로드** 버튼 클릭
4) 목록으로 이동하여 **GOTP 인증 모듈 > 재기동시 설치완료예정** 버튼 클릭 후 팝업창에서 **확인** 버튼 클릭 (관리콘솔 웹 어플리케이션 재기동을 수행해야 최종 설치가 완료됩니다.)

Step 2: 정책서버 플러그인 설정

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 정책서버 플러그인** 메뉴로 이동
2) **GOTP 인증 모듈** 플러그인 클릭
3) **설정항목** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
대기시간	3	GOTP에서 인증코드 발급 시 Timeout 시간 입력 (분 단위)
타이틀	GOTP 인증	Genian NAC를 통해 사용자인증 진행 시 인증창에 표시되는 타이틀 문구 입력
URL	/plugin/gwp100006/otpAuth.xhtml?initial	GOTP 서버로 API 호출 시 사용되는 Parameter 값
Width	300	인증코드 입력 창의 가로 크기 입력 (최소 300px 권장)
height	130	인증코드 입력 창의 세로 크기 입력 (최소 130px 권장)
mode	active	정책서버 플러그인 사용 모드 선택 (active: 사용 모드 / test: 테스트 모드)

Step 3: Genian NAC 정책서버의 Hostname 확인 및 변경

Genian NAC와 GOTP 연동 시 정책서버 플러그인 업로드 이후 GPKI API(라이선스)는 Genian NAC 정책서버의 Hostname에 맵핑되어 있는 서버 IP를 체크합니다.

Genian NAC에 기본으로 설정되는 Hostname은 **Genians** 입니다. GOTP와 연동을 위해서는 Hostname을 서버 IP가 맵핑되어 있는 **GPKI** 로 설정되어 있어야 합니다.

- 지니언스 기술지원팀 또는 지니언스의 공식적인 기술파트너사의 지원으로 진행됩니다.

Step 4: Genian NAC 정책서버에 필수 라이브러리 설치

Genian NAC와 GOTP 제품간 정상적인 연동을 위해 Genian NAC 정책서버의 업데이트가 필요합니다.

- 지니언스 기술지원팀 또는 지니언스의 공식적인 기술파트너사의 지원으로 진행됩니다.

Step 5: 연동기능 적용을 위한 노드정책 설정

1) Genian NAC Web콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 GOTP 연동을 적용할 노드그룹(ex. 모든노드)이 포함된 **노드정책** 클릭 (특정그룹에만 적용시, 별도의 노드그룹을 생성하여 활용)
3) **세부설정 > 인증정책 > 인증방법** 항목 셀렉트박스에서 **비밀번호인증** 선택
4) **세부설정 > 인증정책 > 인증방법 > 인증방식** 항목 우측 **할당** 버튼 클릭
5) **GOTP** 항목만 우측으로 이동 후 **확인** 버튼 클릭 (GOTP를 제외한 나머지 인증 방식 제거)
6) 하단부 **수정** 버튼 클릭
7) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

이 과정을 통해서 Genian NAC와 GOTP가 연동되어 Genian NAC 사용자인증 수행 시 일반 사용자는 GOTP 인증이 가능하도록 구성됩니다.

케이사인 KSignAccess

본 가이드는 통합인증 보안플랫폼(SSO)인 케이사인의 KSignAccess와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

Genian NAC와 KSignAccess 제품 간 연동 전, 사용자는 제품별로 각각 사용자인증을 수행하는 불편함이 있지만, **연동 후 두 제품간의 SSO가 구현되어 사용자는 KSignAccess의 사용자인증 수행 시 Genian NAC에는 사용자 인증이 자동으로 처리됩니다.**

Genian NAC 에이전트 플러그인은 사용자의 인증을 위해 사용자PC에 암호화된 인증 정보가 담긴 토큰 값을 케이사인에서 제공하는 별도의 프로그램으로 복화화하여 사용자인증 여부를 확인 후, 정상적인 인증상태에서 네트워크를 활용할 수 있도록 합니다.

이 과정을 통하여, 사용자에게는 단 한번의 로그인 과정으로 두 제품의 로그인 과정을 수행하는 편의성을 제공합니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2019.03 이후 Release 버전
Genian NAC (에이전트)	V5.0 이상	2020.07 이후 Release 버전
KSignAccess	V4.0 이상	2020.06 이후 Release 버전

연동의 목적

Genian NAC와 케이사인 KSignAccess 연동은 다음의 효과를 제공합니다.

SSO 환경 제공

- 사용자는 KSignAccess에 먼저 사용자인증을 진행하고, Genian NAC 에이전트 플러그인 연동을 통해 Genian NAC 사용자인증이 자동으로 진행됩니다. Genian NAC는 KSignAccess의 사용자인증 여부를 통해 Genian NAC에 사용자인증이 대체되어 SSO 환경이 구성됩니다.

KSignAccess 미인증 사용자에게 네트워크 차단 사유 및 안내페이지 자동 연결

- Genian NAC는 KSignAccess 미인증 사용자에게 네트워크 차단 사유를 안내하여 정상적인 네트워크 사용을 위한 조치 방법에 대한 안내페이지를 제공합니다.

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 준비

Genian NAC는 KSignAccess와 SSO 구현을 위해 사용자인증 연동 구현에 별도 제작된 Genian NAC 에이전트용 플러그인이 활용되며, 플러그인 정보는 다음과 같습니다.

Genian NAC 에이전트 플러그인 파일명	비고
NAC-C_KsignSSO-R-89872-1.1.8.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상 (2020.07 이후 Release 버전)

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 KSignAccess와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 업로드

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인** 메뉴로 이동
2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **NAC-C_KsignSSO-R-89872-1.1.8.gpf** 플러그인 선택
3) **업로드** 버튼 클릭

Step 2: 에이전트 플러그인 설정

1) Genian NAC Web콘솔에서 **정책 > 노드정책 > 노드액션** 메뉴로 이동
2) **Ksign 대체 인증** 플러그인 클릭
3) **액션 수행설정** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
연동 범위	로그인, 로그인/로그아웃 중 선택	로그인/로그아웃 옵션은 로그인 후, Genian NAC가 지속적으로 KSignAccess로 인증여부를 확인하여, KSignAccess에서 로그아웃된 경우 로그아웃 처리함
		로그인 옵션은 최초 SSO 로그인 이후, 추가적으로 KSignAccess와 로그인 정보를 공유하지 않고 Genian NAC의 인증갱신 주기를 따름

Step 3: 연동기능 적용을 위한 노드정책 설정

다음의 과정을 통해서 Genian NAC의 에이전트 플러그인을 이용하여, 사용자 PC와 서버간 인증을 위한 정상적인 통신 확인과 사용자인증 여부를 확인한 후, 네트워크 접속을 허가할 수 있도록 정책을 생성합니다.

1) Genian NAC Web콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 연동을 적용할 **노드그룹** (ex. 모든노드)이 포함된 **노드정책** 클릭 (특정그룹에만 적용시, 별도의 노드그룹을 생성하여 활용)
3) **세부설정 > 인증정책 > 인증대체정보** 항목으로 이동 후 셀렉트박스에서 **연동API** 선택
4) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭
5) **Ksign 대체 인증** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭
6) 하단부 **수정** 버튼 클릭
7) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

펜타시큐리티 ISign+

본 가이드는 통합인증 보안플랫폼(SSO) 인 Penta Security ISign+와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

Genian NAC와 ISign+ 제품 간 연동 전, 사용자는 제품별로 각각 사용자인증을 수행하는 불편함이 있지만, 연동 후 두 제품간의 SSO가 구현되어 사용자는 ISign+의 사용자인증 수행 시 Genian NAC에는 사용자인증이 자동으로 처리됩니다.

Genian NAC 에이전트에서 ISign+의 인증을 대체하여 적용하도록 구성되어, 사용자의 인증을 위해 Genian NAC 에이전트가 ISign+ 에이전트를 경유하여, ISign+ 서버의 사용자 인증여부를 확인하며, 정상적인 인증상태에서 네트워크를 활용할 수 있도록 합니다.

이 과정을 통하여, 사용자의 인증정보를 사용자의 PC에 보관하지 않은 상태에서 인증을 수행하여 사용자 계정의 안전을 보장하면서 사용자에게는 단 한번의 로그인 과정으로 두 제품의 로그인 과정을 수행하는 편의성을 제공합니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2019.03 이후 Release 버전
Genian NAC (에이전트)	V5.0.32 이상	2020.06 이후 Release 버전
ISign+	3.0 이상	2020.06 이후 Release 버전

연동의 목적

Genian NAC와 Penta Security ISign+의 연동은 다음의 효과를 제공합니다.

SSO 환경 제공

- Genian NAC 에이전트가 ISign+의 인증 정보를 활용하는 형태로 구성되어, 사용자 인증여부를 ISign+ 서버에 확인하여 정상 인증된 사용자에 대해서 Genian NAC의 추가적인 인증없이 네트워크를 활용하도록 구성합니다

ISign+ 미인증 사용자에게 네트워크 차단 사유 및 안내페이지 자동 연결

- Genian NAC는 KSignAccess 미인증 사용자에게 네트워크 차단 사유를 안내하여 정상적인 네트워크 사용을 위한 조치 방법에 대한 안내페이지를 제공합니다.

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 준비

Genian NAC 는 ISign+와 SSO 구현을 위해 사용자인증 연동 구현에 별도 제작된 Genian NAC 에이전트용 플러그인이 활용되며, 플러그인 정보는 다음과 같습니다

Genian NAC 에이전트 플러그인 파일명	비고
NAC-C_Penta2SSO-B-89852-2.1.8.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상 (2020.08 이후 Release 버전)

ISign+의 인증정보를 확인하기 위한 SSO 모듈경로, 서버접속 정보의 준비

ISign+의 인증 정보와 인증 여부를 확인하기 위한 아래의 정보를 확인합니다.

1) SSO 모듈 경로: 사용자 PC 의 ISign+의 SSO 모듈경로를 확인합니다.
2) Check Server URL: ISign+서버의 도메인주소 또는 IP 정보
3) Validate Server URL: ISign+서버의 도메인주소 또는 IP 정보
4) Server Port: 기본포트 9080
5) Agent ID: 각 연동대상 제품 별로 ID 가 존재함 (예. PSI_nac_CS_Prod / Genian NAC 의 ISign+ 연동 ID)

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC 의 설정 부분은 ISign+와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 업로드

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인** 메뉴로 이동
2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **NAC-C_Penta2SSO-B-89852-2.1.8.gpf** 플러그인 선택
3) **업로드** 버튼 클릭

Step 2: 에이전트 플러그인 설정

1) Genian NAC Web콘솔에서 **정책 > 노드정책 > 노드액션** 메뉴로 이동
2) **Penta SSO 대체 인증 2** 플러그인 클릭
3) **액션 수행설정** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
SSO 모듈 경로	*ISign 의 설치경로 + /SA_CSI.dll*	ISign+ 에이전트 경로
Check Server URL	*http://'ISign+ 서버'/api/v1/sso/checkserver*	인증서버와 통신확인
Validate Server URL	*http://'ISign+ 서버'/api/v1/sso/_validate*	인증여부 확인
Server Port	*9080*	기본값
Agent ID	*PSI_nac_CS_Prod*	Genian NAC 의 ISign+ 연동 ID
재시도 주기	*10* 초	연동 실패시 재시도 주기
재시도 횟수	*3* 회	초과시 인증실패 처리
수행 계정	에이전트 기본 수행 계정 선택	해당 플러그인을 수행할 계정의 선택. SSO 모듈의 설치경로, 구동권한에 따라 선택함

Step 3: 연동기능 적용을 위한 노드정책 설정

다음의 과정을 통하여, Genian NAC 의 에이전트 플러그인을 이용하여, 사용자 PC 와 서버간 인증을 위한 정상적인 통신확인과 사용자인증의 여부를 확인한 후, 네트워크 접속을 허가할 수 있도록 정책을 생성합니다.

1) Genian NAC Web 콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 연동을 적용할 **노드그룹** 이 포함된 **노드정책** 클릭 (ex. 노드그룹: 모든노드(특정그룹에만 적용시, 별도로 노드그룹을 생성하여 활용))

3) **세부설정 > 인증정책 > 인증대체정보** 항목으로 이동 후, 셀렉트박스에서 **연동 API** 선택

4) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭

5) **Penta SSO 대체 인증 2** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭

6) 하단 부 **수정** 버튼 클릭

7) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

NetMan 사의 SmartNAC

본 가이드는 네트워크 접근제어 솔루션(NAC) 인 NetMan 사의 SmartNAC와 Genian NAC의 연동 기능을 수행하기 위한 설정방법을 안내합니다.

개요

SmartNAC와 Genian NAC 연동 구성 시, **SmartNAC 사용자 인증 > Genian NAC 사용자 인증** 과정의 프로세스로 수행됩니다.

연동의 목적

Genian NAC Agent 사용 목적이 네트워크 접근제어가 아닌 EDR 운영 목적일 경우 사용자 인증정보를 연동하기 위해 사용됩니다.

사전 준비사항

인증정보를 호출하는 암호화된 레지스트리 정보 확인

- SmartNAC에서 인증정보를 저장하는 레지스트리값과 암호화 방식, 복호화를 위한 Key / 초기백터 값을 확인합니다.

연동을 위한 Genian NAC 에이전트 플러그인 준비

- SSO 연동을 사용하기 위해 확장 플러그인으로 등록된 항목을 사용합니다.

연동을 위한 Genian NAC 설정

Step 1: 에이전트 플러그인 설정

1) Genian NAC Web 콘솔에서 **정책 > 노드정책 > 노드액션** 메뉴로 이동

2) **NetMan SmartNAC 대체 인증** 플러그인 클릭

3) **액션 수행설정** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
동작방법	인증대체 수행, 인증정보 저장 항목중 인증대체 수행 선택	NAC 인증대체 항목을 선택
레지스트리 경로	입력 값 : HKEY_LOCAL_MACHINE\SOFTWARE\NetMan	암호화된 사용자 정보가 저장된 레지스트리 경로 입력 SNPC_SSOState
레지스트리 이름	입력값 : SNPC_LoginID	암호화된 레지스트리 값 이름 입력
로그아웃 사용	ON, OFF 항목 선택	로그아웃 기능 연동 시 ON 설정
암호 알고리즘	BASE64, AES_256_CBC 항목중 선택	레지스트리 암호화 알고리즘 선택

Step 2: 연동기능 적용을 위한 노드정책 설정

다음의 과정을 통해서 Genian NAC의 에이전트 플러그인을 이용하여, 사용자 PC와 서버간 인증을 위한 정상적인 통신 확인과 사용자인증 여부를 확인한 후, 네트워크 접속을 허가할 수 있도록 정책을 생성합니다.

1) Genian NAC Web콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 연동을 적용할 **노드그룹** (ex. 모든노드) 이 포함된 **노드정책** 클릭 (특정그룹에만 적용시, 별도의 노드그룹을 생성하여 활용)
3) **세부설정 > 인증정책 > 인증대체정보** 항목으로 이동 후 셀렉트박스에서 **연동API** 선택
4) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭
5) **NetMan SmartNAC 대체 인증** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭
6) 하단부 **수정** 버튼 클릭
7) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

Genian ZTNA 인증이후, 타사의 인증을 진행하기 위한 SSO 구현가이드

SK인포섹 이글아이(Eagleye)

본 가이드는 개인정보 탐지 및 관리 제품인 SK인포섹의 이글아이(Eagleye)와 네트워크 접근제어 시스템인 Genian NAC의 사용자 인증에 대한 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

가이드 개요

SK인포섹의 이글아이(Eagleye)와 Genian NAC의 연동 구성시, 로그인 프로세스는 Genian NAC 인증 > 이글아이 인증용 프로그램 자동실행 > 이글아이 인증의 프로세스로 구성됩니다.

(Genian NAC가 사용자 단말에서 타사장비와의 연동 시, 범용적으로 활용하는 에이전트인증-플러그인을 이용한 인증방법으로 설명합니다.)

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2018.8 이후 Release 버전
Genian NAC (에이전트)	V5.0.6 이상	2018.8 이후 Release 버전
Eagleye	3.0 이상(1.x, 2.x 단종(2015))	2016.1 이후 Release 버전

연동의 목적

Genian NAC와 SK 인포섹 이글아이(Eagleye)의 연동은 다음의 효과를 제공합니다.

SSO 환경 구성

- 사용자가 네트워크 접속 요청시 사용자의 인증상태를 체크하여 미인증 상태인 경우 CWP를 통해 NAC 인증을 요청합니다. Genian NAC 인증이 성공하면 SK인포섹 이글아이(Eagleye)의 인증을 자동 수행하도록 구성되어, 사용자는 추가적인 인증이 불필요합니다.

  만약, Genian NAC 사용자 인증과정에서 실패한 경우에는 네트워크 접속이 차단되며 CWP화면이 출력됩니다

SK인포섹 이글아이(Eagleye) 미인증 사용자에게 네트워크 차단 등 조치

- 개인정보 취급 담당자가 Genian NAC인증을 수행하더라도 업무 수행에 필요한 개인정보 관리제품이 정상동작하지 않는 상황에서는 내부 네트워크를 활용할 수 없도록 하여 개인정보를 보호할 수 있도록 합니다.

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 확인

Genian NAC 는 SK 인포섹 이글아이(Eagleye)와 SSO 구현을 위해, 사용자인증 연동구현시에 제품의 기본 패키지에서 제공되는 **에이전트 인증창** 플러그인을 활용합니다.

(기본 제공되므로 별도로 업로드를 하지 않으셔도 됩니다.)

Genian NAC 에이전트 플러그인 파일명	비고
NAC-GeniAuth-R-59378-1.1.0.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상 (2018.8 이후 Release 버전)

기본 제공된 에이전트 플러그인의 버전이 가이드에서의 권장버전보다 같거나 높으면 별도로 업로드는 하지 않으셔도 됩니다.

SK인포섹 이글아이(Eagleye) 인증 연동파일, 파일의 실행경로, 실행옵션 확인

SK인포섹 이글아이(Eagleye) 인증실행용 파일은 SK 인포섹에서 제공받아서 설치하여야 하며, 연동시 사용되는 경로와 실행옵션은 다음과 같습니다.

참고) 각 설정 값은 SK인포섹 이글아이(Eagleye)의 연동인증 실행용 파일에 따라 달라질 수 있습니다.

1) SK인포섹 이글아이(Eagleye) 인증실행용 파일 (예. EYNAC.EXE)
2) 실행경로: C:IECEYNAC.EXE
3) 실행옵션: cmd=–nac “–authid:{AUTH_ID}”

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 SK인포섹 이글아이(Eagleye)와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 버전 확인

시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인 으로 이동 후, **에이전트 인증창** 플러그인 버전을 비교합니다.

NAC-GeniAuth-R-59378-1.1.0.gpf 보다 낮은 버전이면, **Step2** 를 실행합니다.

Step 2: 연동을 위한 에이전트 플러그인 업로드

만약, **NAC-GeniAuth-R-59378-1.1.0.gpf** 이상버전인 경우, **Step2** 를 생략합니다.

1) Genian NAC Web 콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인** 메뉴로 이동합니다.

2) **작업선택 > 플러그인 업로드 > 파일선택** 순으로 선택한 후, **NAC-GeniAuth-R-59378-1.1.X.gpf** 플러그인 선택

3) **업로드** 버튼 클릭

Step 3: 에이전트 노드액션 설정

1) Genian NAC Web 콘솔에서 **정책 > 노드정책 > 노드액션 > 노드액션 관리** 메뉴로 이동

2) **에이전트 인증창** 플러그인 클릭

3) **플러그인 설정 > 기타 > 인증 후 실행** 에서 **추가** 버튼을 클릭하여 다음과 같이 설정 값 추가

설정 항목	설정 값	참고
실행경로	경로명 직접입력 선택	아래 '실행경로 설정' 참고
경로입력창	*C:\IEC\EYNAC.EXE*	고객사별로 상이할 수 있으므로 확인 후 적용권장
실행옵션	*-nac '-authid:{AUTH_ID}'*	
암호화 방식	*None* 입력	암호화 지원안함
암호화 키	입력안함	

Note:

- 실행경로 설정: 경로명 직접입력 외에 8개가 추가옵션으로 제공되지만, 상대경로의 경우, OS 패치 업데이트 등으로 인해, 변경의 가능성이 있으므로, 경로명 직접입력 으로 설정을 권장함

Step 4: 에이전트인증창 플러그인 적용을 위한 노드정책 설정

본 과정에서는 에이전트인증창 플러그인을 노드정책에 적용하기 위한 것으로, 이미 에이전트인증창 플러그인을 활용하고 있다면 생략가능 합니다.

1) Genian NAC Web 콘솔에서 **정책 > 노드정책** 메뉴로 이동

2) 사용자인증 연동을 적용할 **노드그룹** (ex. 모든노드)이 포함된 **노드정책** 클릭 (특정그룹에만 적용시, 별도의 노드그룹을 생성하여 활용)

3) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭

4) **에이전트 인증창** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭

5) 하단 부 **수정** 버튼 클릭

6) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

파수 Enterprise DRM

본 가이드는 문서보안 제품인 파수의 Enterprise DRM과 네트워크 접근제어 시스템인 Genian NAC의 사용자 인증에 대한 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

파수 Enterprise DRM과 Genian NAC의 연동 구성시, 로그인 프로세스는 Genian NAC 인증 > 파수 Enterprise DRM 인증용 프로그램 자동실행 > 파수 Enterprise DRM 인증의 프로세스로 구성됩니다.

(Genian NAC가 사용자 단말에서 타사장비와의 연동 시, 범용적으로 활용하는 에이전트인증-플러그인을 이용한 인증방법으로 설명합니다.)

Genian NAC와 파수 Enterprise DRM제품 간 연동 전, 사용자는 Genian NAC 로그인 이후, 추가적으로 파수 Enterprise DRM의 로그인과정을 수행하여야 하지만, 연동 구성시 Genian NAC의 에이전트를 통한 사용자 인증시, 파수 Enterprise DRM 로그인프로세스가 순차적으로 수행하도록 구성됩니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2016.12 이후 Release 버전
Genian NAC (에이전트)	V5.0.6 이상	2016.12 이후 Release 버전
Fasoo Enterprise DRM	5.0 이상	2016.11 이후 Release 버전

연동의 목적

Genian NAC와 파수 Enterprise DRM의 연동은 다음의 효과를 제공합니다.

SSO 환경 구성

- Genian NAC 에이전트가 사용자 인증시, 파수 Enterprise DRM의 인증을 이어서 수행하도록 구성되어, 사용자는 추가적인 파수 Enterprise DRM 인증의 과정 없이 인증과정을 수행할 수 있습니다.

NAC 미인증 사용자에게 네트워크 차단 및 PC를 사용할 수 없도록 조치

- Genian NAC 인증을 거친 후, 파수 Enterprise DRM의 인증을 수행하도록 구성되며, 인증을 거치지 않은 사용자는 PC를 사용할 수 없도록 조치하는 기능을 제공합니다.
- 이는 사용자가 네트워크에 접근하지 않더라도 PC 내부의 정보에 접근할 우려가 있기 때문에 파수 Enterprise DRM의 목적인 문서보안을 항시수행하도록 Genian NAC가 미인증 사용자는 PC에 어떠한 행위도 못하도록 하여, 내부정보를 보호하는데 도움을 줍니다.

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 확인

Genian NAC 는 파수 Enterprise DRM 과 SSO 구현을 위해, 사용자인증 연동 구현시에 제품의 기본패키지에서 제공되는 **에이전트 인증창** 플러그인을 활용합니다. (기본 제공되므로 별도로 업로드를 하지 않으셔도 됩니다.)

Genian NAC 에이전트 플러그인 파일명	비고
NAC-GeniAuth-R-59378-1.1.0.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상 (2016.12 이후 Release 버전)

기본 제공된 에이전트 플러그인의 버전이 가이드에서의 권장버전보다 같거나 높으면 별도로 업로드는 하지 않으셔도 됩니다.

파수 Enterprise DRM 인증연동파일, 파일의 실행경로, 실행옵션, 암호화 방식의 확인(파수 제공)

파수Enterprise DRM 인증실행용 파일은 ㈜파수에서 제공 받아야하며, 연동시 사용되는 경로와 실행옵션은 다음과 같습니다.

참고) 파수Enterprise DRM의 연동인증 실행용 파일에 따라 아래의 각 설정 값은 달라질 수 있습니다.

1) 파수Enterprise DRM 인증실행용 파일 (예. f_ssoex_cast.exe)
2) 실행경로: C:WindowsSystem32f_ssoex_cast.exe
3) 실행옵션: -username={AUTH_ID} -password={AUTH_PWD}
4) 암호화 방식: BASE64, AES, BLOWFISH, CAST, SEED중 선택

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 파수 Enterprise DRM과 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 버전 확인

시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인 으로 이동 후, **에이전트 인증창** 플러그인 버전을 비교합니다.

NAC-GeniAuth-R-59378-1.1.0.gpf 보다 낮은 버전이면, **Step2** 를 실행합니다.

Step 2: 연동을 위한 에이전트 플러그인 업로드

만약, **NAC-GeniAuth-R-59378-1.1.0.gpf** 이상버전인 경우, **Step2** 를 생략합니다.

1) Genian NAC Web 콘솔에서 **시스템> 업데이트 관리 > 소프트웨어 > 에이전트 플러그인** 메뉴로 이동합니다.
2) **작업선택 > 플러그인 업로드 > 파일선택** 순으로 선택한 후, **NAC-GeniAuth-R-59378-1.1.X.gpf** 플러그인 선택
3) **업로드** 버튼 클릭

Step 3: 에이전트 노드액션 설정

1) Genian NAC Web 콘솔에서 **정책 > 노드정책 > 노드액션 > 노드액션 관리** 메뉴로 이동
2) **에이전트 인증창** 플러그인 클릭
3) **플러그인 설정 > 기타 > 인증 후 실행** 에서 **추가** 버튼을 클릭하여 다음과 같이 설정 값 추가

설정 항목	설정 값	참고
실행경로	경로명 직접입력 선택	아래 '실행경로 설정' 참고
경로 입력 창	1) *C:\WINDOWS\SysWow64\f_ssoex_cast.exe* 2) *C:\WINDOWS\System32\f_ssoex_cast.exe*	각각 만들어서 두개의 경로를 생성함
실행옵션	*-nac '-authid:{AUTH_ID} -authpw:{AUTH_PWD}'*	AUTH_ID는 입력 아이디, AUTH_PWD는 입력 비밀번호로 자동 변경됨
암호화 방식	암호화 방식의 선택	*BASE64, AES(128bit), BLOWFISH(64bit), CAST(128bit), SEED(128bit)* 중 선택
암호화 키	상호협의한 암호화키 입력	BASE64는 암호화키 생략

Note:

- 실행경로 설정: 경로명 직접입력 외에 8개가 추가옵션으로 제공되지만, 상대경로의 경우, OS 패치 업데이트 등으로 인해, 변경의 가능성이 있으므로, 경로명 직접입력 으로 설정을 권장함

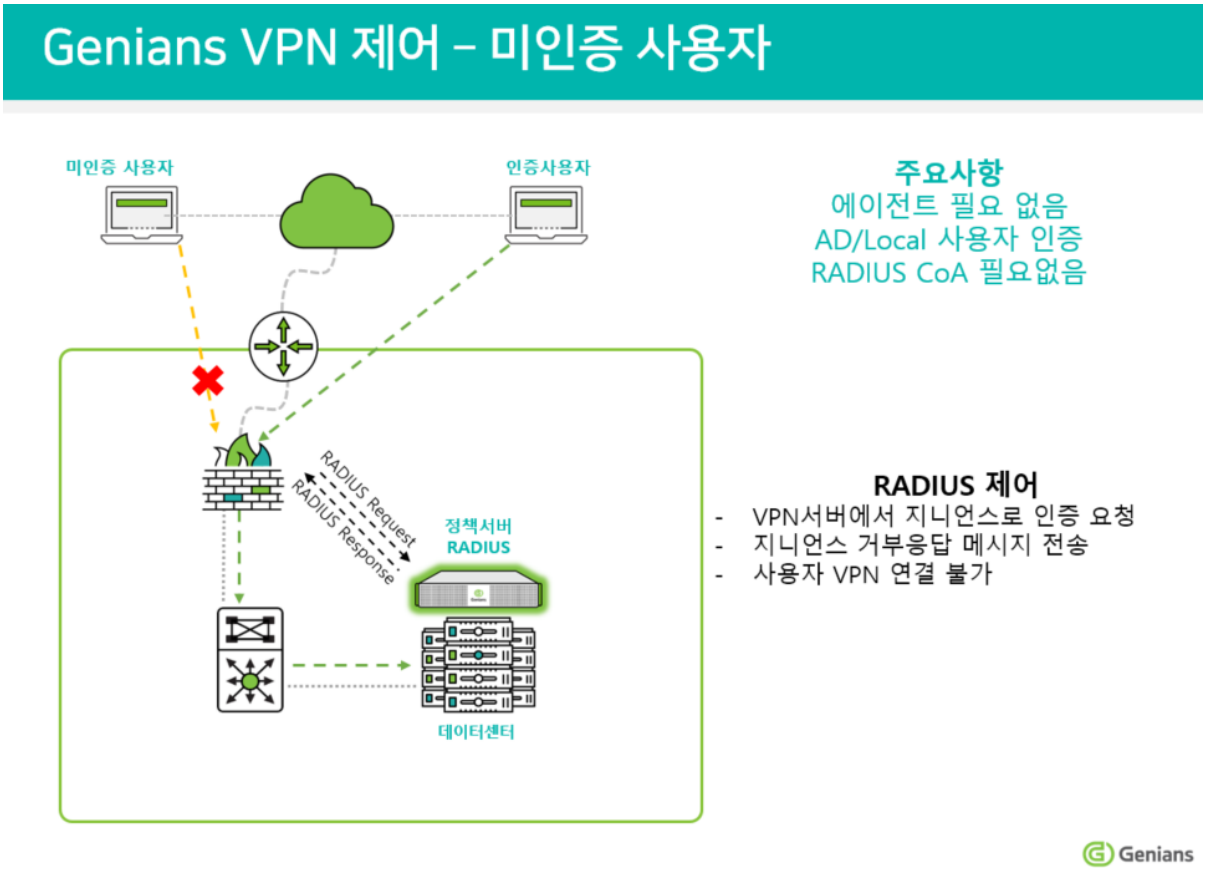
Step 4: 에이전트인증창 플러그인 적용을 위한 노드정책 설정

본 과정에서는 에이전트인증창 플러그인을 노드정책에 적용하기 위한 것으로, 이미 에이전트인증창 플러그인을 활용하고 있다면 생략가능 합니다.

1) Genian NAC Web 콘솔에서 **정책 > 노드정책** 메뉴로 이동
2) 사용자인증 연동을 적용할 **노드그룹** (ex. 모든노드)이 포함된 **노드정책** 클릭 (특정그룹에만 적용시, 별도의 노드그룹을 생성하여 활용)
3) 하단 **노드액션 설정** 항목으로 이동 후 **할당** 버튼 클릭
4) **에이전트 인증창** 노드액션을 우측으로 이동 후 **추가** 버튼 클릭
5) 하단 부 **수정** 버튼 클릭
6) 우측 상단 **변경정책적용** 버튼 클릭하여 정책 적용

7.1.5 VPN 사용자 인증

Genian RADIUS서버는 VPN환경에서 인증서버로 사용할 수 있으며 인증 사용자에 대한 제한이 가능합니다.

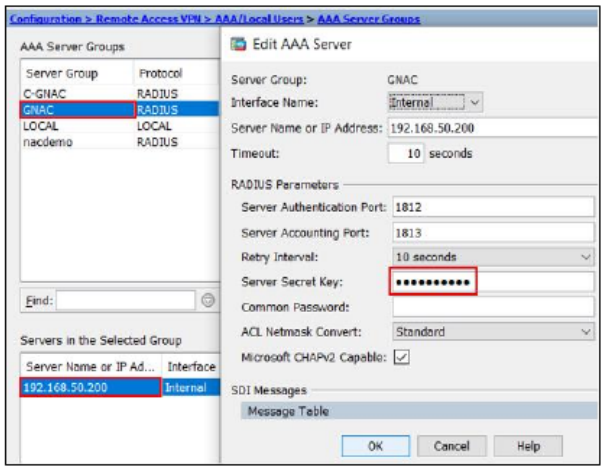


Radius서버 연동

Genian RADIUS 설정을 먼저 구성합니다. *RADIUS 제어 설정* 를 참고 하시길 바랍니다.

RADIUS 서버가 올바르게 설정되어있고 VPN 환경과 호환이 되는지 확인합니다.

아래 예제 이미지와 같이 VPN서버에서 Genian RADIUS 서버와 통신하기 위한 서버 인증키, 서버 주소, Authentication 포트, Accounting 포트 정보 등을 입력합니다.



인증제한 설정

경우에 따라 RADIUS 서버를 사용하여 인증 가능한 사용자를 제한할 수 있습니다. 이 작업은 관리 WebUI **정책 > RADIUS 정책** 을 생성하여 접근정책을 **REJECT** 으로 설정하여 제한합니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴의 **정책 > RADIUS 정책** 으로 이동합니다.
3. **작업선택 > 생성** 을 선택합니다.
4. 기본 설정인 **이름, 우선순위, 적용모드** 를 입력합니다.
5. **조건설정** 에서 **속성** 을 선택합니다.
6. **조건설정** 에서 **조건과 값** 을 입력합니다.
7. **조건설정** 을 **추가** 합니다.
8. **정책설정** 에서 인증자자에 대한 **접근정책** 을 **REJECT** 로 선택합니다.
9. **생성** 을 클릭합니다.

다른 우선 순위가 높은 RADIUS 정책을 적용받지 않는경우 인증 요청이 정의된 조건에 충족하면 접근이 거부됩니다.

7.2 사용자 및 그룹 관리

사용자 및 사용자 그룹과 패스워드 정책을 관리 할 수 있습니다.

7.2.1 사용자 관리

사용자 태그를 생성하고 할당 그리고 그룹화 할 부서 및 직책과 같은 정보를 추가하여 사용자를 관리 할 수 있습니다.

사용자 등록

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. **작업선택 > 사용자등록** 을 클릭합니다.
3. 기타 정보를 입력하고 **생성** 및 **수정** 버튼을 입력합니다. (필수입력 정보: 사용자*ID*, 이름, 비밀번호)

사용자 삭제

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. **사용자ID** 를 찾아 **체크박스** 를 클릭합니다.
3. **작업선택 > 사용자 삭제**
4. **확인** 버튼을 클릭합니다.

사용자 태그 할당

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. **사용자ID** 를 찾아 **체크박스** 를 클릭합니다.
3. **작업선택 > 사용자 태그설정** 을 클릭합니다.
4. **사용자 태그설정** 창에서 **선택한 태그 추가** 를 선택하고 원하는 **태그명** 의 **체크박스** 를 클릭합니다.
5. **설정** 버튼을 클릭합니다.

사용자 부서 할당하기

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. **사용자ID** 를 클릭합니다.
3. **추가정보 설정** 항목에서 부서를 할당합니다.
4. **수정** 버튼을 클릭합니다.

7.2.2 사용자 그룹 관리

부서, 직책 또는 사용하는 시스템 유형별로 고유하게 식별하는 사용자 그룹을 관리 할 수 있습니다. 이렇게 하면 네트워크에서 사용자를보다 효과적으로 제어 할 수 있습니다.

Note: 사용자 그룹의 경우 사용자 계정의 상태 와 기타 정보(예: 개인정보, 조직, 직급 등)를 조건으로 활용하여 사용 됩니다.

사용자 그룹 생성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 사용자** 메뉴로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **기본정보** 탭 아래의 옵션(*ID*, 설명, 그룹조건) 들을 설정 헙니다.
5. **생성** 버튼을 클릭합니다.

사용자 그룹 할당

1. 상단 항목에서 **관리 > 사용자** 메뉴를 클릭합니다.
2. 원하는 **사용자ID** 를 찾아 **체크박스** 를 클릭합니다.
3. **작업선택 > 사용자그룹 지정** 을 클릭합니다.
4. **사용자그룹 지정** 창에서 생성되어 있는 사용자 그룹을 선택하여 **설정** 버튼을 클릭합니다.(*Tip.* 사용자 그룹 조건연산이 *OR* 인 그룹만 선택창에서 표시 됩니다.)
5. 화면 우측 상단의 **변경정책적용** 버튼을 클릭합니다.

사용자 그룹 삭제

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 사용자** 메뉴로 이동합니다.
3. 원하는 **사용자그룹** 을 찾아 **체크박스** 를 클릭합니다.
4. **작업선택 > 삭제** 를 클릭합니다.
5. **확인** 버튼을 클릭합니다.

7.2.3 사용자 계정 비밀번호 정책

최종 사용자에게 적용되는 비밀번호 정책을 구성하려면 다음과 같이합니다.

Note: 비밀번호 정책의 경우 일반사용자 계정 외 관리자 계정까지 동일하게 설정되는 공통 정책입니다.

비밀번호 정책 설정

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자인증 > 사용자관리** 메뉴로 이동합니다.
3. 옵션을 찾아 입력:
   - **비밀번호 저장방식** - 사용자 비밀번호 저장방식을 선택합니다. RADIUS서버를 통한 MSCHAPv2 인증을 지원하기 위해서는 NT-Hash를 선택해야합니다.
   - **최소길이** - 비밀번호 최소길이를 설정합니다. (9 - 30)
   - **최대길이** - 비밀번호 최대길이를 설정합니다. (9 - 30)
   - **문자로 시작** - 비밀번호가 문자로 시작하도록 강제화 할지 여부를 설정합니다.
   - **대/소문자 혼용** - 비밀번호에 대/소문자를 혼용하도록 강제할지 여부를 설정합니다.
   - **문자반복 불가횟수** - 비밀번호에 동일문자 반복사용 제한을 위한 횟수를 설정합니다. (0: 제한안함, 3: 3자리 이상 동일문자 반복사용 불가)
   - **연속문자 불가횟수** - 비밀번호에 내림/오름차순 연속사용 제한을 위한 횟수를 설정합니다. (0: 제한안함, 3: 3자리 이상 연속문자 사용불가)
   - **검증 정규식 사용** - 비밀번호 검증을 위한 정규식(Regular Expression) 사용여부를 선택합니다.
   - **ID문자열 포함금지** - 비밀번호에 ID문자열 포함금지 여부를 설정합니다.
   - **Blacklist 단어 사용금지** - Blacklist 등록 단어의 비밀번호 사용금지 여부를 설정합니다.
4. **수정** 버튼을 클릭합니다.

7.2.4 사용자 부서관리

사용자 계정에 사용할 수 있는 부서 정보를 추가하거나 삭제하여 부서를 관리 할 수 있습니다.

부서 수동 등록하기

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. 왼쪽 부서관리 항목을 클릭합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 정보를 입력하고 **생성** 버튼을 입력합니다. (필수입력 정보: 부서코드, 부서명)

부서 CSV 파일 가져오기

부서 생성 시 외부 CSV 파일 형태로 사전에 정의된 파일을 기반으로 부서를 생성합니다.

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. 왼쪽 부서관리 항목을 클릭합니다.
3. **작업선택 > 가져오기** 을 클릭합니다.
4. **파일선택** 항목을 클릭하여 가져올 CSV 파일을 선택합니다.
5. **실행** 버튼을 클릭합니다.

부서 삭제하기

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. 왼쪽 부서관리 항목을 클릭합니다.
3. 삭제할 부서에 체그박스를 선택합니다.
4. **작업선택 > 삭제** 를 클릭합니다.

Note: 부서를 삭제하기 위해서는 부서가 할당된 계정에서 부서를 해제하거나 부서에 연결된 하위부서 항목이 없어야 합니다.

부서 노드그룹 지정하기

부서 기반에 IP 신청시스템을 사용하기 위해서는 부서별 할당가능한 IP대역이 포함된 노드그룹을 지정해야 합니다.

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. 왼쪽 부서관리 항목을 클릭합니다.
3. 노드그룹을 지정할 부서에 체크박스를 선택합니다.
4. **작업선택 > 노드그룹 지정** 항목을 클릭합니다.
5. 할당할 **노드그룹** 을 선택합니다.
6. **설정** 버튼을 클릭합니다.

부서 노드그룹 해제하기

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. 왼쪽 부서관리 항목을 클릭합니다.
3. 노드그룹을 해제할 부서에 체크박스를 선택합니다.
4. **작업선택 > 노드그룹 일괄해제** 항목을 클릭합니다.
5. **확인** 버튼을 클릭합니다.

7.2.5 사용자 직급관리

사용자 계정에 사용할 수 있는 직급을 추가하거나 삭제하여 직급을 관리할 수 있습니다.

사용자 직급은 해당 정보를 가지고 사용자 그룹을 정의할 수 있으며, 정의된 사용자 그룹을 조건으로 노드그룹을 생성할 수 있습니다. 생성된 노드그룹을 기반으로 Genian ZTNA에서 정책을 적용받는 대상으로 지정할 수 있습니다.

사용자 직급 생성하기

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. 왼쪽 직급관리 항목을 클릭합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 정보를 입력하고 **생성** 버튼을 입력합니다. (필수입력 정보: 직급코드, 직급명)

사용자 직급 삭제하기

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. 왼쪽 직급관리 항목을 클릭합니다.
3. 삭제할 직급 항목에 체크박스를 선택합니다.
4. **작업선택 > 삭제** 를 클릭합니다.

Attention: 사용자 직급을 삭제하기 위해서는 직급이 할당된 사용자 계정이나 노드그룹이 존재하지 않아야 합니다.

사용자 직급 CSV 가져오기

사용자 직급 생성 시 외부 CSV 파일 형태로 사전에 정의된 파일을 기반으로 직급을 생성합니다.

1. 상단 항목의 **관리 > 사용자** 로 이동합니다.
2. 왼쪽 직급관리 항목을 클릭합니다.
3. **작업선택** 왼쪽  클릭하여 CSV 파일을 다운로드 합니다.
4. 다운로드 된 **CSV 파일** 에 형식에 맞추어 정보를 입력합니다.
5. **작업선택 > 가져오기** 을 클릭합니다.
6. **파일선택** 항목을 클릭하여 작성된 CSV 파일을 선택합니다.
7. **실행** 버튼을 클릭합니다.

사용자 직급을 조건으로 제어정책 생성하기

사용자 직급을 조건으로 사용자 그룹 생성하기

1. 상단 패널에 **정책** 으로 이동합니다.
2. 왼쪽 **그룹** 항목에서 **사용자** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 클릭합니다.
4. **사용자 그룹 생성 창** 에서 **조건** 항목을 **직급** 으로 설정값을 입력합니다.
5. **추가** 버튼을 클릭합니다.
6. **생성** 버튼을 클릭합니다.

7. 좌측 상단 **변경정책적용** 버튼을 클릭합니다.

사용자 그룹을 조건으로 노드 그룹 생성하기

1. 상단 패널에 **정책** 으로 이동합니다.
2. 왼쪽 **그룹** 항목에서 **노드** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 클릭합니다.
4. **노드그룹 생성 창** 에서 **항목** 을 **인증사용자** 로 **조건** 은 **그룹에 속하면** 으로 **설정** 값은 직급으로 생성된 **사용자 그룹** 을 설정합니다.
5. **추가** 버튼을 클릭합니다.
6. **생성** 버튼을 클릭합니다.
7. 좌측 상단 **변경정책적용** 버튼을 클릭합니다.

사용자 직급을 조건으로 제어정책 생성하기

사용자 직급을 조건으로 한 노드그룹에 제어정책 설정 부분은 노드그룹에 대한 제어정책 생성 를 참고 하십시오.

7.2.6 사용자 신청서를 통한 사용자 관리하기

Genian ZTNA 시스템에서는 자체적으로 관리하는 사용자 계정에 대해 계정을 신청할 수 있는 신청서를 작성하여 관리자의 승인절차를 통해 사용자 인증을 사용할 수 있습니다.

사용자 신청서를 사용하기 위한 사전작업

1. 사용자 신청서 용도 작성 (사용자 계정 용도별 속성값 설정하기)
2. 사용자 신청서 사용 설정 (user-application-used)

사용자 신청서 승인/거부 하기

등록된 사용자 신청서에 대해서 관리자가 확인 후 승인, 거부를 수행할 수 있습니다.

1. 상단 패널에 **관리** 에서 **신청** 으로 이동합니다.
2. 완쪽 **사용자 신청서** 항목에서 **신규등록** 을 선택합니다.
3. 오른쪽 **신청서 리스트** 에서 **번호** 를 클릭하여 **신청서 세부정보** 를 확인합니다.
4. 신청서 세부정보 하단에 **승인** , **거부** 중 하나를 클릭합니다.

Note:

1. 사용자 신청서에 대한 자동승인은 사용자 계정 신청을 자동 승인하기 참고하시기 바랍니다.
2. 사용자 신청서에 대한 이메일 승인은 이메일을 통한 사용자 계정 승인하기 참고하시기 바랍니다.

사용자 신청서 처리결과 확인하기

신청서에 대한 관리자의 승인, 거부 결과를 확인할 수 있습니다.

1. 상단 패널에 **관리** 에서 **신청** 으로 이동합니다.
2. 완쪽 **사용자 신청서** 항목에서 **결과조회** 을 선택합니다.

Note: 처리결과 리스트에서 **번호** 를 클릭할 경우 신청서의 세부 항목 정보를 확인할 수 있습니다.

7.2.7 사용자 계정 설정정보 확인 및 수정하기

사용자 인증을 사용하기 위하여 등록된 사용자 계정에 설정된 정보를 확인하거나 수정할 수 있으며 계정 별 제한 설정을 변경할 수 있습니다.

사용자 계정에 대한 설정사항은 다음과 같습니다.

항목	설명
기본설정	사용자 계정에 대한 역할, 용도, 상태등의 정보를 표시합니다.
비밀번호 설정	사용자 계정에 대한 비밀번호 변경 기능을 제공합니다.
인증제한 설정	사용자 인증에 제한되는 항목(IP, MAC, 갯수, 그룹) 정보가 표시됩니다.
추가정보 설정	사용자 계정에 추가적으로 입력된 정보가 표시됩니다.

1. 기본설정 정보 확인하기

Genian ZTNA에서 사용되는 사용자 계정에 기본정보를 표시합니다.

항목	세부항목	설명	수정가능여부
기본설정	사용자 이름	사용자 계정에 이름이 표시됩니다.	O
	관리역할	사용자 계정을 관리자 역할 권한을 부여할 수 있습니다. 관리자의 역할 관련사항은 다음에 관리자 계정 참고하시기 바랍니다.	O
	설명	사용자 계정에 설명이 표시됩니다.	O
	용도	사용자 계정에 용도가 표시됩니다. 용도 관련사항은 다음에 사용자 계정 용도별 속성값 설정하기 참고하시기 바랍니다.	O
	상태	계정에 활성화 상태가 표시됩니다.	O
	사용자 정보 수정	계정에 정보수정 가능여부가 표시됩니다.	X
	계정사용만료	계정에 사용만료 시각이 표시됩니다.	O
	태그	계정에 할당된 태그 정보가 표시됩니다.	O

2. 비밀번호 설정

사용자 인증 시 사용되는 사용자 계정에 비밀번호를 변경할 수 있습니다.

Note: 비밀번호 변경은 사용자 계정에 **사용자 정보수정** 정보에 따라서 수정 여부가 설정됩니다.

사용자 정보수정	변경가능여부
로컬계정으로 설정	비밀번호 수정 가능
모든정보수정불가	비밀번호 수정 불가
비밀번호 수정가능	비밀번호 수정 가능
모든정보수정가능	비밀번호 수정 가능

3. 인증제한 설정

사용자 인증 수행 시 제한되는 조건을 설정할 수 있습니다.

제한항목	설명
IP 인증제한	사용자 인증을 수행할 수 있는 IP 갯수를 설정합니다.
MAC 인증제한	사용자 인증을 수행할 수 있는 MAC 갯수를 설정합니다.
장비 인증제한	사용자 인증을 수행할 수 있는 장비 갯수를 설정합니다.
인증허용 IP	사용자 인증을 수행할 수 있는 IP 대역을 설정합니다.
인증허용 MAC	사용자 인증을 수행할 수 있는 MAC을 지정합니다.

예외처리 설정

인증제한 항목이 설정되어 있더라도 제한설정이 적용되지 않는 예외처리 노드그룹을 설정합니다.

예외항목	설명
인증제한 예외노드그룹	인증 제한설정에 예외처리될 노드그룹을 지정합니다.

4. 추가정보 설정

사용자 계정 신청이나 동기화를 사용하여 ZTNA에 생성된 계정에 일반정보가 표시됩니다. 표시되는 정보는 사용자 계정에 용도에 따라 다르며 용도관련 부분은 다음에 사용자 계정 용도별 속성값 설정하기 참고하시기 바랍니다.

Note: 추가정보 변경은 사용자 계정에 **사용자 정보수정** 정보에 따라서 수정 여부가 설정됩니다.

사용자 정보수정	변경가능여부
로컬계정으로 설정	추가정보 수정 가능
모든정보수정불가	추가정보 수정 불가
비밀번호 수정가능	추가정보 수정 불가
모든정보수정가능	추가정보 수정 가능

7.2.8 사용자 그룹 세부 설정하기

사용자 인증 기능을 제공하는데 사용되는 사용자 계정에 대해서 별도의 조건을 기반으로 사용자 그룹을 생성할 수 있습니다.

- 사용자 그룹을 조건으로 그룹을 생성하여 노드정책 에서 인증적용 대상 으로 지정할 수 있습니다.
- 사용자 그룹을 노드그룹으로 사용하기 위해서는 인증사용자 항목을 사용해야 합니다.

사용자 그룹 생성 조건 확인하기

조건항목	설명	참고사항
IP 인증제한	사용자 계정에 제한설정 유무로 그룹을 생성합니다.	사용자 계정 설정정보 확인 및 수정하기
MAC 인증제한		
장비인증제한		
계정상태	사용자 계정에 사용상태로 그룹을 생성합니다.(정상/사용중지)	
계정용도	사용자 계정이 생성된 용도 정보로 그룹을 생성합니다.	사용자 계정 용도별 속성값 설정하기
계정중지사유	사용중지 상태인 계정에 중지 사유 정보로 그룹을 생성합니다.	
관리자권한	관리자 계정에 권한 정보로 그룹을 생성합니다.	관리자 계정
동기화여부	사용자 계정에 동기화 정보로 그룹을 생성합니다.	
마지막 인증시각	사용자 계정에 마지막 인증시각을 정보로 그룹을 생성합니다.	
만료시각	사용자 계정에 사용 제한 시간 정보로 그룹을 생성합니다.	
멤버쉽	AD/LDAP 멥버쉽(그룹정보) 정보로 그룹을 생성합니다.	
부서	사용자 계정이 속한 부서 정보로 그룹을 생성합니다.	
비밀번호	사용자 계정에 비밀번호 설정 및 비밀번호 강제변경 설정 정보로 그룹을 생성합니다.	
사용자ID	사용자 계정에 ID 정보로 그룹을 생성합니다.	
사용자그룹	사용자 그룹을 포함하는 정보로 그룹을 생성합니다.	
설명	사용자 계정에 설정된 설명 정보로 그룹을 생성합니다.	
이메일주소	사용자 계정에 설정된 이메일주소 정보로 그룹을 생성합니다.	
인증상태	사용자 계정에 인증여부 정보로 그룹을 생성합니다.	
전화번호	사용자 계정에 설정된 전화번호 정보로 그룹을 생성합니다.	
직급	사용자 계정에 설정된 직급 정보로 그룹을 생성합니다.	
태그	사용자 계정에 설정된 태그 정보로 그룹을 생성합니다.	
회사명	사용자 계정에 설정된 회사명 정보로 그룹을 생성합니다.	
휴대전화번호	사용자 계정에 설정된 휴대번호 정보로 그룹을 생성합니다.	

7.2.9 사용자 현황 확인하기

관리> 사용자 항목에서 ZTNA에 등록된 사용자 계정정보를 부서와 직급에 형태에 맞추어 현황을 확인할 수 있습니다.

1. 사용자 전체 현황 확인하기

관리> 사용자> 전체사용자 항목에서 ZTNA 사용자 등록이나 외부 동기화 기능을 사용하여 생성된 사용자 계정 전체를 확인할 수 있습니다.

2. 사용자 부서별 현황 확인하기

관리> 사용자> 전체사용자> 부서별 항목에서 사용자 계정이 속한 부서 기반에 현황을 표시합니다. 추가 옵션으로 하위 부서를 포함하여 사용자 계정 현황을 확인할 수 있습니다.

Note: 부서 관련된 사항은 다음에 사용자 부서관리 항목을 참고하시기 바랍니다.

---

3. 사용자 계정관련 관리자 설정항목

등록된 사용자 계정에 대해서 관리자는 다음에 명령을 사용하여 관리할 수 있습니다.

항목	설명	참고
내보내기	전체 사용자 계정정보를 Excel 과 CSV 파일 선택으로 관리자 단말로 다운로드 합니다.	
사용자 등록	관리자가 수동으로 사용자 계정을 등록합니다.	
사용자 삭제	등록된 사용자 계정을 삭제합니다.	
사용자 태그설정	사용자 계정에 태그를 설정합니다.	노드 태그 할당
시용자그룹 지정	선택된 사용자 계정을 특정 사용자 그룹에 조건으로 포함하도록 설정합니다.	사용자 그룹 세부 설정하기
사용자용도 설정	선택된 사용자 계정의 용도를 특정 사용자 용도로 변경하도록 설정합니다.	사용자 계정 용도별 속성값 설정하기
인증제한 설정	사용자 계정에 제한 항목을 설정합니다.	사용자 계정 설정정보 확인 및 수정하기
비밀번호변경 강제화 설정	사용자 계정 비밀번호 변경 적용을 강제로 설정합니다.	
비밀번호변경 강제회 설정 (임시비밀번호 발급)	비밀번호를 임시비밀번호로 초기화 후 비밀번호 변경 적용을 강제로 설정합니다.	
사용만료시각 변경	사용자 인증을 수행할 수 있는 만료시각을 설정합니다.	
정상 상태로 변경	사용중지 상태인 사용자 계정을 정상 상태로 변경하도록 설정합니다.	
사용중지 상태로 변경	정상 상태인 사용자 계정을 사용중지 상태로 변경하도록 설정합니다.	

7.3 외부 인증서버 설정

LDAP, RADIUS, IMAP, POP3, SMTP 또는 기타 타사 시스템을 사용하여 외부 인증 시스템에 인증하도록 정책 서버를 구성할 수 있습니다.

7.3.1 RADIUS

사용자 인증을 위해 기존의 외부 RADIUS 서버와 연동하도록 정책 서버를 구성 할 수 있습니다. 사용자가 접속인증페이지(CWP) 나 에이전트를 통해 인증되면 사용자 비밀번호 가 RADIUS 서버를 통해 인증 됩니다.

1. 왼쪽 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자 인증 > 인증연동** 으로 이동합니다.

RADIUS 인증연동 메뉴에서 아래를 설정:

1. **서버주소** : 연동하고자하는 외부 RADIUS 인증서버의 IP주소 또는 FQDN 을 설정합니다.
2. **서버포트** : RADIUS 인증서버 서비스포트를 설정합니다.(기본포트: *1812*)
3. **인증키** : RADIUS 인증서버와의 상호인증을 위한 인증키를 설정합니다.
4. **수정** 버튼을 클릭합니다.

7.3.2 LDAP (Active Directory) 서버 연동

사용자 인증 을 **Active Directory** 와 연동 하도록 **정책 서버** 를 구성 할 수 있습니다.

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자 인증 > 인증연동** 으로 이동합니다.
3. 인증연동 창에서 **LDAP 인증연동** 메뉴를 찾습니다.
4. 아래 옵션을 찾아 입력:
   - **서버주소**: LDAP(ActiveDirectory) 인증연동을 위한 서버시스템의 주소/도메인을 설정합니다.
   - **서버포트**: LDAP 서비스 포트번호를 설정합니다. (표준값: *Non-SSL=389, SSL=636*)
   - **Base DN**: LDAP Base DN을 설정합니다. (예: *CN=Users,DC=geni,DC=genians,DC=com*)
   - **Bind DN**: 사용자 검색을 위한 Bind DN 값을 설정합니다. Anonymous 검색이 가능 할 경우 공백.(도메인 예:*Administrator@genians.com / Bind* 계정에는 관리자 권한이 있어야합니다.)
   - **Bind Password**: 사용자 검색을 위한 Bind DN 비밀번호를 설정합니다.
   - **Serch Attribute**: 사용자 ID를 담고있는 속성값 이름(ActiveDirectory: sAMAccountName)을 설정합니다.
   - **SSL 접속**: LDAP 서버 접속시 SSL 연결을 사용할지 여부를 선택합니다.
   - **Secondary LADP 사용** : Secondary LDAP 사용여부를 선택합니다.
5. **수정** 버튼을 클릭합니다.
6. 테스트 를 클릭 하여 구성 설정을 테스트합니다. (테스트 계정은 *BASE DN* 에있는 모든 사용자 계정이 될 수 있습니다)

Note: 알려진 이슈

- 오류 메시지: **"LDAP 서버에 연결하지 못했습니다. URI=ldaps://[IP]:[PORT]/, ERRMSG='-1:Can't contact LDAP server, TLSv1.0=-1:Can't contact LDAP server' "**
- 해결 방법: LDAP 서버 펌웨어를 최신 패치로 업데이트합니다. "보안패치가 되지 않은 서버의 LDAP을 통해 Active Directory에 대해 인증하려고 하는 알려진 문제" 이며, 이는 암호화 호환성으로 인해 발생합니다.

이메일 은 대부분의 조직에서 제공하는 서비스이므로 사용자 디렉토리를 제공하는 것이 가장 쉽습니다. **이메일** 에서 사용되는 **SMTP** , **POP3** 및 **IMAP** 을 사용하여 사용자의 아이디 와 비밀번호 를 확인할 수 있습니다 .

7.3.3 IMAP

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자 인증 > 인증연동** 으로 이동합니다.
3. 메인창에서 **IMAP 인증연동** 을 찾습니다.
4. **IMAP 서버**, **IMAP 포트**, **사용자도메인** 을 입력합니다.
5. **수정** 버튼을 클릭합니다.
6. **인증테스트 > 테스트** 버튼을 클릭하여 사용자 인증을 테스트합니다.

예제

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

7.3.4 POP3

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자 인증 > 인증연동** 으로 이동합니다.
3. 메인창에서 **POP3 인증연동** 을 찾습니다.
4. **POP3 서버**, **POP3 포트**, **사용자도메인** 을 입력합니다.
5. **수정** 버튼을 클릭합니다.
6. **인증테스트 > 테스트** 버튼을 클릭하여 사용자 인증을 테스트합니다.

예제

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

7.3.5 SMTP

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자 인증 > 인증연동** 으로 이동합니다.
3. 메인창에서 **SMTP 인증연동** 을 찾습니다.
4. **SMTP 서버, SMTP 포트, 사용자도메인** 을 입력합니다.
5. **수정** 버튼을 클릭합니다.
6. **인증테스트 > 테스트** 버튼을 클릭하여 사용자 인증을 테스트합니다.

Note: Genian ZTNA는 오직 smtps만 지원합니다. (SMTP over SSL)

예제

Service Name	Server Name	Port	Domain
Google G Suites	smtp.gmail.com	465	Your Domain

문제 해결

Error: Gmail SMTP 인증연동에 확인 된 이슈 :

- 인증 테스트: 인증 실패. Authentication failed.SMTP(535-5.7.8:Username and Password not accepted. Learn more at 535 5.7.8 https://support.google.com/mail/?p=BadCredentialsy32sm41405227qt)
- Genian ZTNA 로그 : Login failed. ERRMSG='Authorize(Account disabled)'
- **수정** : Google 계정 설정/보안에서 보안이 낮은 앱 액세스를 설정합니다.

7.3.6 SAML 2.0

SAML (Security Assertion Markup Language)은 당사자 간에 인증 및 인증 데이터를 교환 할 수 있는 개방형 표준입니다. SAML은 인증이 필요한 최종 사용자 및 SP(서비스 공급자)와 인증 서비스를 제공하는 IdP(인증 공급자)로 구성 됩니다. Genian ZTNA가 SAML을 통해 Google과 통합되면 Genian ZTNA는 SP가 되고 Google은 IdP가 됩니다.

다음은 SAML 연동을 위한 기본 구성 단계입니다.

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자 인증 > 인증연동** 으로 이동합니다.
3. 메인창에서 **SAML2** 를 찾습니다.
4. **SP Entity ID** 및 **SP ACS URL** 값을 복사합니다.
5. Genian ZTNA 의 복사 된 해당값을*IdP server* 에 입력합니다.
6. **IdP Entity ID** 및 **IdP SSO URL** 에 IdP 서버로 부터 얻은 값들을 입력합니다.
7. **x509 Certificate** 의 경우 IdP 서버에서 발급한 인증서를 입력합니다.
8. **수정** 버튼을 클릭합니다.
9. **인증테스트 > 테스트** 버튼을 클릭하여 사용자 인증을 테스트합니다.

okta (SAML2.0) - CWP

본 가이드는 okta 와 네트워크 접근제어 시스템인 Genian ZTNA의 인증연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

Genian ZTNA와 okta 솔루션의 APP 연동을 통하여 Genian ZTNA자체 사용자DB를 관리할 필요가 없이 okta를 통해 사용자 인증을 수행할 수 있습니다.

사용자 인증을 위해 Genian ZTNA CWP페이지에서 SAML2.0 프로토콜을 이용하여 okta 인증을 호출하고 okta에서 사용자 인증 여부를 확인하여 정상적인 SSO가 이루어집니다.

권장버전

제품명(구성요소)	버전	비고
Genian ZTNA(정책서버)	V6.0 이상	2022.05 이후 Release 버전
okta APP	SAML2.0	2021.05 현재 연동가능

연동의 목적

Genian ZTNA와 okta 연동은 다음의 효과를 제공합니다.

- ZTNA, okta 개별 인증을 위한 사용자 DB 관리가 필요하지 않습니다.
- okta 계정을 이용하여 SSO로 ZTNA를 인증할 수 있습니다.

지원되는 기능

okta SAML App 연동은 다음과 같은 기능을 지원합니다:

- SP-initiated SSO
- IdP-initiated SSO
- JIT (Just-In-Time) Provisioning
- Single Logout (SLO)
- Signed Requests

위 기능에 대한 자세한 정보는 , https://help.okta.com/okta_help.htm?type=oie&id=ext_glossary 에서 확인하세요.

연동 설정 방법

본 가이드에서 다루는 Genian ZTNA와 okta 설정 방법은 연동을 위한 필수 항목만을 안내합니다. 최초 1회 설정 이후 자동으로 적용됩니다.

Step 1: okta 연동을 위한 계정등록

1. https://www.okta.com/free-trial/ 접속하여 트라이얼 계정을 신청합니다.
   - 사용자 정보와 국가를 선택합니다.
2. 신청한 메일주소로 수신된 인증확인 메일을 확인합니다.
   - 신청한 메일주소로 'Activate your okta account' 라는 제목으로 계정정보 확인 메일이 발송됩니다.
3. 메일 내 'Activate okta Accout' 버튼을 클릭하여 계정을 활성화 하십시오.
   - 인증을 위한 초기 패스워드 변경과 2차 인증에 대한 설정을 합니다.
   - okta 콘솔접속시 OTP 2factor 인증을 요구하며 아이폰, 안드로이드 OTP 앱 설치 및 OTP 등록이 필요합니다.
   - OTP 등록과 로그인을 완료하였다면 이제 연동을 위한 SAML APP 설정이 시작됩니다.

Step 2: 인증연동을 위한 SAML APP 추가 및 설정

1. 메뉴에서 **Applications > Applications** 로 이동합니다.
2. **Browse App Catalog** 메뉴에서 Genians ZTNA application을 검색하세요.
3. 검색된 ZTNA앱을 선택한 후 **Add Integration** 버튼을 클릭하여 추가합니다.
4. Application label을 입력합니다.
5. **Base URL** 입력란에 ZTNA 정책서버의 URL을 아래의 예시처럼 입력합니다.
   - ex) https://test.genians.net/cwp2
6. Sign On 탭을 선택하세요.
7. 화면 중간에 **Settings > Sign on methods > SAML 2.0 > More details** 버튼을 클릭하여 IdP 정보를 확인합니다.
8. Genian ZTNA **Web콘솔 > 설정 > 사용자인증 > 인증연동 > SAML2 인증연동** 에 다음 각 항목의 값을 okta에서 복사해서 입력하십시오.
   - **IdP SSO URL** - okta의 **Sign on URL**.
   - **IdP Entity ID** - okta의 **Issuer**.
   - **x509 Certificate** - okta의 **Signing Certificate** 를 다운로드해서 파일 내용을 복사하여 입력하십시오.
9. JIT provisioning 기능을 사용할려면 ZTNA에서 **JIT provisioning** 을 'On'으로 변경하십시오.
   - ZTNA UI의 **JIT provisioning > 추가정보** 에서 추가 버튼을 클릭해서 사용자 계정의 이름, 이메일을 설정하십시오.
     - 이름에 **{lastName}{firstName}** 입력하십시오.
     - 이메일에 **email** 을 입력하십시오.

    * SAML Attributes (firstName, lastName, email) 항목은 okta에 이미 사전 정의 되어 있습니다.
    * 사전 정의된 속성 이외의 속성도 **Attributes (Optional)** 메뉴를 이용해서 추가가 가능합니다.

10. Single Logout(SLO)를 사용할려면 ZTNA에서 **Single Logout(SLO)** 설정을 'On' 하십시오.
    - okta의 Sign on > Settings 에서 **Enable Single Logout** 항목을 체크하십시오.
    - ZTNA의 SP X.509 certificate 를 다운로드해서 okta의 Signature Certificate 에 업로드 하십시오. SLO 기능을 사용하기 위해서는 SP의 인증서가 필요합니다.
    - ZTNA의 **IdP SLO URL** - okta의 **Single Logout URL** 을 복사해서 입력하십시오..
      – okta 화면에서 **Single Logout URL** 이 보이지 않는 경우 **Enable Single Logout** 설정이 체크된 상태에서 **Save** 버튼을 클릭해서 저장하시기 바랍니다.
      – 다시 Sign On 탭으로 돌아와서 **Single Logout URL** 을 확인하십시오.
11. Signed Requests를 사용할려면 **Signed Requests** 설정을 'On' 하십시오.
    - Signed Requests의 경우 okta의 **Applications > Create App Integration** 을 통해 SAML 설정을 해야 기능을 사용할 수 있습니다.
    - SP X.509 certificate 를 다운로드해서 okta의 Signature Certificate 에 업로드 하십시오. Signed Requests 기능을 사용하기 위해서는 SP의 인증서가 필요합니다.
    - okta의 SAML Settings에서 Signed Requests를 체크하시기 바랍니다.
12. Genian ZTNA CWP 인증 화면에서 표시할 okta 인증버튼에 표시할 문구를 **로그인 버튼 문구** 에 입력합니다.
13. Genian ZTNA Web 콘솔 설정 화면 하단 **수정** 버튼을 클릭합니다.

Note: Sign On tab의 Base URL 필드에 올바른 값을 입력했는지 확인하세요. 잘못된 값을 사용하면 SAML을 통해 ZTNA로 인증할 수 없습니다. ex) https://test.genians.net/cwp2

Step 3: okta 인증연동에 사용할 계정 추가 및 할당

이미 사용자가 등록되어 있다면 5번으로 이동

1. okta 콘솔 화면 메뉴 **Directory > Groups** 으로 이동합니다.
2. 화면 중간 **Add Group** 버튼을 클릭하여 그룹을 생성합니다.
3. okta 콘솔 화면 메뉴 **Directory > People** 으로 이동합니다.
4. 화면 중간 **Add Person** 버튼을 클릭하여 사용자를 추가합니다.

   Note: Password 항목은 관리자가 패스워드를 지정하여 생성할지 사용자 최초로그인시 변경하도록 할지 선택합니다.

   ---

5. okta 콘솔 화면 메뉴 **Application > Application** 으로 이동합니다.
6. 위에서 등록한 APP 우측 삼각형아이콘을 클릭하여 **Assign to Users** 를 클릭합니다.
7. 팝업 화면에서 APP을 통하여 인증연동에 사용할 계정의 우측 **Assign** 버튼을 클릭하여 APP에 할당해줍니다.

인증연동 테스트 방법

okta My Apps 페이지에서 테스트 하는 방법 (IdP-initiated SSO)

1. okta My Apps 페이지에 접속하여 생성한 ZTNA SAML App을 클릭합니다.

App Embed Link 사용방법 (IdP-initiated SSO)

1. okta의 General tab 화면 아래쪽으로 이동하면 **App Embed Link** 를 제공합니다.
2. 해당 링크를 통해 ZTNA에 로그인할 수 있습니다.

Genian ZTNA Web콘솔에서 테스트하는 방법 (SP-initiated SSO)

1. Web콘솔에 접속하여 **설정 > 사용자인증 > 인증연동 > 인증테스트** 항목에 **테스트** 버튼을 클릭합니다.
2. 팝업창에서 인증정보 저장소를 **SAML2** 를 선택합니다.
3. 새로운 팝업창에 okta 인증페이지가 표시되며 사용자명, 암호를 입력하여 인증합니다.
4. '인증에 성공하였습니다.' 메시지가 표시되면 정상적으로 인증연동이 되었습니다.

Genian ZTNA CWP 페이지에서 테스트하는 방법 (SP-initiated SSO)

1. Genian ZTNA 노드정책 비밀번호 정책을 할당 받은 단말(노드)를 준비합니다.
2. Genian ZTNA CWP페이지에 접속합니다.
3. CWP페이지에 **인증** 버튼을 클릭합니다.
4. 인증 화면에 위 Step2 5번 항목에서 설정한 인증버튼을 클릭합니다.
5. 새로운 팝업창에 okta 인증페이지가 표시되며 사용자명, 암호를 입력하여 인증합니다.

Single Logout (SLO) 테스트하는 방법

1. SLO 기능을 사용하도록 설정합니다.
2. SSO 기능을 이용해서 인증을 합니다.
3. CWP 페이지 상단의 로그아웃 버튼을 이용해서 로그아웃을 합니다.
4. 다시 SAML 인증을 시도할 때 okta의 계정정보를 입력하라고 표시되면 정상적으로 SLO가 동작한 것입니다.

Note: 인증연동 설정 후 정책적용시 제어정책 권한에 okta IdP 도메인을 추가해주어야 차단상태에서도 인증연동 창이 표시됩니다.

```
1. 권한 추가 방법
2. 정책 > 객체 > 네트워크
3. 작업선택 > 생성
4. 기본정보 입력
5. 네트워크주소 > FQDN 선택 > IdP 도메인 입력(e.g. genians.okta.com)
6. 생성 클릭
7. 권한 메뉴로 이동
8. 생성한 네트워크객체를 이용하여 권한 생성
9. 단말 네트워크를 제어하는 제어정책에 생성한 권한 할당
```

okta (SAML2.0) - Web 콘솔

본 가이드는 okta 와 네트워크 접근제어 시스템인 Genian ZTNA의 인증연동 기능을 수행하기 위한 설정 방법을 안내합니다.

관리자 인증을 위해 Genian ZTNA Web 콘솔 페이지에서 SAML2.0 프로토콜을 이용하여 okta인증을 호출하고 okta에서 사용자인증여부를 확인하여 정상적인 SSO가 이루어집니다.

권장버전

제품명(구성요소)	버전	비고
Genian ZTNA(정책서버)	V6.0 이상	2022.05 이후 Release 버전
okta APP	SAML2.0	2021.05 현재 연동가능

연동 전 필요한 사항

연동의 목적

Genian ZTNA와 okta 연동은 다음의 효과를 제공합니다.

- ZTNA, okta 개별 인증을 위한 사용자 DB 관리가 필요하지 않습니다.
- okta 계정을 이용하여 SSO로 ZTNA를 인증할 수 있습니다.

지원되는 기능

okta SAML App 연동은 다음과 같은 기능을 지원합니다:

- SP-initiated SSO
- IdP-initiated SSO
- JIT (Just-In-Time) Provisioning
- Single Logout (SLO)
- Signed Requests

위 기능에 대한 자세한 정보는 , https://help.okta.com/okta_help.htm?type=oie&id=ext_glossary 에서 확인하세요.

연동 설정 방법

본 가이드에서 다루는 Genian ZTNA와 okta 설정 방법은 연동을 위한 필수 항목만을 안내합니다. 최초 1회 설정 이후 자동으로 적용됩니다.

Step 1: okta 연동을 위한 계정등록

1. https://www.okta.com/free-trial/ 접속하여 트라이얼 계정을 신청합니다.
   - 사용자 정보와 국가를 선택합니다.
2. 신청한 메일주소로 수신된 인증확인 메일을 확인합니다.
   - 신청한 메일주소로 'Activate your okta account' 라는 제목으로 계정정보 확인 메일이 발송됩니다.
3. 메일 내 'Activate okta Accout' 버튼을 클릭하여 계정을 활성화 하십시오.
   - 인증을 위한 초기 패스워드 변경과 2차 인증에 대한 설정을 합니다.
   - okta 콘솔접속시 OTP 2factor 인증을 요구하며 아이폰, 안드로이드 OTP 앱 설치 및 OTP 등록이 필요합니다.
   - OTP 등록과 로그인을 완료하였다면 이제 연동을 위한 SAML APP 설정이 시작됩니다.

Step 2: 인증연동을 위한 SAML APP 추가 및 설정

1. 메뉴에서 **Applications > Applications** 로 이동합니다.
2. **Browse App Catalog** 메뉴에서 Genians ZTNA application을 검색하세요.
3. 검색된 ZTNA앱 선택한 후 **Add Integration** 버튼을 클릭하여 추가합니다.
4. **Application label을 입력합니다.**
   1. **Base URL** 입력란에 ZTNA 정책서버의 URL을 아래의 예시처럼 입력합니다.
   - ex) https://test.genians.net/mc2
5. Sign On 탭을 선택하세요.
6. 화면 중간에 **Settings > Sign on methods > SAML 2.0 > More details** 버튼을 클릭하여 IdP 정보를 확인합니다.
7. Genian ZTNA **Web콘솔 > 설정 > 환경설정 > 관리콘솔 > SAML2 인증 > IdP** 에 다음 각 항목의 값을 okta에서 복사해서 입력하십시오.
   - **IdP SSO URL** - okta의 **Sign on URL**.
   - **IdP Entity ID** - okta의 **Issuer**.
   - **x509 Certificate** - okta의 **Signing Certificate** 를 다운로드해서 파일 내용을 복사하여 입력하십시오.
8. JIT provisioning 기능을 사용할려면 ZTNA에서 **JIT provisioning** 을 'On'으로 변경하십시오.
   - ZTNA UI의 **JIT provisioning > 추가정보** 에서 추가 버튼을 클릭해서 사용자 계정의 이름, 이메일을 설정하십시오.
     - 이름에 **{lastName}{firstName}** 입력하십시오.
     - 이메일에 **email** 을 입력하십시오.
       * SAML Attributes (firstName, lastName, email) 항목은 okta에 이미 사전 정의 되어 있습니다.
       * 사전 정의된 속성 이외의 속성도 **Attributes (Optional)** 메뉴를 이용해서 추가가 가능합니다.
   - ZTNA UI의 **JIT provisioning > 관리자 관리역할** 에서 추가 버튼을 클릭해서 관리역할을 추가 하십시오.

  - okta의 Configured SAML Attributes 항목에 설정되어 있는 이름 **_ADMINROLE_superAdmin** 을 입력하시기 바랍니다.
  - 다른 관리 역할을 추가할려면 okta의 **Attributes (Optional)** 클릭해서 Group Attribute Statements를 통해 다른 역할 Group을 설정해야 합니다.
  - JIT provisioning 기능을 사용하기 위해서 Group Attributes를 설정해야 합니다.
    * 아래의 예와 같이 Name에 _ADMINROLE_ prefix를 붙여서 지정해야 합니다.
    * Configured SAML Attributes 항목에 _ADMINROLE_superAdmin가 이미 사전 설정되어 있습니다. superAdmin 역할을 하는 Group을 아래와 같이 설정하면 됩니다.

Name	Filter
_ADMINROLE_superAdmin	Equals superAdmin

    * Group 이름은 아래의 Step 3 **Add Group** 설명을 참고하여 작성하시기 바랍니다.

9. Single Logout(SLO)를 사용할려면 ZTNA에서 **Single Logout(SLO)** 설정을 'On' 하십시오.
   - okta의 Sign on > Settings 에서 **Enable Single Logout** 항목을 체크하십시오.
   - ZTNA의 SP X.509 certificate 를 다운로드해서 okta의 Signature Certificate 에 업로드 하십시오. SLO 기능을 사용하기 위해서는 SP의 인증서가 필요합니다.
   - ZTNA의 **IdP SLO URL** - okta의 **Single Logout URL** 을 복사해서 입력하십시오.
     - okta 화면에서 **Single Logout URL** 이 보이지 않는 경우 **Enable Single Logout** 설정이 체크된 상태에서 **Save** 버튼을 클릭해서 저장하시기 바랍니다.
     - 다시 Sign On 탭으로 돌아와서 **Single Logout URL** 을 확인하십시오.
10. Signed Requests를 사용할려면 **Signed Requests** 설정을 'On' 하십시오.
    - Signed Requests의 경우 okta의 **Applications > Create App Integration** 을 통해 SAML 설정을 해야 기능을 사용할 수 있습니다.
    - SP X.509 certificate 를 다운로드해서 okta의 Signature Certificate 에 업로드 하십시오. Signed Requests 기능을 사용하기 위해서는 SP의 인증서가 필요합니다.
    - okta의 SAML Settings에서 Signed Requests를 체크하시기 바랍니다.
11. Genian ZTNA Web 콘솔 인증 화면에서 표시할 okta 인증버튼에 표시할 문구를 **로그인 버튼 문구** 에 입력합니다.
12. Genian ZTNA Web 콘솔 설정 화면 하단 **수정** 버튼을 클릭합니다.

Note: Sign On tab의 Base URL 필드에 올바른 값을 입력했는지 확인하세요. 잘못된 값을 사용하면 SAML을 통해 ZTNA로 인증할 수 없습니다. ex) https://test.genians.net/mc2

Step 3: okta 인증연동에 사용할 계정 추가 및 할당

이미 사용자가 등록되어 있다면 5번으로 이동

1. okta 콘솔 화면 메뉴 **Directory > Groups** 으로 이동합니다.
2. 화면 중간 **Add Group** 버튼을 클릭하여 그룹을 생성합니다.
   - JIT provisioning 기능을 위해서는 관리자 Role Group을 생성해야 합니다. (예) superAdmin)
   - Group 이름은 ZTNA에서 사용되는 관리역할 ID와 동일(대소문자 구분함.)하게 생성해야 합니다. 아래 표를 참고하세요.

ID	설명
superAdmin	수퍼 관리자
audit	감사 관리자

     설정 > 사용자 인증 > 관리역할에서 ZTNA에서 제공하는 모든 관리역할을 확인할 수 있습니다.
3. okta 콘솔 화면 메뉴 **Directory > People** 으로 이동합니다.
4. 화면 중간 **Add Person** 버튼을 클릭하여 사용자를 추가합니다.
   - JIT provisioning이 필요한 사용자의 경우는 2번에서 생성한 Group을 선택해야 한다.

Note: Password 항목은 관리자가 패스워드를 지정하여 생성할지 사용자 최초로그인시 변경하도록 할지 선택합니다.

---

5. okta 콘솔화면 메뉴 **Application > Application** 으로 이동합니다.
6. 위에서 등록한 APP 우측 삼각형아이콘을 클릭하여 **Assign to Users** 를 클릭합니다.
7. 팝업 화면에서 APP을 통하여 인증연동에 사용할 계정의 우측 **Assign** 버튼을 클릭하여 APP에 할당해줍니다.

인증연동 테스트 방법

okta My Apps 페이지에서 테스트 하는 방법 (IdP-initiated SSO)

1. okta My Apps 페이지에 접속하여 생성한 ZTNA SAML App을 클릭한다.

App Embed Link 사용방법 (IdP-initiated SSO)

1. okta의 General tab 화면 아래쪽으로 이동하면 **App Embed Link** 를 제공합니다.
2. 해당 링크를 통해 ZTNA에 로그인할 수 있습니다.

Genian ZTNA Web 콘솔 페이지에서 테스트하는 방법 (SP-initiated SSO)

1. Genian ZTNA Web 콘솔 페이지에 접속합니다.
2. **SAML 로그인** 버튼을 클릭합니다.
3. 인증 화면에 위 Step2 5번 항목에서 설정한 인증버튼을 클릭합니다.
4. 새로운 팝업창에 okta 인증페이지가 표시되며 사용자명, 암호를 입력하여 인증합니다.

Single Logout (SLO) 테스트하는 방법

1. SLO 기능을 사용하도록 설정합니다.

2. SSO 기능을 이용해서 인증을 합니다.
3. Web 콘솔 상단의 로그아웃 버튼을 이용해서 로그아웃을 합니다.
4. 다시 SAML 인증을 시도할 때 okta의 계정정보를 입력하라고 표시되면 정상적으로 SLO가 동작한 것입니다.

Note: 인증연동 설정 후 정책적용시 제어정책 권한에 okta IdP 도메인을 추가해주어야 차단상태에서도 인증연동 창이 표시됩니다.

1. 권한 추가 방법
2. 정책 > 객체 > 네트워크
3. 작업선택 > 생성
4. 기본정보 입력
5. 네트워크주소 > FQDN 선택 > IdP 도메인 입력(e.g. genians.okta.com)
6. 생성 클릭
7. 권한 메뉴로 이동
8. 생성한 네트워크객체를 이용하여 권한 생성
9. 단말 네트워크를 제어하는 제어정책에 생성한 권한 할당

7.3.7 인증 연동 테스트

RADIUS, **LDAP**, **IMAP**, **POP3** 또는 **SMTP** 의 연동 구성을 테스트하여 성공적인 연결을 확인 할 수 있습니다.

1. 왼쪽 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자 인증 > 인증연동** 으로 이동합니다.
3. 메인창에서 **인증 테스트** 을 찾습니다.
4. 설정을 변경한 경우 **수정** 을 클릭합니다.
5. **테스트** 를 클릭하여 변경한 설정에 대해 테스트합니다.

7.4 외부 사용자 정보 동기화

고객사에서 사용중인 계정시스템과 동기화 하여 계정정보 이외에 사용자의 부서, 직책, 전자메일 등의 추가 사용자 정보를 수집할 수 있습니다. 이러한 정보들을 활용해서 사용자 그룹을 만들고 사용자 그룹을 이용한 노드그룹을 생성할 수 있습니다. ZTNA는 RDBMS, LDAP, CSV, Google G Suite, REST API Server 등 다양한 외부시스템을 지원합니다.

7.4.1 RDBMS

Note: 이 기능을 사용하려면 Enterprise Edition이 필요합니다.

사용자 디렉토리를 RDBMS(Relational Database Management System: 관계형 데이터베이스 관리 시스템) 와 동기화 할 수 있습니다. RDBMS는 관계 모델을 기반으로 하는 데이터베이스 시스템입니다.

접속 테스트 하기

접속 테스트가 가능한 데이터베이스 종류는 다음과 같습니다.

지원가능한 동기화 서버유형	항목	접속 테스트
관계형 데이터베이스	Oracle Database	O
	MYSQL	O
	MSSQL/Sybase	O
	IBM DB2	O
	Tibero	O
	Altibase	O
	CUBRID	O

Note: **정책서버** 와 **동기화 서버** 간 정상적인 통신 여부를 우선적으로 확인하여 접속 테스트를 사전에 수행하시기 바랍니다.

동기화 설정하기

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자인증 > 정보 동기화** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 메인창에서 **기본설정** 메뉴를 찾습니다.
5. **동기화 수행주기** 및 **수행 옵션** 을 설정합니다.
6. 메인창에서 **상세설정 > DB타입** 메뉴를 찾습니다. 데이터를 읽어올 **데이터베이스 타입** 을 선택 해 입력 정보를 설정합니다.
7. 메인창에서 **상세설정 > 사용자정보, 부서정보, 직급정보, 노드정보, 장비수명주기정보** 항목들을 찾아 필요한 정보들을 추가합니다.(*CSV*를 사용할 경우 비워 둡니다).
8. **생성** 버튼을 클릭합니다.
9. **정보 동기화** 목록에서 동기화하고자 하는 항목을 선택합니다.
10. **작업선택 > 즉시수행** 을 클릭합니다.

7.4.2 LDAP (Active Directory)

Genian ZTNA는 LDAP 디렉토리를 사용자 및 조직 정보의 소스로 사용할 수 있습니다. LDAP 동기화를 통해 사용자 계정을 로컬에서 생성하여 관리 또는 정책에 사용 할 수 있습니다. LDAP 동기화는 일반적으로 Microsoft AD(Active Directory) 시스템에서 사용됩니다.

다음은 AD를 기반으로 사용자 및 조직 정보를 동기화하는 방법에 대해 설명합니다.

접속 테스트 하기

접속 테스트를 수행하기 위해서는 다음에 기본값이 입력되어야 합니다.

항목	설정값	설명
LDAP	DB Server	LDAP 서버 IP를 입력합니다.
	DB PORT	LDAP 서버 접속 포트를 입력합니다.
		SSL OFF : 389
		SSL ON : 636
	SSL 접속	SSL 접속 유무를 설정합니다.
	DB USER	Bind DN을 입력합니다.
	DB PASSWORD	Bind Password를 입력합니다.
	데이터소스 구분값	다수의 동기화 서버 사용 시 설정합니다.

Note: 접속 테스트가 정상적으로 되지 않을 경우 **정책서버** 와 **동기화 서버** 간 정상적인 통신 여부를 우선적으로 확인하시기 바랍니다.

동기화 설정하기

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자인증 > 정보 동기화** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.

기본설정 옵션

1. **ID** : 고유의 이름을 입력합니다.
2. **동기화 수행주기** : 동기화에 대해 지정된 시간 또는주기적인 간격을 선택합니다.
3. **정책적용여부** : 동기화 후 변경사항 반영을 위해 적용함 을 선택합니다 . 동기화 설정이 여러 개인 경우 적용안함 으로 설정하고 마지막 동기화만 사용하도록 설정 할 수 있습니다.

데이터베이스 옵션

1. **DB타입** : `LDAP`
2. **DB SERVER** : Active Directory 서버의 IP 주소 또는 FQDN 을 입력합니다.
3. **DB PORT**: AD의 LDAP 서비스 포트를 입력합니다. 기본 LDAP 포트는 `389` 입니다. LDAPS(LDAP over SSL)를 사용하는 경우 기본 포트는 `636` 입니다.
4. **SSL 접속** : LDAPS를 사용할 경우``On`` 을 선택합니다.
5. **DB USER** : Active Directory의 Bind DN을 입력합니다. 일반적으로 `administrator@company.com` 과 같은 이메일 형식을 사용할 수 있습니다.
6. **DB PASSWORD** : Bind DN 사용자 비밀번호를 입력합니다.

사용자정보 옵션

1. **사용자테이블명** : 사용자의 기본 고유 이름(DN)을 입력합니다. 보통은, `CN=Users,DC=company, DC=com` 입니다.
2. **사용자조건문** : 사람 객체를 필터링하기 위해 `(&(objectClass=user)(objectCategory=person))` 를 입력합니다.
3. **사용자ID컬럼명** : `sAMAccountName` 을 입력합니다.

4. **사용자이름컬럼명** : `displayName` 을 입력합니다.
5. **부서ID컬럼명** : `$distinguishedName, IF(LOCATE('OU=',$)>0,SUBSTRING($,LOCATE(',',$)+1),'')` 를 입력합니다.
6. 기타 추가 정보는 각 컬럼 이름에 LDAP 속성 이름을 사용할 수 있습니다.

부서정보 옵션

1. **Table Name** : OU(OrganizationUnit)의 기본 고유 이름(DN)을 입력합니다. 일반적으로 `DC=company, DC=com` 입니다.
2. **부서조건문** : OU 객체를 필터링 하려면 `objectClass=organizationalUnit` 를 입력합니다.
3. **출력정렬순서** : 부서명을 기준으로 출력하기 위해 `@NAMEPATH` 을 입력합니다.
4. **부서ID컬럼명** : `distinguishedName` 을 입력합니다.
5. **부서이름컬럼명** : `name` 을 입력합니다.
6. **상위부서컬럼명** : `$distinguishedName, SUBSTRING($,LOCATE(',',$)+1)` 을 입력합니다.
7. **생성** 버튼을 클릭합니다.

Attention: Active Directory는 userPassword 속성을 제공하지 않으므로 사용자 비밀번호를 동기화할 수 없습니다. 따라서 별도의 연동을 설정해야합니다. *LDAP (Active Directory) 서버 연동* 을 참조합니다.

7.4.3 CSV 파일 또는 URL

Note: 이 기능을 사용하려면 Enterprise Edition 이 필요합니다.

CSV(Comma-Separated Value) 파일에서 최종 사용자 정보를 가져 와서 정책 서버에 사용자를 추가 할 수 있습니다.

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자인증 > 정보 동기화** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. 메인창에서 **기본설정** 메뉴를 찾습니다.
5. **동기화 수행주기** 및 **수행옵션** 을 설정합니다.
6. 메인창에서 **상세설정 > 외부 DB 유형** 을 찾아 **CSV** 를 선택합니다.
7. 메인창에서 **상세설정 > (사용자, 부석, 직급, 노드, 및 장비수명주기)** 항목들을 찾아 필요한 정보를 추가합니다. (*CSV*를 사용할 경우 비워 둡니다)
8. **정보 동기화** 리스트에서 원하는 동기화 목록의 **체크박스** 를 클릭합니다.
9. **작업선택 > 즉시수행** 을 클릭합니다.

7.4.4 Google G Suite

Genian ZTNA는 G Suite 디렉토리를 사용자 및 조직 정보의 소스로 사용할 수 있습니다. G Suite 동기화를 통해 사용자 계정을 로컬에서 생성하여 관리 또는 정책에 사용 할 수 있습니다.

다음은 G Suite를 기반으로 사용자 및 조직 정보를 동기화하는 방법에 대해 설명합니다.

접속 테스트 하기

접속 테스트를 수행하기 위해서는 다음에 기본값이 입력되어야 합니다.

항목	설정값	설명
Google G Suite	코드 발급	구글 계정에 OAuth2 인증코드를 발급합니다.
	구글 인증 코드	OAuth2에서 발급받은 인증코드를 입력합니다.
	DOMAIN	계정정보를 가져올 도메인을 입력합니다.
	VIEW TYPE	데이터를 읽어올 필드를 지정합니다.
		admin_view : 관리자 권한
		domian_public : 공개 권한
	데이터소스 구분값	다수의 동기화 서버 사용 시 설정합니다.

Note: 접속 테스트가 정상적으로 되지 않을 경우 **정책서버** 와 **동기화 서버** 간 정상적인 통신 여부를 우선적으로 확인하시기 바랍니다.

동기화 설정하기

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자인증 > 정보 동기화** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.

기본설정 옵션

1. **ID** : 고유의 이름을 입력합니다.
2. **동기화 수행주기** : 동기화에 대해 지정된 시간 또는 주기적인 간격을 선택합니다.
3. **정책적용여부** : 동기화 후 변경사항 반영을 위해 적용함 을 선택합니다. 동기화 설정이 여러 개인 경우 적용안함 으로 설정하고 마지막 동기화만 사용하도록 설정 할 수 있습니다.

데이터베이스 옵션

1. **DB타입** : `Google G Suite`
2. **구글 인증 코드** : 동기화 수행 계정 인증을 위한 코드를 입력합니다. 상단의 구글 인증 코드 발급 버튼을 클릭하고, 팝업창에서 계정 로그인 및 권한 허용 버튼 클릭 후 출력되는 코드를 복사하여 입력합니다.
3. **DOMAIN**: 도메인 입력시 해당 도메인의 정보만 동기화합니다. 미입력시 계정이 속한 모든 도메인에 대한 정보를 동기화합니다.
4. **VIEW TYPE** : 권한에 따른 데이터 동기화 범위를 선택합니다다. 일반적으로 admin 권한의 계정인 경우 `admin_view` 를, 그렇지 않은 경우 `domain_public` 을 선택합니다.

사용자정보 옵션

1. **사용자테이블명** : `users` 을 입력합니다.

2. **사용자ID컬럼명** : `primaryEmail` 을 입력합니다.
3. **사용자이름컬럼명** : `name/fullName` 을 입력합니다.
4. **부서ID컬럼명** : `orgUnitPath` 을 입력합니다.

부서정보 옵션

1. **Table Name** : `orgunits` 을 입력합니다.
2. **출력정렬순서** : 부서명을 기준으로 출력하기 위해 `@NAMEPATH` 을 입력합니다.
3. **부서ID컬럼명** : `orgUnitId` 을 입력합니다.
4. **부서이름컬럼명** : `name` 을 입력합니다.
5. **상위부서컬럼명** : `parentOrgUnitId` 을 입력합니다.
6. **생성** 버튼을 클릭합니다.

Attention: G Suite는 API 사용시 password 속성을 제공하지 않으므로 사용자 비밀번호를 동기화할 수 없습니다. 따라서 별도의 연동을 설정해야합니다. 외부 인증서버 설정 의 `SAML 2.0` 을 참조합니다.

7.4.5 REST API Server

Genian ZTNA는 REST API Server를 사용자 및 조직 정보의 소스로 사용할 수 있습니다.

REST API Server 동기화를 통해 사용자 계정을 로컬에서 생성하여 관리 또는 정책에 사용 할 수 있습니다.

REST API Server 요청은 HTTP GET 방식을 사용하여 호출하며, 응답데이터형식은 JSON Object 형식이어야 합니다.

slack 에서 사용자정보는 users.list API를 통해서 가져올 수 있습니다. Method URL 은 https://slack.com/api/users.list 이며 요청은 GET 과 POST 방식을 지원합니다.

ZTNA 에서 REST API 정보는 Swagger를 통해 제공합니다. 참고 - *API* 활용도구 제공: *Swagger*

REST API 의 상세 내용은 *API* 가이드 를 통해 확인할 수 있습니다.

접속 테스트 하기

접속 테스트를 수행하기 위해서는 다음에 기본값이 입력되어야 합니다.

항목	설정값	설명
REST API Server	서버주소	REST API를 호출할 서버 IP를 입력합니다.
	페이지 파라미터 이름	다수의 출력값을 처리할 페이지 파라미터 이름을 설정합니다.
	페이지 시작번호	페이지 시작번호를 설정합니다.
	페이지 사이즈 파라미터 이름	한 페이지에 출력할 갯수를 지정하는 파라미터 이름을 설정합니다.
	페이지 사이즈	한 페이지에 출력할 갯수를 설정합니다.
	데이터소스 구분값	다수의 동기화 서버 사용 시 설정합니다.

Note: 접속 테스트가 정상적으로 되지 않을 경우 **정책서버** 와 **동기화 서버** 간 정상적인 통신 여부를 우선적으로 확인하시기 바랍니다.

동기화 설정하기

1. 상단 항목의 **설정** 으로 이동합니다.
2. 왼쪽 설정 항목에서 **사용자인증 > 정보 동기화** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.

기본설정 옵션

1. **ID** : 고유의 이름을 입력합니다.
2. **동기화 수행주기** : 동기화에 대해 지정된 시간 또는주기적인 간격을 선택합니다.
3. **정책적용여부** : 동기화 후 변경사항 반영을 위해 적용함 을 선택합니다 . 동기화 설정이 여러 개인 경우 적용안함 으로 설정하고 마지막 동기화만 사용하도록 설정 할 수 있습니다.

데이터베이스 옵션

- DB타입은 REST API Server 를 선택하고, 사용하고 있는 서버주소를 입력합니다.
  - 예) slack의 경우 https://slack.com, ZTNA의 경우 https://(정책서버IP):8443
- 페이징은 지원하지 않으므로 페이징관련 설정은 입력하지 않습니다.

1. **DB타입** : `REST API Server`
2. **서버주소** : REST API Server의 주소를 입력합니다.
3. **페이지 파라미터이름** : 서버측 페이징을 통해서 정보를 가져오는 경우 페이지번호를 의미하는 파라미터 이름을 입력합니다.
4. **페이지 시작번호**: 서버측 페이징을 통해서 정보를 가져오는 경우 페이지 시작번호를 입력합니다.
5. **페이지사이즈 파라미터이름** : 서버측 페이징을 통해서 정보를 가져오는 경우 페이지당 가져오는 데이터 수를 의미하는 파라미터 이름을 입력합니다.
6. **페이지사이즈** : 서버측 페이징을 통해서 정보를 가져오는 경우 페이지당 가져오는 데이터수를 입력합니다.
7. **데이터소스 구분값** : 데이터소스 구분값은 동기화 한 사용자 정보의 출처 식별을 위한 값입니다.

사용자정보 옵션

- 사용자정보출처를 입력할 때 상호인증을 API Key를 활용 한다면 /api/users.list?token=<API Token> 를 입력하거나, API 서비스 계정을 활용 한다면 /api/users.list 만 입력합니다. 자세한 내용은 *API* 활용을 위한 상호 인증 방법 을 참고하시기 바랍니다.
- 컬럼명은 JSON Object에서 값을 추출하기 위한 경로를 입력합니다. 경로는 . 으로 구분합니다.
  - 예) JSON Response [{ "id": "..", "name": ".." }, { "id": "..", "name": ".." }] 인 경우에 ID컬럼명은 id, 이름컬럼명은 name 을 입력합니다.
  - 예) JSON Response { "users": { "members" : [{ "id": "..", "name": ".." }, { "id": "..", "name": ".." }] } } 인 경우에 ID컬럼명은 users.members.id, 이름컬럼명은 users.members.name 을 입력합니다.

1. **사용자정보출처** : 사용자정보동기화를 위한 URI 정보를 입력합니다. 입력된 URI설정은 서버주소 뒤에 경로명으로 추가됩니다.(예. /api/users.list 를 입력한 경우에 https://slack.com/api/users.list 를 호출합니다.)
2. **사용자조건문** : 사용안함.
3. **사용자ID컬럼명** : JSON Object에서 사용자 ID 값의 경로를 입력합니다.(예. users.id)
4. **사용자이름컬럼명** : JSON Object에서 이름 값의 경로를 입력합니다.(예. users.name)
5. **부서ID컬럼명** : JSON Object에서 부서 ID 값의 경로를 입력합니다.(예. users.department_id)

6. 기타 추가 정보는 JSON Object에서 값의 경로를 입력합니다.

Attention: 그외 부서, 직급, 노드, 장비수명 정보 옵션 설정은 사용자정보 옵션과 동일한 방식으로 설정 사용할 수 있습니다.

7.5 사용자 인증 옵션 설정

7.5.1 일반 옵션

인증 기준, 장비 소유권, 로그온 복구 및 제한에 대한 일반 옵션은 **설정 > 사용자 인증 > 사용자 인증** 에서 찾을 수 있습니다.

옵션 종류

- **인증범위**
  - 노드(MAC+IP) or 장비(MAC)
- **인증허용 IP**
  - 사용자 최초 인증된 단말의 IP를 인증허용 IP로 자동설정 하는 옵션입니다.
  - 사용자계정에 인증허용 IP가 존재하지 않을때 사용가능합니다.
- **인증허용 MAC**
  - 사용자 최초 인증된 단말의 MAC을 인증허용 MAC으로 자동설정 하는 옵션입니다.
  - 사용자계정에 인증허용 MAC이 존재하지 않을때 사용가능합니다.
- **소유자 설정**
  - 사용자 인증시 IP또는 장비의 소유자, 소유자 부서정보를 자동 설정하는 옵션입니다.
- **사용자 ID 정규식 적용**
  - 인증하는 사용자계정을 정규식 패턴형태로 치환하여 인증처리하는 옵션입니다.
- **사용자인증시 ID 보호**
  - 사용자 인증시 ID를 마스킹 처리하여 표시합니다.
- **로그아웃 사용**
  - 사용자가 직접 에이전트와 CWP페이지에서 로그아웃 허용여부를 설정하는 옵션입니다.
- **아이디/비밀번호 찾기**
  - 아이디나 비밀번호 분실시 찾기기능 사용여부를 위한 옵션입니다.
- **인증코드 유효시간**
  - 아이디나 비밀번호 찾기사용시 전송되는 SMS의 유효시간 설정 옵션입니다.
- **사용자 인증정보 표시**
  - 에이전트 메뉴와 CWP화면에서 인증된 사용자의 정보를 표시하는 옵션입니다.
- **사용자정보 노드반영**

  - 사용자등록신청서가 승인될때 신청PC의 노드정보에 사용자정보(이름, 설명)을 반영하는 옵션입니다.

7.5.2 개별노드에 인증옵션 설정 방법

1. 노드리스트에서 노드의 IP를 클릭하고 정책탭을 선택
2. 노드(IP+MAC) 정책에서 사용자인증정책으로 이동

옵션 종류

- 사용자인증을 노드정책기준으로 설정
- 모든사용자를 인증할 수 있도록 설정
- 지정한 사용자만 인증할 수 있도록 설정

7.5.3 그룹별 인증정책 설정 방법

노드의 인증정책은 특정 그룹의 노드가 인증 받는 시점과 방법을 결정합니다.

인증방법, 요구 사항, 시간 제한 및 로그온 절차에 대한 옵션을 구성하려면 **정책 > 노드 정책 > [정책이름]** 에서 노드 정책을 선택하고 **세부설정 > 인증정책** 에서 설정 가능합니다.

옵션 종류

- **인증 방법**
  - 호스트인증과 비밀번호 인증을 선택할 수 있습니다.
  - 비밀번호 인증은 허용할 인증 소스와 2팩터인증 사용 여부를 지정할 수 있습니다.
- **인증대체정보**
  - **Active Directory** AD서버 인증정보를 ZTNA인증정보로 대체합니다.
  - **연동 API** 에이전트 인증연동시 사용합니다.
  - **Genian API** 지니언스(주)에서 제공하는 API를 이용하여 서버 to 서버 인증연동시 사용합니다.
- **인증 사용자그룹**
  - 노드정책할 할당받은 노드중 인증을 허용할 사용자그룹을 설정합니다.
- **인증만료 자동 로그아웃**
  - 최초 인증시각 후 지정된 시간이 지나면 자동 로그아웃되도록 설정합니다.
- **미사용노드 자동로그아웃**
  - 노드가 다운되고 지정시간 후 자동로그아웃 처리되도록 설정합니다.
- **주기적 재인증**
  - 지정된 주기마다 인증해제하여 사용자가 재인증하도록 유도하는 설정입니다.
- **인증만료전알림**
  - 인증이 만료되기전 에이전트를 통하여 사용자에게 인증만료를 알리는 설정입니다.
- **사용자인증페이지**

  - 사용자가 인증하는 페이지가 별도로 있는경우 URL을 설정합니다.(미입력시 시스템 기본 인증 페이지가 표시됩니다.)

- **운영체제 시작시 재인증**
  - 시스템 재부팅, 절전모드 해제시 자동 로그아웃이 되고 재인증을 유도하는 설정입니다.
  - 절전모드는 **설정 > 환경설정 > 에이전트 > 절전모드 재시작 시간** 옵션에 따라 자동 로그아웃이 수행됩니다.
  - 인증 대체 정보를 사용할 경우 동작하지 않습니다.
- **사용자명 출력이름, 비밀번호 출력이름**
  - 사용자명과 비밀번호 입력란에 표시할 텍스트를 입력합니다.

7.6 사용자 계정 등록 시 정보 수집 동의 페이지 사용하기

Genian ZTNA 에서는 CWP 페이지를 통해 사용자 계정 등록 시 입력되는 개인정보에 대해서 정보수집에 대한 약관을 표시하고 사용자 동의를 받을 수 있습니다.

7.6.1 사용자 동의페이지 구성하기

사용자에게 표시할 동의페이지 내용을 설정합니다. 사용자 정보 페이지는 사용자에게 표시할 약관과 사용자에게 수집할 정보를 설정하는 수집정보 항목으로 나눠집니다.

1. 상단 패널 **설정** 항목으로 이동합니다.
2. 왼쪽 접속인증페이지에서 **동의페이지 > 사용자정보** 으로 이동합니다.
3. 작업선택에서 **생성** 을 클릭합니다.
4. **약관내용** 과 **수집정보** 를 할당 후 **생성** 을 클릭합니다.

7.6.2 사용자 계정 등록과 사용자 동의 페이지 설정하기

CWP 페이지에서 사용자 계정을 등록하기 위해서는 사용자 등록 기능을 설정해야 합니다.

1. 상단 패널 **정책** 항목으로 이동합니다.
2. 왼쪽 **노드정책** 으로 이동합니다.
3. 노드정책에 **ID** 를 클릭합니다.
4. **인증정책 항목** 에서 **사용자 등록페이지** 사용을 ON **사용자 동의 페이지** 사용을 ON으로 설정합니다.
5. **수정** 버튼을 클릭합니다.
6. 오른쪽 화면 상단의 **변경정책적용** 을 클릭합니다.

7.7 이메일을 통한 사용자 계정 승인하기

Genian ZTNA에서 사용자 계정에 대한 사용 승인을 관리자가 아닌 피방문자(사용자계정이 존재하는 대상)가 이메일을 사용하여 승인처리 할 수 있습니다.

신청된 사용자 계정에 대한 이메일을 통해 승인하는 방식을 사용하여 승인에 대한 권한을 관리자가 아닌 일반 사용자에게 부여하는 방식을 사용하여 관리자의 역할을 대행할 수 있습니다.

Note: 승인방법을 이메일로 사용하기 위해서는 메일연동과 일반 사용자 계정에 이메일 정보가 존재해야 합니다.

7.7.1 사용자 계정 신청서 용도 만들기

사용자 계정 신청서에 대한 승인방식을 이메일로 진행하며, 신청서에 대한 승인권한을 피방문자(사용자계정이 존재하는 대상)에게 부여하는 용도를 생성합니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **용도관리 > 사용자 용도** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. **옵션설정** 항목에서 **용도별 처리옵션 > 피방문자 이메일 승인** 설정값을 **ON** 으로 설정합니다.
5. **이메일 승인자** 항목에 설정값을 **피방문자** 로 설정합니다.
6. **생성** 버튼을 클릭합니다.

7.7.2 일반 사용자가 이메일을 통한 신청된 사용자 계정 승인하기

사용자 계정 신청 시 피방문자 이메일 승인이 가능한 용도를 지정해야 하며, 선택된 피방문자의 이메일을 통해 승인을 수행합니다.

1. 피방문자 계정에 이메일 서버에서 **승인 요청 이메일** 을 확인합니다.
2. 이메일에 **승인** 버튼을 클릭합니다.

7.8 사용자 계정 신청을 자동 승인하기

Genian ZTNA 사용자 계정에 대한 사용 승인을 관리자가 수동으로 승인하지 않고, 자동으로 승인되는 방식을 제공합니다.

게스트 사용자 계정에 대한 사용 승인을 관리자의 확인 없이 자동으로 수행하여 게스트 계정에 대한 사용 편의성을 높일 수 있습니다.

7.8.1 게스트 사용자 계정 신청 용도 만들기

Genian ZTNA에서 사용자 인증을 수행하기 위한 계정 생성 시 승인방식을 자동으로 설정하는 게스트 용도를 생성합니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **용도관리 > 사용자 용도** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. **옵션설정** 항목에서 **용도별 처리옵션 > 피방문자 이메일 승인** 설정값을 **OFF** 으로 설정합니다.
5. **자동승인** 항목에 설정값을 **ON** 로 설정합니다.
6. **생성** 버튼을 클릭합니다.

7.8.2 게스트 사용자 계정 생성 및 인증하기

사용자 계정 신청 시 게스트 사용자 용도를 선택하여 신청을 진행할 경우 신청완료 시 계정승인이 수행되어 신청된 계정이 활성화 됩니다.

1. CWP 페이지에서 **사용자 등록** 버튼을 클릭합니다.
2. **용도** 항목을 **게스트 사용자 용도** 로 선택합니다.
3. 사용자 계정 신청에 **필수사항** 을 입력합니다.
4. **등록** 버튼을 클릭합니다.
5. **처리 결과** 를 확인 후 **초기화면** 버튼을 클릭합니다.
6. **사용자 인증** 버튼을 클릭하여 생성된 계정을 사용하여 **인증** 을 수행합니다.

7.9 사용자 신청 시 사용기간 설정하기

Genian ZTNA에서 사용자 계정 신청 시 계정 사용 기간을 입력받을 수 있습니다.

계정에 대한 사용 기간을 일반 사용자보다 짧게 제한하여 방문자 및 외주 인원을 관리하는 목적으로 사용할 수 있습니다.

7.9.1 사용기간을 설정할 수 있는 사용자 신청서 생성하기

용도별 신청정보에 기간을 입력받는 외부 인원 용도를 생성합니다. 승인방법을 이메일을 통한 승인, 자동승인을 사용할 경우는 다음에 항목을 참고하시기 바랍니다.

사용자 계정 신청을 자동 승인하기 , 이메일을 통한 사용자 계정 승인하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **용도관리 > 사용자 용도** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. **용도별 신청정보** 항목에서 **할당** 을 클릭합니다.
5. **사용자 신청 옵션 필드 할당** 창에서 **기간** 항목을 Add 합니다.
6. **확인** 버튼을 클릭합니다.
7. **생성** 버튼을 클릭합니다.

7.9.2 사용기간 제한 설정하기

생성된 용도의 기간 설정을 변경하여 사용자가 신청서 작성 시 제한할 수 있는 기간을 지정할 수 있습니다. 관리자가 제한날짜를 3 일로 설정할 경우 사용자는 최소 1 일부터 최대3 일까지 사용기간을 입력할 수 있습니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **용도관리 > 사용자 용도** 를 선택합니다.
3. 생성된 용도의 오른쪽 **용도별 정의수정** 항목에서 **신청정보** 를 클릭합니다.
4. 필드명 항목에서 **기간** 을 클릭합니다.
5. 설정 에서 **입력날짜 제한 > 기간** 항목을 **90 일** 에서 **3 일** 로 수정합니다.
6. **필수입력 설정** 항목에 설정값을 **ON** 으로 변경합니다.
7. **수정** 버튼을 클릭합니다.

CHAPTER

EIGHT

엔드포인트 제어

엔드포인트 장치는 TCP/IP 네트워크에서 인터넷이 가능한 컴퓨터 하드웨어 장치입니다. 데스크톱 컴퓨터, 랩톱, 스마트 폰, 태블릿, thin client, 프린터 또는 기타 특수 하드웨어에 이르기까지 다양합니다.

Genian ZTNA Agent를 사용하여 Windows 및 macOS 엔드포인트 단말을 제어 할 수 있습니다. 엔드 포인트에 설치되면 백그라운드에서 실행되고 엔드 포인트에 대한 변경사항이 생기면 정책 서버와 통신합니다. 에이전트는 운영 체제, 업데이트, 응용 프로그램, 레지스트리 항목 및 서비스와 같은 엔드포인트 시스템 정보를 관리하는 정책을 사용하여 엔드포인트의 이상 징후를 감지하고 처리하는데 도움이 됩니다.

8.1 에이전트 기본 구성

에이전트 기본 정책에 따라 엔드포인트에 에이전트의 기본 설치 및 작업이 결정 됩니다. 노드 별 에이전트 설정을 추가로 구성할 수 있습니다. 노드정책의 에이전트 설정 을 참조 하십시오.

에이전트 기본 옵션을 구성하려면 메뉴 모음에서 **설정** 을 선택하고 왼쪽 항목에서 **환경설정 > 에이전트** 를 선택합니다.

8.1.1 설치 경로

- 에이전트 파일을 설치할 위치를 정의합니다. 기본값 : %ProgramFiles%\Geni\Genian (Windows 전용)

8.1.2 설치 전 사용자확인

- 에이전트 설치 전 사용자확인을 거칠지 여부를 선택합니다. (Windows 전용)
- 선택: **On** 또는 **Off**

8.1.3 설치과정 표시

- 에이전트 설치진행과정을 표시할지 여부를 선택합니다. (Windows 전용)
- 선택: **On** 또는 **Off**
- **On** 일 경우, 에이전트 설치완료 후 메시지를 표시할지 여부(**On / Off**)를 선택합니다. (Windows 전용)

8.1.4 설치정보 등록

- 선택: 제어판의 프로그램 추가/제거에 에이전트 설치 정보의 등록 여부(**On / Off**)를 선택합니다. (Windows 전용)

8.1.5 에이전트 삭제방식

- 선택: 트레이메뉴를 통해 에이전트 삭제가 되는 방식을 선택합니다. (Windows 전용)
- 인증코드 사용 : '에이전트 인증코드 발급'을 통한 삭제키가 요구됩니다.
- 인증코드 미사용 : 사용자는 별도의 인증과정 없이 에이전트를 삭제 할 수 있습니다.
- 지원 안 함 : 메뉴를 통한 '에이전트 삭제'를 지원하지 않습니다.

8.1.6 자동업데이트 대상

- 에이전트 자동업데이트를 수행할 대상 네트워크를 선택합니다.

8.1.7 서비스 대상그룹

- 에이전트의 트레이 메뉴에서 내상태를 확인할 수 있는 "내상태 확인"메뉴의 표시 여부를 설정합니다. (Windows and macOS 전용)

8.1.8 내상태 확인 메뉴 표시

- 선택: 에이전트의 트레이 메뉴에서 내상태를 확인할 수 있는 "내상태 확인" 메뉴의 표시 여부(**On / Off**)를 설정합니다. (Windows and macOS 전용)

8.1.9 웹 브라우저

- 선택: 에이전트가 웹페이지를 표시하는 데 사용할 웹브라우저(**Internet Explorer or 브라우저 경로직접입력**)를 선택합니다. (Windows 전용)
- IE 웹브라우저 모양: 에이전트는 Internet Explorer의 툴바 및 버튼을 최소화하여 웹페이지를 표시할 수 있습니다.(**옵션: 표준 / 간략**)
- IE 웹브라우저 크기: **표준** 또는 **최대화**

8.1.10 에이전트 커스텀 아이콘

- 에이전트의 트레이 아이콘에 사용될 커스텀 아이콘(ICO 파일)을 업로드합니다. (Windows 전용)

8.1.11 KeepAlive 전송주기

- 주기 설정: KeepAlive 패킷을 전송하는 주기 (최소값:30초 - 최대값:10분)
- 전송 주기 * 5회의 시간 동안(예: 2분 * 5회 = 10분) KeepAlive가 수신되지 않으면 에이전트 동작 상태를 Down으로 감지합니다.

8.1.12 절전모드 재시작 시간

- 시간 설정: 절전모드진입 후 해당시간이 경과했을 경우 운영체제 시작시 동작하는 기능이 수행됩니다. (최소값:30분 - 최대값:6시간) (Windows and macOS 전용)

8.1.13 정책서버 SSL 인증서 설치

- 옵션 선택: 에이전트가 정책서버의 SSL인증서를 사용자PC에 설치할지 여부를 선택합니다. (Windows and macOS 전용)

8.1.14 토큰 미사용 에이전트 차단

- 옵션 선택: 토큰을 사용하지 않는 에이전트 정책서버접근을 차단합니다.

8.1.15 배포 옵션

- 배포파일 검증 방법: 파일 배포 V2 플러그인을 이용하여 파일을 배포할 때 무결성을 확인하는데 사용할 방법을 설정합니다.

파일 배포 V2 액션 정책을 처음으로 설정하면 옵션이 자동으로 설정 및 에이전트가 정책 갱신할 때 사용자 PC에 자동으로 저장되며, 나중에 변경할 수 없습니다. 신뢰하는 ID 또는 신뢰하는 공개키를 삭제하거나 분실한 경우 제조사의 기술지원을 통해서만 변경가능합니다.

- 복수의 배포 서버 사용: 배포파일 다운로드에 실패할 경우 동일한 Proxy 서비스 대상 네트워크그룹(시스템>시스템관리>환경설정)에 포함된 다른 센서에서 다운로드를 시도할지 여부를 선택합니다.

8.2 운영체제별 플러그인 지원 목록

8.2.1 Windows 플러그인 지원 목록

Genian ZTNA가 Windows 단말의 정보를 수집, 제어하기 위한 플러그인 목록은 다음과 같습니다.

플러그인 이름	설명	에이전트 버전
TCP세션검사	주기적으로 TCP 세션수를 수집하며 임계치이상되는 세션수가 발견되면 네트워크 인터페이스를 차단합니다.	6.0.0~
호스트명 변경	컴퓨터 이름을 변경하는 기능을 제공합니다.	6.0.0~
인터페이스 제어	위험이벤트 발생시 인터페이스를 사용안함으로 바꾸는 기능을 제공합니다.	6.0.0~
비밀번호유효성검사	Windows 계정의 비밀번호에 대한 유효성을 검사하고 검증되지 않은 비밀번호를 안전한 비밀번호로 변경시킵니다.	6.0.0~

continues on next page

Table 1 – continued from previous page

플러그인 이름	설명	에이전트 버전
무선랜제어	무선 네트워크 인터페이스에서 탐지되는 무선 AP에 대한 정보를 제공하며 허용되지 않은 AP 연결을 제한합니다.	6.0.0~
모니터정보 수집	로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다.	6.0.0~
프린터정보 수집	컴퓨터시스템에 등록되어있는 프린터에 대한 정보를 제공합니다.	6.0.0~
WMI정보수집	WMI를 통하여 시스템 정보를 수집합니다.	6.0.0~
모양 및 개인설정	바탕화면, 화면보호기에 대한 설정 정보를 수집 및 제어합니다.	6.0.0~
네트워크 공유폴더	네트워크에 공유된 폴더정보를 수집하며 일정시간 이상 공유되는 폴더를 제어합니다.	6.0.0~
Windows 보안설정	시스템에 설정된 Windows 방화벽, 원격데스크탑, 자동실행의 동작을 제어합니다.	6.0.0~
소프트웨어정보 수집	설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.	6.0.0~
네트워크정보 수집	네트워크 인터페이스 정보와 탐지된 포트정보를 수집하여 노드정보에 표시합니다.	6.0.0~
운영체제정보 수집	Windows 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.	6.0.0~
Windows 업데이트	Windows의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.	6.0.0~
하드웨어정보 수집	마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다.	6.0.0~
백신정보 수집	PC에 설치되어있는 백신프로그램 정보 및 백신으로 검출된 바이러스치료 로그를 실시간으로 수집합니다.	6.0.0~
에이전트 인증창	사용자인증 수행시 WEB페이지가 아닌 에이전트 자체 인증창을 사용합니다.	6.0.0~
시스템 종료	지정된 시각에 Windows 시스템의 절전, 재시작, 종료를 수행합니다.	6.0.0~
프로세스 강제종료	액션 검사조건에 설정된 프로세스에 대해서 강제종료 기능을 수행합니다.	6.0.0~
수행조건만 검사	액션에 설정된 수행 조건을 체크하는데 사용하는 플러그인 입니다.	6.0.0~
파일 배포v2	파일을 실행하거나 특정 위치에 다운로드합니다.	6.0.16~
장치제어	사용자 PC에서 사용금지된 장치들을 사용중지로 변경합니다.	6.0.0~
Malware Detector	Insights ECO 시스템과 연동하여 단말에서 발생하는 악성코드를 감지합니다.	6.0.0~
필수 소프트웨어 검사	사용자 PC에 필수 소프트웨어가 설치되어있는지 검사합니다.	6.0.0~
Windows 방화벽 제어	Windows 방화벽을 사용하여 사용자 네트워크를 제어합니다.	6.0.0~
DNS 제어	DNS 관련 로컬설정을 제어합니다.	6.0.0~
유선인증관리자	유선인터페이스의 인증 설정 및 유선인증창에 대한 옵션을 정의합니다.	6.0.0~
ZTNA 연결 관리자	ZTNA 연결관리자에 대한 옵션 및 동작을 제어합니다.	6.0.0~
웹브라우저 옵션 제어	웹브라우저 옵션을 강제화 하는 기능을 제공합니다.	6.0.0~

8.2.2 macOS 플러그인 지원 목록

Genian ZTNA가 macOS 단말의 정보를 수집, 제어하기 위한 플러그인 목록은 다음과 같습니다.

플러그인 이름	설명	에이전트 버전
운영체제정보 수집	macOS 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.	6.0.0~
하드웨어정보 수집	마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다.	6.0.0~
소프트웨어정보 수집	설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.	6.0.0~
네트워크정보 수집	네트워크 인터페이스 정보와 탐지된 포트정보를 수집하여 노드정보에 표시합니다.	6.0.0~
백신정보 수집	PC에 설치되어있는 백신프로그램 정보를 수집합니다.	6.0.0~
macOS 업데이트	macOS의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.	6.0.0~
프로세스 강제종료	액션 검사조건에 설정된 프로세스에 대해서 강제종료 기능을 수행합니다.	6.0.0~
수행조건만 검사	액션에 설정된 수행 조건을 검사하는데 사용하는 플러그인입니다.	6.0.0~
에이전트 인증창	사용자인증 수행시 WEB페이지가 아닌 에이전트 자체 인증창을 사용합니다.	6.0.0~
모양 및 개인설정	바탕화면, 화면보호기에 대한 설정 정보를 수집 및 제어합니다.	6.0.0~
프린터정보 수집	컴퓨터시스템에 등록되어있는 프린터에 대한 정보를 제공합니다.	6.0.0~
모니터정보 수집	로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다.	6.0.0~
시스템 종료	지정된 시각에 시스템의 절전, 재시작, 종료를 수행합니다.	6.0.0~
필수 소프트웨어 검사	사용자 PC에 필수 소프트웨어가 설치되어있는지 검사합니다.	6.0.0~
사용자 알림메시지	사용자에게 알림메시지를 표시합니다.	6.0.0~
무선랜제어	무선 네트워크 인터페이스 정보를 수집하여 노드정보에 표시합니다.	6.0.0~
ARP관리	사용자 PC의 ARP 테이블에 대한 관리 작업을 수행합니다.	6.0.0~
파일 배포v2	파일을 실행하거나 특정 위치에 다운로드합니다.	6.0.16~
호스트명 변경	호스트명 제한을 설정하거나 호스트명을 변경합니다.	6.0.0~
장치제어	사용자 PC에서 사용금지된 장치들을 사용중지로 변경합니다.	6.0.0~
네트워크 공유폴더	네트워크에 공유된 폴더정보를 수집하며 일정시간 이상 공유되는 폴더를 제어합니다.	6.0.0~
비밀번호유효성검사	macOS 계정의 비밀번호에 대한 유효성을 검사하고 검증되지 않은 비밀번호를 안전한 비밀번호로 변경시킵니다.	6.0.0~
에이전트정보 외부전송	에이전트가 가지고 있는 정보를 외부 프로그램에 전송합니다.	6.0.0~

8.2.3 Linux 플러그인 지원 목록

Genian ZTNA가 Linux 단말의 정보를 수집, 제어하기 위한 플러그인 목록은 다음과 같습니다.

플러그인 이름	설명	에이전트 버전
수행조건만 검사	액션에 설정된 수행 조건을 체크하는데 사용하는 플러그인 입니다.	6.0.0~
하드웨어정보 수집	마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다.	6.0.0~
소프트웨어정보 수집	설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.	6.0.0~
네트워크정보 수집	네트워크 인터페이스 정보와 탐지된 포트정보를 수집하여 노드정보에 표시합니다.	6.0.0~
운영체제정보 수집	리눅스 운영체제 정보를 수집하여 노드정보에 표시합니다.	6.0.0~
인터페이스 제어	위험이벤트 발생시 인터페이스를 사용 안 함으로 바꾸는 기능을 제공합니다.	6.0.0~
ZTNA 연결 관리자	ZTNA 연결관리자에 대한 옵션 및 동작을 제어합니다.	6.0.0~
Linux 업데이트	Linux의 업데이트 상태를 검사하고 보고합니다.	6.0.0~
백신정보 수집	PC에 설치되어있는 백신프로그램 정보를 수집합니다.	6.0.0~
프로세스 강제 종료	액션에 설정된 프로세스에 대해서 강제종료 기능을 수행합니다.	6.0.0~
ARP 관리	사용자 PC의 ARP 테이블에 대한 관리 작업을 수행합니다.	6.0.0~
파일 배포	파일을 실행하거나 특정 위치에 다운로드합니다.	6.0.0~
사용자 알림메시지	사용자에게 알림메시지를 표시합니다.	6.0.0~
모니터정보 수집	로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다.	6.0.0~
비밀번호유효성검사	Linux 계정의 비밀번호에 대한 유효성을 검사하고 검증되지 않은 비밀번호를 안전한 비밀번호로 변경시킵니다.	6.0.0~
장치제어	사용자 PC에서 사용금지된 장치들을 사용중지로 변경합니다.	6.0.0~
네트워크 공유폴더	네트워크에 공유된 폴더정보를 수집하며 일정시간 이상 공유되는 폴더를 제어합니다.	6.0.0~
프로그램 제거	Debian packages 및 Snap으로 설치된 프로그램중 제거 가능한 특정 프로그램을 제거합니다.	6.0.0~

8.3 노드정책의 에이전트 설정

에이전트 정책은 노드 그룹에 적용되는 개별 노드 정책을 기반으로 구성 할 수 있습니다. **정책 > 노드정책 > [정책 ID]** 에서 노드 정책을 선택하고 아래로 스크롤하여 **세부설정 > 에이전트 정책** 에서 다음 옵션에 설정합니다.

8.3.1 사용여부

- 지정:
- **On**, **Off** 또는 **Delete** 는 에이전트 실행 상태를 전환하거나 노드에서 에이전트를 삭제합니다.
- 에이전트삭제시간:
- 정책 서버에 연결되지 않은 경우 에이전트를 삭제 할 **시간**, **일**, **주** 또는 **개월** 의 기간을 정의합니다. 이 기능을 사용하지 않으려면 **0** 을 입력합니다.

8.3.2 Dissolvable Agent

- Dissolvable Agent 기능은 사용자가 시스템에 로그온 할 때 실행되며, 시스템 정보를 수집하고 수집이 완료되면 프로세스가 종료됩니다. (로그온 시 *1*회성 동작 방식)
- **On** 또는 **Off** 를 선택합니다.

8.3.3 Agent Fail-safe

- 에이전트가 정책 서버에 연결되지 않은 시간을 시점으로 **분 시간**, **일**, **주**, 또는 **개월** 로 정의된 기간 후에 에이전트를 비활성화합니다.
- **On** 또는 **Off** 를 선택합니다.

Note: 엔드포인트 제어를 수행하는 플러그인은 개별적으로 Fail safe 설정이 가능합니다.

8.3.4 트레이아이콘 표시

- 트레이아이콘 표시 여부를 선택합니다. (*macOS* 에이전트: 상태 표시줄 에이전트 아이콘 / *Windows* 에이전트: 시스템 트레이 에이전트 아이콘)
- **On** 또는 **Off** 를 선택합니다.

8.3.5 수행 계정

- **PC에 로그인된 계정**, **별도의 수행계정 설정** 또는 **로컬 시스템 계정** 을 선택하여 에이전트를 실행합니다.

선택한 계정에서 설정 된 에이전트 작업을 수행하거나 설치 할 수 있는 적절한 권한이 있는지 확인합니다. ActiveDirectory 환경에서 제한된 권한의 사용자는 에이전트 설치를 위한 별도의 배포 과정이 필요할 수 있습니다. 참고: *Windows* 제어, *macOS* 제어.

- **PC에 로그인된 계정** - 로그인한 모든 계정에서 에이전트를 실행합니다.
- **별도의 수행계정 설정** - 도메인 내의 여러 디바이스가 비관리자에 의해 사용되도록 되어 있다면, 이 옵션을 선택하고 도메인 관리자 자격 증명으로 구성합니다.
- **로컬 시스템 계정** - 로컬 시스템의 루트 수준 자격 증명을 위해 이 계정 옵션을 선택합니다. 단일 디바이스에 적용되는 노드 정책에 가장 적합합니다.

8.3.6 정책변경검사주기

- 에이전트가 정책 서버에서 업데이트 된 정책을 확인 할 수 있도록 **시간** 의 기간을 지정합니다.
- 1-4 **시간** 중에서 선택합니다.

8.3.7 에이전트정보삭제

- 정책 서버에 연결되지 않은 경우 에이전트정보를 삭제 할 **시간**, **일**, **주** 또는 **개월** 의 기간을 정의합니다. 이 기능을 사용하지 않으려면 **0** 을 입력합니다.

8.3.8 Captive Portal 탐지

- 에이전트가 네트워크 상태가 변경되면 Captive Portal을 탐지하여 알림메시지를 표시합니다.

일부 보안소프트웨어는 PC의 보안수준을 체크하여 보안수준이 낮을 경우 네트워크 통신을 차단하고 Captive Portal을 표시합니다. Captive Portal은 사용자가 웹브라우저를 사용하지 않을 경우 네트워크 차단을 인식할 수 없습니다. 사용자는 웹을 사용하지 않을 경우 차단여부를 인식할 수 없으므로 Captive Portal 탐지 기능에 의한 알림메시지 표시가 도움이 될 수 있습니다. 에이전트 정책에 설정된 URL에 접속하여 설정된 메세지가 아닌 별도의 웹페이지가 수신될 경우 알림메시지를 사용자에게 표시합니다.

8.4 운영체제별 플러그인 설정방법

Genian ZTNA Agent에서 단말에 정보를 수집하거나 단말의 설정을 제어하기 위한 플러그인을 운영체제별로 생성할 수 있습니다.

8.4.1 플러그인 타입별 구분사항

Genian ZTNA Agent에서 동작하는 플러그인은 다음과 같은 타입으로 분류할 수 있습니다.

분류	설명
단독 플러그인	노드정책에 하나만 할당 할 수 있는 플러그인
멀티 플러그인	노드정책에 다수를 할당 할 수 있는 플러그인

8.4.2 운영체제별 플러그인

운영체제별 설정할 수 있는 플러그인 항목은 다음과 같습니다.

Note: 플러그인 동작부분을 설정하여 사이트 환경에 맞추어 플러그인을 사용할 수 있습니다.

Windows 제어

다음 플러그인을 사용하여 에이전트가 설치된 Windows 단말을 제어할 수 있습니다.

ARP 테이블 관리

사용자 PC의 ARP 테이블에 대한 관리 작업을 수행합니다. 악의적인 사용자는 ARP 테이블을 변조하여 내부 네트워크 보안 체계를 우회하거나 내부 사용자의 패킷을 가로채려는 시도를 할 수 있습니다. ZTNA는 이러한 시도들을 방지하기 위해 다음과 같은 기능을 제공합니다.

- 악의적인 사용자가 패킷을 가로채는 ARP Spoofing 공격 대응
- 수동으로 ARP 항목을 Static 설정하지 못하도록 강제화하여 네트워킹 보호

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **ARP 관리** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **Static ARP 차단** 의 경우 **On** 으로 설정하여 Static으로 설정된 ARP에 대해서 사용하지 못하도록 강제화합니다.
2. **Anti ARP Spoofing** 를 **On** 으로 설정하여 ARP Spoofing 방지를 위해 충돌 보호된 IP에 대해서 Static ARP를 설정(확인 된 노드의 *ARP* 정보) 합니다.
   - **적용대상 노드그룹** : AAS(Anti ARP Spoofing)를 적용할 IP가 특정 노드그룹에 속하는 경우만 적용할 수 있도록 선택합니다. (미선택시 모든노드에 대해서 적용)
3. **FailSafe 사용** 은 에이전트가 정책서버로 접속이 되지 않을 경우 플러그인 동작을 중지할 수 있는 기능입니다.
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 노드정책 화면에서 **적용하려는 정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **ARP 관리** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

Note: 관리 > 노드 > IP관리 탭 > IP 정책으로 이동하여 충돌 방지 설정을 구성합니다.

DNS 제어

DNS 관련 로컬설정을 제어합니다. 에이전트 설치된 PC가 임의로 DNS를 설정할 수 없게 관리자가 DNS 서버를 지정할 수 있습니다. DNS를 우회할 수 있는 hosts 파일 항목에 대해서도 추가/제거가 가능합니다.

- 관리자가 지정한 DNS 서버로 설정을 강제화하여 기업의 내부 DNS 규정 준수
- 보안사고로 인해 hosts 파일이 변조된 경우 특정항목 제거 가능

> **Warning:** 다른 보안 솔루션이 Hosts 파일을 제어할 경우 본 플러그인과 충돌 가능성이 있으므로 사용전에 꼭 확인바랍니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **DNS 제어** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **플러그인 설정** 이 있습니다.

1. **DNS 구성** 의 경우 제어안함, 자동으로 DNS 서버 주소 받기, 다음 DNS 서버 주소 사용 등이 있습니다.
2. **Hosts 파일 설정** 의 경우 Hosts 파일 내용을 추가하거나 제거할 수 있습니다.
3. **FailSafe 사용** 의 경우 에이전트가 정책서버와 동신이 되지 않을 경우 플러그인의 동작을 중지합니다.
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 적용하고자 하는 **노드정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **DNS 제어** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

웹브라우저 옵션 제어

웹브라우저(Internet Explorer, Edge, Chrome) 옵션을 강제화 하는 기능을 제공합니다. 사용자별로 브라우저 설정을 다르게 사용하여 브라우저 보안이 취약해지는 것을 관리자가 설정을 강제화하여 보호할 수 있습니다.

- 민감한 개인정보에 대한 자동 저장 및 자동 사용을 방지
- 관리중인 Proxy가 아닌 다른 Proxy를 이용하여 네트워크를 우회하는 것을 방지
- 내부에서 관리하는 Proxy가 없는데 사용자가 자체 Proxy를 이용하는 것을 방지
- 취약한 사이트에서 ActiveX를 다운 받아 위험에 노출되는 것을 방지
- 팝업, 브라우저 도우미, Toolbar 등 내부 보안규정에 따라 관리자가 기능 활성/비활성 가능

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.

3. 노드액션 관리창에서 **웹브라우저 옵션 제어** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.

2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **개인정보 및 보안** 설정
   - **세이프 브라우징** 에서 크롬의 세이프 프라우징 옵션을 강제화 합니다. (보호되지 않음/표준 보호 모드/향상된 보호 모드) Safe Browsing.
   - **기본 팝업 설정** 에서는 웹 사이트에서 팝업 창을 표시할 수 있는지 여부를 설정합니다.
   - **다운로드 제한** 에서는 크롬과 엣지 브러우저의 안전하지 않은 다운로드를 차단하는 옵션을 강제화 합니다. (위험한 다운로드 차단/위험할 가능성이 있는 다운로드 차단/모든 다운로드 차단/악성 다운로드 차단)
   - **기본 쿠키 설정** 에서는 크롬과 엣지 브러우저의 사용자 PC에 쿠키 허용 옵션을 강제화 합니다. (모든 사이트에서 로컬 데이터 설정 허용/모든 사이트에서 로컬 데이터 설정 허용 안함/세션이 지속되는 동안 쿠키 유지)
2. **자동 완성 및 비밀번호** 설정
   - **암호를 저장하도록 제안** 에서는 크롬과 엣지 브러우저가 사용자 암호를 저장하도록 허용하는 기능을 사용하지 않도록 설정합니다.
   - **암호 및 암호 자동 채우기** 에서는 엣지 브라우저가 자동으로 암호를 입력하고 사용 가능한 암호를 제안하도록 허용하는 기능을 사용하지 않도록 설정합니다.
   - **유출된 암호 검사** 에서는 엣지 브라우저에 저장된 암호를 노출된 자격 증명의 알려진 리포지토리와 비교해 확인하고 일치하는 항목이 발견되면 경고하는 기능을 사용하지 않도록 설정합니다.
   - **암호필드에 "암호 나타내기" 단추 표시** 에서는 엣지 브라우저에서 암호입력필드에 입력된 암호 정보가 보이는 단추가 표시되는 기능을 사용하지 않도록 설정합니다.
   - **기본 정보 저장 및 채우기** 에서는 크롬과 엣지 브러우저에 전화 번호, 전자 메일 주소 및 배달 주소 정보가 저장되는 기능을 사용하지 않도록 설정합니다.
   - **결제 정보 저장 및 채우기** 에서는 크롬과 엣지 브러우저에 카드및 결제 세부 정보를 저장하고, 자동으로 채우는 기능을 사용하지 않도록 설정합니다.
   - **결제수단 확인 허용** 에서는 엣지 브러우저에 사이트에서 저장된 결제수단이 있는지 확인하도록 허용하는 기능을 사용하지 않도록 설정합니다.
   - **폼 자동완성** 에서는 IE 브러우저에서 웹 양식 내용을 자동으로 완성하는 기능을 사용하지 않도록 설정합니다.
3. **연결** 설정
   - **프록시 서버 사용** 은 사용자 LAN에 프록시 서버 사용 옵션을 지정 할 수 있습니다.(이 설정은 전화 연결이나 *VPN* 연결에는 적용되지 않음)
     - **사용안함** : **프록시 서버** 를 사용 하지 않습니다.
     - **기본설정** : 주소 포트 추가, 선택적 Bypassing Proxy Server 활성화, 예외 사항 입력
     - **고급설정** : HTTP, 보안, FTP, Socks 포트를 입력하십시오. 옵션으로 프록시 서버를 생략하고 예외 상황을 입력하십시오.
4. **IE전용설정** 설정
   - **홈 페이지** 에서 웹브라우저의 시작 페이지를 설정합니다. (공란이면 제어안함)

- **임시인터넷파일 삭제** 는 **강제사용** 을 선택하여 브라우저 종료시 임시인터넷파일폴더를 비우도록 설정합니다.
- **서명 안 된 ActiveX 컨트롤 다운로드** 에서 **사용안함** 을 선택하여 서명되지 않은 ActiveX 컨트롤을 다운로드하지 않습니다.
- **ActiveX 컨트롤을 자동으로 확인** 에서 **사용안함** 을 선택하여 ActiveX 컨트롤 설치 자동 알림을 비활성화합니다.
- **파일 다운로드 시 자동으로 확인** 을 **사용안함** 으로 설정하여 파일 다운로드 시 자동으로 확인되지 않고 알림줄이 표시되도록 설정합니다.
- **신뢰할 수 있는 사이트** 를 **On** 으로 설정하여 신뢰할 수있는 사이트를 추가하거나 제거 할 수 있습니다. 또한 서버 확인을 **활성화** 및 **비활성화** 할 수 있습니다.
- **미사용 ActiveX 삭제** 를 **On** 으로 설정하여 기준일 이상 미사용된 ActiveX를 삭제합니다.
- **Toolbar 삭제** 를 **On** 으로 설정하여 IE에 설치된 모든 Toolbar 를 삭제합니다.
- **브라우저 도우미 삭제** 설정을 **On** 선택하여 IE에 설치된 모든 브라우저 도우미를 삭제합니다.
- **예외**: 삭제하지 않을 IE추가기능(ActiveX, Toolbar, 브라우저 도우미) 이름을 입력합니다.

5. **FailSafe 사용** 은 에이전트가 정책서버로 접속이 되지 않을 경우 플러그인 동작을 중지할 수 있는 기능입니다.
6. **수정** 버튼을 클릭합니다.
7. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
8. 적용하고자 하는 **노드정책** 을 클릭합니다.
9. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
10. **사용가능** 항목에서 **IE보안옵션 제어** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
11. **추가** 버튼을 클릭합니다.
12. **수정** 버튼을 클릭합니다.

Malware 정보 수집

Insights ECO 시스템과 연동하여 단말에서 발생하는 악성코드를 감지합니다.

- 단말의 실행 파일에 대한 정보(소스, 파일보유, 서명)를 수집하여 악성코드 탐지
- ZTNA의 다른 기능과 연동하여 단말 보안 강화 가능

수집된 정보는 벤더나 제3자 분석용으로 제공될 수 있습니다. 수집된 정보는 악성코드 검출 및 분석 이외의 목적으로는 제공되지 않습니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **Malware 정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **정보수집동의** 의 경우 플러그인을 사용하기 위해서는 정보수집에 대한 사용자의 동의가 필요합니다.

2. **수집제외경로** 의 경우 Malware 감지에 필요한 정보 수집에서 제외할 폴더 경로를 설정합니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 노드정책 화면에서 **적용하려는 정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **Malware 정보 수집** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

TCP 세션 검사

주기적으로 TCP 세션수를 수집하며 임계치 이상되는 세션수가 발견되면 네트워크 인터페이스를 차단합니다. 다량의 광고나 링크가 포함된 악성 사이트에 접속하여 단말에서 의도하지 않은 다량의 TCP 세션을 맺게 되었을때 ZTNA는 이를 감지하고 네트워크 차단이 가능합니다.

- 다량의 TCP 연결을 시도하는 악성 코드 또는 사이트에 감염되었을때 네트워크 인터페이스를 제어하여 단말 보호

노드정책에 에이전트 액션 추가

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책창에서 **원하는 노드정책 ID** 를 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **TCP세션검사** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.

TCP세션검사 설정

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **TCP세션검사** 을 찾아 클릭합니다.
4. 옵션 설정에서 **조건설정** 을 입력합니다.

아래에서 **세션정보 전송주기** 을 설정합니다.

1. **세션정보 전송주기** 에서 TCP 세션 정보를 업데이트 할 시간 간격을 지정합니다.(*0:* 전송안함)
2. **업데이트 최소비율** 에서 TCP 세션 전체의 수가 이전에 보낸 세션수와 설정비율 이상 차이가 나면 정보를 전송합니다.(*LISTENNING* 상태는 제외)
3. **업데이트 최소값** 의 경우 세션수가 설정값 미만이면 업데이트 최소비율이 적용되지 않고 업데이트되지 않습니다.

아래에서 **인터페이스 제어** 에 대해 설정합니다.

4. **인터페이스 제어** 의 경우 세션상태임계치를 정의하여 임계치 초과시 인터페이스를 차단시킬지 여부를 선택합니다.(*On:* 차단 / *Off:* 차단안함)

아래에서 **인터페이스 차단알림** 에 대해 설정합니다.

5. **인터페이스 차단알림** 의 경우 TCP 세션수가 임계치를 초과하여 인터페이스 제어되었을 때 사용자에게 차단사실을 알리는 3가지 방법을 제공합니다.
   - **사용안함** : 장치가 차단되어도 사용자에게 차단알림을 하지 않습니다.
   - **사용자메시지** : 직접 사용자에게 보여질 메시지를 정의하여 인터페이스 장치가 차단됨을 알립니다.
   - **에이전트팝업** : 에이전트 기본팝업창을 사용하여 인터페이스 장치가 차단되었음을 알립니다.
6. **FailSafe 사용** 은 에이전트가 정책서버로 접속이 되지 않을 경우 플러그인 동작을 중지할 수 있는 기능입니다.
7. **수정** 버튼을 클릭합니다.

Windows 방화벽 제어

Windows 방화벽을 사용하여 사용자 네트워크를 제어합니다. 센서가 동작하지 않을때 접근제어를 엔드포인트(PC)에서 에이전트로 수행이 가능합니다.

- 제어정책 자동 규칙 기반 아웃바운드 트래픽 차단
- 커스텀 규칙을 통한 외부 악성 C&C 서버 차단

플러그인 할당시 **자동 규칙 설정 사용** 옵션을 사용할 경우 노드가 속한 **제어 정책의 권한 객체 정보로 Windows 방화벽 아웃바운드 규칙이 설정** 됩니다.
또한 다양한 조건으로 Windows 방화벽 규칙을 직접 설정할 수 있습니다.

Windows 방화벽 제어 옵션 구성

1. **자동 규칙 설정 사용** : 제어정책의 권한 설정에 따라 Windows 방화벽 아웃바운드 규칙을 자동으로 설정합니다.
2. **알림 메시지** : 자동 규칙 설정시 사용자에게 팝업 메시지를 표시합니다.
3. **메시지 내용** : 자동 규칙 설정시 팝업 메시지에 대한 내용을 입력합니다.
4. **커스텀 규칙** : Windows 방화벽 규칙을 직접 설정할 수 있습니다.
5. **FailSafe 사용** : 센터에 접속이 불가능할 경우 플러그인을 중지할 수 있습니다.

노드정책을 통하여 네트워크 차단 정책 구성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **Windows 방화벽 제어** 을 찾아 클릭합니다.
4. **조건설정** 및 옵션을 입력합니다.
5. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
6. 네트워크 차단 정책을 구성할 노드정책을 클릭합니다.

7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **Windows 방화벽 제어** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.
11. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

제어정책을 통하여 네트워크 차단 정책 구성

1단계. 제어 대상 노드그룹 생성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **추가** 버튼을 클릭합니다.
5. 제어 대상의 조건 설정 후 **추가** 버튼을 클릭합니다.
6. **생성** 버튼을 클릭합니다.

2단계. 제어 액션 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어액션** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭합니다.
3. 플러그인 선택 항목에서 **Windows 방화벽 제어** 플러그인을 선택합니다.
4. **조건설정** 및 옵션을 입력합니다.
5. **생성** 버튼을 클릭합니다.

3단계. 제어정책 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어정책** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭하고, **제어정책 마법사** 를 완료 시킵니다.
3. **정책 기본설정** 탭에서 **ID** 항목에 **사용할 정책 ID** 를 입력합니다.
4. **노드그룹 설정** 탭에서 **새로 추가한 노드그룹** 을 선택하고, **선택** 항목으로 이동 시킵니다.
5. **권한 할당** 과 **제어 옵션** 탭에서 **원하는 옵션** 을 입력합니다.
6. **제어액션 설정** 탭에서 **생성한 제어액션** 을 찾아 **선택** 항목으로 이동 시킵니다.
7. **완료** 버튼을 클릭합니다.
8. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

Windows 보안설정

시스템에 설정된 Windows 방화벽, 원격데스크탑, 자동실행 등의 동작을 제어합니다. 시간동기화, 게스트 계정 제한, 전원관리 등 윈도우의 다양한 보안 설정을 지원합니다.

- 게스트 계정 잠금을 통해 RID 하이재킹(게스트 계정의 권한을 상승시키는 공격) 방지
- RDP(원격데스크탑) 프로토콜에 대해 무차별 패스워드를 대입하는 공격

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **Windows 보안설정** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **게스트계정 잠그기** 에서 **On** 설정을 하여 게스트계정을 비활성화 시킵니다.
2. **Windows 방화벽** 에서 **강제사용** 선택하여 Windows 방화벽 설정을 활성화 시킵니다.
3. **원격 데스크톱** 에서 **사용안함** 을 선택하여 원격 데스크톱 사용을 비활성화 시킵니다.(예: 미디어, 외부 장치, 기타)
4. **복구 콘솔 자동 로그온** 에서 **사용안함** 을 선택하여 복구 콘솔에 대한 자동 관리 로그온 허용 값을 비활성화 시킵니다.
5. **자동실행** 에서 **사용안함** 을 선택하여 외부 장치의 자동실행을 비활성화합니다.
6. **시간 동기화서버** 에서 **강제사용** 을 선택하여 NTP(*Network Time Protocol*) 서버와의 시간 동기화를 적용합니다. **시간 동기화서버 주소** 및 **동기화 주기** 를 입력합니다.
7. **절전모드 해제시 암호 보호** 에서 **강제사용** 을 선택하여 절전모드 해제시 암호 보호 설정을 적용합니다.(절전모드 해제 시 로그*Off* 상태에서 비밀번호 입력창이 나타나도록합니다)
8. **빠른 시작 켜기** 에서 전원 단추 동작에 대한 빠른 시작 옵션을 설정합니다. (Windows 8 이상)
9. **Windows XP 예약작업** 에서 **사용안함** 을 설정하여 Windows XP의 스케줄링 된 작업만 제어합니다.
10. **수정** 버튼을 클릭합니다.
11. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
12. 노드정책창에서 **기본정책** 을 클릭합니다.
13. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
14. **사용가능** 항목에서 **Windows 보안설정** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
15. **추가** 버튼을 클릭합니다.
16. **수정** 버튼을 클릭합니다.

Windows 시스템 WMI정보 수집

WMI를 통하여 시스템 정보를 수집합니다. WMI는 윈도우 관리 도구(Windows Management Instrumentation)로 단말로부터 모니터 정보, 시리얼 넘버 등 다양한 정보를 쿼리를 통해 수집할 수 있습니다.

- WMI 쿼리를 이용하여 USB로 연결된 프린터 정보 수집
- 비인가 프린터 정보를 탐지하여 사용자 네트워크 차단에 활용

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭하여 새로운 노드액션을 생성합니다.
4. **액션명** 의 경우 고유 이름(예: *WMI 내부 배터리 식별*)을 입력합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **플러그인선택** 의 경우, 드롭다운에서 **WMI정보 수집** 을 선택합니다.
2. **NameSpace** 설정의 경우, 드롭다운에서 적절한 네임스페이스를 선택하거나 **직접입력** (예: *rootCIMV2*)에서 네임스페이스를 정의합니다.
3. **WMI 쿼리** 의 경우 세미콜론으로 구분 된 선택적 쿼리를 입력합니다.(예: *SELECT Caption FROM Win32_Battery*)
4. **수행주기** 의 경우 실행 주기 간격(초 - 개월)을 조정합니다.
5. **수정** 버튼을 클릭합니다.
6. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
7. 적용하고자 하는 **노드정책** 을 클릭합니다.
8. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
9. 새로 생성한 **노드액션** (예: *WMI 내부 배터리 식별*)을 찾아서 더블클릭합니다.
10. **추가** 버튼을 클릭합니다.
11. **수정** 버튼을 클릭합니다.

WMI 결과 보기

정책이 정의 된 일정에 따라 실행 될 때까지 기다리거나 지금 바로 실행하여 결과를 즉시 볼 수 있습니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
3. 기본정책의 **체크박스** 를 클릭합니다.
4. **작업선택 > 즉시수행** 을 클릭합니다. (이 작업을 실행하려면 몇 분 정도 기다립니다)
5. **관리 > 노드** 로 이동하여 에이전트가 설치된 Windows 노드의 **IP** 를 찾아 클릭합니다.
6. **WMI 정보수집결과** 항목을 찾아 WMI 결과를 확인합니다.

WMI 결과에 대한 상태 그룹 만들기

위에 생성 된 **노드액션** 의 WMI 결과를 바탕으로 상태 그룹을 만듭니다 . 그런 다음 이 상태 그룹을 통해 네트워크 요구 사항에 따라 정책을 식별하고 적용 할 수 있습니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 상태그룹 생성** 을 클릭합니다.

아래 **기본정보** 를 설정합니다.

1. **Category** 의 경우 기본값 또는 새로 만들어 사용합니다.(*Node Groups*를 분류할 수 있습니다)
2. **ID** 의 경우 고유 이름(예: *WMI* 내부 배터리 그룹)을 입력합니다.
3. **설명** 이 노드그룹에 대한 내용을 작성합니다.
4. **적용모드 : 사용함** 설정

아래의 **그룹조건** 을 설정합니다.

1. "**AND**" 또는 "**OR**" **조건연산** 을 선택합니다. ("*AND*" 는 모든 조건이 만족되어야합니다. "*OR*" 는 조건 중 하나만 만족해도 됩니다)
2. **조건설정** 에서 **추가** 를 클릭합니다. (이 조건은 적절한 그룹화에 적용할 다양한 조건입니다.)
3. **항목** 에서 **WMI정보수집** 을 선택합니다.
4. **조건** 의 경우 드롭다운에서 적절한 옵션을 선택합니다(예: 같으면*(*클래스*/*속성명*,*속성값*)*)
5. **설정** 에서 적절한 클래스*/*속성명*,*속성값을 입력합니다. (예: *Win32_Battery/Caption, Internal Battery*)
6. **추가** 버튼을 클릭합니다.
7. **생성** 버튼을 클릭합니다.

WMI Query 예제:

WMI Name	Namespace	WMI Query
Battery Info	rootCIMV2	SELECT Caption FROM Win32_Battery
HDD Vendor	rootCIMV2	SELECT Caption FROM Win32_DiskDrive
HDD Size	rootCIMV2	SELECT Size FROM Win32_DiskDrive
HDD Model	rootCIMV2	SELECT Model FROM Win32_DiskDrive
HDD Serial	rootCIMV2	SELECT SerialNumber FROM Win32_DiskDrive
Volume Serial	rootCIMV2	SELECT VolumeSerialNumber FROM Win32_LogicalDisk
Graphics Card Info	rootCIMV2	SELECT Caption, DriverVersion FROM Win32_DisplayConfiguration
Graphics Card Resolution	rootCIMV2	SELECT CurrentHorizontalResolution, CurrentVerticalResolution FROM Win32_VideoController
HP Driver Version	rootCIMV2	SELECT * FROM Win32_PnPSignedDriver WHERE Devicename LIKE 'HP%'
NDIS Driver Version	rootCIMV2	SELECT * FROM Win32_PnPSignedDriver WHERE Devicename LIKE 'NDIS%'
Printer Info	rootCIMV2	SELECT Drivername FROM Win32_Printer
DHCP service	rootCIMV2	SELECT Description, DHCPEnabled, IPEnabled FROM Win32_NetworkAdapterConfiguration
NIC Traffic Info	rootCIMV2	SELECT BytesSentPersec,BytesReceivedPersec FROM Win32_PerfRawData_Tcpip_NetworkInterface

WMI 상태그룹 예제: (설정 사용 예제 : 같거나 같지 않음, 크거나 같음)

상태 그룹	항목	조건	설정
WMI Internal Battery	WMI	같으면(클래스/속성명,속성값)	Win32_Battery/Caption, Internal Battery
WMI HDD Size	WMI	보다작으면(클래스/속성명,속성값)	Win32_DiskDrive/Size, 536870912000

Windows 업데이트

Windows의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다. 사용자가 다양한 이유로 자동 업데이트를 비활성화 해놓은 경우 강제 자동 업데이트 활성화가 가능합니다.

Windows 운영체제 업데이트 환경 설정하기

Windows 업데이트 기능을 사용할 경우 사전에 업데이트를 수행하는 환경을 설정해야 합니다.

1. Windows 운영체제 업데이트 환경 설정하기(검색/연결방법)

Windows 운영체제 업데이트 환경설정은 업데이트 파일에 대한 검색방법과 Mircosoft에서 제공하는 업데이트 서버와의 연결방법 설정으로 나눠집니다. 네트워크 환경에 따라서 검색방법과 연결방법을 변경해서 사용할 수 있습니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **환경설정** 항목에 **에이전트 > 운영체제 업데이트** 를 선택합니다.
3. **Windows 업데이트** 항목을 설정합니다.
4. **수정** 버튼을 클릭합니다.

Note:

1. **Mircosoft Windows Update** : 외부망(인터넷)에 연결된 Mircosoft 제공하는 업데이트 서버와 통신하는 방식
2. **WSUS** : 내부망에 연결된 WSUS 서버와 통신하는 방식
3. **Offline Scan File** : 내부망에 연결된 Genian ZTNA 정책서버와 통신하는 방식

검색방법	연결방법	환경사항
Mircosoft Windows Update	Mircosoft 직접연결	전체 내부망 네트워크에 대한 방화벽 허용권한 필요
	ZTNA를 통한 연결(다운로드)	전체 내부망 네트워크에 대한 방화벽 허용권한 필요
	ZTNA를 통한 연결(다운로드+검색)	ZTNA 장비(ZTNA Proxy 서비스 설정된 대상)에 대한 방화벽 허용권한 필요
WSUS	WSUS 직접연결	WSUS 위치(서버팜)에 따라서 서버팜 방화벽 허용권한 필요
	ZTNA를 통한 연결(다운로드)	WSUS 위치(서버팜)에 따라서 서버팜 방화벽 허용권한 필요
	ZTNA를 통한 연결(다운로드+검색)	ZTNA 장비(ZTNA Proxy 서비스 설정된 대상)에 대한 서버팜 방화벽 허용권한 필요
Offline Scan File	설정 없음	외부망(인터넷)과 통신하지 못하는 환경에서 설정

2. Proxy 서버 설정하기

운영체제 업데이트 시 연결방법을 **ZTNA를 통한 연결** 을 사용할 경우에 한해서 설정할 수 있습니다.

방화벽에서 **운영체제 업데이트 Proxy 서비스설정** 된 네트워크 센서 모두에 허용권한을 부여할 수 없을 경우 사용됩니다.

Note: Proxy 서버 설정 시 설정된 서버 IP로 외부망 접속을 수행합니다.

3. 접속허용 도메인 설정하기

Genian ZTNA에 의해 **네트워크가 차단된 대상** 에 대해서 운영체제 업데이트를 수행할 수 있도록 접속허용 도메인을 설정할 수 있습니다.

플러그인 설정

- 사용자가 시스템 지연등의 이유로 자동 업데이트를 꺼놓은 경우

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **Windows 업데이트** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **업데이트 모음** 옵션의 드롭 다운 메뉴에서 설정을 선택하거나 업데이트 모음을 추가하려면 +를 클릭합니다.
2. **검사 시점** : 예약 된 시간에 업데이트를 확인할지 여부를 지정합니다.(옵션: *1.* 주기적 검사 */2.* 지정시간 검사)
    - **수행 주기** : 시간 간격을 조정하여 업데이트의 검사/설치 시점을 확인합니다. (시간 - 개월)
3. **동작 모드** : 검사와 설치를 수행 또는 검사만 수행 할 지를 선택합니다.
4. **설치 시점** : 업데이트 설치를 수행하는 시점을 선택합니다.(옵션: *1.* 검사 후 즉시 설치 */2.* 종료시 설치 */3.* 지정시간 설치)
5. **리부팅옵션** : 사용자에게 알림을 할지 자동 리부팅을 할지 선택합니다.
6. **자동업데이트** : 중요 업데이트를 확인하고 드롭다운의 설정을 사용하여 설치할지 여부를 지정합니다.
7. **수정** 버튼을 클릭합니다.
8. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
9. 적용하고자 하는 **노드정책** 을 클릭합니다.
10. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
11. **사용가능** 항목에서 **Windows 업데이트** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
12. **추가** 버튼을 클릭합니다.
13. **수정** 버튼을 클릭합니다.
14. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

특정 OS 또는 패치에 대한 새 Windows 업데이트 만들기

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > Windows 업데이트 정책** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.

아래에서 **기본정보** 및 **자동승인 설정** 을 구성합니다.

1. **ID** 의 경우 고유 이름을 입력합니다.
2. **설명** 의 경우 간단한 설명을 입력합니다.
3. **제품** : 적용할 제품 또는 전체 선택
4. **분류** : 적용할 항목 또는 전체를 선택합니다.
5. **생성** 버튼을 클릭합니다.
6. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

또는

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 설정창에서 **Windows 업데이트** 를 찾아 클릭합니다.
4. **노드액션: Windows 업데이트** 를 찾아 클릭하고 **수정** 합니다.

아래에서 **기본정보** 및 **자동승인 설정** 을 구성합니다.

1. **ID** 의 경우 고유 이름을 입력합니다.
2. **설명** 의 경우 간단한 설명을 입력합니다.
3. **제품** : 적용할 제품 또는 전체 선택
4. **분류** : 적용할 항목 또는 전체를 선택합니다.
5. **생성** 버튼을 클릭합니다.
6. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

   (더 이상 사용되지 않은 *Windows* 업데이트를 삭제하려면 정책 > 윈도우 업데이트 정책으로 이동 후 삭제 할 윈도우 업데이트 항목의 체크박스를 선택하고 작업선택 > 석제 버튼을 클릭합니다.)

Genian Syncer 소프트웨어 구성

Genian Syncer 소프트웨어는 Microsoft 웹사이트에서 Microsoft 업데이트 및 패치를 가져와 인터넷에 액세스할 수 없는 정책 서버와 동기화하도록 설계되었습니다. Genian Syncer를 통해 정책서버에 패치파일들을 업로드 했다면 정책 서버 Windows Update 정책 설정을 통해 주기적으로 인터넷에 엑세스할 수 없는 Windows 기기에 Windows Update를 수행합니다.

Genian Syncer 소프트웨어 사용하기

1. **Genians에 문의하여 Genian Syncer 소프트웨어 다운로드 주소를 받습니다.**
2. **Genian Syncer.zip을 다운로드합니다.**
3. **Genian Syncer.zip을 압축 해제합니다.**
4. **Genian Syncer.exe를 실행합니다.** (설치화면이 나타납니다)
5. 실행된 Genian Syncer 창에서 **센터에서 다운로드** 을 클릭합니다. (새로운 대화 상자 창이 나타납니다)
6. **다운로드할 폴더를 지정합니다.**
7. 다시한번 **센터에서 다운로드** 를 클릭합니다.
8. **정책 서버 주소** 와 **관리자 계정정보** 를 입력합니다. (정책서버에서 라이선스 등 정보를 수집합니다)
9. **설정** 을 클릭하여 업데이트항목을 선택합니다. (다운로드할 파일의 범위를 좁히기 위해 분류 및 제품을 지정할 수 있습니다)
10. Microsoft에서 파일을 다운로드하려면 **온라인 다운로드** 를 클릭합니다. (선택한 패치항목들이 다운로드 됩니다)
11. 업데이트 및 패치 파일을 정책 서버에 업로드하려면 **센터에 업로드** 를 클릭합니다.
12. **정책 서버 IP 주소** 또는 **정책서버 도메인** 을 입력하세요. 그런 다음 **관리자 계정정보** 를 입력하고 **확인** 을 클릭합니다.
13. 정책 서버에 파일이 성공적으로 업로드되었을 때 **확인을 클릭합니다.**

업데이트 및 패치가 성공적으로 업로드되었는지 확인하기

1. 상단 패널에서 **정책** 으로 이동합니다.
2. 왼쪽 정책 패널에서 **정책 > 노드정책 > Windows 업데이트 정책** 으로 이동합니다.
3. Windows 업데이트 창에서 **원하는 업데이트 이름** 을 클릭합니다.
4. **업데이트** 탭을 찾아 클릭합니다. (새로운 업데이트 및 패치가 표시됩니다)

업데이트 서비스 설정 구성하기

(에이전트가 인터넷이 아닌 정책 서버를 통하여 업데이트 및 패치를 찾도록 설정하는 것입니다)

1. 상단 패널에서 **설정**으로 이동합니다.
2. 왼쪽 설정 패널에서 **환경설정 > 에이전트 > 운영체제 업데이트** 로 이동합니다.
3. **Windows 업데이트: 검색방법** 항목을 **Offline Scan file** 을 선택합니다.
4. 하단 **수정** 을 클릭합니다.

정책서버 프록시서버 설정 구성하기

(정책 서버가 에이전트에 업데이트 및 패치를 프록시하는 것을 설정하는 것입니다)

1. 상단 패널에서 **시스템**으로 이동합니다.
2. **정책 서버 IP 주소 > 환경설정** 탭으로 이동합니다.
3. **운영체제 업데이트 Proxy 서비스설정** 섹션을 찾으세요. **사용여부** 를 **On** 으로 선택합니다.
4. 하단 **수정** 를 클릭합니다.

네트워크 트래픽 제어

주기적으로 네트워크 사용량을 수집하여 설정된 수치 이상일 경우 네트워크 인터페이스를 차단합니다.

- 네트워크 트래픽이 급격하게 상승하여 설정된 임계치를 넘었을 경우 인터페이스를 차단하여 네트워크를 보호하고 사용자 알림
- 네트워크 사용량을 수집하여 네트워크 모니터링에 활용 가능

노드정책에 에이전트 액션 추가

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책창에서 **원하는 노드정책ID** 를 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **네트워크 트래픽 제어** 를 찾아 **선택** 항목으로 이동 시킵니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.

네트워크 트래픽 제어 설정

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **네트워크 트래픽 제어 설정** 을 찾아 클릭합니다.
4. **조건설정** 및 옵션을 입력합니다.

네트워크 트래픽 제어 설정을합니다.

1. **확인 주기** : 인터페이스의 인/아웃바운드 정보 확인 주기를 설정합니다.
2. **이동평균 시간** : 이동평균을 계산할 시간을 설정합니다.
3. **전체 임계치** : 네트워크 사용량의 전체 임계치를 입력합니다. (*B/s* 기준)
4. **인바운드 임계치** : 인바운드 네트워크 사용량의 임계치를 입력합니다. (*B/s* 기준)
5. **아웃바운드 임계치** : 아웃바운드 네트워크 사용량의 임계치를 입력합니다. (*B/s* 기준)

차단 알림 설정을합니다.

1. **인터페이스 차단 알림**
   [설정된 규칙을 위반하여 네트워크 인터페이스가 차단되었을 때 사용자에게 알리는 방법을 선택합니다.]
   - **사용안함** : 장치가 차단되어도 사용자에게 차단알림을 하지 않습니다.
   - **사용자메시지** : 직접 사용자에게 보여질 메시지를 정의하여 장치가 차단됨을 알립니다.
   - **에이전트팝업** : 에이전트 기본팝업창을 사용하여 장치가 차단됨을 알립니다.
2. **수정** 버튼을 클릭합니다.

네트워크 폴더 공유 제어

네트워크에 공유된 폴더정보를 수집하며 일정시간 이상 공유되는 폴더를 제어합니다. 플러그인을 통해 특정 시간, 특정 권한으로 제한적인 허용이 가능합니다.

- 네트워크 폴더 공유에 대한 정보 제공
- 불필요한 폴더 공유로 인한 파일 노출 방지를 위하여 제한적인 허용 기능

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **네트워크 공유폴더** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **공유 폴더 정보 수집** 에 대해 **Off** 를 선택하여 네트워크를 통해 공유 폴더에 대한 정보를 수집하지 않습니다.
2. **공유폴더 해제** 에 대해 **On** 을 설정하여 폴더 공유 상태를 해제합니다.
   - **공유 허용 시간** : 공유폴더의 임시 사용 가능 시간을 설정합니다. (초 - 개월)
   - **읽기권한만 허용** 에 대해 **On** 으로 설정하여 읽기권한만 있는 폴더는 허용하고 쓰기권한이 있는 폴더는 공유를 해제합니다.
   - **Everyone권한 외 허용** 에 대해 **On** 으로 설정하여 Everyone 권한이 존재하는 폴더만 공유를 해제합니다.
   - **관리폴더 허용** 을 **Off** 로 설정하여 관리 공유에 대한 액세스를 비활성화합니다.(예: *admin$, c$, d$, e$*)
3. **공유해제알림 방법** 은 사용자메시지 또는 에이전트팝업을 선택하여 공유 해제를 사용자에게 알려 줍니다.
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 노드정책 창에서 **원하는 정책ID** 를 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **네트워크 공유폴더** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.

10. **수정** 버튼을 클릭합니다.

네트워크정보 수집

네트워크 인터페이스 정보와 탐지된 포트 정보를 수집하여 노드정보에 표시합니다. 관리자에게 가시성을 제공하여 네트워크 제어에 활용 가능합니다.

- 트래픽 정보를 모니터링하여 관리자의 네트워크 제어에 활용
- 포트정보를 수집하여 오픈 포트 목록을 통해 관리자가 이상징후 확인 가능

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **네트워크정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.

아래 **플러그인설정** 이 있습니다.

1. **트래픽 정보 업데이트 비율** 의 경우 마지막으로 전송한 인터페이스 트래픽의 이동평균 차이가 설정비율 이상 차이 나면 인/아웃바운드 정보를 전송합니다.
2. **전송주기** 에 대해 주기적 간격(초 - 시간)을 조정합니다.
3. **이동평균 시간** 의 경우, 전송주기 보다 이동평균 시간을 더 크게 조정합니다.
4. **열린포트 정보 수집** 에 대해 **On** 으로 설정하여 열린포트 정보를 수집합니다.
5. **수정** 버튼을 클릭합니다.
6. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
7. 적용하고자 하는 **노드정책** 을 클릭합니다.
8. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
9. 사용가능 항목에서 **네트워크정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
10. **추가** 버튼을 클릭합니다.
11. **수정** 버튼을 클릭합니다.

모니터정보 수집

로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다. 모니터 정보를 수집하여 자산 관리/교체 등에 활용 가능합니다.

- 특정 inch 이하의 모니터 정보를 수집하여 하드웨어 교체 작업에 활용

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **모니터정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. 사용가능 항목에서 **모니터정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

모양 및 개인설정

바탕화면, 화면보호기에 대한 설정 정보를 수집 및 제어합니다. 사내 표준 바탕화면 및 화면보호기 규정 강제 적용 기능을 제공합니다.

- 화면보호기 해제시 재로그인 강제화
- 사내 표준 바탕화면 또는 화면보호기를 강제 적용하여 내부 보안 정책 준수

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **모양 및 개인설정** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **화면 보로기정보 수집** 에서 **Off** 옵션을 설정하여 사용 중인 화면 보호기 설정 정보를 수집하지 않습니다.
2. **화면 보호기 제어** 에서 **On** 을 설정하여 화면 호보기를 설정합니다.
    - **화면 보호기 에서 직접 업로드 를 선택합니다. (옵션: 없음, *Genian* 화면 보호기, 직접 업로드)**
        - **화면 보호기 업로드** : 확장자가 scr인 파일을 업로드합니다.
        - **파일 이름** : 화면 보호기 파일 이름으로 설정됩니다. (예: *Genian.scr* / 미입력시 *"Genian.scr"* 로 적용)

- **사용자지정 화면 보호기 허용** 을 **On** 으로 설정하여 사용자가 화면 보호기를 선택할 수 있도록합니다.
- **대기시간** : 화면보호기로 전환되기 전까지의 동작 대기시간을 설정합니다. (분 - 시간)
- **대기시간 고정** 을 **On** 으로 설정하여 관리자가 설정한 시간보다 PC에 사용중인 대기시간이 짧을 경우에도 대기시간을 변경합니다.
- **Windows 로그온 화면 표시** 을 **On** 으로 설정하여 화면보호기 해제 시 Windows 로그온 화면 표시 기능을 활성화합니다.

3. **ZTNA 재인증** : 화면 보호기 해제 시 ZTNA 사용자 인증을 다시 수행할지 여부를 선택합니다. (*On / Off*)
4. **바탕 화면 이미지 제어** : 바탕 화면에 사용 할 이미지를 업로드 하여 사용할 수 있습니다. 기능은 화면 보호기 제어의 메뉴와 동일합니다.(이미지 위치: 가운데, 바둑판식, 늘리기)
5. **무결성 검사 주기** : 설정 주기에 화면보호기와 바탕화면 이미지에 대한 무결성을 검증하며 파일이 손상된 경우 파일을 새로 다운로드 받습니다.(분 - 시간)
6. **수정** 버튼을 클릭합니다.
7. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
8. 적용하고자 하는 **노드정책** 을 클릭합니다.
9. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
10. **사용가능** 항목에서 **모양 및 개인설정** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
11. **추가** 버튼을 클릭합니다.
12. **수정** 버튼을 클릭합니다.

화면 잠금 해제 시 인증 코드 추가

사용자가 잠김 화면에서 윈도우 로그인을 하고 화면 잠금 해제 를 할 수 없는 경우(에이전트 정책)에 대해 인증 코드를 활성화할 수 있습니다. 사용자가 오프라인 상태(정책 서버와 통신을 할 수 없는 상태)일 수 있으며 화면의 잠금을 해제 하려면 인증해야합니다. 아래 옵션은 관리자에게 관리자 코드를 생성하여 화면 잠금에 들어가기위한 인증 코드를 얻는 버튼을 제공합니다.

Note: **모양 및 개인설정** 플러그인이 노드 정책에서 이미 할당 및 정책이 적용되어 있어야합니다. (기본정책)

---

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책창에서 **원하는 노드정책ID** 를 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **에이전트인증창** 를 찾아 **선택** 항목으로 이동 시킵니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.
8. **정책 > 노드정책 > 노드액션** 으로 이동하여, 노드액션 관리창에서 **에이전트인증창** 을 클릭합니다.

아래에서 **에이전트 액션 플러그인 설정(기타)** 을 구성합니다.

1. **종료 금지** 옵션을 **On** 으로 설정하여 인증화면을 종료할 수 없도록 강제화합니다.
2. **잠금화면 배경색** 옵션에서 배경색을 변경합니다.

3. **잠금 해제 버튼 표시** 를 **On** 으로 설정하여 **화면 잠금 해제 버튼** 을 표시하도록합니다.
4. **수정** 버튼을 클릭합니다.

Note: 사용자가 "화면 잠금 해제 버튼"을 클릭하여 "에이전트 코드"를 생성하고 관리자에게 제공합니다. 그런 다음 관리자는 이를 사용하여 사용자가 입력할 수 있는 "인증 코드"를 발급하고 사용자는 "화면 잠금 해제"를 진행합니다.

무선 연결관리자 구성

Wireless Connection Manager 프로그램에 대한 옵션및 동작을 제어합니다. 무선 연결 설정에 대한 편의성을 제공합니다.

- 윈도우에서 기본으로 제공하는 무선 연결 서비스보다 사용자가 더욱 쉽게 무선랜을 이용 가능
- WCM을 활용하여 무선 AP 802.1X 인증 가능

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **무선연결관리자** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **무선랜정책** 에서 **할당** 을 클릭하여 시스템에 등록할 무선랜 정책을 선택합니다.
2. **무선 연결 관리자 사용** 을 **On** 으로 설정하여 Genian WCM(*Wireless Connection Manager*)을 적용합니다.
    - **강제실행** 을 **On** 으로 설정하여 무선연결관리자 프로그램을 항상 동작하도록 강제화합니다.
    - **유선사용시 숨김** 은 유선이 활성화되어 있으면 자동으로 무선연결관리자 프로그램이 바탕화면에서 사라 집니다.
    - **자동재연결** 은 AP와의 연결이 끊어진 경우 지정 된 무선랜정책 중 신호가 가장 좋은 AP로 자동 재연결을 시도합니다.
    - **비밀번호 만료전 알림시간** 은 인증 후 비밀번호 만료전에 사용자에게 알려주는 기간을 설정합니다.(시간 - 개월)
    - **AP 선택 기능** 은 연결가능한 AP들을 사용자가 직접 선택하거나, 가장 신호가 강한 항목만 연결하도록합니다.
    - **아이디 설명 문자열** 은 무선연결관리자 접속창의 인증ID 출력 문자열을 나타 냅니다.
    - **비밀번호 설명 문자열** 은 무선연결관리자 접속창의 비밀번호 출력 문자열을 나타 냅니다.
    - **아이디 저장 허용** 을 **On** 으로 설정하여 최근 인증 된 아이디를 입력창에 자동 입력되도록합니다.
    - **비밀번호 저장 허용** 을 **On** 으로 설정하여 최근 인증 된 비밀번호를 입력창에 자동 입력되도록합니다.
    - **자동연결 허용** 을 **On** 으로 설정하여 프로그램 시작 시 최근 연결된 무선 AP로 자동연결 시킵니다.
    - **출력이미지 선택** 의 **업로드** 버튼을 클릭하여 무선연결관리자 로그인창 상단에 출력되는 이미지를 업로드합니다.(*BMP* 포멧만 지원 가능)

- **배경색상** 은 대화상자의 배경색상을 나타 냅니다.
- **글자색상** 은 대화상자의 글자색상을 나타 냅니다.
- **도움말** 에서 대화상자에 출력 될 도움말 내용을 입력합니다.
- **도움말 html 사용** 을 **On** 으로 설정하여 대화상자에 출력되는 도움말을 html 처리 하도록합니다.
- **연결 후 실행** 에서 **추가** 를 클릭하여 무선연결이 성공적으로 완료된 이후에 실행 될 프로그램을 등록합니다.(프로그램 경로 또는 *CLI* 매개 변수 지정)

3. **무선 연결 관리자 사용** 을 **Off** 로 설정할 경우 설치되어있는 Genian WCM(*Wireless Connection Manager*) 이 제거됩니다.
   - 적용받는 노드정책에 플러그인 액션 정책이 제거된 경우에도 Genian WCM(*Wireless Connection Manager*) 이 제거됩니다.
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 노드정책창에서 **기본정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
8. **사용가능** 항목에서 **무선연결관리자** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

무선랜 제어

무선 네트워크 인터페이스에서 탐지되는 무선 AP에 대한 정보를 제공하며 허용되지 않은 AP 연결을 제한합니다. 무선랜을 사용하는 환경에서 AP에 대한 가시성을 제공합니다.

- AP 목록을 수집하여 인가/비인가 AP에 대한 가시성 확보 가능
- 무선랜 인터페이스의 AP모드를 비활성화하여 보안사고 방지 가능

무선랜 관리 환경설정

무선 네트워크 관련 수집된 데이터의 정확도를 높이기 위한 항목을 설정할 수 있습니다.

1. 상단 패널에 **설정 > 환경설정** 을 선택합니다.
2. 왼쪽 메뉴에서 **무선랜 관리** 를 클릭합니다.

항목	설명	참고
무선 AP Down 감지 (AP Down 감지시간)	수집된 AP 상태를 확인하는 최대시간을 설정합니다.	
무선 AP 자동삭제 (삭제대기시간)	수집된 AP 정보를 삭제하는 최대시간을 설정합니다.	
접속정보 자동삭제 (삭제대기시간)	수집된 무선 네트워크 접속 Client 정보를 삭제하는 최대시간을 설정합니다.	
내부 AP 감지	AP 위치를 감지하는 방식을 설정합니다.	내부 *SSID* 탐지

플러그인 설정

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **무선랜제어** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **플러그인 설정** 이 있습니다.

1. **AP 정보 수집 대상** : WLAN 인터페이스에서 탐지 및 연결된 SSID에 대한 정보를 수집합니다.
2. **무선 연결 이력 정보 수집** : **On** 을 설정하여 무선 연결 기록에 대한 정보를 수집합니다.
   - **정보 일괄 전송시간대** : 무선 연결 기록을 업데이트할 시간 범위를 지정합니다. (예: *0:00-23:59*)
   - **최대 시도 일수** : 조회할 일수를 지정하고 연결 기록을 수집합니다. (정보를 전송할 수 없는 경우 시작 시 업데이트됨)
   - **연결 이력 정보 유효 시간** : 수집된 연결 기록에 대한 시간을 지정합니다.
3. **AP 연결 제어** : 허용되지 않은 무선 AP에 대한 연결 해제 여부를 지정합니다.
   - **허용 AP 검색 방법** : 허용할 SSID 정의 방법을 선택합니다. (*WLAN* 그룹 선택, *SSID* 입력, 정규식 사용)
   - **허용 무선랜 그룹** : 드롭다운에서 허용될 WLAN 그룹을 선택합니다.
   - **제어 유보 시간** : 허용 AP 목록을 갱신하기 위한 AP 연결 허용 시간을 지정합니다. (초 - 분)
   - **차단알림** : AP 연결이 차단되었을 때 사용자에게 알리는 방법을 선택합니다. (에이전트 팝업 *or* 코드인증)
   - **허용 AP 자동 연결** : 허용된 SSID에 자동으로 연결할지를 지정합니다. (*(Windows Vista* 이상 동작*)*)
4. **AP 모드 차단** : 무선랜 인터페이스의 SoftAP나 Adhoc와 같은 무선 AP 모드를 차단합니다. (핫스팟 제어까지 가능)
   - **차단알림** : **On** 을 설정하여 사용자에게 무선 AP 모드가 비활성화되었음을 알립니다.
5. 네트워크 요구 사항을 기반으로 **CWP 메시지** , **조건설정** 및 **플러그인설정** 을 조정하여 입력합니다.
6. **수정** 버튼을 클릭합니다.
7. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
8. 노드정책 창에서 **기본정책** 을 클릭합니다.
9. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
10. **사용가능** 항목에서 **무선랜제어** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
11. **추가** 버튼을 클릭합니다.
12. **수정** 버튼을 클릭합니다.

백신정보 수집

PC에 설치되어있는 백신프로그램 정보 및 백신으로 검출된 바이러스치료로그를 실시간으로 수집합니다. 다양한 벤더들의 백신 정보를 ZTNA에서 수집합니다.

- 글로벌 벤더의 백신명, 버전, 패턴정보, 실시간 감시 정보 등을 수집하여 단말보안을 강화합니다.
- '안랩 V3', '하우리 바이로봇', '이스트소프트 알약' 등 국산 기업용 백신과 연동하여 실시간 감시 강제화, 검사 방식 등을 설정합니다.

백신 지원 목록

Genian ZTNA에서 지원되는 모든 안티바이러스를 버전별로 확인합니다.

벤더	제품명	제 품 버 전	정보제공 항목	v4.0.1x	v5.0.x
AhnLab	V3 Internet Security	7.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
AhnLab	V3 Internet Security	8.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
AhnLab	V3 Internet Security	9.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	4.0.106~	5.0.3~
ESTSecurity	Alyac Enterprise	2.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
ESTSecurity	Alyac Enterprise	3.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
ESTSecurity	Alyac Enterprise	4.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.146~	5.0.43~
ESTSecurity	Alyac Enterprise	5.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.146~	5.0.43~
Hauri	ViRobot	VRIS 2011	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
Hauri	ViRobot Desktop	5.5	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
Hauri	ViRobot	7.x	백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
INCA	nProtect Anti-Virus/Spyware	3.x	백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
SGA Solution	VirusChaser		백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
Avira	Free Antivirus	15.x	백신명, 현재패턴 버전명, 현재패턴 날짜	N/S	5.0.3~

continues on next page

Table 2 – continued from previous page

벤더	제품명	제 품 버 전	정보제공 항목	v4.0.1x	v5.0.x
Avira	Internet Security Suite	15.x	백신명, 현재패턴 버전명, 현재패턴 날짜	N/S	5.0.3~
Avira	An-tivirus Pro	15.x	백신명, 현재패턴 버전명, 현재패턴 날짜	N/S	5.0.3~
Avira	End-point Suite	15.x	백신명, 현재패턴 버전명, 현재패턴 날짜	N/S	5.0.3~
Bitde-fender	An-tivirus Plus	23.x	백신명, 제품버전, 실시간감시	N/S	5.0.14~
Bitde-fender	Internet Security	23.x	백신명, 제품버전, 실시간감시	N/S	5.0.14~
Bitde-fender	Total Security	23.x	백신명, 제품버전, 실시간감시	N/S	5.0.14~
Cylance	PRO-TECT	2.0.1420.13	백신명, 제품버전, 실시간감시	4.0.106~	5.0.24~
Crowd-Strike	Crowd-Strike FAL-CON Sensor		백신명, 제품버전, 실시간감시	N/S	5.0.29~
ESET	NOD32 An-tivirus	9.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.3~
ESET	NOD32 An-tivirus	12.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.3~
ESET	End-point Security	12.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.3~
ESET	Internet Security	12.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.3~
ESET	Smart Security	12.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.3~
F-Secure	F-Secure Anti-Virus	17.x	백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.15~
Kasper-sky	An-tivirus		백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
Kasper-sky	End-point Security	11.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
McAfee	Desktop Protec-tion		백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~

continues on next page

Table 2 – continued from previous page

벤더	제품명	제 품 버 전	정보제공 항목	v4.0.1x	v5.0.x
McAfee	Total Protection (VirusScan)	22.3	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.24~
McAfee	Endpoint Security	10.6.0.542	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	4.0.106~	5.0.24~
Microsoft	Security Essentials		백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.3~
Microsoft	Forefront		백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
Microsoft	System Center		백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.3~
Microsoft	Windows Defender		백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
Panda Security	Panda Endpoint Protection Plus	8.0.15	백신명, 제품 버전, 현재패턴 날짜(마지막 업데이트 날짜), 실시간감시	N/S~	5.0.30~
Sophos	Home	1.3.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	N/S	5.0.17~
Sophos	Endpoint	2.1.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	N/S	5.0.17~
Symantec	Endpoint Protection	12.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
Trend Micro	OfficeScan	10.x	백신명, 현재패턴 버전명, 현재패턴 날짜	4.0.106~	5.0.3~
Trend Micro	APex One		백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	N/S	5.0.42~
Check Point	Endpoint security		백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	N/S	5.0.42~

백신정보 수집

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **백신정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **백신정보 검사주기** 에서 백신정보를 검사하는 주기를 정의합니다.(초 - 시간)
2. **실시간감시OFF 보류 횟수** 는 일정횟수 이상 연속 Off로 수집될 경우에만 실시간감시 Off 로 보고되도록 설정합니다.
3. **백신연동** 을 **On** 으로 설정하여 백신소프트웨어 연동기능을 사용하도록합니다.
   - **연동가능 백신**
   - 안랩 V3
   - 하우리 바이로봇
   - 이스트소프트 알약
   - INCA nProtect
   - **치료 감사기록** 에서 치료한 바이러스에 대한 감사기록 여부를 선택합니다.
   - **중복로그 제외시간** 은 바이러스에 대한 동일한 로그를 남기지 않는 시간을 설정 (분 - 시간)
   - **실시간감시 강제화** 를 **Off** 로 선택하여 실시간 검색을 비활성화합니다.
   - **강제검사** 는 마지막 바이러스 검사시각이 설정주기이상일때 강제로 검사를 수행합니다.(시간 - 개월 */0*이면 수행하지 않음)
   - **검사 방식** 은 **전체검사** 선택합니다.
   - **검사창 UI 숨기기** 를 **On** 으로 설정하여 사용자에게 바이러스검사창 UI 를 표시하지 않습니다.
   - **강제업데이트** 는 마지막 백신엔진 업데이트시각이 설정주기이상일 때 강제로 업데이트를 수행합니다. (시간 - 개월)
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 적용하고자 하는 **노드정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **백신정보 수집** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

비밀번호 유효성 검사

Windows 계정의 비밀번호에 대한 유효성을 검사하고 검증되지 않은 비밀번호를 안전한 비밀번호로 변경시킵니다. 특수문자 사용 등 비밀번호 규칙을 강제화하여 단말 보안을 강화합니다.

- 관리자가 정한 비밀번호 문자열의 규칙 준수를 강제화하여 패스워드 보안을 강화
- 비밀번호 변경 주기를 설정하여 주기마다 패스워드 변경을 강제화

노드정책에 에이전트 액션 추가

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책창에서 **원하는 노드정책 ID** 를 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **비밀번호유효성검사** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.

비밀번호유효성검사 설정

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **비밀번호유효성검사** 을 찾아 클릭합니다.
4. 옵션 설정에서 **조건설정** 을 입력합니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **검증된 계정표시** : **On/Off** 설정을 통해 대화상자에 검증된 계정에 대해서도 표시를 할지 여부를 선택합니다.
2. **검증창 고정** : **On/Off** 대화상자를 화면의 중앙에 고정합니다.
3. **Windows 로그온 계정** 에서 다음을 설정합니다.
   - **비밀번호 문자열 검사방법** : "규칙검사" 를 설정합니다. (비밀번호 규칙의 경우 "설정 > 환경설정 > 사용자인증 > 비밀번호정책" 규칙이 적용 됩니다)
   - **비밀번호 변경주기** : 윈도우 로그인 계정에 대한 비밀번호 변경주기를 설정합니다. (시간 - 개월)
   - **만료전알림** : 비밀번호 시간이 만료되기 전에 알림을 발생합니다. (만료시간은 정책이 적용 된 시점부터 적용 됩니다.)
   - **검사예외ID** : 검사 예외대상의 사용자 ID의 전체문자열을 입력합니다. (여러개 입력시 콤마로 구분, 대소문자를 구분하지 않습니다.)
4. **수행주기** 의 경우 주기 간격(초 - 개월)을 조정합니다.
5. **수정** 버튼을 클릭합니다.

비밀번호 유효성 검사 결과 확인

Note: 정책이 적용되면 검증되지 않은 단말에 비밀번호 검증창이 팝업 되고 사용자는 자신의 윈도우 계정 비밀번호를 입력합니다.

1. 상단 항목의 **관리 > 노드** 로 이동합니다.
2. 노드리스트 창에서 에이전트가 설치 된 노드의 **IP** 를 클릭합니다.
3. **시스템정보** 탭 아래로 스크롤 하여 **계정비밀번호 검증 정보** 항목의 결과를 확인합니다.

사용자 알림메시지

사용자에게 알림메시지를 표시합니다. 관리자가 에이전트를 통해서 사용자에게 메시지를 전달합니다.

- 사용자에게 알림 메시지를 표시하여 클릭시 설정된 URL로 리다이렉션
- 공지사항 등을 메시지 확인 알림을 통해 감사기록 저장

사용자 알림메시지 옵션 구성

1. **메시지 제목** 에 에이전트 알림 시 표시할 제목을 설정합니다.
2. **클릭시 CWP 접속** 을 **On** 으로 설정하여 에이전트 알림 클릭 시 CWP 페이지로 이동하도록합니다.
   - **CWP URL** 에 **설정** 버튼을 클릭하여 템플릿을 사용하거나 URL을 직접 입력합니다.
3. **팝업창 고정** 의 경우 에이전트 알림을 닫지 못하도록 할지 여부를 선택합니다. (*On/Off*)
   - **메시지 타입** : 사용자메시지 타입을 선택합니다. (일반, 경고)
   - **메시지확인 알림** : 사용자가 메시지를 확인했으면 감사 로그를 기록하도록 설정합니다. (*On/Off*)

노드정책을 통하여 사용자 알림메시지 정책 구성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **사용자 알림메시지** 를 찾아 클릭합니다.
4. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
5. 사용자 알림메시지 정책을 구성할 노드정책을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **사용자 알림메시지** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.
10. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

제어정책을 통하여 사용자 알림메시지 정책 구성

1단계. 제어 대상 노드그룹 생성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **추가** 버튼을 클릭합니다.
5. 제어 대상의 조건 설정 후 **추가** 버튼을 클릭합니다.
6. **생성** 버튼을 클릭합니다.

2단계. 제어액션 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어액션** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭합니다.
3. 플러그인선택 항목에서 **사용자 알림메시지** 플러그인을 선택합니다.
4. **조건설정** 및 옵션을 입력합니다.
5. **생성** 버튼을 클릭합니다.

3단계. 제어정책 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어정책** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭하고, **제어정책 마법사** 를 완료합니다.
3. **정책 기본설정** 탭에서 **ID** 항목에 **사용할 정책 ID** 를 입력합니다.
4. **노드그룹 설정** 탭에서 **새로 추가한 노드그룹** 을 선택하고, **선택** 항목으로 이동합니다.
5. **권한 할당** 과 **제어 옵션** 탭에서 **원하는 옵션** 을 입력합니다.
6. **제어액션 설정** 탭에서 **생성한 제어액션** 을 찾아 **선택** 항목으로 이동합니다.
7. **완료** 버튼을 클릭합니다.
8. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

소프트웨어 정보 수집

설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.

- 단말에 설치된 소프트 웨어 목록을 수집하여 비인가 소프트웨어 설치 여부 확인 제공

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **소프트웨어 수집** 을 찾아 클릭합니다. (*Windows*에 하나, *MacOS*에 하나씩 있음)

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **수행주기** 의 경우 실행 주기 간격(초 - 개월)을 조정합니다.

2. **수정** 버튼을 클릭합니다.
3. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
4. 적용하고자 하는 **노드정책** 을 클릭합니다.
5. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
6. 사용가능 항목에서 **소프트웨어정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
7. **추가** 버튼을 클릭합니다.
8. **수정** 버튼을 클릭합니다.

수행조건만 검사

액션에 설정된 수행 조건을 검사하는데 사용하는 플러그인입니다. 프로세스, 파일, 시스템 및 인증된 사용자 등 조건을 설정하여 검사할 수 있습니다.

- 특정 프로세스의 해쉬값 검사
- 사내 필수프로그램 설치 여부 확인

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창 **작업선택** 오른쪽의 드롭다운 버튼을 클릭하여 **Windows** 운영체제를 선택합니다.
4. 노드액션 리스트에서 **수행조건만 검사** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다. (이 플러그인이 작동하려면 조건이 추가되어야합니다)

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.
3. **수행주기** : 설정된 주기마다 액션을 수행합니다. (초 - 개월)
4. **추가** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 적용하고자 하는 **노드정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **수행조건만 검사** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

스크립트 수행

Note: 스크립트 수행 플러그인은 CC 평가 항목에 포함된 기능이 아니므로 CC 인증을 요구하는 공공기관에서는 해당 플러그인을 사용할 수 없습니다.

vbs 또는 bat 파일 형식의 스크립트를 수행합니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **스크립트 수행** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.

아래 **플러그인설정** 이 있습니다.

1. **스크립트 형식** : 수행 할 스크립트의 형식을 설정합니다.(*Batch Script, VB Script*)
2. **스크립트** 에서 수행 할 스크립트를 입력합니다.
3. **수행 계정** : 스크립트를 수행 할 때 사용할 수행계정을 설정합니다.
4. **리부팅옵션** 의 경우 사용자에게 알림을 보낼 지 자동 재부팅을 할지 선택합니다.
5. **수행주기** 는 설정 된 주기마다 액션을 수행합니다. (초 - 개월)
6. **수정** 버튼을 클릭합니다.
7. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
8. 적용하고자 하는 **노드정책** 을 클릭합니다.
9. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
10. **사용가능** 항목에서 **스크립트 수행** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
11. **추가** 버튼을 클릭합니다.
12. **수정** 버튼을 클릭합니다.

시스템 종료

지정된 시각에 Windows 시스템의 절전, 재시작, 종료를 수행합니다. 사용자의 시스템 전원을 제어하여 단말 보안을 강화합니다.

- ZTNA의 여러 제어 기능 중 시스템 전원 제어 제공
- 직원 퇴근시간에 맞춰 시스템 자동 종료

시스템 종료 옵션 구성

1. **동작방식** 의 경우 PC의 전원을 제어하는 방식(절전, 다시시작, 시스템 종료)을 선택합니다.
2. **강제화모드** 를 **On** 으로 설정하여 사용자가 취소할 수 없도록합니다.
3. **종료전 알림 시간** 에 PC의 전원이 제어되기 전 사용자에게 알람을 표시할 시간을 설정합니다. (초 - 분)
4. **PC가동시간** 이 지난 경우에만 전원 제어를 수행합니다. 본 플러그인에 의해 절전으로 전환된 후 해제 시점을 가동 시작 시각으로 간주합니다. (분 - 개월)
5. **타이틀 표시** 를 **On** 으로 설정하여 대화상자의 타이틀을 표시합니다.
6. **메시지 표시 방법** : 제어 전 알림 시간동안 대화상자에 표시할 내용을 선택합니다. (*HTML*, 이미지)
   - **HTML** 을 설정할 경우 사용자에게 표시할 HTML 메시지를 입력합니다.
   - **이미지** 를 설정할 경우 사용자에게 표시할 Bitmap 이미지를 업로드합니다.

노드정책을 통하여 시스템 종료 정책 구성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **시스템 종료** 를 찾아 클릭합니다.
4. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
5. 시스템 종료 정책을 구성할 노드정책을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **시스템 종료** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.
10. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

제어정책을 통하여 시스템 종료 정책 구성

1단계. 제어 대상 노드그룹 생성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **추가** 버튼을 클릭합니다.
5. 제어 대상의 조건 설정 후 **추가** 버튼을 클릭합니다.
6. **생성** 버튼을 클릭합니다.

2단계. 제어액션 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어액션** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭합니다.
3. 플러그인선택 항목에서 **시스템 종료** 플러그인을 선택합니다.

4. **조건설정** 및 옵션을 입력합니다.
5. **생성** 버튼을 클릭합니다.

3단계. 제어정책 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어정책** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭하고, **제어정책 마법사** 를 완료합니다.
3. **정책 기본설정** 탭에서 **ID** 항목에 **사용할 정책 ID** 를 입력합니다.
4. **노드그룹 설정** 탭에서 **새로 추가한 노드그룹** 을 선택하고, **선택** 항목으로 이동합니다.
5. **권한 할당** 과 **제어 옵션** 탭에서 **원하는 옵션** 을 입력합니다.
6. **제어액션 설정** 탭에서 **생성한 제어액션** 을 찾아 **선택** 항목으로 이동합니다.
7. **완료** 버튼을 클릭합니다.
8. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

에이전트 인증창

사용자인증 수행시 WEB페이지가 아닌 에이전트 자체 인증창을 사용합니다. 에이전트를 통해서 CWP 인증보다 간편한 사용자 인증을 제공합니다.

- 지문 등 2차 인증 기능 제공
- 종료 금지를 통한 사용자 인증 강제화

노드정책에 에이전트 액션 추가

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책창에서 **원하는 노드정책ID** 를 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **에이전트인증창** 를 찾아 **선택** 항목으로 이동 시킵니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.

에이전트를 통한 사용자 인증 설정

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **에이전트인증창** 을 찾아 클릭합니다.

아래 **인증정책** 설정

1. **인증방법** 에서 사용자 인증 방법을 선택합니다.
2. **2단계 인증** 에서 2단계 인증 방법을 선택합니다.

아래 **화면설정** 구성

1. **이미지 사용** 의 경우 에이전트 인증창의 이미지를 지정합니다.
2. **타이틀바 표시** 의 경우 에이전트 인증창의 타이틀 문구를 표시할지 여부를 지정합니다.
3. **배경색** 은 인증창의 색상을 지정합니다.
4. **글자색** 은 대화상자의 글자색상을 나타 냅니다.
5. **HTML 사용** 은 HTML을 사용하여 도움말을 표시합니다.

아래 **기타** 설정

1. **종료 금지** 의 경우 에이전트 인증 대화 상자에 대한 닫기 작업을 사용하지 않도록 설정하여 인증을 적용할지 여부를 지정합니다.
2. **인증 후 실행**, 사용자가 인증된 후 실행되는 프로그램을 추가합니다.
3. **수정** 버튼을 클릭합니다.

에이전트센서

에이전트센서 플러그인은 네트워크센서가 없는 네트워크 세그먼트에서 기본적인 노드 감지를 수행합니다.

네트워크를 실시간으로 모니터링하고 새로운 노드정보 또는 변경된 노드정보를 정책 서버로 전송합니다. 관리자는 정책 서버가 제공하는 관리 콘솔을 통하여 에이전트센서가 동작중인 네트워크 대역의 정보를 조회할 수 있습니다.

에이전트센서는 노드에서 주기적으로 발생되는 DHCP, NetBIOS, UPNP 및 mDNS와 같은 패킷에 포함된 정보를 수신하여 노드에 영향을주지 않고 정보를 수집할 수 있습니다. nmap,snmp 등을 이용한 정보 수집은 에이전트센서가 등록된 물리적인 센서 장비에 의해서 정보를 수집합니다.

- 네트워크 센서를 설치 하기 어려운 네트워크 세그먼트의 노드 모니터링
- 네트워크 제어가 필요 없이 노드 모니터링만 수행하고자 하는 네트워크 세그먼트

세부 기능 상세

- 본 플러그인은 별도의 설정이 필요하지 않습니다.
- 에이전트 기반 센서 플러그인은 정책서버와 직접 통신하며 에이전트센서라는 가상센서로 등록됩니다.
- 에이전트 기반 센서는 Windows 로그인(서비스)에 관계없이 작동 가능
- 에이전트 플러그인 기능:
  - **신규 노드 등록** : 수신 된 트래픽을 기반으로 **노드를 등록** 합니다.
  - **서브넷 스캔너** : 6시간 주기로 관리 네트워크(C Class)에 대산 ARP Request에 대한 응답결과를 기반으로 신규 노드를 감지합니다.
  - **노드 헬스 체크** : 10초 마다 한번씩 ICMP를 보내고 Windows에서 ARP 테이블을 확인하여 노드 링크 상태를 업데이트합니다.
  - 2분 동안 ARP 테이블에서 노드가 식별되지 않으면 10초마다 ICMP가 전송됩니다.
  - ARP 테이블에서 3분 동안 노드가 식별되지 않으면 링크 상태가 **DOWN** 으로 표시됩니다.
  - 플러그인은 포트 3871에서 수신 대기하여 해당 네트워크대역의 센서상태를 모니터링합니다.
    - 물리 네트워크센서가 감지되면 에이전트 센서는 대기 상태로 전환됩니다.
    - 여러 에이전트 센서 플러그인이 동일대역 에이전트에 다수 배포가 될 경우 한대의 에이전트센서만 동작합니다.

에이전트센서 사용방법

1. 물리 네트워크센서에 에이전트센서 대역을 설정하여 에이전트센서가 해당 네트워크센서 하위로 추가될 수 있도록 합니다.

- 상단 항목의 **시스템** 으로 이동합니다.
- 장비 목록에서 네트워크센서를 선택합니다.
- **환경설정** 탭으로 이동하여 **기타설정 항목 > 에이전트센서 네트워크** 에 에이전트센서에서 사용할 네트워크대역을 입력합니다.
- **수정** 버튼을 클릭합니다.

2. 에이전트센서를 사용할 대역의 노드정책에 센서노드액션을 할당합니다.

- 상단 **정책** 메뉴로 이동합니다.
- 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
- 적용하고자 하는 **노드정책명** 을 클릭합니다.
- **노드액션 설정** 항목에서 **할당** 을 클릭합니다.
- 사용가능 항목에서 **에이전트센서** 을 찾아 선택 항목으로 드래그하여 이동합니다.
- **추가** 버튼을 클릭합니다.
- **수정** 버튼을 클릭합니다.

노드에 설치된 에이전트에 플러그인이 설치되고 동작하게되면 정책서버에 가상의 에이전트센서가 추가됩니다.

운영체제정보 수집

Windows 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.

- 관리자가 운영체제 정보를 수집하여 운영체제별 별도 정책 적용

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **운영체제정보 수집** 을 찾아 클릭합니다. (*Windows*에 하나, *MacOS*에 하나씩 있음)

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 " 설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. 사용가능 항목에서 **운영체제정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

유선인증관리자

유선인터페이스의 인증 설정 및 유선인증창에 대한 옵션을 정의합니다. Windows에서 기본적으로 제공하는 설정보다 간편한 802.1X 설정을 제공합니다.

- 802.1X 유선인증에 대해 간편한 인증방법 및 SSO 연동 제공

802.1x는 엔드 포인트 단말을 사용하는 사용자의 검증을 제공하는 IEEE 표준 스위치 포트 인증입니다. 유선 환경에서 이것은 스위치의 물리적 포트이고, 무선 환경에서는 AP (Access Point)와의 연결입니다. 포트 기반 인증은 네트워크에 연결하려는 엔드포인트 단말이 802.1x 요청자를 사용하고 다른 내부 네트워크 장치와의 통신이 시작되기 전에 EAP 메시지를 사용하여 연결 지점에서 요청되어야 한다는 것입니다. 802.1x를 통해 사용자 액세스를 인증하도록 정책 서버를 구성할 수 있습니다.

1 단계. 802.1x 인증을 위한 노드그룹 생성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 정책그룹 생성** 을 클릭합니다.
4. **ID** 입력란에 **802.1x 인증** 을 기입합니다.
5. 그룹조건 메뉴에서 **조건설정 > 추가** 버튼을 클릭합니다.
6. 다음 정보 입력:
   - 항목: **IP 주소**
   - Operator: **서브넷에 속하여**
   - Value: **(Network Subnet)**
7. **추가** 버튼 클릭
8. **생성** 버튼 클릭
9. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

2 단계. 802.1x 인증을 위한 노드 정책 생성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭하고, **노드정책 마법사** 를 완료 시킵니다.
4. **정책 기본설정** 탭에서 **ID** 항목에 **802.1x 인증** 을 입력합니다.
5. **노드그룹 설정** 탭에서 **802.1x 인증** 노드그룹을 선택하고, **선택** 항목으로 이동 시킵니다.
6. **정책 세부설정** 탭에서 **원하는 옵션** 을 입력합니다.
7. **노드액션 설정** 탭에서 **유선인증관리자** 를 찾아 **선택** 항목으로 이동 시킵니다.
8. **위험감지 설정** 탭의 설정은 패스. (이 탭에는 아무것도 필요하지 않습니다)
9. **완료** 버튼을 클릭합니다.
10. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

3 단계. 유선인증관리자 플러그인 구성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. **유선인증관리자** 를 찾아 클릭합니다.
4. **플러그인설정** 을 원하는 옵션으로 설정합니다.
5. **수정** 버튼을 클릭합니다.
6. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

(아래 단계는 새 노드 정책을 생성하지 않고 기존 노드 정책을 사용하는 옵션입니다)

4단계. 노드 정책에 에이전트 액션 할당

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. **노드정책의 ID** 를 찾아 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **유선인증관리자** 위치를 **선택** 항목으로 이동 시킵니다.
6. **추기** 버튼을 클릭합니다.
7. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

노드정책에서 에이전트 액션 제거

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. **노드정책의 ID** 를 찾아 클릭합니다.
4. **노드액션 설정** 에서 **유선인증관리자** 위치를 **사용가능** 항목으로 이동 시키거나, **노드액션 설정** 의 노드 액션 리스트에서 오른쪽 **삭제** 버튼을 클릭합니다.
5. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

인터페이스 제어

위험이벤트 발생시 인터페이스를 사용안함으로 바꾸는 기능을 제공합니다. ZTNA의 여러가지 제어방식 중 인터페이스 제어 기능을 제공합니다.

- 관리자가 여러가지 조건을 정책으로 정의하여 단말의 네트워크 인터페이스 제어

유선, 무선, 브리지 및 비규칙(Promiscuous) 모드를 사용하지 않도록 설정하여 엔드포인트 사용자의 Windows 단말에서 유선 및 무선 네트워크 인터페이스를 제어 할 수 있습니다. 또한 팝업으로 표시되는 사용자 지정 메시지와 함께 인터페이스 사용 안 함 이벤트 알림을 보낼 수도 있습니다.

네트워크 인터페이스 제어 옵션 구성

1. **타입별 차단** : 사용하지 않도록 설정할 네트워크 유형을 지정합니다. (유선, 무선, 또는 전체)
2. **기본장치 예외** : "On" 설정 시 정책서버와 통신이 가능한 네트워크 장치는 차단대상에서 제외 시킵니다.
3. **브리지 차단** : "On" 설정 시 브리지 인터페이스를 사용안함으로 강제화합니다. 기본장치 예외 옵션과 상관없이 차단됩니다.
4. **Promiscuous 차단** : "On" 설정 시 Promiscuous인 인터페이스를 사용안함으로 강제화합니다. 기본장치 예외 옵션과 상관없이 차단됩니다.
5. **차단알림** : 인터페이스 차단 이벤트에 대해 사용자에게 옵션 별(사용자메시지 *or* 에이전트팝업)로 메시지를 전달합니다.
6. **인터넷연결공유** : 인터페이스의 인터넷 연결공유 속성을 해제합니다.
7. **IPv6** : 인터페이스의 IPv6 속성을 해제합니다.

노드정책을 통하여 네트워크 인터페이스 제어 정책 구성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **인터페이스 제어** 을 찾아 클릭합니다.
4. **플러그인설정** 항목에서 필요한 옵션으로 설정합니다.
5. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
6. 인터페이스 제어 정책을 구성할 노드정책을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **인터페이스 제어** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.
11. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

제어정책을 통하여 네트워크 인터페이스 제어 정책 구성

1단계. 제어 대상 노드그룹 생성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **추가** 버튼을 클릭합니다.
5. 제어 대상의 조건 설정 후 **추가** 버튼을 클릭합니다.
6. **생성** 버튼을 클릭합니다.

2단계. 제어액션 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어액션** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭합니다.

3. 플러그인선택 항목에서 **인터페이스 제어** 플러그인을 선택합니다.
4. **조건설정** 및 옵션을 입력합니다.
5. **생성** 버튼을 클릭합니다.

3단계. 제어정책 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어정책** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭하고, **제어정책 마법사** 를 완료 시킵니다.
3. **정책 기본설정** 탭에서 **ID** 항목에 **사용할 정책 ID** 를 입력합니다.
4. **노드그룹 설정** 탭에서 **새로 추가한 노드그룹** 을 선택하고, **선택** 항목으로 이동 시킵니다.
5. **권한 할당** 과 **제어 옵션** 탭에서 **원하는 옵션** 을 입력합니다.
6. **제어액션 설정** 탭에서 **생성한 제어액션** 을 찾아 **선택** 항목으로 이동 시킵니다.
7. **완료** 버튼을 클릭합니다.
8. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

장치 제어

사용자 PC에서 사용금지된 장치들을 사용중지로 변경합니다. 시스템에 물리적으로 연결하는 모든 장치를 제어합니다.

- 외부 장치를 실행 중지 또는 제거
- 관리자가 에이전트를 통해 장치에 대한 사용 신청을 받아 승인 여부 결정

Note: 장치사용신청서 설정부분은 다음에 external-device-request 참고하시기 바랍니다.

---

1 단계. 장치 그룹 생성

- 장치 그룹은 제어에 필요한 일련의 장치를 정의하는 기능입니다. 정책에 대한 차단 또는 예외로 사용될 수 있습니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 장치제어 정책 > 장치그룹** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **기본정보** 에서 고유한 **ID 이름** 을 입력합니다. (예 : *"USB* 저장 장치*"*).
5. **조건설정** 에서 다음을 입력합니다.
    - **클래스명** : 장치 관리자에 있는 "**일부 이름**" (예: 범용 직렬 버스 컨트롤러)
    - **장치명**: 장치 관리자 정보에 있는 "**일부 공급 업체 이름**" (예: *USB* 대용량 저장소 장치)
    - **장치설명**: "**장치에 대한 설명**" 은 장치 관리자 세부 정보(속성정보)에서 확인
    - **이동장치 속성** : 이동식 장치 속성에 대한 옵션 선택
    - **USB 제조사** : USB 공급업체 이름을 지정
    - **USB 모델** : USB 모델 이름을 지정
    - **USB 시리얼** : USB 일련 번호 지정

6. **생성** 버튼을 클릭합니다.

설정 예:

기기 종류	클래스명	장치설명
외부 저장 장치	범용 직렬 버스 컨트롤러	USB 대용량 저장 장치
	스토리지 컨트롤러	USB 부착 SCSI (UAS) 대용량 저장 장치
	휴대용 장치	*
광학 장치	DVD / CD-ROM 드라이브	*
인쇄기	프린터	*

Note: 장치 그룹에 대한 세부사항은 external-device-group-detail 확인하시기 바랍니다.

2 단계. 장치제어 정책 생성

- 장치 제어 정책은 대상이 장치 제어를 수행하도록 차단하거나 허용 할 장치 그룹을 정의합니다.
- 플러그인이 업로드 되면 기본적인 출력장치에 대한 장치정책이 템플릿으로 제공됩니다. (장치제어 정책 ID : Data Leakage Prevention)

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 장치제어 정책** 으로 이동합니다.
3. **작업선택 > 생성** 버튼을 클릭합니다.
4. **기본정보** 에서 고유의 **ID 이름** 을 입력합니다. (예: *"USB* 스토리지 정책*"*)
5. **노드그룹 설정** 에서 **할당** 버튼을 클릭하고 **노드그룹** 을 선택합니다.
6. **차단장치 설정** 에서 **할당** 버튼을 클릭하고 **USB 저장 장치** 를 선택합니다.
7. 1단계에서 설정한 장치그룹이 아니더라도 아래의 **기본장치그룹** 으로 정의되어있는 항목을 선택 할 수 있습니다.

Bluetooth	• 블루투스 클래스에 속한 장치
CD/DVD/Floppy	• CD롬, 플로피 디스크 드라이브 클래스에 속한 장치
Local Printer	• 로컬PC에 직접 연결된 프린터 (프린터 클래스에 속하는 장치를 제거) • 로컬 프린터가 장치목록에서 "사용안함" 상태여도 프린트 출력이 가능하므로 장치를 제거한다.
USB Disk	• USB 타입의 저장장치 (장치속성의 인스턴스 경로가 'USBSTOR'로 시작하는 디스크 드라이브)
USB Network Adapter	• USB 포트로 연결된 네트워크 어댑터 (장치속성의 인스턴스경로가 'USB'로 시작하는 네트워크 어댑터)
USB Tethering	• 모바일기기에 USB 케이블로 연결된 네트워크 어댑터 (장치속성의 서비스가 usbrndis나 Netaapl인 네트워크 어댑터) • 안드로이드로 연결된 경우 네트워크 어댑터는 usbrndis 서비스를 사용하며, 아이폰의경우 Netaapl서비스를 사용한다.
Wireless Network Adapter	• 무선 네트워크 카드 장치

8. 만약 USB저장장치 중에서 제어를 허용할 별도의 장치가 존재한다면 **1단계. 장치그룹생성** 과 동일하게 예외그룹을 생성하여 **차단예외장치 설정** 에 할당 할 수 있습니다.
9. **생성** 버튼을 클릭합니다.

3 단계. 장치 제어 플러그인 설정

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **장치 제어** 을 찾아 클릭합니다.
4. **액션 수행설정 > 장치제어 방식** 에서 **제거** 또는 **중지** 를 선택합니다.
5. **수정** 버튼을 클릭합니다.

4 단계. 노드정책에 에이전트 액션 추가

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책창에서 **원하는 노드정책ID** 를 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **장치 제어** 를 찾아 **선택** 항목으로 이동 시킵니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.

파일 관리

Note: 파일 관리 플러그인은 CC 평가 항목에 포함된 기능이 아니므로 CC 인증을 요구하는 공공기관에서는 해당 플러그인을 사용할 수 없습니다.

파일을 복사, 삭제, 이동 및 이름을 변경하여 Windows의 파일을 관리 할 수 있습니다. 특정 파일을 실행할 수도 있습니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **파일 관리** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정 창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.

아래 **플러그인설정** 이 있습니다.

1. **파일 경로** 에서 관리 할 소스 파일을 지정합니다.
2. **관리 옵션** 에서 소스 파일에 대한 수행 옵션을 선택합니다. (실행, 삭제, 복사, 이동, 이름변경)
    - **실행 옵션** : 파일을 실행할 때 인수로 넘겨줄 추가적인 옵션을 설정합니다.
3. **수행계정** 의 경우 drop-down 에서 파일을 관리할 계정을 지정합니다.
4. **리부팅옵션** 의 경우 사용자에게 알림을 보낼지 자동 재부팅을 할지 선택합니다.
5. **수행주기** 는 설정 된 주기마다 액션을 수행합니다. (초 - 개월)
6. **수정** 버튼을 클릭합니다.
7. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
8. 노드정책 창에서 **기본정책** 을 클릭합니다.
9. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
10. **사용가능** 항목에서 **파일 관리** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.

11. **추가** 버튼을 클릭합니다.
12. **수정** 버튼을 클릭합니다.

파일 배포v2

Note: 파일 배포 플러그인은 CC 평가 항목에 포함된 기능이 아니므로 CC 인증을 요구하는 공공기관에서는 해당 플러그인을 사용할 수 없습니다.

파일 배포 플러그인은 파일을 실행하거나 특정 위치에 다운로드합니다. 정책서버는 에이전트와 통신하여 단말에게 파일에 대한 배포, 실행, 설치를 할 수 있습니다.

- 단말에 필요한 파일 배포
- 단말의 미설치 소프트웨어 설치

파일 배포v2 플러그인은 기존 파일배포 플러그인에서 보안성 강화에 치중하여 추가되었습니다.

파일 배포v2 플러그인은 안전한 파일 배포를 위해 파일 무결성 검증과 배포자 신원확인을 제공합니다.

- 3단계에 걸친 무결성 검증을 수행
- 최종 사용자의 배포자 식별 및 승인

파일 배포v2 플러그인은 배포하는 파일에 대한 전자서명을 필수로 요구하며 전자서명과 서명검증을 위해 공급망 보안을 위해 설계된 Sigstore Signing 방식을 사용합니다. 파일 배포v2 플러그인은 Sigstore Signing을 사용하여 Sigstore Keyless Signing과 Public Key Signing 2가지 방식을 선택적으로 사용할 수 있습니다.

전자서명 및 전자서명 검증을 위한 도구와 서비스(Sigstore)

Sigstore 개요

Sigstore 는 소프트웨어 공급망 보안을 위해 설계된 개방형 분산 인프라입니다.

Sigstore는 소프트웨어를 서명하고, 서명을 검증하고, 서명을 추적할 수 있는 도구와 서비스를 제공합니다. 또한 소프트웨어 공급망 보안을 개선하기 위해 설계된 프레임워크인 SLSA(Software Supply Chain Levels of Assurance)를 구현하기 위한 도구와 서비스를 제공합니다.

Sigstore는 소프트웨어 공급망 보안을 개선하기 위해 다음과 같은 기능을 제공합니다.

- 소프트웨어를 서명하여 소프트웨어의 무결성을 보장합니다.
- 서명을 검증하여 소프트웨어가 변조되지 않았는지 확인합니다.
- 서명을 추적하여 소프트웨어의 소스와 배포를 추적합니다.
- SLSA를 구현하여 소프트웨어 공급망의 보안을 향상시킵니다.

Sigstore는 소프트웨어 공급망 보안을 개선하기 위해 설계된 개방형 분산 인프라로, 소프트웨어 공급망의 보안을 향상시키는 데 도움이 될 수 있습니다.

Genian NAC에서의 Sigstore

Genian NAC에서는 강화된 보안을 위하여 파일배포 플러그인v2에서는 **Sigstore에서 제공하는 소프트웨어 무결성 보장을 위한 도구** 를 사용합니다.

배포할 파일에 Sigstore에서 제공되는 **cosign** 이라는 전자서명 및 서명 검증을 위한 도구를 사용하며 추가적으로 검증을 위한 불변 원장 기반의 서비스에서 전자서명정보를 검증합니다.

전자서명 검증을 위해 정책서버 및 플러그인에는 cosign 도구가 추가되어있습니다.

검증 방식	Sigstore Keyless Signing (Keyless)	Public Key Signing (self-managed-key)
검증 내용	• Google/Github/MS 에서 OIDC(OpenID Connect) 를 방식으로 인증하여 신원 정보로 배포 파일에 전자서명 수행 • 파일을 전송 받은 단말은 사용자ID(e.g. Google ID) 와 OIDC(Google Account) 정보를 통해서 Sigstore에 서명된 파일이 맞는지 검증	• 자체적으로 보유한 비밀키/공개키를 사용하여 배포 파일에 전자서명 수행 • 검증을 위한 인증서(공개키) 는 노드액션 수신 시 배포
환경 구성	• 인터넷이 가능한 환경에서만 사용 가능	• 인터넷망/폐쇄망 환경에서 모두 사용 가능
키 관리	• 별도의 키 사용하지 않는 방식으로 관리자 계정에 대한 보안만 요구	• 별도의 비밀키를 안전하게 보관 필요
준비사항	• 배포파일 전자서명을 위한 cosign 바이너리 파일 필요 (Sigstore Git hub Release v2.1.1 하단 **Assets** 에서 cosign-windows-amd64.exe 다운로드) • 배포파일 전자서명/서명검증에 사용되는 외부 인터넷 통신 허용 필요 (전자서명 PC, 정책서버, 사용자단말), 도메인 정보 • 배포파일 전자서명에 사용되는 OIDC(Google, Git, MS) 계정이 필요	• 배포파일 전자서명을 위해 cosign 바이너리 파일이 필요 • 배포파일 전자서명에 사용될 키가 필요하며 cosign을 사용해 생성하거나 별도의 키 준비 필요
제약사항	• 최초 등록된 배포자에서 다른 배포자로 변경 불가	• 최초 등록된 배포자에서 다른 배포자로 변경 불가 • 배포파일 전자서명에 사용된 키파일을 별도 관리(USB 등)

Sigstore Keyless Signing 방식

Sigstore는 **OpenID Connect(OIDC)를 사용하여 짧은 유효 기간의 인증서** 를 생성합니다.
이 인증서는 소프트웨어를 서명하는 데 사용 되며, 서명된 소프트웨어는 cosign을 통해 공개적으로 검증할 수 있습니다.

OIDC는 OAuth 2.0의 확장으로, 사용자에게 리소스에 대한 액세스를 제공하기 위해 로그인 인증을 사용하는 프레임워크입니다. OIDC는 사용자의 암호를 요구하지 않고도 인증서를 생성할 수 있기 때문에, Sigstore에서 짧은 유효 기간의 인증서를 생성하는 데 사용됩니다.

Sigstore Keyless Signing 사용 방법

Step1. 배포파일 전자서명

1. cosign을 다운로드 받아 배포파일 전자서명에 사용할 디렉토리에 저장합니다.
2. 파일명을 cosign.exe로 변경합니다.
3. 전자서명할 파일을 디렉토리에 복사합니다.
4. 시작 > 실행 > cmd를 입력한 후 실행하여 cosign.exe 파일이 위치하는 디렉토리로 이동합니다.
5. 아래 명령어를 입력하여 전자서명을 수행합니다.

```
> cosign.exe sign-blob {배포파일명} --output-certificate {생성할 cert 파일명.cert}␣
↪--output-signature {생성할 시그니처 파일명.sig}
```

6. cmd 창에 표시된 URL 정보를 복사하여 브라우저를 사용하여 Web 페이지에 접속합니다.
7. cmd 창에 표시된 8자리 문자 값과 cmd 창에 표시된 8자리 문자값이 동일한지 확인하고 `Submit` 버튼을 클릭합니다.
8. `Git`, `Google`, `Microsoft` 세가지 OIDC중 하나를 선택하고 인증을 수행합니다.
9. 잠시 후 cmd창에 서비스 약관 동의에 `y` 를 입력합니다.
10. 디렉토리내에 `Cert`, `Sig` 파일이 정상적으로 생성되었는지 확인합니다.

Step2. 전자서명 검증하기

1. 시작 > 창에서 아래 명령어를 입력합니다.

```
> cosign.exe verify-blob {배포파일명} --certificate {생성된 cert 파일명.cert} --
↪signature {생성된 시그니처 파일명.sig} --certificate-identity={인증에 사용한 ID} --
↪certificate-oidc-issuer={OIDC 발행자}
예시> cosign.exe verify-blob agent.zip --certificate agent.cert --signature␣
↪agent.sig --certificate-identity=genian@genians.com --certificate-oidc-
↪issuer=https://accounts.google.com
```

2. 정상적으로 전자서명이 이루어진 경우 **Verified OK** 라고 표시됩니다.

Step3. 노드액션 생성하기

1. 정책서버 Web콘솔에 접속하여 상단 **정책** 으로 이동합니다.
2. 좌측 메뉴 **노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **작업선택 > 생성** 을 클릭합니다.

아래 **기본설정** 이 있습니다.

4. **액션명** 은 용도에 따라 "(용도) 액션명" 형태로 사용하시면 향후 운영시 편하게 노드액션을 구분할 수 있습니다.

5. **설명** 은 용도에 따라 다르게 사용하는 경우 어떤 목적으로 사용하는 노드액션인지 구분할 수 있습니다.
6. **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

7. **OS 종류** 는 macOS, Linux, Windows 대상에 맞는 OS를 선택합니다.
8. **조건 설정** 은 일반적으로 배포를 할 때 특정조건에 맞는 사용자에게 배포하기 위해 사용합니다.

```
예시: "c:\%ProgramFiles%\abc.exe 가 존재하지 않는 경우" 라는 조건을 사용하여 배포하게 되면
↪abc.exe 가 존재하지 않는 단말에만 배포가 가능합니다.
```

9. **플러그인선택** 에서는 **파일 배포 V2** 를 선택합니다.
10. **배포 파일** 에는 업로드 버튼을 클릭하여 파일을 선택합니다.
11. **배포파일 검증방법** 은 Sigstore Keyless Signing을 선택합니다.
12. **신뢰하는 OIDC 발행자** 에는 전자서명 시 인증에 사용한 OIDC(Github, Google, Microsoft)를 선택합니다.
13. **신뢰하는 ID** 에는 전자서명 시 인증에 사용한 ID(email주소 형태)를 입력합니다.
14. **Certificate** 는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 **cert** 파일을 추가합니다.
15. **Signature** 는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 **sig** 파일을 추가합니다.
16. **배포 옵션** 의 경우 배포할 방식을 설정합니다.
    - **파일 실행**: 압축파일일 경우 "파일 경로"에 실행할 파일을 설정하고, "실행옵션"과 실행할 "수행 계정"을 설정하여 해당 파일을 실행시킵니다. "리부팅 옵션"을 통해 파일 실행 이후 리부팅여부를 설정합니다.
    - **다운로드**: 배포 파일을 복사할 단말의 파일 및 폴더 경로를 지정합니다.
17. **수정** 버튼을 클릭합니다.
18. 왼쪽 정책 항목에서 **노드정책** 으로 이동한 후 **기본정책** 을 클릭합니다.
19. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
20. **사용가능** 항목에서 **파일 배포** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
21. **수정** 버튼을 클릭한 후 **수정** 버튼을 클릭합니다.

Note:

Sigstore Keyless Siging 방식의 경우 전자서명/서명검증을 위하여 외부와 통신이 필수적이며 아래 도메인에 대한 통신이 허용되어야합니다.
(출발지: 정책서버, 에이전트), (서비스포트: TCP/443)
rekor.sigstore.dev : 원장 기록 시스템
oauth2.sigstore.dev : Sigstore oauth 흐름 제공 서버
accounts.google.com : OIDC 제공자(다른 OIDC인 경우 해당 OIDC 도메인)
fulcio.sigstore.dev : sigstore CA 서버
tuf-repo-cdn.sigstore.dev : SLSA 검증

Public Key Signing 방식

Sigstore cosign은 자체관리 키 전자서명 방식도 제공하고 있습니다.
Public Key Signing 방식은 직접 키를 생성하여 전자서명을 하거나 별도로 제작하여 사용중인 키를 사용하여 전자서명을 하는 방식입니다.

Public Key Signing 사용 방법

Step1. 배포파일 전자서명

1. Sigstore Keyless Signing 방식의 Step1 의 1~4 를 수행 후 다음으로 진행합니다.
2. 별도로 사용하는 전자서명용 키가 없다면 아래 명령어를 입력하여 전자서명용 비밀키와 공개키를 생성합니다.

```
> cosign.exe generate-key-pair
> 비밀키 패스워드 입력
> 비밀키 패스워드 확인
> dir 을 입력하여 비밀키(key) 파일과 공개키(pub) 파일이 생성되었는지 확인합니다.
```

3. 키를 생성했다면 아래와 같이 생성한 키를 사용하여 배포파일에 전자서명을 수행합니다.

```
> cosign.exe sign-blob {배포파일명} --key cosign.key --tlog-upload=false --
↪output-signature {생성할 시그니처 파일명.sig}
예시> cosign.exe sign-blob agent.zip --key cosign.key --tlog-upload=false --
↪output-signature agent.sig
```

Step2. 전자 서명 검증하기

1. CMD 창에서 아래 명령어를 입력합니다.

```
> cosign.exe verify-blob {배포파일명} --key {공개키 파일명.pub} --signature {생성된
시그니처 파일명.sig} --insecure-ignore-tlog=true --insecure-ignore-sct=true
예시> cosign.exe verify-blob agent.zip --key cosign.pub --signature agent.sig -
↪-insecure-ignore-tlog=true --insecure-ignore-sct=true
```

2. 정상적으로 전자서명이 이루어진 경우 **Verified OK** 라고 표시됩니다.

Step3. 노드액션 생성하기

1. Sigstore Keyless Signing 방식의 Step3 의 1~10 를 수행 후 다음으로 진행합니다.
2. **배포파일 검증방법** 은 Public Key Signing을 선택합니다.
3. **신뢰하는 공개키** 는 우측 파일읽기 버튼을 클릭하여 키생성 시 함께 생성되었던 **pub** 파일을 추가합니다.
4. **Signature** 는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 **sig** 파일을 추가합니다.
5. Sigstore Keyless Signing 방식의 Step3 의 16~21 를 수행합니다.

Danger:

최초 설정된 배포방식과 배포자 변경이 불가능 하기때문에 최초 노드액션 생성 시 사용한 Private key 는 **분실위험이 없도록 안전하게 보관** 해야 합니다.
등록된 배포자정보는 Web콘솔 설정 > 환경설정 > 에이전트 > 배포 옵션 섹션에서 확인할 수 있습니다.

Yubikey 를 이용한 개인키 관리방법

Public Key 방식으로 개인를 관리하면서, 관리되고있는 PC 의 포멧 등으로 사용되고 있는 키 분실 사례가 많이 발생하고 있습니다. 또 한 외부토큰에 개인키를 저장하면 물리적으로 분리되어 있어 해킹이나 악성 소프트웨어로부터 보호됩니다. 이러한 이유로 외부 토큰(YubiKey)을 이용하여 개인키를 안전하게 관리하는것을 권장합니다.

`cosign piv-tool` 명령으로 하드웨어 토큰을 관리하기 위한 유틸리티를 제공합니다.

Step1. Yubikey 초기화

이 소개에 사용된 모델 : yubikey 5 nfc

```
> cosign piv-tool reset
```

Danger:

하드웨어 토큰을 초기화 하는 명령어이므로 기존에 Yubikey 에 저장되어있는 인증서있다면 삭제됩니다.

Step2. Pin 설정

- 초기화 후 PIN 기본값은 123456
- 아래는 PIN 을 '111222' 으로 정의한 예제입니다.

```
> cosign piv-tool set-pin --new-pin=111222
? pin. This will overwrite the previous pin.: y
Setting new pin. This will overwrite the previous pin.: y
```

- Pin 이 이미 정의되어있는 상태에서 PIN 변경하려면 다음과 같이 명령어를 수행합니다.

```
> cosign piv-tool set-pin --old-pin=111222 --new-pin=232323
? pin. This will overwrite the previous pin.: y
Setting new pin. This will overwrite the previous pin.: y323
```

- Pin 이 '111222' 에서 '232323' 으로 변경됩니다.

Step3. 인증서 생성

- Yubikey에 인증서를 생성합니다.

```
> cosign piv-tool generate-key --random-management-key
```

Step4. 등록된 키 확인

- Yubikey에 저장되어있는 인증서 정보를 출력합니다.

```
> cosign piv-tool attestation
```

Step5. 공개키 추출

- 앞서 위에서도 설명되었듯이 전자 서명 검증하기위해서는 대상파일, 공개키, 시그니처 가 필요합니다.
- 다음 명령을 통하여 Yubikey 공개키를 파일로 내보내기 할 수 있습니다. publickey.pub 파일이 생성됩니다.

```
> cosign.exe public-key –sk > publickey.pub
```

Step6. 코드사인(Signature생성)

- **Public Key Signing 방식 - Step1. 배포파일 전자서명** 에서의 `cosign.exe sign-blob` 명령과 유사하지만 스마트카드토큰을 사용하는것에 차이가 있습니다.
- piv 가 연결이 되어있으므로 이번 명령에서는 `--key` 항목을 생략하고 코드사인을 시도합니다.

```
> cosign.exe sign-blob {배포파일명} --tlog-upload=false --output-
↪signature {생성할 시그니처 파일명.sig}
예시> cosign.exe sign-blob agent.zip --tlog-upload=false --output-
↪signature agent.sig
> 등록된 PIN 입력
> Yubikey 에 물리적인 터치 수행
```

Step7. 무결성 확인

- Public Key Signing 방식 - Step2. 전자 서명 검증하기 와 동일하게 수행합니다.

프로그램 제거

제어판의 프로그램 제거에 등록된 프로그램 중 제거 가능한 특정 프로그램을 제거합니다. 관리자가 허용하지 않은 프로그램을 제거하여 Windows 단말의 소프트웨어를 제어합니다.

- 비인가 소프트웨어 삭제

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **프로그램 제거** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.

아래 **플러그인설정** 이 있습니다.

1. **프로그램 이름** 의 경우 제어판의 프로그램 제거에 등록된 프로그램중 제거할 프로그램 이름을 설정합니다.
2. **삭제전 알림** : 프로그램 삭제전 사용자에게 메시지 표시 여부를 설정합니다.
   - **메시지 내용** : 프로그램 삭제전 사용자에게 보여질 메시지를 입력합니다.
3. **수행 계정** : 프로그램 제거시 사용할 수행계정을 설정합니다.
4. **리부팅옵션** 의 경우 사용자에게 알림을 보낼 지 자동 재부팅을 할지 선택합니다.
5. **수행주기** 는 설정 된 주기마다 액션을 수행합니다. (초 - 개월)
6. **수정** 버튼을 클릭합니다.
7. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
8. 적용하고자 하는 **노드정책** 을 클릭합니다.

9. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
10. **사용가능** 항목에서 **프로그램 제거** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
11. **추가** 버튼을 클릭합니다.
12. **수정** 버튼을 클릭합니다.

프로세스 강제종료

액션 검사조건에 설정된 프로세스에 대해서 강제종료 기능을 수행합니다. 실행 주기를 지정하여 반복 수행 기능을 제공합니다.

- 비인가 프로세스 강제 종료 기능 제공

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **프로세스 강제종료** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **조건연산** 의 경우 **OR** 를 선택하여 종료시킬 프로세스명을 조건으로 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정 창에서 옵션들을 설정합니다. **항목(프로세스) / 조건(동작하면) / 설정(프로세스명)** 입니다.

아래 **플러그인설정** 이 있습니다.

1. **차단 팝업메시지 표시** 을 **On** 으로 설정하여 프로세스 강제종료에 대한 팝업메시지를 표시하도록합니다.
   - **팝업메시지 내용** : 프로세스 강제종료에 대한 팝업메시지 내용을 입력합니다. (*{_PROCESSNAME}* 매크로를 이용하여 종료된 프로세스의 이름을 표시할 수 있습니다)
2. **수행주기** 는 설정 된 주기마다 액션을 수행합니다. (초 - 개월)
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 노드정책 창에서 **기본정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **프로세스 강제종료** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

프린터정보 수집

컴퓨터시스템에 등록되어있는 프린터에 대한 정보를 제공합니다. 정책서버는 에이전트와 통신하여 Windows 단말의 프린터 정보를 수집합니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **하드웨어정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **가상 프린터 수집 제외** 옵션을 **On** 으로 설정하여 프린터수집항목 중 물리적으로 연결되어있지 않은 로컬프린터 항목을 제외시킵니다.
2. **수행주기** 의 경우 주기 간격(초 - 개월)을 조정합니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. 사용가능 항목에서 **프린터정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

필수 소프트웨어 검사

사용자 PC에 필수 소프트웨어가 설치되어있는지 검사합니다. 특정 제품 이름 선택만으로 사용자 PC에 해당 제품이 설치되어있는지 검사할 수 있습니다.

- 사내 필수 프로그램 검사 기능 제공

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **필수 소프트웨어 검사** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **소프트웨어** 에서 검사할 소프트웨어의 분류를 선택합니다.
2. **제품** 에서 검사할 제품을 선택합니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.

5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **필수 소프트웨어 검사** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

백신 제품 목록

벤더	제품명	제품버전
Avira GmbH	Avira Antivirus Pro	15.x
Avira GmbH	Avira Free Antivirus	15.x
Avira GmbH	Avira Endpoint Security	15.x
ESET	ESET Endpoint Security	12.x
ESET	ESET Internet Security	12.x
ESET	ESET Smart Security	12.x
ESET	ESET NOD32 Antivirus	12.x
Bitdefender	Bitdefender Antivirus Plus	23.x
Bitdefender	Bitdefender Internet Security	23.x
Bitdefender	Bitdefender Total Security	23.x
Bitdefender	Bitdefender Antivirus Free Edition	1.x
AhnLab, Inc.	AhnLab V3 Lite	3.x
AhnLab, Inc.	AhnLab V3 Lite	4.x
AhnLab, Inc.	AhnLab V3 Net for Windows Server	9.x
AhnLab, Inc.	AhnLab V3 Endpoint Security	9.x
AhnLab, Inc.	AhnLab V3 Internet Security	9.x
AVG Technologies CZ, s.r.o.	AVG Business	18.x
AVG Technologies CZ, s.r.o.	AVG Internet Security Business Edition	18.x
AVG Technologies CZ, s.r.o.	AVG AntiVirus Business Edition	18.x
AVG Technologies CZ, s.r.o.	AVG AntiVirus Free	18.x
AVG Technologies CZ, s.r.o.	AVG Internet Security	18.x
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

continues on next page

Table 3 – continued from previous page

벤더	제품명	제품버전
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.	알약(공개용)	2.x
ESTSecurity Corp.	알약	3.x
ESTSecurity Corp.	알약	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

디스크 암호화 제품 목록

벤더	제품명	제품버전
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

패치 관리 제품 목록

벤더	제품명	제품버전
Kaspersky Lab	Kaspersky Small Office Security	19.x
F-Secure Corporation	F-Secure PSB Workstation Security	12.x

하드웨어정보 수집

마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다. 정책서버는 에이전트와 통신하여 단말의 CPU, 메모리, 저장장치 등의 정보를 수집합니다.

- 하드웨어 사용량 정보를 수집하여 시스템 자원 관리

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **하드웨어정보 수집** 을 찾아 클릭합니다. (*Windows*에 하나, *MacOS*에 하나씩 있음)

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **플러그인 설정** 이 있습니다.

1. **CPU 업데이트 최소비율** 의 경우 마지막으로 전송한 CPU 사용량이 현재 사용량과 설정비율 이상 차이가 나면 정보를 전송합니다.
2. **메모리 업데이트 최소비율** 의 경우 마지막으로 전송한 메모리 사용량이 현재 사용량과 설정비율 이상 차이가 나면 정보를 전송합니다.
3. **저장장치 업데이트 최소비율** 의 경우 마지막으로 전송한 저장장치 사용량이 현재 사용량과 설정비율 이상 차이가 나면 정보를 전송합니다.
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 적용하고자 하는 **노드정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. 사용가능 항목에서 **하드웨어정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

Note: 설정비율은 전체 용량 기준으로 계산됩니다.

호스트명 변경

컴퓨터 이름을 변경하는 기능을 제공합니다. Windows PC의 호스트 이름을 제어할 수 있습니다.

- 호스트명을 변경하여 부서 단위 또는 사내 명명 규칙에 맞는 관리 기능 제공

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **호스트명 변경** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **호스트 이름** 에 변경할 호스트 이름을 지정합니다. (문자는 영문기준 *15*자를 초과할 수 없고 하이픈*(-)*만 설정 가능)
2. **리부팅방법** 에 대한 옵션(리부팅 안함 / 사용자에게 알림 / 자동 리부팅)을 지정합니다.
   - 사용자에게 알림을 설정할 경우 리부팅 **지연시간** 을 지정합니다. (초 - 시간)
3. **수행계정** 에서 호스트 이름을 변경할 수행계정 옵션을 선택합니다. (에이전트 기본 수행계정 또는 별도의 수행계정 설정)
4. **수행주기** 는 설정 된 주기마다 액션을 수행합니다. (초 - 개월)

5. **수정** 버튼을 클릭합니다.
6. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
7. 적용하고자 하는 **노드정책** 을 클릭합니다.
8. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
9. 사용가능 항목에서 **호스트명 변경** 을 찾아 선택 항목으로 드래그하여 이동합니다.
10. **추가** 버튼을 클릭합니다.
11. **수정** 버튼을 클릭합니다.

macOS 제어

다음 플러그인을 사용하여 에이전트가 설치된 macOS 단말을 제어할 수 있습니다.

ARP 테이블 관리

사용자 PC의 ARP 테이블에 대한 관리 작업을 수행합니다. 악의적인 사용자는 ARP 테이블을 변조하여 내부 네트워크 보안 체계를 우회하거나 내부 사용자의 패킷을 가로채려는 시도를 할 수 있습니다. ZTNA는 이러한 시도들을 방지하기 위해 다음과 같은 기능을 제공합니다.

- 악의적인 사용자가 패킷을 가로채는 ARP Spoofing 공격 대응
- 수동으로 ARP 항목을 Static 설정하지 못하도록 강제화하여 네트워킹 보호

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **ARP 관리** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **Static ARP 차단** 의 경우 **On** 으로 설정하여 Static으로 설정된 ARP에 대해서 사용하지 못하도록 강제화 합니다.
2. **Anti ARP Spoofing** 를 **On** 으로 설정하여 ARP Spoofing 방지를 위해 충돌 보호된 IP에 대해서 Static ARP 를 설정(확인 된 노드의 *ARP* 정보) 합니다.
   - **적용대상 노드그룹** : AAS(Anti ARP Spoofing)를 적용할 IP가 특정 노드그룹에 속하는 경우만 적용할 수 있도록 선택합니다. (미선택시 모든노드에 대해서 적용)
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 노드정책 창에서 **기본정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **ARP 관리** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

Note: 관리 > 노드 > IP관리 탭 > IP 정책으로 이동하여 충돌 방지 설정을 구성합니다.

macOS 업데이트

macOS의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다. 사용자가 다양한 이유로 자동 업데이트를 비활성화 해놓은 경우 강제 자동 업데이트 활성화가 가능합니다.

- 사용자가 시스템 지연등의 이유로 자동 업데이트를 꺼놓은 경우

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **macOS 업데이트** 를 찾아 클릭합니다

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 " 설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **수행주기** 를 설정하여 일정에 따라 작업을 실행하는 시간 간격을 지정합니다. (시간 - 개월)
2. **지정시각검사** 의 설정을 **On** 변경하여 지정 된 시간대에 업데이트 확인을 수행합니다.
3. **동작모드** 에서 " 설치" 또는 " 검사" 만 수행 할 지 선택하여 지정합니다.
    - **설치시점** : 동작모드가 설치모드 일 경우 업데이트 설치를 수행 할 시점을 선택합니다. (즉시설치 *or* 지정된 시각에 설치)
4. **재부팅 옵션** : 사용자에게 알림 메시지를 보낼 시 자동 재부팅을 할지 선택하여 설정합니다.
5. **수정** 버튼을 클릭합니다.
6. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
7. 적용하고자 하는 **노드정책** 을 클릭합니다.
8. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
9. **사용가능** 항목에서 **macOS 업데이트** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
10. **추가** 버튼을 클릭합니다.
11. **수정** 버튼을 클릭합니다.

네트워크 폴더 공유 제어

네트워크에 공유된 폴더정보를 수집하며 일정시간 이상 공유되는 폴더를 제어합니다. 플러그인을 통해 특정 시간, 특정 권한으로 제한적인 허용이 가능합니다.

- 네트워크 폴더 공유에 대한 정보 제공
- 불필요한 폴더 공유로 인한 파일 노출 방지를 위하여 제한적인 허용 기능

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **네트워크 공유폴더** 를 찾아 클릭합니다.

아래 **플러그인설정** 이 있습니다.

1. **공유 폴더 정보 수집** 에 대해 **Off** 를 선택하여 네트워크를 통해 공유 폴더에 대한 정보를 수집하지 않습니다.
2. **공유폴더 해제** 에 대해 **On** 을 설정하여 폴더 공유 상태를 해제합니다.
   - **공유 허용 시간** : 공유폴더의 임시 사용 가능 시간을 설정합니다. (초 - 개월)
   - **읽기권한만 허용** 에 대해 **On** 으로 설정하여 읽기권한만 있는 폴더는 허용하고 쓰기권한이 있는 폴더는 공유를 해제합니다. (smb_read_only 값 체크)
   - **Everyone권한 외 허용** 에 대해 **On** 으로 설정하여 Everyone 권한이 존재하는 폴더만 공유를 해제합니다. (smb_guest_access 값 체크)
3. **공유해제알림 방법** 은 사용자메시지 또는 에이전트팝업을 선택하여 공유 해제를 사용자에게 알려 줍니다.
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 노드정책 창에서 **원하는 정책ID** 를 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **네트워크 공유폴더** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

네트워크정보 수집

네트워크 인터페이스 정보와 탐지된 포트 정보를 수집하여 노드정보에 표시합니다. 관리자에게 가시성을 제공하여 네트워크 제어에 활용 가능합니다.

- 네트워크 인터페이스 정보를 수집하여 비인가 네트워크사용을 감지 가능
- 포트정보를 수집하여 오픈 포트 목록을 통해 관리자가 이상징후 확인 가능

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창 **작업선택** 오른쪽의 드롭다운 버튼을 클릭하여 **macOS** 운영체제를 선택합니다.
4. 노드액션 리스트에서 **네트워크정보 수집** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **전송주기** 에 대해 주기적 간격(초 - 시간)을 조정합니다.
2. **열린포트 정보 수집** 에 대해 **On** 으로 설정하여 열린포트 정보를 수집합니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.

6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. 사용가능 항목에서 **네트워크정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

모니터정보 수집

로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다. 모니터 정보를 수집하여 자산 관리/교체 등에 활용 가능합니다.

- 특정 inch 이하의 모니터 정보를 수집하여 하드웨어 교체 작업에 활용

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **모니터정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. 사용가능 항목에서 **모니터정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

모양 및 개인설정

바탕화면, 화면보호기에 대한 설정 정보를 수집 및 제어합니다. 사내 표준 바탕화면 및 화면보호기 규정 강제 적용 기능을 제공합니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **모양 및 개인설정** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **화면보호기정보 수집** 에서 **On** 옵션을 설정하여 사용 중인 화면 보호기 설정 정보를 수집합니다.
2. **화면보호기 제어** 에서 **On** 을 설정하여 대기시간을 설정합니다.
    - **대기시간** : 화면 보호기로 전환되기 전까지의 동작 대기시간을 설정합니다. (분 - 시간)

- **대기시간 고정** 을 **On** 으로 설정하여 관리자가 설정한 시간보다 PC에 사용 중인 대기시간이 짧을 때도 대기시간을 변경합니다.

3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **모양 및 개인설정** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

무선랜 제어

무선 네트워크 인터페이스에서 탐지되는 무선 AP에 대한 정보를 제공하며 허용되지 않은 AP 연결을 제한합니다. 무선랜을 사용하는 환경에서 AP에 대한 가시성을 제공합니다.

- AP 목록을 수집하여 인가/비인가 AP에 대한 가시성 확보 가능
- 무선랜 인터페이스의 AP모드를 비활성화하여 보안사고 방지 가능

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **무선랜제어** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **플러그인 설정** 이 있습니다.

1. **AP 정보 수집 대상** : WLAN 인터페이스에서 탐지 및 연결된 SSID에 대한 정보를 수집합니다.
2. **AP 연결 제어** : 허용되지 않은 무선 AP에 대한 연결 해제 여부를 지정합니다.
    - **허용 AP 검색 방법** : 허용할 SSID 정의 방법을 선택합니다. (*WLAN* 그룹 선택, *SSID* 입력, 정규식 사용)
    - **허용 무선랜 그룹** : 드롭다운에서 허용할 WLAN 그룹을 선택합니다.
    - **제어 주기** : 연결된 AP가 허용된 AP 인지 확인하기 주기를 지정합니다. (초 - 분)
    - **제어 유보 시간** : 허용 AP 목록을 갱신하기 위한 AP 연결 허용 시간을 지정합니다. (초 - 분)
    - **차단알림** : AP 연결이 차단되었을 때 사용자에게 알리는 방법을 선택합니다. (에이전트 팝업 *or* 코드인증)
3. 네트워크 요구 사항을 기반으로 **CWP 메시지** , **조건설정** 및 **플러그인설정** 을 조정하여 입력합니다.
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 노드정책 창에서 **기본정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **무선랜제어** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.

9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

백신정보 수집

PC에 설치되어있는 백신프로그램 정보 및 백신으로 검출된 바이러스치료로그를 실시간으로 수집합니다. 다양한 벤더들의 백신 정보를 ZTNA에서 수집합니다.

- 글로벌 벤더의 백신명, 버전, 패턴정보, 실시간 감시 정보 등을 수집하여 단말보안을 강화합니다.

백신 지원 목록

Genian ZTNA에서 지원되는 모든 안티바이러스를 버전별로 확인합니다.

벤더	제품명	정보제공 항목	v5.0.x
AhnLab	V3 for Mac	백신명, 제품버전	5.0.13~
Avast	Mac Security	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	5.0.9~
AVG	Antivirus	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	5.0.9~
Bitdefender	Antivirus for Mac	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	5.0.9~
ESET	Cyber Security	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	5.0.9~
ESET	Endpoint Antivirus	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	5.0.13~
Kaspersky	Internet Security	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	5.0.9~
Sophos	Home	백신명, 제품버전, 현재패턴 버전명, 실시간감시	5.0.17~
Sophos	Endpoint	백신명, 제품버전, 현재패턴 버전명, 실시간감시, 최근검사시간	5.0.17~
Symantec	Norton Security	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜	5.0.9~
Trend-Micro	Apex One	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	5.0.63~
ESET	Endpoint Security	백신명, 제품버전, 현재패턴 버전명, 패턴 생성 날짜, 실시간 감시 여부, 최근검사시간	5.0.46~

백신정보 수집

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **백신정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.

6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **백신정보 수집** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

사용자 알림메시지

사용자에게 알림메시지를 표시합니다. 관리자가 에이전트를 통해서 사용자에게 메시지를 전달합니다.

- 사용자에게 알림 메시지를 표시하여 클릭시 설정된 URL로 리다이렉션
- 공지사항 등을 메시지 확인 알림을 통해 감사기록 저장

사용자 알림메시지 옵션 구성

1. **메시지 제목** 에 에이전트 알림 시 표시할 제목을 설정합니다.
2. **클릭시 CWP 접속** 을 **On** 으로 설정하여 에이전트 알림 클릭 시 CWP 페이지로 이동하도록합니다.
   - **CWP URL** 에 **설정** 버튼을 클릭하여 템플릿을 사용하거나 URL을 직접 입력합니다.
3. **팝업창 고정** 의 경우 에이전트 알림을 닫아도 다시 표시할 지 여부를 선택합니다. (*On/Off*)
   - **메시지 타입** : 사용자메시지 타입을 선택합니다. (일반, 경고)
   - **메시지확인 알림** : 사용자가 메시지를 확인했으면 감사 로그를 기록하도록 설정합니다. (*On/Off*)

노드정책을 통하여 사용자 알림메시지 정책 구성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **사용자 알림메시지** 를 찾아 클릭합니다.
4. **플러그인설정** 에서 필요한 **메시지 제목**, **클릭시 CWP 접속** 옵션, **메시지 내용** 등을 입력합니다.
5. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
6. 사용자 알림메시지 정책을 구성할 노드정책을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **사용자 알림메시지** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.
11. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

제어정책을 통하여 사용자 알림메시지 정책 구성

1단계. 제어 대상 노드그룹 생성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **추가** 버튼을 클릭합니다.
5. 제어 대상의 조건 설정 후 **추가** 버튼을 클릭합니다.
6. **생성** 버튼을 클릭합니다.

2단계. 제어액션 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어액션** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭합니다.
3. 플러그인선택 항목에서 **사용자 알림메시지** 플러그인을 선택합니다.
4. **조건설정** 및 옵션을 입력합니다.
5. **생성** 버튼을 클릭합니다.

3단계. 제어정책 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어정책** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭하고, **제어정책 마법사** 를 완료합니다.
3. **정책 기본설정** 탭에서 **ID** 항목에 **사용할 정책 ID** 를 입력합니다.
4. **노드그룹 설정** 탭에서 **새로 추가한 노드그룹** 을 선택하고, **선택** 항목으로 이동합니다.
5. **권한 할당** 과 **제어 옵션** 탭에서 **원하는 옵션** 을 입력합니다.
6. **제어액션 설정** 탭에서 **생성한 제어액션** 을 찾아 **선택** 항목으로 이동합니다.
7. **완료** 버튼을 클릭합니다.
8. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

소프트웨어 정보 수집

설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.

- 단말에 설치된 소프트 웨어 목록을 수집하여 비인가 소프트웨어 설치 여부 확인 제공

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창 **작업선택** 오른쪽의 드롭다운 버튼을 클릭하여 **macOS** 운영체제를 선택합니다.
4. 노드액션 리스트에서 **소프트웨어정보 수집** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
3. **수행주기** 의 경우 실행 주기 간격(초 - 개월)을 조정합니다.

4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 적용하고자 하는 **노드정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. 사용가능 항목에서 **소프트웨어정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

수행조건만 검사

액션에 설정된 수행 조건을 검사하는데 사용하는 플러그인입니다. 프로세스, 파일, 시스템 및 인증된 사용자 등 조건을 설정하여 검사할 수 있습니다.

- 특정 프로세스의 해쉬값 검사
- 사내 필수프로그램 설치 여부 확인

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창 **작업선택** 오른쪽의 드롭다운 버튼을 클릭하여 **macOS** 운영체제를 선택합니다.
4. 노드액션 리스트에서 **수행조건만 검사** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다. (이 플러그인이 작동하려면 조건이 추가되어야합니다)

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.
3. **수행주기** : 설정된 주기마다 액션을 수행합니다. (초 - 개월)
4. **추가** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 적용하고자 하는 **노드정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **수행조건만 검사** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

시스템 종료

지정된 시각에 Windows 시스템의 절전, 재시작, 종료를 수행합니다. 사용자의 시스템 전원을 제어하여 단말 보안을 강화합니다.

- ZTNA의 여러 제어 기능 중 시스템 전원 제어 제공
- 직원 퇴근시간에 맞춰 시스템 자동 종료

시스템 종료 옵션 구성

1. **동작방식** 의 경우 PC의 전원을 제어하는 방식(잠자기, 재시동, 시스템 종료)을 선택합니다.
2. **강제화모드** 를 **On** 으로 설정하여 사용자가 취소할 수 없도록합니다.
3. **종료전 알림 시간** 에 PC의 전원이 제어되기 전 사용자에게 알람을 표시할 시간을 설정합니다. (초 - 분)
4. **PC가동시간** 이 지난 경우에만 전원 제어를 수행합니다. 본 플러그인에 의해 잠자기로 전환된 후 해제 시점을 가동 시작 시각으로 간주합니다. (분 - 개월)
5. **타이틀 표시** 를 **On** 으로 설정하여 대화상자의 타이틀을 표시합니다.
6. **메시지 표시 방법** : 제어 전 알림 시간동안 대화상자에 표시할 내용을 선택합니다. (*HTML,* 이미지)
   - **HTML** 을 설정할 경우 사용자에게 표시할 HTML 메시지를 입력합니다.
   - **이미지** 를 설정할 경우 사용자에게 표시할 이미지를 업로드합니다.

노드정책을 통하여 시스템 종료 정책 구성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **시스템 종료** 를 찾아 클릭합니다.
4. **플러그인설정** 에서 **동작방식**, **강제화모드**, **종료전 알림 시간** 등을 설정합니다.
5. **수정** 버튼을 클릭합니다.
6. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
7. 시스템 종료 정책을 구성할 노드정책을 클릭합니다.
8. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
9. **사용가능** 항목에서 **시스템 종료** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
10. **추가** 버튼을 클릭합니다.
11. **수정** 버튼을 클릭합니다.
12. 오른쪽 상단의 **변경정책적용** 버튼을 클릭합니다.

제어정책을 통하여 시스템 종료 정책 구성

1단계. 제어 대상 노드그룹 생성

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **그룹 > 노드** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **추가** 버튼을 클릭합니다.
5. 제어 대상의 조건 설정 후 **추가** 버튼을 클릭합니다.
6. **생성** 버튼을 클릭합니다.

2단계. 제어액션 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어액션** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭합니다.
3. 플러그인선택 항목에서 **시스템 종료** 플러그인을 선택합니다.
4. **조건설정** 및 옵션을 입력합니다.
5. **생성** 버튼을 클릭합니다.

3단계. 제어정책 생성

1. 왼쪽 정책 항목에서 **정책 > 제어정책 > 제어정책** 으로 이동합니다.
2. **작업선택 > 생성** 을 클릭하고, **제어정책 마법사** 를 완료합니다.
3. **정책 기본설정** 탭에서 **ID** 항목에 **사용할 정책 ID** 를 입력합니다.
4. **노드그룹 설정** 탭에서 **새로 추가한 노드그룹** 을 선택하고, **선택** 항목으로 이동합니다.
5. **권한 할당** 과 **제어 옵션** 탭에서 **원하는 옵션** 을 입력합니다.
6. **제어액션 설정** 탭에서 **생성한 제어액션** 을 찾아 **선택** 항목으로 이동합니다.
7. **완료** 버튼을 클릭합니다.
8. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

에이전트 인증창

사용자인증 수행 시 WEB 페이지가 아닌 에이전트 자체 인증 창을 사용합니다. 에이전트를 통해서 CWP 인증보다 간편한 사용자 인증을 제공합니다.

노드정책에 에이전트 액션 추가

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책 창에서 **원하는 노드정책 ID** 를 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **에이전트 인증창** 을 찾아 **선택** 항목으로 이동시킵니다.
6. **추가** 버튼을 클릭합니다.

7. **수정** 버튼을 클릭합니다.

에이전트를 통한 사용자 인증 설정

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **에이전트 인증창** 을 찾아 클릭합니다.
4. **이미지 사용** 의 경우 에이전트 인증창의 이미지를 지정합니다.
5. **타이틀바 표시** 의 경우 에이전트 인증창의 타이틀 문구를 표시할지를 지정합니다. (OS X Yosemite 이상)
6. **배경색** 은 인증 창의 색상을 지정합니다.
7. **글자색** 은 대화상자의 글자색상을 나타냅니다.
8. **HTML 사용** 은 HTML을 사용하여 도움말을 표시합니다.
9. **수정** 버튼을 클릭합니다.

운영체제 정보 수집

Windows 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.

- 관리자가 운영체제 정보를 수집하여 운영체제별 별도 정책 적용

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창 **작업선택** 오른쪽의 드롭다운 버튼을 클릭하여 **macOS** 운영체제를 선택합니다.
4. 노드액션 리스트에서 **운영체제정보 수집** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **운영체제정보 수집** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

장치 제어

사용자 PC에서 사용금지된 장치들을 사용중지로 변경합니다. 시스템에 물리적으로 연결하는 모든 장치를 제어합니다.

- 외부 장치를 실행 중지 또는 제거
- 관리자가 에이전트를 통해 장치에 대한 사용 신청을 받아 승인 여부 결정

Note: 장치사용신청서 설정부분은 다음에 mac-external-device-request 참고하시기 바랍니다.

---

1 단계. 장치 그룹 생성

- 장치 그룹은 제어에 필요한 일련의 장치를 정의하는 기능입니다. 정책에 대한 차단 또는 예외로 사용될 수 있습니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 장치제어 정책 > 장치그룹** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **기본정보** 에서 고유한 **ID 이름** 을 입력합니다. (예 : *"USB* 저장 장치").
5. **OS 종류 > macOS** 를 선택합니다.
6. 제어 하려고 하는 장치명을 선택합니다.
7. 장치가 USB Disk 인 경우 **조건설정** 에서 다음을 입력합니다.
   - **USB 제조사** : USB 공급업체 이름을 지정
   - **USB 모델** : USB 모델 이름을 지정
   - **USB 시리얼** : USB 일련 번호 지정
8. **생성** 버튼을 클릭합니다.

2 단계. 장치제어 정책 생성

- 장치 제어 정책은 대상이 장치 제어를 수행하도록 차단하거나 허용 할 장치 그룹을 정의합니다.
- 플러그인이 업로드 되면 기본적인 출력장치에 대한 장치정책이 템플릿으로 제공됩니다. (장치제어 정책 ID : Data Prevention)

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 장치제어 정책** 으로 이동합니다.
3. **작업선택 > 생성** 버튼을 클릭합니다.
4. **기본정보** 에서 고유의 **ID 이름** 을 입력합니다. (예: *"USB* 스토리지 정책")
5. **노드그룹 설정** 에서 **할당** 버튼을 클릭하고 **노드그룹** 을 선택합니다.
6. **차단장치 설정** 에서 **할당** 버튼을 클릭하고 **USB 저장 장치** 를 선택합니다.
7. 1단계에서 설정한 장치그룹이 아니더라도 아래의 **기본장치그룹** 으로 정의되어있는 항목을 선택 할 수 있습니다.

Bluetooth Tethering	블루투스 클래스에 속한 장치
CD/DVD	CD롬 드라이브 클래스에 속한 장치
Local Printer	로컬PC에 직접 연결된 프린터
USB Disk	USB 타입의 저장장치 (시스템 프로파일의 SPUSBDataType 정보)
USB Network Adapter	USB 포트로 연결된 네트워크 어댑터 (네트워크 하드웨어 포트명 내에 USB, LAN 존재하는 장치)
USB Tethering	모바일기기에 USB 케이블로 연결된 네트워크 어댑터 (네트워크 하드웨어 포트명이 iPhone USB인 장치), 안드로이드는 macOS에 USB Tethering 불가

8. **생성** 버튼을 클릭합니다.

3 단계. 장치 제어 플러그인 설정

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **장치 제어** 을 찾아 클릭합니다.
4. **액션 수행설정 > 장치제어 방식** 에서 **제거** 또는 **중지** 를 선택합니다.
5. **수정** 버튼을 클릭합니다.

4 단계. 노드정책에 에이전트 액션 추가

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책창에서 **원하는 노드정책ID** 를 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **장치 제어** 를 찾아 **선택** 항목으로 이동 시킵니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.

파일 관리

파일을 복사, 삭제, 이동 및 이름을 변경하여 macOS의 파일을 관리 할 수 있습니다. 특정 파일을 실행할 수도 있습니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **파일 관리** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정 창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.

아래 **플러그인설정** 이 있습니다.

1. **파일 경로** 에서 관리 할 소스 파일을 지정합니다.
2. **관리 옵션** 에서 소스 파일에 대한 수행 옵션을 선택합니다. (실행, 삭제, 복사, 이동, 이름변경)
   - **실행 옵션** : 파일을 실행할 때 인수로 넘겨줄 추가적인 옵션을 설정합니다.
   - **리부팅옵션** 의 경우 사용자에게 알림을 보낼지 자동 재부팅을 할지 선택합니다.
3. **수행주기** 는 설정 된 주기마다 액션을 수행합니다. (초 - 개월)
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 적용하고자 하는 **노드정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **파일 관리** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

파일 배포v2

Note: 파일 배포 플러그인은 CC 평가 항목에 포함된 기능이 아니므로 CC 인증을 요구하는 공공기관에서는 해당 플러그인을 사용할 수 없습니다.

파일 배포 플러그인은 파일을 실행하거나 특정 위치에 다운로드합니다. 정책서버는 에이전트와 통신하여 단말에게 파일에 대한 배포, 실행, 설치를 할 수 있습니다.

- 단말에 필요한 파일 배포
- 단말의 미설치 소프트웨어 설치

파일 배포v2 플러그인은 기존 파일배포 플러그인에서 보안성 강화에 치중하여 추가되었습니다.

파일 배포v2 플러그인은 안전한 파일 배포를 위해 파일 무결성 검증과 배포자 신원확인을 제공합니다.

- 3단계에 걸친 무결성 검증을 수행
- 최종 사용자의 배포자 식별 및 승인

파일 배포v2 플러그인은 배포하는 파일에 대한 전자서명을 필수로 요구하며 전자서명과 서명검증을 위해 공급망 보안을 위해 설계된 Sigstore Signing 방식을 사용합니다. 파일 배포v2 플러그인은 Sigstore Signing을 사용하여 Sigstore Keyless Signing과 Public Key Signing 2가지 방식을 선택적으로 사용할 수 있습니다.

Sigstore Keyless Signing 방식

Sigstore는 **OpenID Connect(OIDC)를 사용하여 짧은 유효 기간의 인증서** 를 생성합니다.
이 인증서는 소프트웨어를 서명하는 데 사용 되며, 서명된 소프트웨어는 cosign을 통해 공개적으로 검증할 수 있습니다.

OIDC는 OAuth 2.0의 확장으로, 사용자에게 리소스에 대한 액세스를 제공하기 위해 로그인 인증을 사용하는 프레임워크입니다. OIDC는 사용자의 암호를 요구하지 않고도 인증서를 생성할 수 있기 때문에, Sigstore에서 짧은 유효 기간의 인증서를 생성하는 데 사용됩니다.

Sigstore Keyless Signing 사용 방법

Step1. 배포파일 전자서명

1. cosign을 다운로드 받아 배포파일 전자서명에 사용할 디렉토리에 저장합니다.
2. 파일명을 cosign 으로 변경합니다.
3. 전자서명할 파일을 디렉토리에 복사합니다.
4. 터미널에서 cosign 파일이 위치하는 디렉토리로 이동합니다.
5. 아래 명령어를 입력하여 전자서명을 수행합니다.

```
> cosign sign-blob {배포파일명} --output-certificate {생성할 cert 파일명.cert} --
↪output-signature {생성할 시그니처 파일명.sig}
```

6. 잠시 후 터미널에 서비스 약관 동의에 `y` 를 입력합니다.
7. 인증을 위한 URL이 브라우저로 실행되면, `Git`, `Google`, `Microsoft` 세가지 OIDC중 하나를 선택하고 인증을 수행합니다.
8. 디렉토리내에 `Cert`, `Sig` 파일이 정상적으로 생성되었는지 확인합니다.

Step2. 전자서명 검증하기

1. 터미널에서 아래 명령어를 입력합니다.

```
> cosign verify-blob {배포파일명} --certificate {생성된 cert 파일명.cert} --
↪signature {생성된 시그니처 파일명.sig} --certificate-identity={인증에 사용한 ID} --
↪certificate-oidc-issuer={OIDC 발행자}
예시> cosign verify-blob agent.zip --certificate agent.cert --signature agent.
↪sig --certificate-identity=genian@genians.com --certificate-oidc-
↪issuer=https://accounts.google.com
```

2. 정상적으로 전자서명이 이루어진 경우 **Verified OK** 라고 표시됩니다.

Step3. 노드액션 생성하기

1. 정책서버 Web콘솔에 접속하여 상단 **정책** 으로 이동합니다.
2. 좌측 메뉴 **노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **작업선택 > 생성** 을 클릭합니다.

아래 **기본설정** 이 있습니다.

4. **액션명** 은 용도에 따라 "(용도) 액션명" 형태로 사용하시면 향후 운영시 편하게 노드액션을 구분할 수 있습니다.
5. **설명** 은 용도에 따라 다르게 사용하는 경우 어떤 목적으로 사용하는 노드액션인지 구분할 수 있습니다.
6. **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

7. **OS 종류** 는 macOS, Linux, Windows 대상에 맞는 OS를 선택합니다.
8. **조건 설정** 은 일반적으로 배포를 할 때 특정조건에 맞는 사용자에게 배포하기 위해 사용합니다.

   예시: `"c:\%ProgramFiles%\abc.exe 가 존재하지 않는 경우"` 라는 조건을 사용하여 배포하게 되면 `abc.exe` 가 존재하지 않는 단말에만 배포가 가능합니다.

9. **플러그인선택** 에서는 **파일 배포 V2** 를 선택합니다.
10. **배포 파일** 에는 업로드 버튼을 클릭하여 파일을 선택합니다.
11. **배포파일 검증방법** 은 Sigstore Keyless Signing을 선택합니다.
12. **신뢰하는 OIDC 발행자** 에는 전자서명 시 인증에 사용한 OIDC(Github, Google, Microsoft)를 선택합니다.
13. **신뢰하는 ID** 에는 전자서명 시 인증에 사용한 ID(email주소 형태)를 입력합니다.
14. **Certificate** 는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 **cert** 파일을 추가합니다.
15. **Signature** 는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 **sig** 파일을 추가합니다.
16. **배포 옵션** 의 경우 배포할 방식을 설정합니다.
    - **앱 실행**: 앱 파일(.app)을 실행합니다.
    - **파일 실행**: 압축파일일 경우 "파일 경로"에 실행할 파일을 설정하고, "실행옵션"과 실행할 "수행 계정"을 설정하여 해당 파일을 실행시킵니다. "리부팅 옵션"을 통해 파일 실행 이후 리부팅여부를 설정합니다.
    - **다운로드**: 배포 파일을 복사할 단말의 파일 및 폴더 경로를 지정합니다.
    - **패키지 설치**: macOS 패키지 파일(.pkg) 파일을 단말에 설치합니다.
    - **파일 열기**: 업로드 된 파일을 실행(open)합니다.
    - **스크립트 실행**: 업로드 된 스크립트 파일을 실행(sh)합니다.
17. **수정** 버튼을 클릭합니다.
18. 왼쪽 정책 항목에서 **노드정책** 으로 이동한 후 **기본정책** 을 클릭합니다.
19. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
20. **사용가능** 항목에서 **파일 배포** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
21. **수정** 버튼을 클릭한 후 **수정** 버튼을 클릭합니다.

Note:

Sigstore Keyless Siging 방식의 경우 전자서명/서명검증을 위하여 외부와 통신이 필수적이며 아래 도메인에 대한 통신이 허용되어야합니다.
(출발지: 정책서버, 에이전트), (서비스포트: TCP/443)
rekor.sigstore.dev : 원장 기록 시스템
oauth2.sigstore.dev : Sigstore oauth 흐름 제공 서버
accounts.google.com : OIDC 제공자(다른 OIDC인 경우 해당 OIDC 도메인)
fulcio.sigstore.dev : sigstore CA 서버
tuf-repo-cdn.sigstore.dev : SLSA 검증

Public Key Signing 방식

Sigstore cosign은 자체관리 키 전자서명 방식도 제공하고 있습니다.
Public Key Signing 방식은 직접 키를 생성하여 전자서명을 하거나 별도로 제작하여 사용중인 키를 사용하여 전자서명을 하는 방식입니다.

Public Key Signing 사용 방법

Step1. 배포파일 전자서명

1. Sigstore Keyless Signing 방식의 Step1 의 1~4 를 수행 후 다음으로 진행합니다.
2. 별도로 사용하는 전자서명용 키가 없다면 아래 명령어를 입력하여 전자서명용 비밀키와 공개키를 생성합니다.

```
> cosign generate-key-pair
> 비밀키 패스워드 입력
> 비밀키 패스워드 확인
> ls 을 입력하여 비밀키(key) 파일과 공개키(pub) 파일이 생성되었는지 확인합니다.
```

3. 키를 생성했다면 아래와 같이 생성한 키를 사용하여 배포파일에 전자서명을 수행합니다.

```
> cosign sign-blob {배포파일명} --key cosign.key --tlog-upload=false --output-
↪signature {생성할 시그니처 파일명.sig}
예시> cosign sign-blob agent.zip --key cosign.key --tlog-upload=false --output-
↪signature agent.sig
```

Step2. 전자 서명 검증하기

1. CMD 창에서 아래 명령어를 입력합니다.

```
> cosign verify-blob {배포파일명} --key {공개키 파일명.pub} --signature {생성된
시그니처 파일명.sig} --insecure-ignore-tlog=true --insecure-ignore-sct=true
예시> cosign verify-blob agent.zip --key cosign.pub --signature agent.sig --
↪insecure-ignore-tlog=true --insecure-ignore-sct=true
```

2. 정상적으로 전자서명이 이루어진 경우 **Verified OK** 라고 표시됩니다.

Step3. 노드액션 생성하기

1. Sigstore Keyless Signing 방식의 Step3 의 1~10 를 수행 후 다음으로 진행합니다.
2. **배포파일 검증방법** 은 Public Key Signing을 선택합니다.
3. **신뢰하는 공개키** 는 우측 파일읽기 버튼을 클릭하여 키생성 시 함께 생성되었던 **pub** 파일을 추가합니다.
4. **Signature** 는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 **sig** 파일을 추가합니다.
5. Sigstore Keyless Signing 방식의 Step3 의 16~21 를 수행합니다.

Danger:

최초 설정된 배포방식과 배포자 변경이 불가능 하기때문에 최초 노드액션 생성 시 사용한 Private key 는 **분실위험이 없도록 안전하게 보관** 해야 합니다.
등록된 배포자정보는 Web콘솔 설정 > 환경설정 > 에이전트 > 배포 옵션 섹션에서 확인할 수 있습니다.

프로세스 강제종료

액션 검사조건에 설정된 프로세스에 대해서 강제종료 기능을 수행합니다. 실행 주기를 지정하여 반복 수행 기능을 제공합니다.

- 비인가 프로세스 강제 종료 기능 제공

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **프로세스 강제종료** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **조건연산** 의 경우 **OR** 를 선택하여 종료시킬 프로세스명을 조건으로 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정 창에서 옵션들을 설정합니다. **항목(프로세스) / 조건(동작하면) / 설정(프로세스명)** 입니다.

아래 **플러그인설정** 이 있습니다.

1. **차단 팝업메시지 표시** 을 **On** 으로 설정하여 프로세스 강제종료에 대한 팝업메시지를 표시하도록합니다.
   - **팝업메시지 내용** : 프로세스 강제종료에 대한 팝업메시지 내용을 입력합니다. (*{_PROCESSNAME}* 매크로를 이용하여 종료된 프로세스의 이름을 표시할 수 있습니다)
2. **수행주기** 는 설정 된 주기마다 액션을 수행합니다. (초 - 개월)
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 노드정책 창에서 **기본정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **프로세스 강제종료** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

프린터정보 수집

컴퓨터시스템에 등록되어있는 프린터에 대한 정보를 제공합니다. 정책서버는 에이전트와 통신하여 macOS 단말의 프린터 정보를 수집합니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **프린터정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.
3. **수행주기** 의 경우 주기 간격(초 - 개월)을 조정합니다.

4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 적용하고자 하는 **노드정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. 사용가능 항목에서 **프린터정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

필수 소프트웨어 검사

사용자 PC에 필수 소프트웨어가 설치되어있는지 검사합니다. 특정 제품 이름 선택만으로 사용자 PC에 해당 제품이 설치되어있는지 검사할 수 있습니다.

- 사내 필수 프로그램 검사 기능 제공

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리 창에서 **필수 소프트웨어 검사** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **소프트웨어** 에서 검사할 소프트웨어의 분류를 선택합니다.
2. **제품** 에서 검사할 제품명을 선택합니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. **사용가능** 항목에서 **필수 소프트웨어 검사** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

백신 제품 목록

벤더	제품명	제품버전
AhnLab, Inc.	AhnLab V3 for Mac	9.x
Avast Software s.r.o.	Avast Mac Security	13.x
Avast Software s.r.o.	Avast Business Security	13.x
AVG Technologies CZ, s.r.o.	AVG AntiVirus	19.x
Avira GmbH	Avira Security	2.x
Bitdefender	Bitdefender Antivirus for Mac	8.x
Bitdefender	Bitdefender Virus Scanner	3.x
ESET	ESET Cyber Security	6.x
ESET	ESET Cyber Security Pro	6.x
ESET	ESET Endpoint Antivirus	6.x
ESET	ESET Endpoint Security	6.x
G Data Software AG	G DATA AntiVirus for Mac	1.x
Kaspersky Lab	Kaspersky Internet Security	19.x
Kaspersky Lab	Kaspersky Endpoint Security	10.x
Kromtech Alliance Corp.	MacKeeper	2.x
Malwarebytes Corporation	Malwarebytes	3.x
McAfee, Inc.	McAfee Endpoint Protection for Mac	10.x
McAfee, Inc.	McAfee Endpoint Security for Mac	10.x
McAfee, Inc.	McAfee LiveSafe	4.x
McAfee, Inc.	McAfee All Access - Internet Security	4.x
McAfee, Inc.	McAfee Total Protection	4.x
Sophos Limited	Sophos Endpoint	9.x
Sophos Limited	Sophos Home	2.x
NortonLifeLock Inc.	Norton Security	8.x
Trend Micro Inc.	Trend Micro Antivirus	8.x
Webroot Inc.	Webroot SecureAnywhere	9.x

디스크 암호화 제품 목록

벤더	제품명	제품버전
BeLight Software	Concealer	1.x
ENC Security	EncryptStick	6.x
Kromtech Alliance Corp.	MacKeeper	2.x
MadowSoft Software	MacFort	4.x
NCH Software	MEO File Encryption Software	2.x
Sophos Limited	Sophos SafeGuard	8.x
NortonLifeLock Inc.	Symantec Encryption Desktop	10.x

패치 관리 제품 목록

벤더	제품명	제품버전
G Data Software AG	G DATA Antivirus for Mac	1.x
Kromtech Alliance Corp.	MacKeeper	2.x

하드웨어정보 수집

마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다. 정책서버는 에이전트와 통신하여 단말의 CPU, 메모리, 저장장치 등의 정보를 수집합니다.

- 하드웨어 사용량 정보를 수집하여 시스템 자원 관리

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창 **작업선택** 오른쪽의 드롭다운 버튼을 클릭하여 **macOS** 운영체제를 선택합니다.
4. 노드액션 리스트에서 **하드웨어정보 수집** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. 사용가능 항목에서 **하드웨어정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

호스트명 변경

컴퓨터 이름을 변경하는 기능을 제공합니다. Windows PC의 호스트 이름을 제어할 수 있습니다.

- 호스트명을 변경하여 부서 단위 또는 사내 명명 규칙에 맞는 관리 기능 제공

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **호스트명 변경** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **호스트 이름** 에 변경할 호스트 이름을 지정합니다. (문자는 영문기준 *63*자를 초과할 수 없고 하이픈*(-)*만 설정 가능)
2. **수행주기** 는 설정 된 주기마다 액션을 수행합니다. (초 - 개월)
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 적용하고자 하는 **노드정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
7. 사용가능 항목에서 **호스트명 변경** 을 찾아 선택 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

비밀번호 유효성 검사

macOS 계정의 비밀번호에 대한 유효성을 검사하고 검증되지 않은 비밀번호를 안전한 비밀번호로 변경시킵니다. 특수문자 사용 등 비밀번호 규칙을 강제화하여 단말 보안을 강화합니다.

- 관리자가 정한 비밀번호 문자열의 규칙 준수를 강제화하여 패스워드 보안을 강화
- 비밀번호 변경 주기를 설정하여 주기마다 패스워드 변경을 강제화

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **에이전트 정보 외부 전송** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정 창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.

아래 **플러그인설정** 이 있습니다.

1. **검증된 계정표시** : **On/Off** 설정을 통해 대화상자에 검증된 계정에 대해서도 표시를 할지 여부를 선택합니다.
2. **검증창 고정** : **On/Off** 대화상자를 화면의 중앙에 고정합니다.
3. **로그온 계정** 에서 다음을 설정합니다.
   - **비밀번호 문자열 검사방법** : "규칙검사" 를 설정합니다. (비밀번호 규칙의 경우 "설정 > 환경설정 > 사용자인증 > 비밀번호정책"규칙이 적용 됩니다)
   - **비밀번호 변경주기** : 윈도우 로그인 계정에 대한 비밀번호 변경주기를 설정합니다. (시간 - 개월)
   - **만료전알림** : 비밀번호 시간이 만료되기 전에 알림을 발생합니다. (만료시간은 정책이 적용 된 시점부터 적용 됩니다.)
   - **검사예외ID** : 검사 예외대상의 사용자ID의 전체문자열을 입력합니다. (여러개 입력시 콤마로 구분, 대소문자를 구분하지 않습니다.)
4. **수행주기** 의 경우 주기 간격(초 - 개월)을 조정합니다.

5. **수정** 버튼을 클릭합니다.

아래 **비밀번호 검사 결과** 확인 방법이 있습니다.

Note: 정책이 적용되면 검증되지 않은 단말에 비밀번호 검증창이 팝업 되고 사용자는 자신의 윈도우 계정 비밀번호를 입력합니다.

---

1. 상단 항목의 **관리 > 노드** 로 이동합니다.
2. 노드리스트 창에서 에이전트가 설치 된 노드의 **IP** 를 클릭합니다.
3. **시스템정보** 탭 아래로 스크롤 하여 **계정비밀번호 검증 정보** 항목의 결과를 확인합니다.

에이전트 정보 외부 전송

에이전트가 가지고 있는 정보를 외부 프로그램에 전송합니다.

- 현재 에이전트의 특정 상태정보 전송

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **에이전트 정보 외부 전송** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정 창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.

아래 **플러그인설정** 이 있습니다.

1. 외부전송목록의 **추가** 버튼을 선택합니다.
   - **파일 경로** : 정보 전송을 위해 실행할 파일의 경로를 설정합니다.
   - **전송정보** : 전송할 정보의 종류를 설정합니다.
   - **인증정보변환** : 인증 사용자의 ID에 대한 변환 방법을 설정합니다. (정규표현식, 대소문자 변환)
   - **전송주기** : 정보를 전송할 주기를 선택합니다. (주기적 전송시 분 - 시간)
   - **암호화 방식** : 에이전트가 전송하는 정보를 암호화 하기 위한 옵션을 설정합니다. (*BASE64, AES, BLOWFISH, CAST, SEED*)
2. **추가** 버튼을 클릭합니다.
3. **수정** 버튼을 클릭합니다.

Linux 제어

Linux 에이전트가 설치된 Linux 단말에서는 다음 플러그인을 사용하여 에이전트가 설치된 Linux 단말의 정보를 수집/제어할 수 있습니다.

ARP 테이블 관리

사용자 PC의 ARP 테이블에 대한 관리 작업을 수행합니다. 악의적인 사용자는 ARP 테이블을 변조하여 내부 네트워크 보안 체계를 우회하거나 내부 사용자의 패킷을 가로채려는 시도를 할 수 있습니다. ZTNA는 이러한 시도들을 방지하기 위해 다음과 같은 기능을 제공합니다.

- 수동으로 ARP 항목을 Static으로 설정하지 못하도록 강제화하여 네트워킹 보호

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **ARP 관리** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **Static ARP 차단** 의 경우 **On** 으로 설정하여 Static으로 설정된 ARP에 대해서 사용하지 못하도록 강제화합니다.
2. **수정** 버튼을 클릭합니다.
3. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
4. 노드정책창에서 **기본정책** 을 클릭합니다.
5. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
6. **사용가능** 항목에서 **ARP 관리** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
7. **추가** 버튼을 클릭합니다.
8. **수정** 버튼을 클릭합니다.

Genian Login PAM

Linux OS 로그인과 함께 VPN 연결 및 프로그램 실행을 수행합니다.

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **Genian Login PAM** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **VPN 연결** 에서 **On** 옵션을 설정하여 Linux OS 로그인과 함께 VPN 연결을 수행합니다.
   - **연결 관리자**: 연결할 VPN을 설정합니다.
   - **사이트**: 연결할 VPN의 사이트를 설정합니다.
2. **실행 연동 설정** 의 경우 Linux OS 로그인과 함께 실행할 프로그램을 설정합니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 노드정책창에서 **기본정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
7. **사용가능** 항목에서 **Genian Login PAM** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

Linux 업데이트

Linux의 업데이트 상태를 검사하고 보고합니다.

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **Linux 업데이트** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **수정** 버튼을 클릭합니다.
2. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
3. 노드정책창에서 **기본정책** 을 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **Linux 업데이트** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.

ZTNA 연결 관리자

ZTNA 연결관리자에 대한 옵션 및 동작을 제어합니다.

- NAC와 외부 VPN 업체와의 연동 및 NAC 내부에서의 VPN 연동을 지원

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **ZTNA 연결 관리자** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **연결 관리자** 의 경우 연결 관리자의 종류를 지정합니다.
    - **사이트**: 연결 관리자의 **사이트 설정 정보** 를 설정합니다.
2. **수정** 버튼을 클릭합니다.
3. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
4. 노드정책창에서 **기본정책** 을 클릭합니다.
5. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
6. **사용가능** 항목에서 **ZTNA 연결 관리자** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
7. **추가** 버튼을 클릭합니다.
8. **수정** 버튼을 클릭합니다.

네트워크정보 수집

네트워크 인터페이스 정보를 노드정보에 표시합니다. 관리자에게 가시성을 제공하여 네트워크 제어에 활용 가능합니다.

- 인터페이스 정보를 모니터링하여 비인가 H/W나 인터페이스정보를 모니터링합니다.

Step1: 노드액션 설정하기

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **네트워크정보 수집** 을 찾아 클릭합니다.
5. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
6. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
7. 네트워크수집 플러그인은 별도의 플러그인 설정 없이 단말에 설치와 함께 자동으로 정보를 수집합니다.

Step2: 노드정책에 노드액션 할당하기

1. 왼쪽 정책 메뉴에서 **노드정책** 으로 이동합니다.
2. 적용하고자 하는 **노드정책** 을 클릭합니다.
3. **노드액션 설정** 을 찾아 할당 을 클릭합니다.
4. 사용가능 항목에서 **네트워크정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
5. 추가 버튼을 클릭합니다.
6. 수정 버튼을 클릭합니다.

모니터정보 수집

로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다. 모니터 정보를 수집하여 자산 관리/교체 등에 활용 가능합니다.

- 특정 inch 이하의 모니터 정보를 수집하여 하드웨어 교체 작업에 활용

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **모니터정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 노드정책창에서 **기본정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
7. **사용가능** 항목에서 **모니터정보 수집** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

모양 및 개인설정

화면보호기에 대한 설정 정보를 수집 및 제어합니다.

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **모양 및 개인설정** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시할 메시지를 추가합니다.

2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 **플러그인설정** 이 있습니다.

1. **화면보호기정보 수집** 에서 **On** 으로 설정하여 사용중인 화면 보호기 설정 정보를 수집합니다.
2. **화면보호기 제어** 에서 **On** 으로 설정하여 대기시간을 설정합니다.
   - **대기시간**: 화면 보호기로 전환되기 전까지의 동작 대기시간을 설정합니다. (분 - 시간)
   - **대기시간 고정**: **On** 으로 설정하여 관리자가 설정한 시간보다 PC에 사용 중인 대기시간이 짧을 때도 대기시간을 변경합니다.
3. **NAC 재인증** 에서 **On** 옵션을 설정하여 화면 보호기 해제 시, NAC 재인증을 요구합니다.
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 노드정책창에서 **기본정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
8. **사용가능** 항목에서 **모양 및 개인설정** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

백신정보 수집

PC에 설치되어있는 백신프로그램 정보를 실시간으로 수집합니다. 다양한 벤더들의 백신 정보를 ZTNA에서 수집합니다.

- 글로벌 벤더(clamAV, sophos 등)의 백신명, 버전, 패턴정보, 실시간 감시 정보 등을 수집하여 단말보안을 강화합니다.

백신 지원 목록

Genian ZTNA에서 지원되는 모든 안티바이러스를 버전별로 확인합니다.

벤더	제품명	정보제공 항목
Cisco Systems	ClamAV	백신명, 백신코드, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간
sophos	Sophos server protection	백신명, 백신코드, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간

백신정보 수집

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **백신정보 수집** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.

2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **수정** 버튼을 클릭합니다.
2. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
3. 노드정책창에서 **기본정책** 을 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **백신정보 수집** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.

사용자 알림메시지

사용자에게 알림메시지를 표시합니다. 관리자가 에이전트를 통해서 사용자에게 메시지를 전달합니다.

- 사용자에게 알림 메시지를 표시하여 클릭시 설정된 URL로 리다이렉션
- 알림 메시지 확인을 통해 감사기록 저장

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **사용자 알림메시지** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **메시지 제목** 에 에이전트 알림 시 표시할 제목을 설정합니다.
2. **클릭시 CWP 접속** 을 **On** 으로 설정하여 에이전트 알림 클릭 시 CWP 페이지로 이동하도록합니다.
    - **CWP URL** 에 **설정** 버튼을 클릭하여 템플릿을 사용하거나 URL을 직접 입력합니다.
3. **팝업창 고정** 의 경우 에이전트 알림을 닫지 못하도록 할지 여부를 선택합니다. (*On/Off*)
    - **메시지 타입** : 사용자메시지 타입을 선택합니다. (일반, 경고)
    - **메시지확인 알림** : 사용자가 메시지를 확인했으면 감사 로그를 기록하도록 설정합니다. (*On/Off*)
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 노드정책창에서 **기본정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
8. **사용가능** 항목에서 **파일 배포** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

소프트웨어 정보 수집

단말에 설치된 소프트웨어정보를 수집하여 노드상세정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.

- 단말에 설치된 소프트웨어 목록을 수집하여 비인가 소프트웨어 설치 여부 확인
- 특정 소프트웨어 미설치 단말이나 설치단말을 분류하여 정책 적용에 활용

Step1: 노드액션 설정

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
5. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

Step2: 노드정책에 노드액션 적용하기

1. 왼쪽 정책 메뉴에서 **노드정책** 으로 이동합니다.
2. 적용하고자 하는 **노드정책** 을 클릭합니다.
3. **노드액션 설정** 을 찾아 할당 을 클릭합니다.
4. 사용가능 항목에서 소프트웨어정보 수집 을 찾아 선택 항목으로 드래그하여 이동합니다.
5. 추가 버튼을 클릭합니다.
6. 수정 버튼을 클릭합니다.

수행조건만 검사

액션에 설정된 수행 조건을 검사하는데 사용하는 플러그인입니다. 프로세스, 파일, 시스템 및 인증된 사용자 등 조건을 설정하여 검사할 수 있습니다.

- 특정 프로세스의 해쉬값 검사
- 사내 필수프로그램 설치 여부 확인

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창 **작업선택** 오른쪽의 드롭다운 버튼을 클릭하여 **Linux** 운영체제를 선택합니다.
4. 노드액션 리스트에서 **수행조건만 검사** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다. (이 플러그인이 작동하려면 조건이 추가되어야합니다)

1. **조건연산** 의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.

2. **조건설정** 의 경우 **추가** 를 클릭하고 조건설정창에서 옵션들을 설정합니다. **항목 / 조건 / 설정** 입니다.
3. **수행주기** : 설정된 주기마다 액션을 수행합니다. (초 - 개월)
4. **추가** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 적용하고자 하는 **노드정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 을 클릭합니다.
8. **사용가능** 항목에서 **수행조건만 검사** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

운영체제정보 수집

Linux 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.

- 운영체제 정보를 수집하여 수집한 정보를 활용하여 노드를 분류하거나 정책적용에 활용 할 수 있습니다.

Step1: 노드액션 설정

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **운영체제정보 수집** 을 찾아 클릭합니다.
5. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
6. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

Step2: 노드정책에 노드액션 적용하기

1. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
2. 적용하고자 하는 **노드정책** 을 클릭합니다.
3. **노드액션 설정** 을 찾아 할당 을 클릭합니다.
4. 사용가능 항목에서 **운영체제정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
5. 추가 버튼을 클릭합니다.
6. 수정 버튼을 클릭합니다.

인터페이스 제어

단말의 유선, 무선 인터페이스를 제어하는 기능을 제공합니다.

- 관리자가 유선, 무선 차단 정책으로 정의하여 단말의 네트워크 인터페이스 제어

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **인터페이스 제어** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **타입별 차단** 의 경우 사용하지 않도록 설정할 네트워크 유형을 지정합니다.
   - **제어 안 함**: 단말의 모든 인터페이스에 대해 제어하지 않습니다.
   - **전체**: 단말의 유선, 무선의 인터페이스를 차단합니다.
   - **유선**: 단말의 유선 인터페이스를 차단합니다.
   - **무선**: 단말의 무선 인터페이스를 차단합니다.
2. **수정** 버튼을 클릭합니다.
3. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
4. 노드정책창에서 **기본정책** 을 클릭합니다.
5. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
6. **사용가능** 항목에서 **인터페이스 제어** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
7. **추가** 버튼을 클릭합니다.
8. **수정** 버튼을 클릭합니다.

파일 배포

Note: 파일 배포 플러그인은 CC 평가 항목에 포함된 기능이 아니므로 CC 인증을 요구하는 공공기관에서는 해당 플러그인을 사용할 수 없습니다.

파일을 실행하거나 특정 위치에 다운로드합니다. 정책서버는 에이전트와 통신하여 단말에게 파일에 대한 배포, 실행, 설치를 할 수 있습니다.

- 단말에 필요한 파일 배포
- 단말의 미설치 소프트웨어 설치

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **파일 배포** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **배포 파일** 의 경우 관리자가 파일을 배포하는 방식을 설정합니다.
   - **직접 업로드**: 관리자 로컬에 있는 파일을 직접 업로드 합니다.
   - **URL 입력**: 다운로드 URL을 입력하여 파일을 배포합니다.
2. **배포 옵션** 의 경우 배포할 방식을 설정합니다.
   - **파일 실행**: 압축파일일 경우 "파일 경로"에 실행할 파일을 설정하고, "실행옵션"과 실행할 "수행계정"을 설정하여 해당 파일을 실행시킵니다.
   - **다운로드**: 배포 파일을 복사할 단말의 파일 및 폴더 경로를 지정합니다.
   - **debian 패키지 실행**: 압축파일일 경우 "파일 경로"에 설치할 파일을 설정하고, 단말 PC에 설치합니다.
3. **수정** 버튼을 클릭합니다.
4. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
5. 노드정책창에서 **기본정책** 을 클릭합니다.
6. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
7. **사용가능** 항목에서 **파일 배포** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
8. **추가** 버튼을 클릭합니다.
9. **수정** 버튼을 클릭합니다.

프로세스 강제종료

관리자가 설정한 프로세스에 대해서 강제종료 기능을 수행합니다. 실행 주기를 지정하여 반복 수행 기능을 제공합니다.

- 비인가 프로세스 강제 종료 기능 제공

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **프로세스 강제종료** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **차단 프로세스** 의 경우 해당 옵션을 통해 단말에서 사용되면 안되는 프로세스를 설정합니다.(강제 종료)
2. **수정** 버튼을 클릭합니다.
3. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
4. 노드정책창에서 **기본정책** 을 클릭합니다.

5. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
6. **사용가능** 항목에서 **프로세스 강제종료** 를 찾아 **선택** 항목으로 드래그하여 이동합니다.
7. **추가** 버튼을 클릭합니다.
8. **수정** 버튼을 클릭합니다.

하드웨어정보 수집

마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다. 정책서버는 에이전트와 통신하여 단말의 CPU, 메모리, 저장장치 등의 정보를 수집합니다.

- 하드웨어 사용량 정보를 수집하여 시스템 자원 관리
- 각 하드웨어 사용량 정보 업데이트 주기

Step1: 노드액션 설정

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **하드웨어정보 수집** 을 찾아 클릭합니다.
5. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
6. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
7. **CPU 업데이트 최소비율** 의 경우 마지막으로 전송한 CPU 사용량이 현재 사용량과 설정비율 이상 차이가 나면 정보를 전송합니다.
8. **메모리 업데이트 최소비율** 의 경우 마지막으로 전송한 메모리 사용량이 현재 사용량과 설정비율 이상 차이가 나면 정보를 전송합니다.
9. **저장장치 업데이트 최소비율** 의 경우 마지막으로 전송한 저장장치 사용량이 현재 사용량과 설정비율 이상 차이가 나면 정보를 전송합니다.
10. **수행주기** 는 항상수행으로 10분 주기로 변경된 데이터가 존재하는 경우 업데이트됩니다.

> **Note:** 정보업데이트 설정비율은 전체 용량 기준으로 계산됩니다.

Step2: 노드정책에 노드액션 적용하기

1. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
2. 적용하고자 하는 **노드정책** 을 클릭합니다.
3. **노드액션 설정** 을 찾아 할당 을 클릭합니다.
4. 사용가능 항목에서 **하드웨어정보 수집** 을 찾아 선택 항목으로 드래그하여 이동합니다.
5. 추가 버튼을 클릭합니다.
6. 수정 버튼을 클릭합니다.

비밀번호 유효성 검사

Linux 계정의 비밀번호에 대한 유효성을 검사하고 검증되지 않은 비밀번호를 안전한 비밀번호로 변경시킵니다. 특수문자 사용 등 비밀번호 규칙을 강제화하여 단말 보안을 강화합니다.

- 관리자가 정한 비밀번호 문자열의 규칙 준수를 강제화하여 패스워드 보안을 강화
- 비밀번호 변경 주기를 설정하여 주기마다 패스워드 변경을 강제화

1. 상단 메뉴의 **정책** 으로 이동합니다.
2. 왼쪽 메뉴 트리에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 리스트에서 **비밀번호유효성검사** 을 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 **액션 수행설정** 을 구성합니다.

1. **검증된 계정표시** 의 경우 관리자가 검증된 계정에 대해서도 표시를 할지 여부를 설정합니다.
2. **검증창 고정** 의 경우 대화상자를 화면의 중앙에 고정을 할지 여부를 설정합니다.
3. **Linux 로그온/로그아웃 계정** 의 경우 로그온 및 로그아웃 계정에 대한 정책을 설정합니다.
   - **비밀번호 문자열 검사방법** : "규칙검사" 를 설정합니다. (비밀번호 규칙의 경우 "설정 > 사용자인증 > 비밀번호정책"규칙이 적용 됩니다)
   - **비밀번호 변경주기** : Linux 로그인 계정에 대한 비밀번호 변경주기를 설정합니다. (일 - 개월)
   - **만료전알림** : 비밀번호 시간이 만료되기 전에 알림을 발생합니다. (만료시간은 정책이 적용 된 시점부터 적용 됩니다.)
   - **검사예외ID** : 검사 예외대상의 사용자ID의 전체문자열을 입력합니다. (여러개 입력시 콤마로 구분, 대소문자를 구분하지 않습니다.)
4. **수정** 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 노드정책창에서 **기본정책** 을 클릭합니다.
7. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
8. **사용가능** 항목에서 **비밀번호유효성검사** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
9. **추가** 버튼을 클릭합니다.
10. **수정** 버튼을 클릭합니다.

장치 제어

사용자 PC에서 사용금지된 장치들을 사용중지로 변경합니다. 시스템에 물리적으로 연결하는 모든 장치를 제어합니다.

- 외부 장치를 실행 중지 또는 제거
- 관리자가 에이전트를 통해 장치에 대한 사용 신청을 받아 승인 여부 결정

Note: 장치사용신청서 설정부분은 다음에 linux-external-device-request 참고하시기 바랍니다.

---

1 단계. 장치 그룹 생성

- 장치 그룹은 제어에 필요한 일련의 장치를 정의하는 기능입니다. 정책에 대한 차단 또는 예외로 사용될 수 있습니다.

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 장치제어 정책 > 장치그룹** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **기본정보** 에서 고유한 **ID 이름** 을 입력합니다. (예 : *"USB* 저장 장치").
5. **OS 종류 > Linux** 를 선택합니다.
6. 제어 하려고 하는 장치명을 선택합니다.
7. 장치가 USB Disk 인 경우 **조건설정** 에서 다음을 입력합니다.
   - **USB 제조사** : USB 공급업체 이름을 지정
   - **USB 모델** : USB 모델 이름을 지정
   - **USB 시리얼** : USB 일련 번호 지정
8. **생성** 버튼을 클릭합니다.

2 단계. 장치제어 정책 생성

- 장치 제어 정책은 대상이 장치 제어를 수행하도록 차단하거나 허용 할 장치 그룹을 정의합니다.
- 플러그인이 업로드 되면 기본적인 출력장치에 대한 장치정책이 템플릿으로 제공됩니다. (장치제어 정책 ID : Data Prevention(Linux))

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 장치제어 정책** 으로 이동합니다.
3. **작업선택 > 생성** 버튼을 클릭합니다.
4. **기본정보** 에서 고유의 **ID 이름** 을 입력합니다. (예: *"USB* 스토리지 정책")
5. **노드그룹 설정** 에서 **할당** 버튼을 클릭하고 **노드그룹** 을 선택합니다.
6. **차단장치 설정** 에서 **할당** 버튼을 클릭하고 **USB 저장 장치** 를 선택합니다.
7. 1단계에서 설정한 장치그룹이 아니더라도 아래의 **기본장치그룹** 으로 정의되어있는 항목을 선택 할 수 있습니다.

USB Disk	USB 타입의 저장 장치
CD/DVD	CD롬 드라이브 클래스에 속한 장치
USB Network	USB 포트로 연결된 네트워크 장치(USB Tethering, USB LAN Adapter...)
Local Printer	로컬PC에 직접 연결된 프린터
Bluetooth	블루투스 클래스에 속한 장치
Camera	카메라 클래스에 속한 장치
Mouse	마우스 클래스에 속한 장치
Keyboard	키보드 클래스에 속한 장치
Sound	오디오 출력에 속한 장치
Microphone	오디오 입력에 속한 장치

8. **생성** 버튼을 클릭합니다.

3 단계. 장치 제어 플러그인 설정

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 노드액션 관리창에서 **장치 제어** 을 찾아 클릭합니다.
4. **액션 수행설정 > 장치제어 방식** 에서 **제거** 또는 **중지** 를 선택합니다.
5. **수정** 버튼을 클릭합니다.

4 단계. 노드정책에 에이전트 액션 추가

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책창에서 **원하는 노드정책ID** 를 클릭합니다.
4. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
5. **사용가능** 항목에서 **장치 제어** 를 찾아 **선택** 항목으로 이동 시킵니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭합니다.

프로그램 제거

Debian packages 및 Snap으로 설치된 프로그램중 제거 가능한 특정 프로그램을 제거합니다.

- 비인가 소프트웨어 삭제

1. 상단 항목의 **정책** 으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
3. 상단 **운영체제** 드롭다운 메뉴에서 **Linux** 를 선택합니다.
4. 노드액션 관리 창에서 **프로그램 제거** 를 찾아 클릭합니다.

아래 **기본설정** 이 있습니다.

1. **CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.

2. **라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래 **액션 수행설정** 이 있습니다.

1. **프로그램 이름** 의 경우 제어판의 프로그램 제거에 등록된 프로그램중 제거할 프로그램 이름을 설정합니다.
2. **강제 제거** 의 경우 프로그램 삭제 시, 의존성 등의 문제들을 무시하고 강제로 제거합니다.
3. **삭제전 알림** : 프로그램 삭제전 사용자에게 메시지 표시 여부를 설정합니다.
   - **메시지 내용** : 프로그램 삭제전 사용자에게 보여질 메시지를 입력합니다.
4. **리부팅옵션** 의 경우 사용자에게 알림을 보낼 지 자동 재부팅을 할지 선택합니다.
5. **수정** 버튼을 클릭합니다.
6. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
7. 노드정책창에서 **기본정책** 을 클릭합니다.
8. **노드액션 설정** 을 찾아 **할당** 버튼을 클릭합니다.
9. **사용가능** 항목에서 **프로그램 제거** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
10. **추가** 버튼을 클릭합니다.
11. **수정** 버튼을 클릭합니다.

8.5 확장 플러그인 설정방법

Genian ZTNA Agent에서 사용되는 연동 및 대체인증에 대한 확장 플러그인을 설정하여 사용할 수 있습니다.

8.5.1 확장 플러그인 항목

확장 플러그인은 정책서버에 자동으로 생성되어 있으며 생성되는 목록은 아래와 같습니다. 해당 확장 플러그인은 사용 목적에 따라 별도의 액션정책으로 생성하여 사용할 수 있습니다.

플러그인 이름	설명	설정방법
C_Suser	SafePC Enterprise 대체 인증	바이오닉스진 *SafePC*
C_PassNiSSO	Pass-Ni SSO 대체 인증	
C_NC_IBK	INISAFE Nexess 대체 인증	이니텍 *INISAFE Nexess*
C_PentaSSO	Penta Security SSO V2.0 대체 인증	
C_RathonSSO	Rathon SSO 대체 인증	라톤테크 *Rathon-SSO*
C_KsignSSO	Ksign SSO 대체 인증	케이사인 *KSignAccess*
C_Penta2SSO	Penta Security SSO V3.0 대체 인증	
C_SIClient2SSO	SafeIdentity SSO 대체 인증	
C_SecuRegAuth	Smart NAC 대체 인증	
C_NetsESSO	Nets EnterpriseSSO 대체 인증	
RegAuth	외부인증연동(레지스트리)	
ExeAuth	외부인증대체(실행파일)	
GnManager	Genian 통합에이전트	

8.6 에이전트 기타 기능

8.6.1 CLI 명령어를 통한 에이전트 사용 (Linux 전용)

gncli 명령어를 사용하여 UI가 없는 환경에서도 **Agent의 필수 기능** 을 사용할 수 있습니다.

- `tab` 버튼을 활용한 **자동완성 기능** 을 제공합니다.

1. Agent가 설치된 단말에서 **terminal** 을 실행합니다.
2. **"gncli --help"** 를 입력하여 사용가능한 명령어를 확인합니다.
3. **명령어** 를 입력하여 **Agent의 필수 기능** 을 사용합니다.

아래의 **명령어** 를 제공합니다.

$ gncli about
제품 정보를 표시합니다.

$ gncli version
프로그램 버전을 표시합니다.

$ gncli delete
에이전트 삭제작업을 수행합니다.

$ gncli deployer
신뢰할 수 있는 배포자 정보를 출력합니다.

$ gncli user
사용자 작업을 수행합니다.

$ gncli user status : 사용자 상태를 표시합니다.

$ gncli user login : 사용자 로그인작업을 수행합니다.

$ gncli user logout : 사용자 로그아웃작업을 수행합니다.

$ gncli network
네트워크 접속 관리 작업을 수행합니다.

$ gncli network status : 네트워크 연결 상태를 표시합니다.

$ gncli network site : 연결 가능한 네트워크 사이트 정보를 나열합니다.

$ gncli network connect : 네트워크 연결작업을 수행합니다.

$ gncli network disconnect : 네트워크 연결을 해제합니다.

$ gncli compresslog
에이전트 로그를 압축합니다.

Note: 각 명령에 대한 자세한 내용을 보려면 **"gncli [옵션] --help"** 를 입력하세요.

CHAPTER

NINE

위험감지

위험감지는 네트워크 또는 단말에 커다란 위협을 가할 수 있는 여러가지 일반적이지 않는 상황들을 모니터링 해서 위험상황이 발생하였을 때 보다 신속하고 효과적으로 대응할 수 있도록 합니다. Genian ZTNA는 네트워크의 트래픽을 검사하거나 단말의 이상 행위 모니터링해서 위험단말을 찾아냅니다. 관리자는 사전에 정의된 위험이벤트를 활용하여 **Ad Hoc 네트워크, ARP Bomb, ARP Spoofing, MAC/IP Clone, Port Scan** 등과 같은 주요 위험에 노출되어 있는 단말을 감지할 수 있습니다.

9.1 위험감지의 이해

센서 및 에이전트는 네트워크 트래픽의 이상행위를 탐지하여 위험이 있는 단말을 식별하고 정책에 따라 차단합니다.

ARP Bomb, MAC+IP Clone, ARP Spoofing, Ad Hoc 네트워크 등과 같은 비정상적인 행위를 탐지합니다.

위와 같은 위험행위를 탐지 하려면 노드 정책에 위험감지 항목들을 할당 해야합니다.

9.1.1 ARP Bomb

네트워크센서가 ARP를 모니터링할 때, 과도한 ARP 패킷이 발생하는 장치가 감지되면 해당 노드를 위험 노드로 분류합니다. 공격자 노드는 Request 패킷을 대상 노드에 지속적으로 전송하여 빠르게 캐쉬를 가득 채웁니다. 곧 대상 노드는 캐시를 유지하기 위해 더 많은 리소스를 사용할 것이며, 이로 인해 버퍼 오버플로우가 발생할 수 있습니다. 그리고 정상적인 패킷이 캐쉬에 입력되지 않을 것입니다.

Genian ZTNA는 다양한 방법으로 전송되는 과도한 ARP Request 패킷을 감지할 수 있습니다. 네트워크센서는 각 노드가 전송한 ARP 패킷 수를 계산합니다. ARP Request가 지정된 값보다 많은 경우, ARP Bomb으로 판단하고 위험노드로 지정합니다.

- **감지기간** 은 위험으로 감지하기 위한 기간을 설정합니다.
- **요청횟수** ARP Request 횟수를 설정합니다. 감지기간 동안 ARP Request가 지정한 횟수 이상일 경우에 위험으로 감지합니다.
- **공격자 검색방법** 과도한 ARP 패킷을 전송하는 노드를 찾기 위한 방법을 선택합니다.

9.1.2 MAC/IP Clone

IP 프로토콜은 IP 및 MAC 주소를 사용하여 통신 대상을 식별합니다. 별다른 검증 절차가 없기에 쉽게 탈취 할 수 있습니다. 만약 악성 단말이 MAC/IP를 복제한 경우 패킷 수준에서 일반 시스템과 도난된 시스템을 구분하는 것은 매우 어렵습니다.

그러나 Genian ZTNA는 다양한 방법으로 MAC/IP 탈취를 탐지 할 수 있습니다. 네트워크센서는 주기적으로 ARP Request를 전송하여 장치의 동작 상태를 확인합니다. 동시에 두 개의 응답이 수신되면 MAC / IP Clone을 의심하고 위험 노드로 지정합니다. 추가적으로 악성 단말이 에이전트가 설치되어 있는 단말의 MAC으로 변경한다면, 즉시 공격 단말을 위험노드로 지정합니다.

인가된 MAC / IP 도용 단말 제어하기

비인가 단말이 인가된 단말의 MAC 과 IP를 도용해서 네트워크 접근을 시도할 수 있습니다. 인가 단말과 동일한 MAC 과 IP 를 사용하게 되면 네트워크수준(IP, MAC 주소)에서는 인가/비인가 여부를 구분하기 어렵습니다. 따라서 MAC/IP 기본정보 이외에 동일 MAC/IP를 가진 네트워크 패킷 감지, 에이전트에서의 MAC 변경 감지를 통해 IP/MAC 도용을 제어합니다.

해결방법

MAC/IP Clone 단말을 제어하기 위해 Genian ZTNA에서는 네트워크센서와 에이전트에서 제어 방법을 제공합니다.

- 네트워크센서에서 제공하는 MAC/IP Clone 탐지기능을 사용합니다.
- 에이전트를 통한 MAC Clone 탐지기능을 사용합니다.
- MAC/IP Clone 위험감지 정책을 사용합니다.

Step.1 네트워크센서 MAC/IP Clone 탐지 설정

1. 상단 시스템메뉴로 이동합니다.
2. 좌측 패널의 센서관리로 이동합니다.
3. 네트워크 센서 항목 좌측 체크박스에 체크합니다.
4. **작업선택** 에서 센서 일괄 설정을 클릭합니다.
5. 노드상태 검사항목에 **MAC+IP Clone 감지** 항목을 체크합니다.
6. 하단 저장 버튼을 클릭합니다.

Step.2 네트워크센서 노드상태검사 설정확인

1. 상단 시스템메뉴로 이동합니다.
2. Step1 에서 설정한 네트워크센서 **장비의 IP** 를 클릭합니다.
3. 환경설정 탭으로 이동합니다.
4. **기타설정 항목에 노드상태검사 항목의 설정이 아래와 같은지 확인합니다.**
    - 노드상태검사: On
    - 노드 상태검사 방법: 최소 주기

Step.3 MAC/IP Clone 위험감지 설정과 노드정책 할당

1. 상단 정책메뉴로 이동합니다.
2. 좌측 패널의 위험감지 메뉴로 이동합니다.

3. **MAC/IP Clone 위험감지** 를 선택합니다.
4. 하단 옵션설정에서 **MAC Spoofing 감지** 옵션을 `On` 으로 변경하고 하단 수정 버튼을 클릭합니다.
5. 좌측 패널 노드정책으로 이동합니다.
6. MAC/IP Clone 탐지를 적용하고자 하는 대상의 **노드정책명** 을 클릭합니다.
7. 최하단 위험감지 항목에서 할당 버튼을 클릭합니다.
8. 팝업창에서 MAC / IP Clone 항목을 우측으로 이동시키고 수정 버튼을 클릭합니다.
9. 하단 수정 버튼을 클릭하여 수정사항을 저장합니다.
10. 우측 상단 변경 정책 적용 버튼을 클릭하여 정책을 적용합니다.

Step.4 위험노드 네트워크 차단

위험에 탐지된 노드는 다음방법을 통해 네트워크를 제어할 수 있습니다. 위험 노드 차단

9.1.3 Malware Detection

에이전트를 통해 엔드포인트에 존재하는 악성 PE (Portable Excutable) 파일을 탐지할 수 있습니다.

9.1.4 Ad Hoc 네트워크 연결

에이전트는 다양한 방법의 multi-homed 설정이나 Ad Hoc 네트워크 연결을 즉시 감지할 수 있습니다. IP 주소가 두 개 이상인 컴퓨터가 두 개 이상의 네트워크에 연결되어 있고 그 중 하나가 신뢰할 수 없는 경우 위험노드로 지정합니다. 이는 에이전트 제어 옵션뿐만 아니라 노드액션의 인터페이스 제어와 함께 수행할 수 있습니다. client-to-client 통신 탐지 (에이전트 필요)

- **차단방법:** 장치차단 또는 감사로그
- **차단팝업 사용:** 예 또는 아니오
- **예외장치명:** 위험감지에 예외할 장치를 지정 (장치명이 정확히 일치해야하므로 *Interface Type Exception* 로 설정하는 것이 더 효율적입니다.)
- **예외장치타입:** 유선, 무선, 가상

9.1.5 Port Scan

Genian ZTNA는 다양한 방법으로 수행하는 포트스캔을 감지할 수 있습니다. 네트워크센서는 포트 스캔 이벤트를 감지하기 위해 네트워크 트래픽의 흐름을 모니터링합니다. 가상 IP 주소에 대해 취약점을 찾기 위해 포트를 스캔한다면, 해당 노드를 위험노드로 지정합니다. 추가적으로 특정 기간 사이에 지정 횟수 이상으로 포트가 스캔 된다면, 위험노드로 지정합니다. TCP 또는 UDP 포트를 스캔하려는 단말을 감지합니다. Genian ZTNA는 스캐닝 단말을 감지하기 위해 허니팟 IP를 사용합니다.

- **감지기간** 은 위험으로 감지하기 위한 기간을 설정합니다.
- **요청횟수** 포트 접근 횟수를 설정합니다. 감지기간 동안 지정한 횟수 이상의 포트 접근 시 위험으로 감지합니다.
- **공격자 검색방법** 위험탐지 시 공격자 노드를 찾기 위한 방법을 선택합니다.

9.1.6 비정상적인 DHCP서버 감지

DHCP 서버가 분배하는 DNS값을 센서에 설정된 DNS와 일치여부를 비교하여, 비정상적인 DHCP 서버를 감지할 수 있습니다.

9.1.7 잘못된 게이트웨이 사용

에이전트는 허용되지 않은 게이트웨이 설정을 즉시 감지 할 수 있습니다. 만약 노드에 신뢰할 수 없는 게이트웨이 주소 (또는 기본 게이트웨이) 가 설정 되어있다면, 해당 노드를 위험노드로 지정합니다. 이는 에이전트 제어 옵션뿐만 아니라 노드액션의 인터페이스 제어와 함께 수행할 수 있습니다.

- **차단방법:** 장치차단 또는 감사로그
- **차단팝업 사용:** 예 또는 아니오
- **예외장치명:** 위험감지에 예외할 장치를 지정 (장치명이 정확히 일치해야 하므로 *Interface Type Exception* 로 설정하는 것이 더 정확합니다.)
- **예외장치타입:** 유선, 무선, 가상

9.1.8 센서 MAC Clone

센서의 MAC 주소가 복제 되었는지를 감지합니다. (설정 필요 없음)

9.1.9 ARP Spoofing

Genian ZTNA는 다양한 방법으로 ARP 변조 패킷을 감지할 수 있습니다. 네트워크센서는 네트워크의 ARP 응답을 수신하며 ARP sender와 source MAC 주소의 변화나 차이점을 검사합니다. 또한, 스푸핑을 시도한 장치를 차단하고 ARP Detox를 통해 정상 MAC으로 갱신합니다.

- **감지기간** 은 위험으로 감지하기 위한 기간을 설정합니다.
- **공격횟수** ARP 변조 패킷 횟수를 설정합니다. 감지기간 동안 지정한 횟수 이상의 ARP변조 패킷을 보낼 경우 위험으로 감지합니다.

ARP Enforcement은 네트워크 장치의 통신을 차단하는데 사용하는 기술이지만, ARP Spoofing은 주로 악성코드로 사용되며 또한 다른 단말간의 통신을 도청하는데 사용합니다. .. note:: VRRP(Virtual Router Redundancy Protocol) 를 사용하는 경우 ARP Sender MAC 주소가 실제 MAC 주소인 ether src MAC 주소와 다를 수 있습니다. Genian ZTNA는 VRRP, HSRP 또는 GLBP 등 알려진 프로토콜에 대하여 감지되지 않도록 예외처리합니다.

9.1.10 알수없는 서비스 요청

Genian ZTNA는 다양한 방법으로 제공하지 않는 서비스 요청시도를 감지할 수 있습니다. 네트워크센서는 가상의 허니팟을 이용하여 서비스요청을 감지합니다. 만약 가상IP 주소로 제공하지 않은 서비스 요청시도가 감지되면, 일정 기간 내에 지정된 값 이상의 서비스를 요청하면 위험노드로 지정합니다.

- **감지기간** 은 위험으로 감지하기 위한 감지기간을 설정합니다.
- **요청횟수** 감지기간동안 지정된 횟수이상 서비스요청시 위험으로 탐지합니다.
- **공격자 검색방법** 공격자 노드를 찾기 위한 방법을 선택합니다.

9.1.11 SNMP 차단요청

Genian ZTNA에서는 외부 시스템과 SNMP Trap 연동을 통해 네트워크 제어와 네트워크 제어 해제요청을 수신하여 해당 단말을 위험노드로 지정할 수 있습니다. 또한, 태그 할당 기능을 통해 SNMP Trap이 수신된 단말에 제어를 수행할 수 있습니다.

태그 할당 기능을 로그 발생 시 태그 할당 를 참고하시기 바랍니다.

9.2 위험감지 생성

사용자 개별 위험감지 정책을 만들어 노드그룹에 적용 할 수 있습니다.

기본적으로 자주 사용되는 **위험감지** 10 가지가 정의되어 있습니다. 아래의 단계를 따라 새로운 위험감지를 생성할 수 있습니다.

9.2.1 위험감지를 생성하는 방법

1. 상단 메뉴바에서 **정책** 을 클릭합니다.
2. 왼쪽의 정책 패널에서 **정책 > 노드정책 > 위험감지** 로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.

기본설정

1. **ID** 에는 고유 한 이름을 입력합니다.
2. **CWP메시지** 에는 사용자에게 표시할 메시지를 입력합니다.
3. **중요도** 는 , 위험 정도에 따라 **낮음, 중간, 높음** 을 선택할 수 있습니다.
4. **적용모드** 는 반드시 **사용함** 이어야 동작합니다.
5. **예외 노드 그룹** 설정은 선택 옵션입니다. 해당 위험에서 예외 시킬 그룹을 선택합니다.

이벤트 정의 설정

1. **이벤트** 에는 어떤 위험감지를 사용할 것인지 선택합니다.
2. **옵션설정** 은 **이벤트** 를 동작시키고자 하는 대로 설정합니다.
3. **생성** 버튼을 클릭합니다.

9.2.2 위험감지를 삭제하는 방법

1. 상단 메뉴바에서 **정책** 을 클릭합니다.
2. 왼쪽의 정책 패널에서 **정책 > 노드정책 > 위험감지** 로 이동합니다.
3. 삭제하고 싶은 **위험감지** 의 **체크박스를** 선택합니다.
4. **작업선택 > 삭제** 를 클릭합니다.
5. **확인** 을 클릭합니다.
6. **변경정책적용** 을 클릭합니다.

9.3 위험 모니터링

위험정의 를 적용할 **노드정책** 에 할당하면 **네트워크센서** 또는 **에이전트** 에 의하여 즉시 위험이 감지됩니다. 관리자는 다양한 방법으로 결과를 확인할 수 있습니다.

- **노드관리** 에서 표시된 **위험** 확인
- **위험뷰** 로 관리뷰를 변경
- **위험 로그** 확인
- **대시보드** 의 **위험** 탭
- **현황 & 필터** 에서 위험감지 확인

더 나아가, 위험에 대해 관리자에게 알릴 수 있습니다.

관리자에게 감지된 위험을 알리는 방법은 발생 로그(이벤트) 보내기 를 참조 하세요.

9.3.1 기본 정의된 위험감지를 노드정책에 할당

기본적으로 노드 정책은 위험을 감지하지 않습니다. 위험감지 정책을 만들려면 다음을 참조 하세요. 위험감지 생성

노드 정책에 위험감지를 추가하고 이상 행위를 능동적으로 감지하려면 다음과 같이합니다.

1. 상단 메뉴바에서 **정책** 을 클릭합니다.
2. 왼쪽의 정책 패널에서 **정책 > 노드정책** 으로 이동합니다.
3. 노드정책 화면에서 **노드정책의 ID** 를 찾아 클릭합니다.
4. 맨 아래의 **위험감지 설정** 으로 이동하여 **할당** 버튼을 클릭합니다.
5. **사용가능** 컬럼에서 **위험** 을 클릭 후 **선택** 으로 옮깁니다.
6. **추가** 버튼을 클릭합니다.
7. **수정** 버튼을 클릭하여 설정을 저장합니다.
8. **변경정책적용** 을 클릭합니다.

9.3.2 위험감지 확인

감지된 위험은 다음 방법으로 볼 수 있습니다.

노드관리의 위험 컬럼

1. 상단 메뉴바에서 **관리 > 노드** 로 이동합니다.
2. 위험 컬럼을 찾아 아이콘을 확인합니다. (표시된 아이콘을 클릭하여 세부 정보를 볼 수 있습니다)

노드관리의 위험뷰

1. 상단 메뉴바에서 **관리 > 노드** 로 이동합니다.
2. 작업선택 버튼 옆에 위치한 **메뉴 버튼(3개의 점과 줄)** 을 찾아 클릭합니다.
3. **뷰** 항목 중 **위험뷰** 를 선택합니다.
4. **위험정의** 와 **위험감지** 컬럼을 확인 할 수 있습니다. (**관리뷰 편집** 을 클릭하여 컬럼을 구성할 수 있음)

위험 로그

1. 상단 메뉴바에서 **감사 > 로그** 로 이동합니다.
2. 왼쪽의 로그 항목에서 **로그검색 > 위험** 을 클릭합니다.

대시보드의 위험 탭

1. 상단 항목에 있는 **대시보드** 로 이동합니다.
2. **위험** 탭 으로 이동합니다.

현황 & 필터

1. 상단 메뉴바에서 **관리 > 노드** 로 이동합니다.
2. 왼쪽의 하단 항목에서 **현황 & 필터 > 위험감지** 또는 **위험노드** 로 이동합니다.

9.3.3 위험감지 해제

1. 상단 메뉴바에서 **관리 > 노드** 로 이동합니다.
2. 원하는 노드를 찾아 **체크박스** 를 선택합니다.
3. **작업선택 > 노드장비관리 > 노드위험해제** 를 클릭합니다.
4. **확인** 을 클릭합니다.

9.4 위험 노드 차단

상태그룹을 통해 위험 노드들을 그룹화 하고, 제어정책으로 해당 노드들을 차단할 수 있습니다.

9.4.1 상태그룹 생성

위험감지를 사용하여 기본 정책에 의해 식별되는 모든 노드가 그룹화 됩니다.

1. 상단 메뉴바에서 **정책** 을 클릭합니다.
2. 왼쪽의 정책 패널에서 **정책 > 그룹 > 노드** 로 이동합니다.
3. **작업선택 > 상태그룹 생성** 을 클릭합니다.
4. **ID:** 고유 한 이름을 입력합니다. (예시 위험 상태 그룹)
5. **적용모드:** 사용함을 선택합니다.

6. **조건연산** 은 **OR** 로 선택합니다.
7. **조건설정** 의 **추가** 버튼을 클릭합니다.
8. 아래의 **조건설정** 항목을 원하는 대로 설정합니다.
    - **항목:** 위험감지
    - **조건:** 특정위험이 감지되면
    - **설정:** (목록 중에 하나를 선택)
9. **추가** 를 클릭합니다.
10. 필요에 따라 **조건설정** 을 계속 추가합니다.
11. **생성** 버튼을 클릭합니다.

9.4.2 제어정책 생성

노드정책에 의해 식별된 모든 위험감지 노드들은 위험 상태그룹에 리스트화 되어 차단 할 수 있습니다.

1. 상단 메뉴바에서 **정책** 을 클릭합니다.
2. 왼쪽의 정책 패널에서 **정책 > 제어정책** 으로 이동합니다.
3. **작업선택 > 생성** 을 클릭합니다.
4. **정책선택** 탭에서, **다음** 버튼을 클릭합니다.
5. **정책 기본설정** 탭은
    - **ID:** 고유한 이름을 입력(예시 위험 제어 정책)
    - **설명:** 위험으로 감지된 노드를 차단하기 위한 위험정책
    - **적용모드:** 사용함
    - **다음** 버튼을 클릭
6. **노드그룹 할당** 탭에서, **상태그룹** 을 찾아 더블클릭합니다.(예시 위험 상태 그룹) **다음** 버튼을 클릭합니다.
7. **권한할당** 탭에서 , **PERM-DNS** 를 더블 클릭 한 후 **다음** 버튼을 클릭합니다.
8. **제어옵션 설정** 탭에서, **다음** 버튼을 클릭합니다.
9. **제어액션 설정** 탭에서, **완료** 버튼을 클릭합니다.
10. **변경정책적용** 을 클릭합니다.

9.5 위험감지 사전 환경설정

네트워크 센서와 에이전트에서 위험을 감지하기 위해서는 탐지 주체에 대한 환경설정을 해야합니다.

9.5.1 위험감지 탐지 주체

다음과 같이 위험감지 항목 별 위험을 탐지하는 주체가 나눠지게 됩니다. 각각의 탐지 주체에 따라서 위험을 감지하기 위한 사전 설정이 필요합니다.

위험감지의 탐지 주체가 **에이전트** 일 경우에는 노드액션을 **노드정책** 에 할당해야 위험감지가 가능합니다.

위험감지 ID	위험감지 탐지 주체	설정사항
Ad Hoc 네트워크 연결	에이전트	네트워크 정보수집 플러그인
ARP Bomb	네트워크 센서	위험 트래픽 유도용 가상 IP 설정
ARP Spoofing	네트워크 센서	위험 트래픽 유도용 가상 IP 설정
MAC / IP Clone	네트워크 센서 / 에이전트 (ARP Spoofing)	네트워크 센서 MAC / IP Clone 탐지 기능
Malware Detection	에이전트	Malwaer Detection 플러그인
Port Scan	네트워크 센서	위험 트래픽 유도용 가상 IP 설정
SNMP 차단요청	정책서버	SNMP Trap 수신기능
비정상적인 DHCP 서버 감지	네트워크 센서	네트워크 센서 DHCP Server Scan 기능
센서 MAC Clone	네트워크 센서	네트워크 센서 MAC / IP Clone 탐지 기능, 센서 MAC 충돌회피 기능
알수없는 서비스 요청	네트워크 센서	위험 트래픽 유도용 가상 IP 설정
잘못된 게이트웨이 사용	에이전트	네트워크 정보수집 플러그인

9.5.2 환경 설정하기

위험 트래픽 유도용 가상 IP 설정하기

가상 IP 설정은 가상IP 설정하기 를 참고하시기 바랍니다.

네트워크 센서 DHCP Server Scan 기능 설정하기

1. 상단 패널에 **시스템** 을 선택합니다.
2. 왼쪽 시스템 메뉴에서 센서관리를 클릭합니다.
3. 설정 대상 네트워크 센서의 체크박스를 선택합니다.
4. 작업선택 메뉴에서 **센서 일괄 설정** 항목을 선택합니다.
5. 센서 설정 메뉴에서 네트워크 스캔 항목에 DHCP Server Scan 값을 ON으로 변경합니다.
6. 저장 버튼을 클릭합니다.

정책서버 SNMP Trap 수신기능 설정하기

1. 상단 패널에 **설정** 을 선택합니다.
2. 왼쪽 환경설정 메뉴에서 감사기록을 선택합니다.
3. SNMP Trap 수신 항목에서 사용유무를 ON으로 설정하고, Community 값을 입력합니다.
4. 수정 버튼을 클릭합니다.

네트워크 센서 MAC / IP Clone 탐지 기능 설정하기

1. 상단 패널에 **시스템** 을 선택합니다.
2. 왼쪽 시스템 메뉴에서 센서관리를 클릭합니다.
3. 설정 대상 네트워크 센서의 체크박스를 선택합니다.
4. 작업선택 메뉴에서 **센서 일괄 설정** 항목을 선택합니다.
5. 센서 설정 메뉴에서 노드상태 검사 항목에 MAC+IP Clone 감지 값을 ON으로 변경합니다.
6. 저장 버튼을 클릭합니다.

CHAPTER

TEN

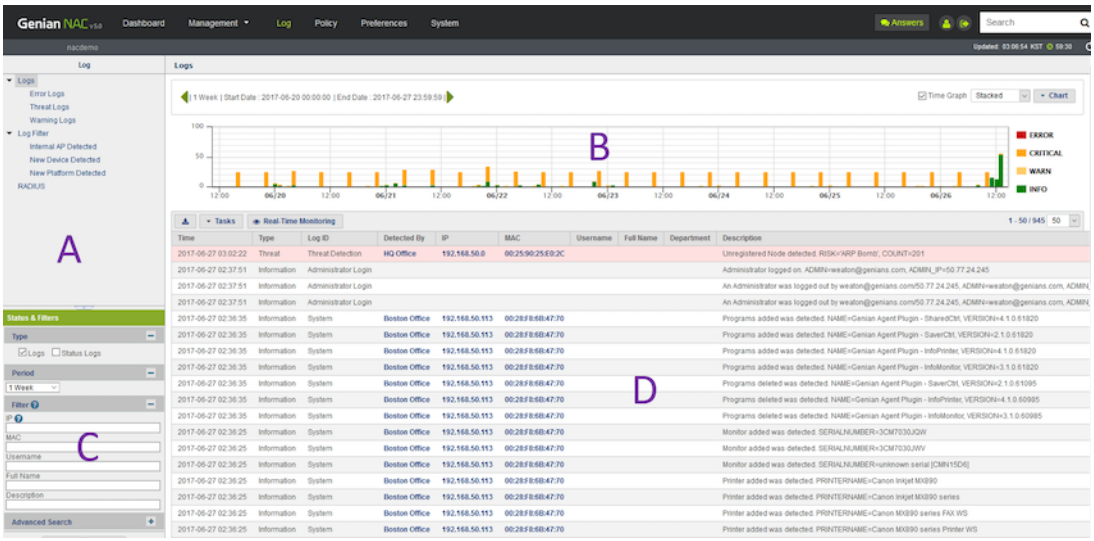
로그 및 이벤트 관리

정책서버는 에이전트, 네트워크센서, 3rd party 시스템 등으로 부터 수집한 정보 및 이벤트를 바탕으로 보안관리 목적의 로그를 생성합니다. 장비의 운영과정에서 발생하는 내용들(장비의 장애발생, 불법적인 접근 시도, 정책변경, 작업수행 결과 등)이 발생시간 등과 함께 기록된 자료입니다. 관리자는 로그를 통하여 긴급 상황에 대하여 신속히 대처할 수 있고, 로그 검색을 통하여 노드들의 패턴을 파악하여 효율적으로 정책을 수립할 수 있습니다. 본 로그는 SIEM 솔루션과 같은 외부 솔루션으로 전송이 가능합니다.

로그 검색은 4개의 주요 항목으로 구성됩니다.

- A 항목: 심각도, 자주 사용되는 로그 및 RADIUS로 분류되는 미리 정의된 로그
- B 항목: 시간 그래프 및 차트
- C 항목: 검색 및 필터 조건
- D 항목: 검색 및 필터링의 결과 창

로그 표시 및 생성 옵션은 **설정** 항목의 **환경설정 > 감사기록** 에서 구성할 수 있습니다.



10.1 로그 관리

실시간 검색, 필터링, 태그 지정 및 시각화를 통해 특정 데이터를 찾을 수 있습니다. Genian ZTNA는 심각도에 따라 로그를 제공하고 일반적인 사용법에 따라 사전 정의 된 로그 필터를 제공합니다.

10.1.1 감사로그 추가정보 설정하기

기본 감사로그에 저장하는 정보외 노드, 호스트명, 노드 플랫폼, 노드 설명 등의 추가정보를 감사로그에 저장하는 방법을 안내합니다.

1. Web콘솔에 접속합니다.
2. 상단 **설정 > 환경설정 > 감사기록** 으로 이동합니다.

감사로그 추가정보 컬럼

1. 추가정보 저장 옵션 선택에서 추가할 항목을 선택합니다.
2. 하단 수정 버튼을 클릭합니다.
3. 상단 감사 메뉴로 이동하여 새로 추가된 감사로그의 **추가정보 컬럼** 에 위에서 설정한 정보가 표시되는지 확인합니다.

추가 가능한 정보

- 노드이름
- 노드설명
- 호스트명
- 도메인
- DNS 이름
- 플랫폼
- 인증 사용자 직급
- 연결 스위치 이름
- 연결 스위치 포트
- 센서그룹명

노드 동작상태 이력 저장

- 노드의 Up/Down 동작상태를 기록하려면 `On` 이나 `Off` 를 선택 합니다.(Default On)
- 노드 Up/Down 동작상태 확인은 노드 상세정보 이력관리 `UP/DOWN` 버튼을 클릭하거나 상단 감사메뉴에서 `UP/DOWN` 버튼을 클릭하여 확인 가능합니다.

에이전트 동작상태 이력 저장

- 에이전트의 Up/Down 동작상태를 기록하려면 `On` 이나 `Off` 를 선택합니다.(Default Off)

10.1.2 로그 검색

검색 섹션에서 로그 내 특정 정보를 검색하거나 고급 검색 필드에 있는 옵션을 추가하여 로그를 검색할 수 있습니다. 또한 **연산자** 및 **특수 문자** 를 사용하여 검색이 가능합니다.

1. Web콘솔 상단메뉴 **감사** 로 이동합니다.

감사로그 검색은 화면 상단 좌측에서 우측순서대로 설정합니다.

1. 우측 화면 상단에서 감사로그 OR `UP/DOWN` 선택
2. **달력 버튼 클릭하여 감사로그 검색 기간 선택**
    - `Add filters` 클릭
    - IP 지정
    - MAC 지정
    - 사용자 ID
    - 부서명
    - 관리장비명
    - 추가정보
    - 설명
    - 로그타입(복수선택 가능)
    - 로그ID
3. **검색** 버튼을 클릭합니다.

Note: 감사로그 > 로그검색 > 검색창 클릭 > **필터** 우측 ? 를 클릭하면 검색에 도움이 되는 검색방법에 대한 안내페이지가 팝업 됩니다.

10.1.3 시간 그래프 및 분석차트

시간 그래프

시간 그래프에는 일별 로그 발생량이 표시됩니다. 상단의 달력 버튼을 클릭하여 기간별로 로그 발생량 추이를 확인할 수 있습니다. 시간 그래프는 기본으로 **Stacked(로그타입)** 형식과 **Logarithmic(발생시간)** 2가지 형태로 표현이 가능하며 기본은 **Stacked** 입니다. `Stacked` OR `Logarithmic` 을 선택하여 그래프 형태를 변경하여 감사로그 발생추이를 확인 가능합니다.

분석차트

그래프 아이콘을 클릭하여 분석차트 버튼을 선택하면 차트 기능을 사용가능합니다.

설정한 기간동안의 감사로그 정보를 항목별 차트로 표시합니다. 아래는 표시되는 차트의 종류입니다.

- 로그타입별 현황
- 로그ID별 현황
- 로그IP별 현황
- 로그MAC별 현황
- 관리장비별 현황
- 로그메시지별 현황

Note: **타임차트** 토글버튼을 이용하여 그래프를 비활성화 할 수 있습니다.

10.1.4 실시간 모니터링

이벤트가 발생할 때 로그를 실시간으로 볼 수 있으므로 신속하게 대응하고 즉각적인 조치를 취할 수 있습니다. 동일한 브라우저 내에서 이러한 이벤트를 보거나 새 개별 창에서 이벤트를 볼 수 있습니다.

실시간 모드

1. 상단 항목의 **감사** 로 이동합니다.
2. 실시간 모드 버튼을 찾아 클릭합니다.
3. 로그 리스트 오른쪽 상단에서 **주기** 옵션을 사용하여 새로 고침 빈도를 설정합니다. (예: *5,10,15,30,60 /* 초)
4. 별도의 창에서 보려면 팝업 버튼을 찾아서 클릭합니다.

10.1.5 검색필터 생성

미리 정의해놓은 로그검색 조건을 검색 필터로 생성하여 매번 검색조건 입력없이 바로 로그조회를 가능하게 하는 기능입니다. 기본 검색 필터 일부 제공하고 있으며 사용자가 직접 **검색필터** 를 만들어서 사용할 수 있습니다.

- 검색필터 생성 시 다음 항목을 추가적으로 설정할 수 있습니다.
- 외부전송설정에 세부사항은 다음에 로그 전송 참고하시기 바랍니다.

항목	세부항목	내용
출력컬럼		검색필터 결과값에 표시할 정보를 선택합니다.
외부전송 설정	알람전송	검색필터로 생성된 로그 발생 시 관리자 전달 항목(SMS, E-Mail)을 설정합니다.
	SYSLOG 전송	검색필터로 생성된 로그 발생 시 내용이 전달될 SYSLOG Server를 설정합니다.
	SNMP Trap 전송	검색필터로 생성된 로그 발생 시 내용이 전달될 SNMP Server를 설정합니다.
	Webhook 전송	검색필터로 생성된 로그 발생 시 내용이 전달될 Web Server URL을 설정합니다.
태그 설정		검색필터로 생성된 로그 발생 시 태그를 할당 / 해제할 대상을 설정합니다.

새 검색필터 만들기

1. 상단 메뉴의 **감사 > 로그** 를 클릭합니다.
2. 로그종류, 기간, 검색조건을 입력하여 검색합니다.
3. 저장 버튼을 클릭합니다.
4. **이름** : 검색필터 이름을 입력합니다.
5. **설명** : 검색필터에 대한 설명을 입력합니다.
6. **관심필터** : 체크시 검색필터 트리에 표시됩니다.
7. **출력컬럼** : 검색필터 선택시 표시할 컬럼명을 선택합니다.
8. 생성 버튼을 클릭합니다.

검색필터 수정

1. 상단 항목의 **감사 > 로그** 로 이동합니다.
2. 왼쪽 항목에서 **검색필터** 로 이동합니다.
3. **검색필터 이름** 을 찾아 클릭합니다.
4. 우측 로그뷰 상단 수정 버튼을 클릭합니다.
5. 필요에 따라 항목을 수정합니다.
6. 수정 버튼을 클릭합니다.

검색 필터 삭제

1. 상단 항목의 **감사 > 로그** 로 이동합니다.
2. 왼쪽 항목에서 **검색필터** 로 이동합니다.
3. 메인창에서 삭제 할 **검색필터 이름** 좌측 **체크박스** 를 선택합니다.
4. **작업선택 > 삭제** 를 클릭합니다.
5. 오른쪽 상단의 변경정책적용 버튼을 클릭합니다.
6. 확인 버튼을 클릭합니다.

10.1.6 로그 발생 시 태그 할당

감사로그 발생시 로그를 발생시킨 자산(노드, 장비, 사용자, 무선랜)에 태그를 할당하거나 해제할 수 있습니다. 검색필터를 만들어 검색필터에 포함되는 감사로그 발생시 해당 자산에 태그를 할당하여 별도의 정책에 자동으로 할당하거나 제외할 수 있습니다.

검색필터에 태그 설정

1. 상단 항목의 **감사** 로 이동 하세요.
2. 왼쪽 항목에서 **로그 > 검색필터** 로 이동 하세요.
3. **검색필터 이름** 을 클릭합니다.
4. 아래 **태그** 매뉴에서 **할당** 을 선택합니다.
5. 태그를 할당할 **검색대상** 과 **할당대상** 을 선택합니다.
6. 태그 추가 버튼을 클릭하여 할당 할 태그를 체크하고 설정 버튼을 클릭합니다.
7. 수정 버튼을 클릭합니다.

검색필터에 태그 해제

1. 상단 항목의 **감사** 로 이동 하세요.
2. 왼쪽 항목에서 **로그 > 검색필터** 로 이동 하세요.
3. **검색필터 이름** 을 클릭합니다.
4. 아래 **태그** 매뉴에서 **해제** 을 선택합니다.
5. 태그를 해제할 **검색대상** 과 **할당대상** 을 선택합니다.
6. 태그 추가 버튼을 클릭하여 해제 할 태그를 체크하고 설정 버튼을 클릭합니다.
7. 수정 버튼을 클릭합니다.

10.1.7 태그를 이용한 정책 적용

이 기능의 목적은 특정 로그가 생성되는 대상에 태그를 할당하고 태그를 기반으로 그룹을 생성하여 정책을 적용하는 것입니다.

태그 기능 사용 방법

1. 태그를 생성합니다.
2. 검색필터에 태그 설정 을 이용하여 태그를 지정하기위한 대상을 검색한 후 태그를 지정합니다.
3. 태그 할당을 위한 노드그룹을 생성합니다.
4. 노드그룹을 사용하여 정책을 적용합니다.

태그 생성

노드 태그 할당 방법을 참조 하세요.

검색필터를 통하여 검색 된 대상에 대한 태그 할당

태그를 할당하기 위한 대상에 대한 검색조건은 정확해야합니다.

1. 검색필터에 태그 설정 을 참고하여 검색필터를 생성합니다.
2. 검증
    - 검색필터 조건에 맞는 감사로그를 발생시킵니다.
    - 생성한 검색필터를 선택하여 감사로그를 발생시킨 IP를 클릭합니다.
    - 노드리스트 뷰에서 노드의 IP를 선택합니다.
    - **노드정보** 탭에서 대상에 할당된 태그를 확인합니다.

Note: 태그를 삭제하려면 태그 설정이 아닌 **해제** 를 선택합니다.

태그 할당을 위한 노드 그룹 생성

노드 그룹 조건:

- 항목: 태그
- 조건: 존재하면
- 설정: [태그명]

노드 그룹 관리 를 참조 하세요.

노드그룹을 사용하여 정책 적용

노드 그룹에 대한 제어 정책 생성 을 참조 하세요.

10.1.8 로그설명

Genian ZTNA는 감사로그 포맷 정보를 제공하여 검색필터 설정 및 타 장비와 연동 시 활용 가능합니다.

컬럼정의

컬럼정보	내용	상세내용
시간	로그 발생 시간	로그발생날짜 YYYY-MM-DD , 로그발생시각 HH:MM:SS (ex. 2020-01-01 11:11:11)
종류	로그 생성 종류	ERROR: 에러로그, ANOMALY : 위험로그, WARN : 경고로그, INFO : 정보로그
로그ID	로그 생성 분류 ID	로그 별 대분류
관리장비명	로그 발생 센터와 센서의 IP 혹은 장비명	로그가 발생된 센터와 센서의 IP또는 노드를 관리하는 장비명
IP	로그 발생 노드 IP	로그가 발생된 노드의 IP
MAC	로그 발생 노드 MAC	로그가 발생된 노드의 MAC
사용자ID	로그 발생 사용자 인증 ID	사용자 인증 시 사용자의 ID
사용자명	로그 발생 인증 사용자 명	사용자 인증 시 사용자ID 내 사용자명
부서명	로그 발생 사용자 부서명	사용자 인증 시 사용자ID 내 부서명
설명	로그 발생 시 상세 설명	텍스트 형태 및 각 로그종류마다 KEY=VALUE 형태의 데이터를 가짐
추가정보	로그 발생 시 추가 설명	관리자가 설정한 추가적인 정보

Note:

- 로그ID 컬럼의 상세한 내용은 아래 이벤트 항목 별 로그 *ID* 정의 를 참고하시길 바랍니다.
- 추가정보 컬럼은 **설정 > 환경설정 > 감사기록 > 노드 감사기록 선택 > 추가정보 저장** 항목에서 선택하여 추가 가능합니다.

10.2 발생 로그(이벤트) 보내기

정책서버는 내부적으로 발생한 다양한 로그들에 대하여 관리자 알람 및 외부 솔루션으로 전송이 가능합니다. 다양한 프로토콜을 사용하는 SIEM과 같은 타사 보안 솔루션에 이벤트를 보낼 수 있습니다.

10.2.1 메시지 작성

로그 전송 시 메시지 내용에 매크로 추가

Genian ZTNA는 메시지내용에 미리 정의되어있는 매크로를 사용할 수 있습니다. 사전 정의되어 있는 매크로를 추가하여 사용자가 원하는 형태의 메시지로 전송할 수 있습니다. 로그 알림 메시지 입력란이 공란일 경우 툴팁에 작성된 메시지 기본값 이 전송됩니다.

1. **설정** 으로 이동합니다.
2. 왼쪽 항목의 **설정** 에서 **환경설정 > 감사기록** 으로 이동합니다.
3. **노드 감사기록 선택 - 추가정보 저장** 에서 감사기록 시 추가적으로 남길 정보 항목을 선택합니다. - 노드 및 에이전트 동작상태 이력 저장은 선택 옵션입니다.
4. 상단 항목의 **감사** 로 이동합니다.
5. 왼쪽 항목의 **로그 > 검색필터** 로 이동합니다.
6. **검색필터 이름** 찾아 클릭합니다.

7. **알람전송 > SMS** 옵션을 체크합니다.
8. **SMS 내용** 입력상자에 **매크로** 를 추가합니다.
9. **알람전송** 메뉴 위의 매크로 도움말 물음표 버튼을 찾아 클릭합니다.
10. 원하는 **매크로** 를 선택하여 알람전송 메시지 본문에 추가합니다. (예: 메시지 *{_SWNAME}{SWPORT}* 입니다.)
11. 수정 버튼을 클릭합니다.

메시지 기본값

- 알람전송

```
SMS - [사이트명]{_HEADMSG}: 로그필터이름
Email 제목 - [사이트명]{_HEADMSG}: 로그필터이름
Email 내용 - {_DATETIME} {_LOGTYPE} {_LOGID} {_SENSORNAME} {_IP} {_MAC} {_FULLMSG}
↪{_DETAILMSG}
```

Note: SMS 전송은 라이선스 종류에 따라 월 최대 전송수량에 제한이 있을 수 있습니다.

- SYSLOG 전송

```
Default - {_DATETIME} {_LOGTYPE} {_LOGID} {_SENSORNAME} {_IP} {_MAC} {_FULLMSG} {_
↪DETAILMSG}
CEF - CEF:0|GENIANS|Genian ZTNA|{_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 전송

```
{_DATETIME} {_LOGTYPE} {_LOGID} {_SENSORNAME} {_IP} {_MAC} {_FULLMSG} {_DETAILMSG}
```

- 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}",
```

(continues on next page)

(continued from previous page)

```
"switchname": "{_SWNAME}",
"switchport": "{_SWPORT}",
"detail": "{_DETAILMSG}"
}
```

매크로 포맷 정의

관리자는 사전에 정의되어 있는 매크로를 활용하여 이벤트 전송 시 필요한 정보를 선택하여 전송할 수 있습니다.

매크로 포맷	내용
{_FULLMSG}	로그 메시지 전체 내용
{_HEADMSG}	로그 메시지 머리말
{_TAILMSG}	머리말 이후 데이터 부분 (KEY=VALUE, ...)
{_EXTRAINFO}	추가정보 전체
{_IP}	로그 노드 IP
{_IP_HTML}	로그 노드 IP(하이퍼링크)
{_MAC}	로그 노드 MAC
{_MAC_HTML}	로그 노드 MAC(하이퍼링크)
{_SENSORIP}	로그 센서 IP
{_SENSORNAME}	로그 센서 이름
{_LOGID}	로그ID
{_LOGIDSTR}	로그ID문자열
{_LOGTYPE}	로그 종류
{_DATETIME}	로그 발생 시각 날짜 (2009/11/27 14:22:32)
{_DATETIMETZ}	로그 발생 시각과 TimeZone
{_DETAILMSG}	로그 상세 메시지
{_USERID}	인증 사용자 ID
{_USERNAME}	인증 사용자 이름
{_USERDEPT}	인증 사용자 부서
{_POS}	인증 사용자 직급 (추가정보필요)
{_NNAME}	노드 이름 (추가정보필요)
{_HOSTNAME}	노드 호스트 명 (추가정보필요)
{_PLATFORM}	노드 플랫폼 (추가정보필요)
{_DESC}	노드 설명 (추가정보필요)
{_DOMAIN}	노드 도메인 (추가정보필요)
{_DNSNAME}	노드 DNS 이름 (추가정보필요)
{_SWNAME}	노드 연결 스위치 이름 (추가정보필요)
{_SWPORT}	노드 연결 스위치 포트 (추가정보필요)

Note: 기존 매크로에 **_upper** or **_lower** 를 붙여서 대소문자로 변환을 할 수 있습니다.

10.2.2 로그 전송

여러가지 방법으로 SIEM 솔루션과 같은 외부 솔루션으로 이벤트를 보낼 수 있습니다.

검색필터를 사용하여 전송

새 필터를 생성하거나 기존 필터를 수정하여 이벤트를 보낼 수 있습니다. 다음 문서를 참고하십시오.

- 검색필터 생성
- 검색필터 수정

1. 이벤트 전송 방식을 선택합니다.
   - 알람전송(SMS, Email)
   - SYSLOG
   - SNMP Trap
   - Webhook
2. 항목을 채우고 생성 또는 수정 버튼을 클릭합니다.
3. 필터 수정 이후 생성된 로그에 대해서 이벤트 전송이 시작됩니다.

SYSLOG 연동 예제 (Splunk)

다음과 같은 순서로 Splunk 솔루션과 연동합니다.

1. Splunk 에서 **Settings > Data Inputs** 아래 Local UDP 를 설정합니다.
2. 원하는 **data input port** 를 구성하고 ZTNA 정책서버 IP를 "Only accept connection from" 항목에 입력합니다. (선택 사항)
3. ZTNA의 검색필터에서 SYSLOG 전송을 체크합니다.
4. 다음과 같이 SYSLOG 관련 항목을 입력합니다.
   - **서버주소** : Splunk 서버 IP
   - **프로토콜** : **UDP**
   - **전송포트** : Splunk에서 정의한 포트 (기본포트는 UDP:514)
   - **SYSLOG 메시지** : {_DATETIME},LOGTYPE={_LOGTYPE},LOGID={_LOGID},IP={_IP},MAC={_MAC},MSG={_F DETAIL={_DETAILMSG}
5. 생성 버튼을 클릭합니다.

SNMP Trap 연동 예제

SNMP Trap은 주로 디바이스 간 이벤트 전송에 활용되고, 설정 방법은 다음과 같습니다.

1. ZTNA의 검색필터에서 SNMP Trap 전송을 체크합니다.
2. 다음과 같이 SNMP Trap 관련 항목을 입력합니다.
   - **서버주소** : SNMP Trap 서버 IP
   - **Community** : SNMP Trap 서버에서 정의한 Community

- **SNMP 메시지** : DATETIME={_DATETIME},LOGTYPE={_LOGTYPE},LOGID={_LOGID},IP={_IP},MAC={_MAC} DETAIL={_DETAILMSG}
- **CHARSET** : SNMP Trap 서버에서 정의한 Character Set (UTF-8 / EUC-KR)

3. 생성 버튼을 클릭합니다.

Note: 이메일 알람을 전송하려면 메일서버 설정 및 관리자 메일 설정을 모두 완료해야합니다.

참고 링크: 외부 전송 이메일 서버 설정 , 관리자 계정

10.2.3 Slack 연동 가이드

Note: 본문 중의 incoming webhook 의 경우, Slack의 정식 라이선스 사용자만 사용가능합니다.

이 가이드는 Genian ZTNA와 Slack 연동에 대한 정보를 제공합니다. 여기에는 다음 정보가 포함 됩니다.

연동의 목적

연동을 위한 *Slack* 설정

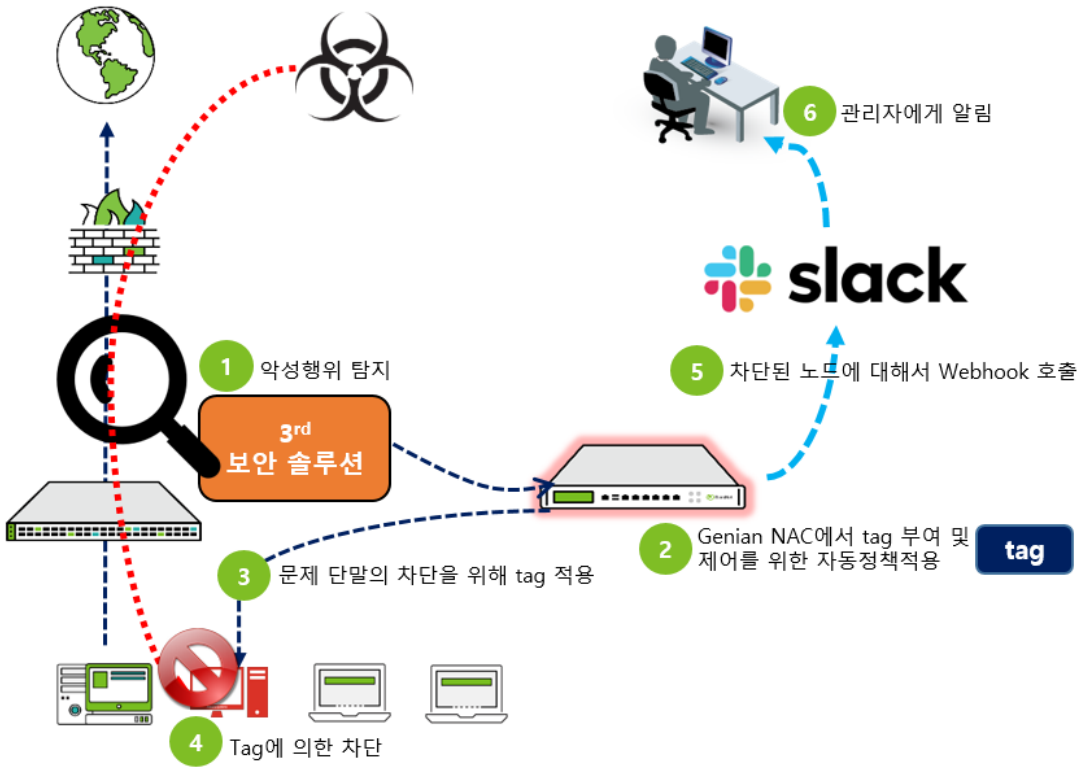
- Slack App(bot) 생성하기
- Slack App 설정 확인

연동을 위한 *Genian ZTNA* 설정

- 검색필터 설정하기
- Webhook 전송 설정하기

가이드 개요

- 이 가이드는 Genian ZTNA와 Slack의 연동설정방법 및 활용예시를 제공합니다.
- Genian ZTNA에서 제공하는 단말의 위협정보, 단말의 정보변경 등의 이벤트 정보를 Slack으로 관리자에게 전송하여, 관리자가 빠르게 인지하고 대응할 수 있도록 도움을 제공합니다.



연동의 목적

Genian ZTNA와 Slack을 연동하여, 다음과 같은 장점 및 효과를 IT관리자와 사용자에게 제공합니다.

- 노드의 모든 정보를 대상으로 하는 Genian ZTNA와 Slack의 시너지 효과
- 네트워크 위협에 대한 신속한 알림
- 노드에서 발생하는 관심정보에 대한 알림정보 제공

연동을 위한 Slack 설정

Slack App(bot) 생성 및 설정하기

https://api.slack.com/apps에 Slack 계정으로 로그인 하신 후, App을 만듭니다.

App의 이름을 정해주고, Slack Workspace를 지정합니다.

- App Name은 Slack에 메시지를 표시하는 Bot의 이름입니다.
- Development Slack Workspace에서 메세지를 전송할 Workspace를 선택합니다. (Slack 계정과 연결된 Workspace 중에서 선택 가능합니다.)

Webhook 전송테스트

정상동작을 확인하기 위해, App 생성과정에서 확인한 Sample Curl을 복사하여, 터미널에서 명령을 적용해 봅니다. (윈도우와 리눅스가 다르므로 주의바랍니다)

- 윈도우 터미널에서 실행 시,

```
curl -X POST -H 'Content-type:application/json' --data "{\"text\
↪":\"Hello, World!\"}" + Webhook URL
```

- 리눅스 터미널에서 실행 시,

```
curl -X POST -H 'Content-type:application/json' --data '{"text":
↪"Hello, World!"}' + webhook URL
```

연동을 위한 Genian ZTNA 설정

검색필터 설정하기

1. Genian ZTNA의 메뉴에서 '감사 > 로그'에서 설정이 가능합니다.
2. 전송할 내용이 포함된 로그에 대해서 검색필터를 설정합니다.
3. 검색필터의 저장 및 전송 설정

- 검색필터의 '저장'을 클릭하여, 필터의 이름을 정해주고, 설명을 추가(생략가능)하고, 전송 방식 중, 'Webhook'을 선택합니다.
- Genian ZTNA는 이벤트 별로 다른 방식으로 메시지 전송이 가능합니다.

Webhook 설정하기

- 검색필터 설정 후, Webhook 호출 옵션을 선택하면 다음의 옵션을 요구합니다.
- Webhook 전송설정 값:

설정 명	설정 값	참고
방식	POST	전송방식 선택
URL 설정	Slack APP의 URL 정보	api.slack.com에서 Features > incoming Webhooks 참고
CHARSET	UTF-8	
POST 데이터	전송할 내용을 설정	아래의 예제 참고
데이터 전송타입	application/x-www-form-urlencoded, application/json 중 선택	전송타입에 POST 데이터 값이 다르므로 주의

- 'application/x-www-form-urlencoded' 선택 시, POST 데이터

```
payload={"channel": "webhook_Alarm_Anthony(App 이름)",
"username": "mkkim(Slack 계정)",
"text": "신규 MAC이 탐지됨.(메시지내용 시작) IP={_IP} MAC={_MAC} HOST={_
↪HOSTNAME} USERNAME={_USERNAME}"
}
```

- 'application/json' 선택 시, POST 데이터

```
{"text":" 신규 MAC이 탐지됨 | IP={_IP} MAC={_MAC}"}
```

- 자세한 설정방법은 장비에서 제공하는 도움말을 활용하시기 바랍니다.

이벤트 전송테스트 하기

- 로그필터에서 설정한 내용이 Slack으로 전송되는지 여부테스트를 진행합니다.

10.3 감사기록 수신

이 옵션은 **설정** 항목의 **환경설정 > 감사기록** 에 있습니다.

Note: SNMP Trap 수신은 On-Premise 에디션만 가능합니다.

10.3.1 SNMP Trap 수신

- **SNMP Trap 수신** 의 **사용여부** 드롭다운 메뉴에서 `On` 또는 `Off` 를 선택하여 사용 또는 사용 안 함을 설정할 수 있습니다.
- 활성화 된 경우, 양식에 `Community` 문자열 을 입력합니다.

10.3.2 Syslog 수신

syslog를 받기 전에 서버 규칙 집합을 추가해야합니다. 다른 수신 기준의 경우 다른 규칙을 구성 할 수 있습니다.

1. **필터** 오른쪽의 **추가** 버튼을 클릭하고 팝업 양식을 작성합니다.
2. 필터 이름을 입력합니다.
3. **필터타입** 의 경우 들어오는 syslog 를 계산 할 변수를 선택합니다. **Program**, **Host**, **Match** 또는 **Netmask** 중에서 선택합니다. 이 옵션을 사용하면 특정 소스 위치 / 프로그램의 syslog 또는 지정된 메시지 내용을 허용 할 수 있습니다.
4. **필터값** 가져온 syslog의 **필터타입** 변수가 **필터값** 과 일치하면 syslog가 정책 서버 로그에 병합됩니다.
5. **IP 키값**, **MAC 키값** 및 **User 키값** 의 접두어를 정의합니다. 이 접두사는 필터가 IP 주소, MAC 주소 및 사용자 이름으로 바로 이어지는 값을 가져 오도록합니다.
6. syslog를 가져올 문자셋을 정의합니다.
7. 팝업 창 하단에서 **추가** 를 클릭합니다.
8. 감사기록 페이지 하단의 **수정** 를 클릭합니다.

가져온 이벤트를 사용하여 정책을 지시하는데 사용할 수있는 노드, 장치, 사용자 및 지문에 태그를 할당 할 수 있습니다.

자세한 내용은 태그를 이용한 정책 적용 을 참조합니다.

10.4 리포트

리포트는 관리자가 쉽게 볼 수 있도록 차트와 표에 원하는 정보를 표시하는 기능입니다. 관리자는 리포트를 사용하여 효율적으로 데이터를 문서화하고 보관하거나, 상급자에게 보고할때 활용할 수 있습니다. 리포트 유형에는 노드 리포트, 로그 리포트, 무선랜 리포트 및 사용자정의 리포트가 있습니다.

10.4.1 리포트 관리

관리자가 원하는 쿼리문(SQL문)에 대한 결과값을 엑셀형식의 리포트로 출력할 수 있습니다. 쿼리 리포트는 쿼리문을 설정하여 리포트를 정의하고, 정의된 리포트에서의 파일생성 작업으로 리포트가 만들어집니다.

쿼리 리포트 생성

1. 상단 패널의 **감사 > 리포트** 로 이동합니다.
2. 좌측 **사용자정의 리포트** 로 이동합니다.
3. **작업선택 > 쿼리리포트 추가** 로 이동합니다.

기본설정

1. **리포트제목** 의 경우 고유 이름을 입력합니다.
2. **리포트설명** 의 경우 이 리포트에 대한 설명을 입력합니다.
3. **적용모드** 에 대해 **사용함** 을 선택합니다.
4. **자동생성** 의 경우, 설정 시간에 실행하려면 **사용함** 을 선택합니다.

세부설정

1. **출력파일** 의 경우, 드롭다운에서 Excel 또는 CSV 를 선택합니다.
2. **메일수신** 의 경우, 관리자의 이메일 주소로 전송이 가능합니다.
3. **수행쿼리** 의 경우, 사용자 지정 쿼리를 추가합니다.
4. **생성** 을 클릭합니다.

예제 쿼리

노드의 열린 포트 정보 조회

```
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
```

동일한 MAC를 사용하는 IP 목록 조회

```
SELECT * FROM (
  SELECT NL_IPSTR, COUNT(NL_MAC) CNT
    from vwNODELIST_VALID
    GROUP BY NL_IP
    ORDER BY NL_IP
       ) A WHERE CNT > 1
```

관리자는 노드리포트를 사용하여 노드 그룹 및 전체 노드에 대한 정보를 표시하고,
작업, 에이전트 설치 및 작업 에이전트 노드 수를 그래프 형식으로 표시합니다.

노드 리포트 생성

1. 상단 패널의 **감사 > 리포트** 로 이동합니다.
2. 좌측 **사용자정의 리포트** 로 이동합니다.
3. **작업선택 > 노드리포트 추가** 로 이동합니다.

기본설정

1. **리포트제목** 의 경우 고유 이름을 입력합니다.
2. **리포트설명** 의 경우 이 리포트에 대한 설명을 입력합니다.
3. **적용모드** 에 대해 **사용함** 을 선택합니다.
4. **자동생성** 의 경우, 설정 시간에 실행하려면 **사용함** 을 선택합니다.

세부설정

Note: **세부설정** 다음 단계를 반복하여 **수집대상** 을 리포트에 추가합니다.

---

1. **수집대상** 의 경우 드롭 다운에서 **전체노드** 또는 **노드그룹** 을 선택합니다.
2. **노드 그룹** 을 선택한 경우 **대상설정** 드롭 다운에서 원하는 그룹을 선택합니다.
3. **항목** 의 경우리포트 대상을 선택합니다.
4. **출력명** 의 경우 기본값을 사용하거나 고유 한 이름을 입력합니다.
5. **설명** 의 경우 설정하는 옵션에 대한 설명을 입력합니다.
6. **차트타입** 의 경우 드롭 다운에서 **선, 막대,** 또는 **면 그래프** 를 선택합니다.
7. **차트색상** 의 경우 드롭 다운에서 원하는 색상을 선택합니다.
8. **감사기록** 의 경우 드롭 다운에서 원하는 기준을 선택합니다.
9. **추가** 를 클릭 한 다음 **생성** 를 클릭합니다.
10. **리포트 정의 > 새로 작성된** 노드리포트 이름** 클릭

차트 탭에서

1. 원하는 **기간** 을 선택하고 **변경** 을 클릭합니다.

테이블 탭 아래

1. 원하는 **기간** 을 선택하고 **변경** 을 클릭합니다.
2. **Excel** 형식으로 보고서를 로컬로 내보내려면 **내보내기** 아이콘을 클릭합니다.

로그 리포트 생성

1. 상단 패널의 **감사 > 리포트** 로 이동합니다.
2. 좌측 **사용자정의 리포트** 로 이동합니다.
3. **작업선택 > 노드리포트 추가** 로 이동합니다.

기본설정

1. **리포트제목** 의 경우 고유 이름을 입력합니다.
2. **리포트설명** 의 경우 이 리포트에 대한 설명을 입력합니다.

3. **적용모드** 에 대해 **사용함** 을 선택합니다.
4. **자동생성** 의 경우, 설정 시간에 실행하려면 **사용함** 을 선택합니다.

세부설정

1. **감사로그필터** 의 경우, 어떤 필터를 적용할지 선택합니다.
2. **출력파일** 의 경우, 출력한 파일의 파일 타입을 선택합니다.
3. **메일수신** 의 경우, 관리자의 이메일 주소로 전송이 가능합니다.

대시보드 리포트 생성

1. 상단 패널의 **감사 > 리포트** 로 이동합니다.
2. 좌측 **사용자정의 리포트** 로 이동합니다.
3. **작업선택 > 대시보드리포트 추가** 로 이동합니다.

기본설정

1. **리포트제목** 의 경우 고유 이름을 입력합니다.
2. **리포트설명** 의 경우 이 리포트에 대한 설명을 입력합니다.
3. **적용모드** 에 대해 **사용함** 을 선택합니다.
4. **자동생성** 의 경우, 설정 시간에 실행하려면 **사용함** 을 선택합니다.

세부설정

1. **대시보드탭** 의 경우, Overview, Anomaly등 대시보드 탭을 설정합니다.
2. **출력파일** 의 경우, 출력한 파일의 파일 타입을 선택합니다.
3. **메일수신** 의 경우, 관리자의 이메일 주소로 전송이 가능합니다.

리포트 내보내기

1. 상단 패널의 **감사 > 리포트** 로 이동합니다.
2. **이메일 발송** 으로 이동하여 원하는 **리포트 이름** 을 클릭합니다.
3. **작업선택 > 즉시수행** (파일을 클릭하여) 하여 리포트를 메일로 발송할 수 있습니다.

리포트를 삭제하는 방법

1. 상단 패널의 **감사 > 리포트** 로 이동합니다.
2. 기본 창에서 **삭제할 리포트 이름** 을 찾아 **체크 상자** 를 클릭합니다.
3. **작업선택 > 삭제** 를 클릭합니다.

10.4.2 노드 리포트 확인하기

노드 리포트는 노드그룹으로 포함된 대상 갯수에 추이 정보를 비교할 경우 사용됩니다. 노드그룹 생성 시 자동으로 노드 리포트 항목으로 포함되며 4가지 값과 3가지 변동폭을 데이터로 제공합니다.

Note: 노드그룹 생성은 노드 그룹 관리 참고하시기 바랍니다.

노드 리포트 제공되는 값

항목	설명
오늘	오늘 날짜를 기준으로 노드그룹에 포함된 노드수를 표시합니다.
전일	어제 날짜를 기준으로 노드그룹에 포함된 노드수를 표시합니다.
전주	오늘 날짜를 기준으로 이전 주에 노드그룹에 포함된 노드수를 표시합니다.
전월	오늘 날짜를 기준으로 이전 월에 노드그룹에 포함된 노드수를 표시합니다.
변 동 폭 (전 일 비)	오늘과 어제에 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변 동 폭 (전 주 비)	오늘과 이전 주에 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변 동 폭 (전 월 비)	오늘과 이전 월에 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변동 그래프	오늘 기준으로 한달간 노드그룹에 포함된 노드수의 변동폭을 선 그래프로 표시합니다.

10.4.3 로그 리포트 확인하기

로그 리포트는 로그 검색 시 생성된 검색필터의 추이 정보를 비교할 경우 사용됩니다.

검색 필터 생성 시 자동으로 로그 리포트 항목으로 포함되며 4가지 값과 3가지 변동폭을 데이터로 제공합니다.

에러, 경고, 위험에 관련한 로그 리포트는 기본으로 생성되어 있습니다.

Note: 검색 필터 생성은 검색필터 생성 참고하시기 바랍니다.

로그 리포트 제공되는 값

항목	설명
오늘	오늘 날짜를 기준으로 검색필터에 포함된 로그수를 표시합니다.
전일	어제 날짜를 기준으로 검색필터에 포함된 로그수를 표시합니다.
전주	오늘 날짜를 기준으로 이전 주에 검색필터에 포함된 로그수를 표시합니다.
전월	오늘 날짜를 기준으로 이전 월에 검색필터에 포함된 로그수를 표시합니다.
변 동 폭 (전 일 비)	오늘과 어제에 검색필터에 포함된 로그수의 변동폭을 표시합니다.
변 동 폭 (전 주 비)	오늘과 이전 주에 검색필터에 포함된 로그수의 변동폭을 표시합니다.
변 동 폭 (전 월 비)	오늘과 이전 월에 검색필터에 포함된 로그수의 변동폭을 표시합니다.
변동 그래프	오늘 기준으로 한달간 검색필터에 포함된 로그수의 변동폭을 선 그래프로 표시합니다.

10.4.4 이메일을 사용하여 리포트 전송하기

리포트 기능을 사용하여 생성된 리포트를 이메일을 사용하여 관리자에게 전달할 수 있습니다.

전송된 리포트를 기반으로 네트워크 현황에 대한 일일보고 및 Genian ZTNA 장비의 현황보고의 용도로 활용할 수 있습니다.

1. 상단 패널에 **감사> 리포트** 로 이동합니다.
2. 왼쪽 **이메일 발송** 항목을 선택합니다.
3. **작업선택** 메뉴에서 **생성** 을 선택합니다.
4. **이메일 발송 정의** 항목을 설정한 후 **생성** 을 클릭합니다.

Note: 이메일로 리포트를 전송하기 위해서는 외부 전송 이메일 서버 설정 설정이 필요합니다.

리포트 종류 선택하기

이메일로 전송할 리포트에 대해서 2가지로 정의된 타입을 지정할 수 있습니다. 각각 타입은 다음과 같습니다.

타입	설명
간편리포트	노드, 장비, 무선랜, 로그(에러, 경보, 위험)에 대한 신규 추가 갯수를 이메일로 제공합니다.
상세리포트	간편리포트에서 생성된 항목 및 리포트(노드리포트, 로그리포트, 무선랜리포트, 사용자 정의리포트) 중 관리자가 선택한 항목을 포함하여 이메일로 제공합니다.

10.4.5 무선랜 리포트 확인하기

무선랜 리포트는 무선랜 노드그룹으로 포함된 대상 갯수에 추이 정보를 비교할 경우 사용됩니다.

무선랜 노드그룹 생성 시 옵션에 따라서 리포트로 생성되며 4가지 값과 3가지 변동폭을 데이터로 제공합니다.

Note: 무선랜 노드그룹 생성은 무선 그룹 생성 참고하시기 바랍니다.

무선랜 리포트 제공되는 값

항목	설명
오늘	오늘 날짜를 기준으로 무선랜 노드그룹에 포함된 노드수를 표시합니다.
전일	어제 날짜를 기준으로 무선랜 노드그룹에 포함된 노드수를 표시합니다.
전주	오늘 날짜를 기준으로 이전 주에 무선랜 노드그룹에 포함된 노드수를 표시합니다.
전월	오늘 날짜를 기준으로 이전 월에 무선랜 노드그룹에 포함된 노드수를 표시합니다.
변 동 폭 (전 일 비)	오늘과 어제에 무선랜 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변 동 폭 (전 주 비)	오늘과 이전 주에 무선랜 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변 동 폭 (전 월 비)	오늘과 이전 월에 무선랜 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변동 그래프	오늘 기준으로 한달간 무선랜 노드그룹에 포함된 노드수의 변동폭을 선 그래프로 표시합니다.

10.4.6 사용자 정의 리포트 확인하기

사용자 정의 리포트는 4가지 항목(쿼리, 노드, 로그, 대시보드)에 대한 리포트를 임의로 생성하여 확인할 수 있습니다.

1. 노드리포트 확인하기

기존 노드그룹 생성 시 자동으로 생성되는 노드리포트와 다르게 다음에 4가지 조건을 추가하여 노드리포트를 생성할 수 있습니다.

추가조건	설명
전체 노드수	노드그룹에 포함되는 전체 노드수에 대한 리포트로 생성합니다.(노드리포트와 같은 정보)
동작 노드수	노드그룹에 포함되는 노드 중 동작상태가 UP인 노드수에 대한 리포트를 생성합니다.
에이전트 설치 노드수	노드그룹에 포함되는 노드 중 에이전트가 설치된 노드수에 대한 리포트를 생성합니다.
동작 에이전트 노드수	노드그룹에 포함되는 노드 중 동작상태가 UP인 에이전트 설치된 노드수에 대한 리포트를 생성합니다.

2. 대시보드 리포트 확인하기

대시보드 탭별로 PDF, Word, PPT 파일로 리포트를 제공합니다.

- 리포트 제목 표시 여부를 설정할 수 있습니다.
- 용지 크기를 설정할 수 있습니다.
  - A4,A3,A2,B4,B3,B2,LETTER 사이즈를 PORTRAIT/LANDSCAPE 별로 선택할 수 있습니다.
  - Custom 가로, 세로 크기 설정을 통해 대시보드에 출력되는 모든 위젯을 한 페이지로 출력할 수 있습니다.

3. 로그 리포트 확인하기

기존 생성된 로그 필터를 기반으로 엑셀(xlsx)과 CSV(comma-separated values) 파일로 리포트를 제공합니다.

4. 쿼리 리포트 확인하기

데이터베이스에 쿼리(SQL)를 수행한 결과값에 대해서 엑셀(xlsx, xls)과 CSV(comma-separated values) 파일로 리포트를 제공합니다.

Note:

1. 쿼리 리포트에 수행되는 계정은 root 가 아닌 별도의 리포트 계정을 사용하여 권한이 제한됩니다.
2. 쿼리를 수행할 수 있는 테이블 정보는 다음에 cusotm-query-table 참고하시기 바랍니다.

10.5 감사기록 추가 정보 수집하기

추가 정보를 감사로그에 추가하여 남기거나, 노드/에이전트의 동작상태 이력을 별도의 감사로그로 남기도록 설정할 수 있습니다.

추가 정보 항목	설명
노드이름	노드 세부사항 중 노드명으로 입력된 항목값 표시
노드설명	노드 세부사항 중 설명으로 입력된 항목값 표시
호스트명	노드 세부사항 중 호스트명으로 지정된 항목값 표시
도메인	노드 세부사항 중 도메인으로 지정된 항목값 표시
DNS 이름	노드 세부사항 중 DNS 이름으로 지정된 항목값 표시
플랫폼	노드 세부사항 중 플랫폼으로 지정된 항목값 표시
인증 사용자 직급	노드에 인증된 사용자의 직급 표시
연결 스위치 이름	네트워크에 연결된 스위치 이름 표시
연결 스위치 포트	네트워크에 연결된 스위치 포트 표시
센서 그룹명	노드를 관리하는 네트워크 센서 이름 표시

10.5.1 추가정보 감사로그에 설정하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **환경설정** 항목에 **감사기록** 을 선택합니다.
3. **추가정보** 로 지정할 항목들에 **체크박스** 를 클릭합니다.
4. **수정** 버튼을 클릭합니다.

10.5.2 동작상태 감사로그 추가하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **환경설정** 항목에 **감사기록** 을 선택합니다.
3. **노드 동작상태 이력 저장** 항목에 설정값을 **ON** 으로 변경합니다.
4. **에이전트 동작상태 이력 저장** 항목에 설정값을 **ON** 으로 변경합니다.
5. **수정** 버튼을 클릭합니다.

CHAPTER

ELEVEN

시스템관리

Genian ZTNA 장비(정책서버, 네트워크센서) 및 서비스, 백업/복원, 관리자 콘솔, 관리자 역할의 환경설정을 확인할 수 있습니다.

11.1 사이트 관리

SASE 구성을 설정하기 위한 관리 페이지 입니다. 사이트 관리를 통해 Cloud에 Service Edge(ZTNA Gateway, Hub)를 만들고 Service Edge에 연결할 Branch를 구성 할 수 있습니다.

11.1.1 사이트 타입

사이트는 **Hub 타입** 과 **Branch 타입** 으로 생성할 수 있습니다.

Hub 타입

Hub 타입의 사이트는 Branch 타입의 사이트와의 **IPsec 터널** 을 중계하는 역할과, 네트워크 접속지점의 역할을 합니다.

- Hub 사이트가 여러개인 경우, Hub 사이트 간 터널 구성을 설정할 수 있습니다.

Branch 타입

Branch 타입은 Branch 사이트 네트워크에 대한 통신만을 라우팅 합니다.

- Parent Hub 사이트 선택시 Hub로 IPsec 터널 구성을 설정할 수 있습니다.

사이트 연결 방식

- ZTNA Gateway에 IPsec을 구동하여 Hub와 연결할 수 있습니다.
- IPsec 전용 장비와(Cisco, Fortinet 등) ZTNA의 Hub 사이트 간 연동이 가능합니다.
- Hub와 Brnach가 직접 라우팅이 가능한 경우 라우팅을 통해 Hub와 연결할 수 있습니다.

11.1.2 사이트 설정 방법

1. **시스템 -> 사이트** 를 클릭
2. **작업선택 -> 생성** 클릭
3. 기본 정보 입력
   - 사용할 **사이트명** 입력
   - 타입 설정(Hub, Branch)
   - **인프라를 설정(Cloud, On-Premises)**
     - **Cloud일 경우 Cloud Provider** , **Region** , **VPC ID** 를 설정해야 합니다.
     - 생성된 Cloud Provider로 설정 합니다. 생성된 Cloud Provider가 없다면 *Cloud Provider 생성 방법* 을 참조하여 생성 합니다.
     - 지역에 맞는 **Region** 을 설정 합니다.
     - 사이트를 구성할 **VPC ID** 를 선택합니다. **VPC ID** 선택 시 , **Network Address** 는 해당 VPC 대역으로 자동 설정 됩니다.
     - **On-premises** 일 경우 생성할 사이트의 IP 대역을 **Network Address** 에서 설정 합니다.
   - 사이트 별 사용할 옵션을 선택 합니다. [**ZTNA-IPsec, ZTNA-Client, Routing, Collector, URL Filter**]

11.1.3 사이트 옵션

사이트 옵션은 **ZTNA-Cient, ZTNA-IPsec , Routing , Collector, URL Filter** 가 있습니다.

ZTNA-Client

ZTNA-Client는 원격지에서 Hub로 설정된 사이트에 VPN으로 접근할 수 있는 옵션입니다. 에이전트를 설치하지 못하는 환경일 경우 OpenVPN 클라이언트를 사용하여 접근할 수 있습니다.

ZTNA-Client 설정 방법

ZTNA-Client 설정 진행전 *Cloud Provider* 설정과 사이트 설정 을 진행해야 합니다.

1. **ZTNA-Client 적용 모드를 사용함** 으로 변경 후 세부설정을 진행합니다.

기능 이름	설명
할당 센서	ZTNA-Client를 구동할 센서를 선택합니다.
클라이언트 할당 네트워크	클라이언트에게 할당 할 DHCP Pool 대역을 설정합니다.
Acess Netwrok	클라이언트에 대한 ACL을 설정합니다.
아이피 고정	On 설정시 사용자의 아이피를 고정합니다.
Isolation	On 설정시 Client 사용자 간의 통신을 차단합니다.
OpenVPN 호환	On 설정시 Agent가 없는 환경에서 OpenVPN클라이언트를 사용하여 접근할 수 있습니다.
서버 도메인	클라이언트가 연결할 도메인을 설정해 줍니다.

Note: ZTNA-Client 적용 모드를 사용함으로 변경시 ZTNA 센서에 TAP 인터페이스가 생성되며, TAP 인터페이스를 통해 Client IP가 DHCP로 설정됩니다.

2. **노드정책 - 노드액션** 에 **ZTNA 연결관리자** 를 추가 합니다.

3. **ZTNA 연결관리자** 노드액션 설정에서 **할당** 을 클릭 후 앞서 생성한 사이트를 추가합니다.

4. 설정 - 서비스 - RADIUS 서버 - RADIUS Secret - 클라이언트 설정에서 추가를 클릭 후 세부 설정을 진행합니다.

5. 시스템 - 센서관리 - 센서 클릭 - 센서설정 - 사용하는 센서의 인터페이스(**기존 인터페이스, 생성된 TAP 인터페이스**)의 센서 설정 클릭 - **센서 동작모드 Inline, 센서 운용모드 Enforcement** 로 수정

6. 에이전트를 설치합니다. [https://정책서버 IP/agent]

7. 에이전트 우클릭 - **Netwrok Access** - 설정한 **사이트** 이름 클릭

8. 사용자 정보 입력 후 **연결** 클릭

ZTNA-Client 세션 확인방법

에이전트 또는 OpenVPN클라이언트를 통해 사이트에 연결이 되면, 웹 콘솔에서 각 사이트에 접근한 세션을 확인할 수 있습니다.

- **시스템 - 사이트** 클릭 , 웹 콘솔에 출력되는 화면에서 ZTNA-Client 탭에 있는 숫자를 클릭하면 해당 사이트에 연결된 세션을 확인할 수 있습니다.
- 해당 **ZTNA Client Sessions** 화면에서는 접속한 **사용자의 ID, 허브명 , 장비명, 사용자 IP, 할당 IP, 패킷량 및 패킷 수, 생성 시간, 마지막 통신 시간** 을 확인할 수 있습니다.

ZTNA-IPsec

ZTNA-IPsec은 다른 네트워크 지점(On-prem,Cloud)에서 ZTNA-Gateway를 통해 인터넷에 접근할 수 있도록, ZTNA-Gateway와 다른 네트워크 지점을 터널링 해주는 옵션입니다.

ZTNA-IPsec 설정 방법

ZTNA-IPsec을 사용하기 위해서는 사전에 *Cloud Provider* 설정과 *Hub* 타입의 사이트 설정 이 필요합니다.

1. 시스템 -> 사이트 -> 생성한 **Hub타입 사이트** 클릭 후, ZTNA-IPsec 적용모드를 **사용함** 으로 변경합니다.

2. **Pre-Shared Key** 값과 **Advance** 설정을 진행합니다.

Warning: 타 사의 VPN 전용장비와 IPsec 터널링을 구성하기 위해서는, **Pre-Shared Key** 값과 **Advance** 옵션이 동일해야 합니다.

항목	항목 설명	비고
Pre-Shared Key	Hub와 Branch간 연결을 위해 사전에 공유 하는 비밀키	
IKE Version	IPsec 연결시 사용할 IKE 버전	IkEv1 , IKEv2 지원
IKE encryption	인증 정보를 암호화할 알고리즘	AES-128, AES-256, blowfish-128, blowfish-192, blowfish-256, Twofish-128, Twofish-192, Twofish-256 지원
IKE integrity	무결성 보장을 위한 암호화 알고리즘	SHA1, SHA2-256, SHA2-384, SHA2-512 지원
Pseudo random function	임의성 제공을 위한 암호화 알고리즘	None, SHA1, SHA2-256, SHA2-384, SHA2-512 지원
IKE DH group	인증 정보를 암호화할 키를 생성하는 대칭키 교환 알고리즘	Off, DH group(5,14,15,16,17,18) 지원
IKE Lifetime	새로운 키를 생성하는 주기	
ESP encryption	데이터 패킷을 암호화하는 알고리즘	AES-128, AES-256, blowfish-128, blowfish-192, blowfish-256, Twofish-128, Twofish-192, Twofish-256 지원
ESP intergrity	무결성 보장을 위한 암호화 알고리즘	SHA1, SHA2-256, SHA2-384, SHA2-512 지원
ESP DH group	데이터 패킷을 암호화할 키를 생성하는 암호화 알고리즘	Off, DH group(5,14,15,16,17,18) 지원
Lifetime	터널 유지 시간	

3. 시스템 -> 사이트 -> 작업선택 -> 생성 클릭 후, **Branch 타입의 사이트** 를 생성 합니다.

- **사이트명** : 사이트 명으로 사용할 이름을 입력합니다.
- **타입** : IPsec 연결을 진행할 Hub사이트를 선택합니다.
- **인프라** : 연결할 장비의 구성 환경을 선택합니다.(Cloud, On-prem).Cloud 선택 시, Cloud Provider, Region, VPC ID를 같이 설정합니다.
- **Network Address** : 사용하는 네트워크 대역을 입력합니다. Cloud일 경우 설정한 VPC 대역을 입력합니다.

4. **ZTNA-IPsec 적용모드를 사용함** 으로 변경 후 , 세부 설정을 진행 합니다.

- **Public IP** : VPN 장비의 공인 IP를 입력합니다.
- **Pre-Shared Key** : Hub사이트에 설정한 Pre-Shared Key를 입력합니다.
- **Networks** : VPN 장비의 subnet을 입력합니다.
- **할당센서** : Brnach사이트의 VPN을 구동할 센서를 선택합니다. VPN 장비를 사용할 경우 선택하지 않습니다.

5. 설정 완료 후 , 시스템 -> 사이트 -> **생성한 Hub 또는 Brach 사이트 -> 상단 탭 ZTNA IPsec Status** 클릭 -> IPsec 터널이 정상적으로 연결되었는지 확인 합니다.

Collector

Genian ZTNA Cloud Collector는 클라우드 환경에서 노드정보를 수집하여, 사용자에게 클라우드에 대한 가시성을 제공합니다.

설정된 수행주기로 Cloud Collector는 Cloud Service Provider에게 쿼리하여 노드의 정보 및 클라우드 관련 세부정보를 수집합니다.

Collector 설정 방법

Genian ZTNA Collector 옵션을 활성화를 위해서는, *Cloud Provider설정* 과 사이트 설정 설정이 필요합니다.

1. 사이트 설정 후, 하단의 Collector 옵션의 **적용모드를 사용함** 으로 변경 합니다.

2. **Proxy HostName**, **Proxy Port** 는 설정하지 않습니다.

3. 시스템 - 센서관리로 이동합니다. 생성한 사이트명으로 Cloud 센서가 생성되었는지 확인합니다.

4. Cloud 센서가 생성 되었으면 , **관리 - 노드** 를 통해 Cloud센서가 정상적으로 Hub 사이트의 VPC 대역 인스턴스를 등록했는지 확인합니다.

5. Collector가 수집한 정보는 Cloud 센서가 등록한 노드를 클릭하여 확인할 수 있습니다.

11.2 시스템 종료 및 재시작

11.2.1 웹 콘솔을 통한 전원 제어

1. 메뉴 표시 줄에서 **시스템** 을 클릭하십시오.
2. 시스템 목록에서 정책서버 또는 네트워크센서의 IP주소를 클릭하십시오.
3. **제어** 탭을 클릭하십시오.
4. **재기동** 또는 **셧다운** 을 클릭 하십시오.

11.2.2 CLI (Command Line Interface)를 통한 전원 제어

참조: *CLI(Command Line Interface)*

1. SSH 프로토콜을 통하여 **정책서버** 또는 **네트워크센서** 에 연결하십시오.
2. **enable** 모드로 전환하십시오.
3. 예:
   - 시스템 종료 : **shutdown service** 또는 **halt** 명령 입력
   - 시스템 재시작 : **shutdown** 또는 **reboot** 명령 입력

> **Warning:** 시스템을 정상 종료하기 전에는 전원케이블을 강제로 제거하거나 수동으로 전원을 끄지 마십시오.

11.3 관리자 관리

관리자는 역할에 따라 다음과 같은 권한을 가지고 있습니다.

- **superAdmin** : 모든 권한을 가진 최고 관리자
- **ipAppManager** : IP주소 사용 신청에 대한 승인 권한을 가진 관리자
- **Auditor** : 감사 기록(로그 및 이벤트) 조회 권한을 가지 관리자

Note: 관리자 권한을 부여하려면 계정을 생성하고, 각 계정에 알맞는 관리자 권한을 할당하시기 바랍니다.

11.3.1 관리자 계정

수퍼관리자(SuperAdmin)의 업무분담을 위해 하위 관리자 계정을 생성할 수 있으며, 생성된 관리자 계정은 업무 역할에 따라 권한을 제어하여 사용할 수 있습니다.

권한 ID	권한명	설명
auditor	감사관리자	Web콘솔 전체메뉴에 대한 읽기권한
ipAppManager	IP신청페이지 관리자	웹콘솔 접속 불가, IP신청페이지에 관리자로 접속가능
ipManager	IP 사용 관리를 위한 관리자	IP 신청에 대한 승인 처리를 수행하는 역할(Web콘솔 IP신청메뉴만 접근)
logAuditor	감사로그 관리자	Web콘솔 감사메뉴만 접근이 가능한 역할
mediaManager	장치사용신청 관리자	Web콘솔 장치사용신청서 메뉴만 접근가능한 역할
nodeAuditor	노드 감사 관리자	Web콘솔 노드관리 메뉴와 감사메뉴만 접근 가능한 역할
superAdmin	수퍼 관리자	Web 콘솔 전체권한 보유 역할
userManager	사용자계정 관리자	Web콘솔 관리 사용자 메뉴만 접근가능한 역할

Note: superadmin 관리역할은 전체 관리자 계정 중 한 계정에만 할당할 수 있습니다.

관리자 추가

1. 상단 패널에서 **관리 > 사용자** 로 이동합니다.
2. **작업선택 > 사용자 등록** 를 클릭합니다.

기본설정

1. **사용자ID** 에 사용자ID를 입력합니다.
2. **사용자이름** 에 이름을 입력합니다.
3. **관리역할** 에 관리자 역할 선택합니다.
4. 계정에 대한 설명이 필요한 경우 **설명** 의 경우 설명을 입력합니다.
5. 사용자 **용도** 의 경우 **선택안함** 을 선택합니다.
6. 사용자 **상태** 의 경우 **정상** 을 선택합니다. (일시적으로 계정을 사용 중지하려면 **사용 중지** 를 선택합니다.)
7. **계정사용만료** 의 경우 체크박스를 클릭하여 날짜와 시간을 선택합니다.

8. **태그** 의 경우 **추가** 를 클릭하여 이 계정에 태그를 추가하도록 선택할 수 있습니다.

비밀번호 설정

1. **비밀번호** 에 비밀번호를 입력합니다.
2. **비밀번호 확인** 에 비밀번호 재입력합니다.

인증제한 설정

1. 상단 패널에서 **관리 > 사용자** 로 이동합니다.
2. **사용자ID** 를 클릭합니다.
3. **IP 인증제한** 의 경우 이 계정에서 사용할 수 있는 인증IP 개수를 지정할 수 있습니다. (최대 256개 설정, 0 입력시 제한설정 안함)
4. **MAC 인증제한** 의 경우 이 계정에서 사용할 수 있는 MAC주소 개수를 지정할 수 있습니다. (최대 256개 설정, 0 입력시 제한설정 안함)
5. **장비 인증제한** 의 경우 이 계정에서 사용할 수 있는 장비 수를 지정할 수 있습니다. (최대 256개 설정, 0 입력시 제한설정 안함)
6. **인증허용 IP** 의 경우 **,** (쉼표) 구분하여 IP 주소를 지정할 수 있습니다. (공란 시 제한설정 안함)
7. **인증허용 MAC** 의 경우 **,** (쉼표) 로 구분하여 MAC 주소를 지정할 수 있습니다. (공란 시 제한설정 안함)
8. **인증제한 예외노드그룹** 의 경우 인증제한이 적용하지 않을 그룹을 할당 할 수 있습니다. **할당** 을 클릭하여 예외노드그룹을 지정합니다.

로그인 설정

1. 관리WEBUI 접속 IP / MAC 을 추가합니다. (공란 시 제한설정 안함)
2. 사용할 2단계 인증을 선택합니다. SMS 인증, OTP 인증, 선택안함을 선택할 수 있습니다.
3. 타임 존을 선택합니다. (*Asia / Seoul(GMT +09:00)*

알람정보 설정

1. **알람수신설정** 에서 **사용자등록 IP신청 장치신청** 에 대한 알람 수신여부를 선택합니다. 선택한 항목의 신규 이벤트 발생 알람을 수신할 수 있습니다.
2. **SMS수신번호** 는 알람을 받은 **휴대폰 번호** 를 설정합니다.
3. **발신번호** 는 SMS에 표시할 발신번호를 입력합니다.
4. **이메일** 은 알람을 수신받을 이메일을 입력합니다.

관리제한 설정

관리제한 설정은 관리자 계정의 권한을 제한하여 사용 할 때 설정하는 항목입니다.

- 관리자 계정의 관리 범위와 설정을 제한할 수 있습니다.

1. **노드 관리범위 제한** : 노드그룹, 네트워크센서, 노드타입을 지정하여 관리범위를 제한
2. **노드 관리명령 제한** : 노드관리 화면에서 수행 할 수 있는 작업의 종류를 제한
3. **노드 관리뷰 제한** : 노드관리 화면에서 선택가능한 뷰의 형태를 제한
4. **노드 상세보기 제한** : 노드의 세부 정보에 탭을 제한
5. **사용자 관리범위 제한** : 사용자가 포함된 부서를 지정하여 사용자관리 범위를 제한
6. **사용자 관리명령 제한** : 사용자관리 화면에서 수행할 수 있는 작업의 종류를 제한
7. **감사로그 검색범위 제한** : 감사메뉴에서 사용 가능한 검색필터를 제한
8. **파일 내보내기 제한** : 파일(Excel) 내보내기 기능을 제한
9. **대시보드 위젯 제한** : 대시보드 위젯 기능을 제한

신뢰연결 설정

신뢰하는 Client만이 외부에서 정책서버로 Web서비스(Genian API, REST API)를 호출할 수 있도록 정보를 설정할 수 있습니다.

1. **IP 패턴** : 웹서비스 호출이 가능한 신뢰하는 Client IP 패턴을 설정합니다.
2. **URL 패턴** : 웹서비스 호출이 가능한 신뢰하는 URL 패턴을 설정합니다.

추가정보 설정

1. **조직명** 에 조직명을 입력합니다.
2. **부서명** 는 검색을 클릭하여 부서를 선택합니다. (부서 생성방법 : 사용자 > 부서 > 작업 > 만들기)
3. **직급** 은 목록에서 직급을 선택합니다. (직급 생성 방법 : 사용자 > 직급관리 > 작업 > 생성)
4. **전화번호** 에 전화번호를 입력합니다. (*e.g. 123-456-7890, or 1234567890*)
5. **휴대폰** 에 휴대폰 번호를 입력합니다. (*e.g. 123-456-7890, or 1234567890*)
6. **전자우편** 에 이메일 주소를 입력합니다.

Note:

전자우편 항목의 이메일주소로 **아이디/비밀번호찾기 인증메일, IP사용신청서/사용자계정/장치신청/사용자변경 승인신청서 메일, 노드대상명령의 이메일전송 메일** 을 수신받을 수 있습니다.

관리자 제거

1. 상단 패널에서 **관리 > 사용자** 로 이동합니다.
2. 삭제할 사용자를 확인하여 **체크박스** 를 선택합니다.
3. **작업선택** 에서 **사용자삭제** 를 선택합니다.
4. **확인** 을 클릭합니다.

11.3.2 2단계 인증

SMS, Google OTP 를 활용한 2단계 인증

SMS

Genian ZTNA는 SMS를 활용하여 관리자 계정 로그인에 대한 2단계 인증을 수행할 수 있습니다.

1 단계. 관리자 계정의 2 단계 인증 사용

1. 상단 패널에서 **관리 > 사용자** 로 이동하십시오.
2. 왼쪽 사용자 관리 패널에서 **전체관리자** 로 이동하십시오.
3. 2단계 인증을 적용할 **사용자ID** 를 찾아 클릭하십시오.
4. **로그인 설정** 에서 **2단계 인증** 을 **SMS** 로 설정하십시오.
5. **알람정보 설정** 에서 다음을 입력하십시오.
   - **SMS수신번호** (*KR* 예: *010-1234-5678*)
   - **발신번호** (*KR* 예: *010-1234-5678*)
6. **수정** 를 클릭하십시오.

Note: 관리자 계정의 2단계 인증을 적용하기 위해서는 정책서버의 2단계 인증 설정도 완료해야합니다.

2단계. 정책서버 2단계 인증 사용

1. 상단 패널의 **설정** 로 이동하십시오.
2. 왼쪽 환경설정 패널에서 **관리콘솔** 로 이동하십시오.
3. **WEB 콘솔에서 2단계 인증 기능활성화** 를 찾습니다.
4. **SMS 체크 박스** 를 클릭하십시오.
5. **수정** 을 클릭하십시오.

3 단계. SMS 인증코드를 활용한 2단계 인증

1. 정책서버 Web UI에서 로그아웃하고 2단계 인증을 설정한 관리자 계정으로 다시 로그인합니다.
2. SMS 2단계 인증을 위한 **SMS 인증코드 입력 창** 이 나타납니다.
3. SMS수신번호로 설정한 스마트폰에 수신된 인증코드 **6 자리 숫자** 를 **인증코드** 입력란에 입력하십시오.
4. **입력** 을 클릭하십시오.

Google OTP

Genian ZTNA는 Google OTP를 설치하여 관리자 계정 로그인에 대한 2단계 인증을 수행할 수 있습니다.

1 단계. 관리자 계정의 2 단계 인증 사용

1. 상단 패널에서 **관리 > 사용자** 로 이동하십시오.
2. 왼쪽 사용자 관리 패널에서 **전체관리자** 로 이동하십시오.
3. 2단계 인증을 적용할 **사용자ID** 를 찾아 클릭하십시오.
4. **로그인 설정** 에서 **2단계 인증** 을 **OTP (Google Authenticator)** 로 설정하십시오.
5. **OTP (Google OTP)** 를 클릭하십시오.
6. **알람정보 설정** 에서 다음을 입력하십시오.
   - **SMS수신번호** (예: *KR +82-010-1234-5678*)
   - **이메일** (쉼표로 구분 하여 여러 개의 이메일 주소를 입력할 수 있습니다.)
7. **수정** 를 클릭하십시오.

Note: 관리자 계정의 2단계 인증을 적용하기 위해서는 정책서버의 2단계 인증 설정도 완료해야합니다.

2단계. 정책서버 2단계 인증 사용

1. 상단 패널의 **설정** 로 이동하십시오.
2. 왼쪽 환경설정 패널에서 **관리콘솔** 로 이동하십시오.
3. **WEB 콘솔에서 2단계 인증 기능활성화** 를 찾습니다.
4. **OTP (Google Authenticator) 체크 박스** 를 클릭하십시오.
5. **수정** 을 클릭하십시오.

3 단계. Google OTP 설정

1. 정책서버 Web UI에서 로그아웃하고 2단계 인증을 설정한 관리자 계정으로 다시 로그인합니다.
2. Google OTP를 설정하기위한 2 단계 인증 마법사가 나타납니다.
3. **설정시작** 을 클릭하십시오.
4. **스마트폰의 앱 스토어 에서 Google OTP** 를 설치하십시오.
5. **다음** 을 클릭합니다.
6. **보안키 전송방법** 의 **QR-Code** 를 선택하고 **보안키 생성** 을 클릭하십시오.
7. **스마트폰** 으로 생성된 **QR 코드** 를 스캔합니다.
8. **Google OTP** 앱에 생성된 **6 자리 숫자** 를 **인증코드** 에 입력하십시오.
9. **입력** 을 클릭하십시오.

외부 OTP 연동을 활용한 2단계 인증

외부 OTP 서버

본 가이드는 외부 OTP 서버와 네트워크 접근제어 시스템인 Genian ZTNA의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

본 연동은 관리자 계정에 대해서 2-Factor 인증을 위한 연동으로 Genian ZTNA 관리자 계정에 대해서 보다 안전한 로그인 과정을 수행하기 위해, 2-Factor 인증을 구현하기 위하여, **관리자는 Genian ZTNA 관리자 페이지에 로그인 시 ID/PW 방식의 Genian ZTNA 관리자 계정으로 로그인 이후, 추가적으로 외부 OTP 서버와의 연동을 통해서 인증을 거치도록 연동됩니다.**

연동의 구성은 관리자가 Genian ZTNA 인증처리와 함께, API 호출을 통해서 OTP 서버에서 관리자의 모바일 단말로 OTP(One Time Password)를 발행하도록 요청하며, 발행된 OTP정보를 확인 후 관리자 로그인을 실행하는 경우 OTP 서버로 입력된 OTP정보에 대한 검증을 요청하고 결과에 따라서 2-Factor 인증을 하게되는 구성입니다.

연동의 목적

Genian ZTNA와 OTP 서버연동은 다음의 효과를 제공합니다.

관리자 로그인 보안을 위한 2-Factor 인증환경 제공

- OTP 서버와 Genian ZTNA의 연동을 통해 관리자는 Genian ZTNA 관리자 페이지에 로그인 시 2단계 인증(OTP)을 추가하여 2-Factor 환경이 구성됩니다.
- OTP 방식의 2단계 인증을 통해 패스워드 도난, 계정 가로채기 등으로 인한 위협에 대비할 수 있도록 합니다.

연동을 위한 Genian ZTNA 설정

본 과정에서 다루는 Genian ZTNA의 설정 부분은 OTP 서버와 연동을 위해 최소한의 부분만을 소개합니다.

Step 1: 연동기능 적용을 위한 2단계 인증 기능활성화 설정

1) Genian ZTNA Web콘솔에서 **설정 > 환경설정 > 관리콘솔** 메뉴로 이동
2) **인증 > 2단계 인증 기능활성화** 항목에서 **OTP 인증서버** 체크박스에 체크
3) 하단부 **수정** 버튼 클릭

Step 2: 연동을 위한 OTP 서버 설정

1) Genian ZTNA Web콘솔에서 **설정 > 사용자 인증 > 인증연동** 메뉴로 이동
2) **OTP 인증서버** 항목에서 OTP 서버 추가
3) OTP 코드 생성 URL 및 OTP 코드 검증 URL 설정

설정 항목	설정 값	참고
이름	XXXXXX	중복되지 않는 OTP 서버의 이름 입력
URL	http(s)://host	OTP 서버의 주소 입력
헤더	키:값	OTP 서버요청시 HTTP 헤더에 포함할 키:값 입력
방식	GET or POST	HTTP요청 방식 선택
POST 데이터	POST 데이터	요청방식이 POST인 경우 데이터 입력
데이터전송타입	XXXX	요청방식이 POST인 경우 데이터 형식 선택
결과검증 정규식	XXXX	응답결과가 성공인지 여부를 확인하는 정규표현식 입력
결과메세지 정규식	XXXX	응답결과에서 실패메세지를 확인하는 정규표현식 입력
결과메세지 문자셋	UTF-8	응답결과메세지의 인코딩 형식

4) 2단계 인증을 적용할 **계정** 클릭 (2단계 인증은 Genian ZTNA 관리자 페이지에 접근 가능한 관리 역할 권한을 부여 받은 계정만 설정 가능합니다.)
5) **기본정보 > 로그인 설정 > 2단계 인증** 항목으로 이동
6) 셀렉트 박스에서 **OTP 인증 서버** 선택
7) 하단부 **수정** 버튼 클릭

이 과정을 통해서 Genian ZTNA와 OTP 서버가 연동되어 Genian ZTNA 관리자 페이지 로그인 수행 시 2-Factor(1단계: Genian ZTNA 계정(ID, PW) / 2단계: OTP 서버) 인증이 가능하도록 구성됩니다.

미래테크놀로지 Secure AnyOTP

본 가이드는 모바일 OTP 시스템인 미래테크놀로지의 Secure AnyOTP(이하, **AnyOTP** 로 표시함)와 네트워크 접근제어 시스템인 Genian ZTNA의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

본 연동은 관리자 계정에 대해서 2-Factor 인증을 위한 연동으로 Genian ZTNA 관리자 계정에 대해서 보다 안전한 로그인 과정을 수행하기 위해, 2-Factor 인증을 구현하기 위하여, **관리자는 Genian ZTNA 관리자 페이지에 로그인 시 ID/PW 방식의 Genian ZTNA 관리자 계정으로 로그인 이후, 추가적으로 AnyOTP의 인증을 거치도록 연동됩니다.**

연동의 구성은 Genian ZTNA가 API 호출방식의 AnyOTP 전용의 연동도구(정책서버 플러그인)를 제공하며, 관리자가 Genian ZTNA 인증처리와 함께, AnyOTP 서버에서 관리자의 모바일 단말로 OTP(One Time Password)를 발행하게 하여, 발행된 OTP정보를 확인 후 관리자 로그인을 실행하는 2-Factor 인증 구성입니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian ZTNA (정책서버)	V5.0 이상	2019.03 이후 Release 버전
Secure AnyOTP		2018.03 이후 Release 버전

연동의 목적

Genian ZTNA와 AnyOTP 연동은 다음의 효과를 제공합니다.

관리자 로그인 보안을 위한 2-Factor 인증환경 제공

- AnyOTP와 Genian ZTNA의 정책서버 플러그인 연동을 통해 관리자는 Genian ZTNA 관리자 페이지에 로그인 시 2단계 인증(OTP)을 추가하여 2-Factor 환경이 구성됩니다.
- OTP 방식의 2단계 인증을 통해 패스워드 도난, 계정 가로채기 등으로 인한 위협에 대비할 수 있도록 합니다.

사전준비 사항

연동을 위한 Genian ZTNA 정책서버 플러그인 준비

Genian ZTNA는 AnyOTP와 2-Factor 연동을 위해 별도 제작된 Genian ZTNA 정책서버 플러그인이 활용되며, 플러그인 정보는 다음과 같습니다.

Genian ZTNA 정책서버 플러그인 파일명	비고
GWP100003-5.0.gwp	2020.11 이후 Release 버전

API 호출을 위한 AnyOTP 서버의 IP, Port 확인 및 SharedKey 발급

아래의 두개 항목은 연동을 위한 *Genian ZTNA* 설정 > *Step 2:* 정책서버 플러그인 설정 > *3*번 항목 설정 시 활용됩니다.

1) API 호출을 위해 인증코드 발급을 요청할 AnyOTP 서버의 **IP** 와 **Port** 를 확인하시기 바랍니다.
2) Genian ZTNA에서 AnyOTP 서버로 인증코드 발급을 위해 API 호출 시 상호 합의되는 **SharedKey** 를 AnyOTP 서버에서 제공 받으시기 바랍니다.

모바일 단말에서 인증코드 발급을 위한 AnyOTP App 설치

관리자는 Genian ZTNA 관리자 페이지에 2단계 인증 진행 시 인증코드를 발급 받을 AnyOTP App을 개인 모바일 단말에 설치하시기 바랍니다.

연동을 위한 Genian ZTNA 설정

본 과정에서 다루는 Genian ZTNA의 설정 부분은 AnyOTP와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 정책서버 플러그인 업로드

1) Genian ZTNA Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 정책서버 플러그인** 메뉴로 이동
2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **GWP100003-5.0.gwp** 플러그인 선택
3) **업로드** 버튼 클릭
4) 목록으로 이동하여 **Any OTP 인증 모듈 > 재기동시 설치완료예정** 버튼 클릭 후 팝업창에서 **확인** 버튼 클릭 (관리콘솔 웹 어플리케이션 재기동을 수행해야 최종 설치가 완료됩니다.)

Step 2: 정책서버 플러그인 설정

1) Genian ZTNA Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 정책서버 플러그인** 메뉴로 이동
2) **Any OTP 인증 모듈** 플러그인 클릭
3) **설정항목** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
SharedKey	XXXXXX	Genian ZTNA와 AnyOTP 제품 간 상호 협의된 SharedKey 입력
GrippinTower 서버 IP	XXX.XXX.XXX.XXX	AnyOTP 서버의 IP 입력
GrippinTower 서버 port	1812	AnyOTP 서버의 Port 입력 (기본값 1812)
대기시간	3	AnyOTP에서 인증코드 발급 시 Timeout 시간 입력 (분 단위)
타이틀	AnyOtp인증	Genian ZTNA 관리자 페이지에서 2단계 인증 진행 시 인증창에 표시되는 타이틀 문구 입력
URL	/plugin/gwp100003/otpAuth.xhtml?initParameter	AnyOTP 서버로 API 호출 시 사용되는 Parameter값
Width	300	인증코드 입력 창의 가로 크기 입력 (최소 300px 권장)
height	130	인증코드 입력 창의 세로 크기 입력 (최소 130px 권장)

Step 3: 연동기능 적용을 위한 2단계 인증 기능활성화 설정

1) Genian ZTNA Web콘솔에서 **설정 > 환경설정 > 관리콘솔** 메뉴로 이동
2) **WEB 콘솔 > 2단계 인증 기능활성화** 항목에서 **Any OTP** 체크박스에 체크
3) 하단부 **수정** 버튼 클릭

Step 4: 연동기능 적용을 위한 2단계 인증 설정

1) Genian ZTNA Web콘솔에서 **관리 > 사용자** 메뉴로 이동
2) 2단계 인증을 적용할 **계정** 클릭 (2단계 인증은 Genian ZTNA 관리자 페이지에 접근 가능한 관리 역할 권한을 부여 받은 계정만 설정 가능합니다.)

3) **기본정보 > 로그인 설정 > 2단계 인증** 항목으로 이동

4) 셀렉트 박스에서 **Any OTP** 선택

5) 하단부 **수정** 버튼 클릭

이 과정을 통해서 Genian ZTNA와 AnyOTP가 연동되어 Genian ZTNA 관리자 페이지 로그인 수행 시 2-Factor(1단계: Genian ZTNA 계정(ID, PW) / 2단계: AnyOTP) 인증이 가능하도록 구성됩니다.

코리아엑스퍼트 아이루키 OTP

본 가이드는 모바일 OTP 시스템인 코리아엑스퍼트의 아이루키와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

본 연동은 관리자 계정에 대해서 2단계 인증을 위한 연동으로 Genian NAC 관리자 계정에 대해서 보다 안전한 로그인 과정을 수행하기 위해, **관리자는 Genian NAC 관리자 페이지에 로그인 시 ID/PW 방식의 Genian NAC 관리자 계정으로 로그인 이후, 추가적으로 아이루키의 인증을 거치도록 연동됩니다.**

연동의 구성은 Genian NAC가 아이루키 전용 연동도구(정책서버 플러그인)를 제공하며, 관리자가 Genian NAC 인증 시, 아이루키 서버에서 관리자의 모바일 단말로 OTP(One Time Password)를 발행하게 하여, OTP 정보를 입력하는 방식의 2-Factor 인증 구성입니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0 이상	2019.03 이후 Release 버전
아이루키		2018.07 이후 Release 버전

연동의 목적

Genian NAC와 아이루키 연동은 다음의 효과를 제공합니다.

관리자 로그인 보안을 위한 2-Factor 인증환경 제공

- 고객사 내부의 주요정보 들이 존재하는 Genian NAC 관리자 페이지에 로그인 시, ID/PW 방식에 비해 보안 수준이 높은 2-factor 인증방식으로 구성하여 고객의 주요정보에 대한 접근시의 보안수준 향상을 통하여 패스워드 도난, 계정 가로채기 등으로 인한 위협에 대비할 수 있도록 합니다.

사전준비 사항

연동을 위한 Genian NAC 정책서버 플러그인 준비

Genian NAC는 아이루키와 2-Factor 연동을 위해 별도 제작된 Genian NAC 정책서버 플러그인이 활용되며, 플러그인 정보는 다음과 같습니다.

Genian NAC 정책서버 플러그인 파일명	비고
GWP100003-5.0.gwp	2020.11 이후 Release 버전

API 호출을 위한 아이루키 서버의 IP 및 어플리케이션ID 확인

아래의 항목은 연동을 위한 *Genian NAC* 설정 > *Step 2:* 정책서버 플러그인 설정 > *3*번 항목 설정 시 활용됩니다.

Genian NAC에서 아이루키 서버로 인증코드 발급을 위해 API 호출 시 활용되는 **서버IP** 및 **어플리케이션 ID (ex. nac_admin: 관리자 계정 전용)** 를 확인하기 바랍니다.

모바일 단말에서 인증코드 발급을 위한 아이루키 App 설치
관리자는 Genian NAC 관리자 페이지에 2단계 인증 진행 시 인증코드를 발급 받을 아이루키 App을 개인 모바일 단말에 설치하시기 바랍니다.

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 아이루키와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1 회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 정책서버 플러그인 업로드

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 정책서버 플러그인** 메뉴로 이동
2) **작업선택 > 플러그인 업로드 > 파일선택** 버튼을 클릭하여 업로드할 **GWP100004-5.0.gwp** 플러그인 선택
3) **업로드** 버튼 클릭
4) 목록으로 이동하여 **아이루키 OTP 인증 모듈 > 재기동시 설치완료예정** 버튼 클릭 후 팝업창에서 **확인** 버튼 클릭 (관리콘솔 웹 어플리케이션 재기동을 수행해야 최종 설치가 완료됩니다.)

Step 2: 정책서버 플러그인 설정

1) Genian NAC Web콘솔에서 **시스템 > 업데이트 관리 > 소프트웨어 > 정책서버 플러그인** 메뉴로 이동
2) **아이루키 OTP 인증 모듈** 플러그인 클릭
3) **설정항목** 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
아이루키 서버 IP	XXX.XXX.XXX.XXX	아이루키 서버의 IP 입력
어플리케이션 ID	nac_admin	Genian NAC와 아이루키 제품 간 상호 협의된 어플리케이션 ID 입력
타이틀	아이루키 OTP 인증	Genian NAC 관리자 페이지에서 2단계 인증 진행 시 인증창에 표시되는 타이틀 문구 입력
URL	/plugin/gwp100004/otpAuth.xhtml?initParameter	아이루키 서버로 API 호출 시 사용되는 값
Width	400	인증코드 입력 창의 가로 크기 입력 (최소 400px 권장)
height	350	인증코드 입력 창의 세로 크기 입력 (최소 350px 권장)

Step 3: 연동기능 적용을 위한 2단계 인증 기능활성화 설정

1) Genian NAC Web콘솔에서 **설정 > 환경설정 > 관리콘솔** 메뉴로 이동
2) **WEB 콘솔 > 2단계 인증 기능활성화** 항목에서 **아이루키 OTP** 체크박스에 체크
3) 하단부 **수정** 버튼 클릭

Step 4: 연동기능 적용을 위한 2단계 인증 설정

1) Genian NAC Web콘솔에서 **관리 > 사용자** 메뉴로 이동

2) 2단계 인증을 적용할 **계정** 클릭 (2단계 인증은 Genian NAC 관리자 페이지에 접근 가능한 관리 역할 권한을 부여 받은 계정만 설정 가능합니다.)

3) **기본정보 > 로그인 설정 > 2단계 인증** 항목으로 이동

4) 셀렉트 박스에서 **아이루키 OTP** 선택

5) 하단부 **수정** 버튼 클릭

이 과정을 통해서 Genian NAC와 아이루키가 연동되어 Genian NAC 관리자 페이지 로그인 수행 시 2-Factor(1단계: Genian NAC 계정(ID, PW) / 2단계: 아이루키 OTP) 인증이 가능하도록 구성됩니다.

11.4 CLI(Command Line Interface)

11.4.1 CLI 접속

Attention: SSH 접속은 허용된 IP 에서만 접근 됩니다. 특정IP의 SSH 접근 허용 설정하는 방법은 default-settings-appliance 을 참조합니다.

SSH 접속을 위한 전용프로그램이나 SSH를 지원하는 콘솔에서 정책서버, 네트워크센서에 연결할 수 있습니다. 여러분이 사용하는 SSH 접속 프로그램의 표준절차에 따라 정책서버, 네트워크센서 IP로 SSH 연결을 수행합니다.

11.4.2 CLI 명령어

콘솔 모드에서는 기본 시스템 상태 및 지원 구성을 확인 할 수 있습니다. 이 문서에서는 콘솔 모드에서의 명령어와 명령어를 사용하는 방법에 대해 설명합니다.

기본 명령어

명령어	설명
enable	글로벌 구성 모드 활성화
exit	현재 모드를 종료합니다.
help	사용 가능한 명령을 표시합니다.
history	사용 된 과거 명령 목록을 표시합니다.
quit	콘솔 모드를 종료합니다.
configure terminal	구성을 즉시 설정하는 글로벌 모드
configure batch	시스템 재시작 후 구성을 설정하는 글로벌 모드
clear arp	시스템 ARP 항목을 삭제합니다.
clear screen	표시 화면을 초기화합니다.
clock set	시스템 날짜와 시간을 설정합니다.
do backup	시스템 백업을 수행합니다.
do cdbackup	연결된 광학 디스크에 시스템 백업 수행합니다.
do cdrestore	연결된 광학 디스크에서 백업 파일 복원합니다.
do initdisk	디스크를 초기화합니다.
do restore	백업 파일에서 시스템 파일을 복원합니다.
do cert-reissuance	인증서를 재발급합니다.
geniup	Genians Update Server가 지정 된 경우 최신 서버 파일로 업그레이드 진행합니다.
halt	시스템 전원 종료 모드 준비
kill pid	PID를 기반으로 프로세스를 종료합니다.
kill pname	이름을 기반으로 프로세스를 종료합니다.
ping	원격 장치에 대한 IP 테스트를위한 ICMP 요청을 생성합니다.
reboot	시스템을 재부팅합니다.
restart system	OS를 다시 시작합니다.
shutdown service	Genian ZTNA OS 서비스를 종료합니다.
traceroute	IP의 라우팅 경로를 표시합니다.
show	명령어 목록을 표시합니다.

보기 명령어

명령어	설명
show arp	IP와 MAC 주소 매핑 표시합니다.
show backup	백업 파일 목록을 표시합니다.
show configuration	현재 시스템 구성을 표시합니다.
Show cpu	CPU 정보를 표시합니다.
show filesystem	어플라이언스의 파일 시스템을 표시합니다.
show hosts	호스트 목록을 표시합니다.
show interface	어플라이언스의 네트워크 인터페이스를 표시합니다.
show logging	시스템 로깅 메시지 목록을 표시합니다.
show memory	메모리 통계를 표시합니다.
show processes	현재 실행중인 프로세스를 표시합니다.
show route	현재 구성된 라우트를 표시합니다.
show superadmin	구성 된 관리자 계정 목록을 표시합니다.
show time	현재 시스템 시간을 표시합니다.
show uptime	시스템 가동 및 가동 시간 표시합니다.
show version	현재 실행중인 시스템 버전을 표시합니다.

명령어 사용방법

CLI 명령프롬프트에서 **?** 를 입력하면 사용 가능한 명령을 볼 수 있다.

예시:

```
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
```

입력한 명령뒤에 바로 **?** 를 입력할 경우 처음 입력한 명령어의 기능설명을 볼 수 있다.

예시:

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

기본 명령어를 타이핑하고 뒤에 공간을 띄우고 **?** 를 입력하면 추가적으로 사용 가능한 명령을 볼 수 있다.

예시:

```
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
```

11.5 네트워크 구성

CLI (Command Line Interface)를 통해 인터페이스 IP 주소를 변경하거나 DHCP 용 인터페이스를 구성 할 수 있습니다.

11.5.1 인터페이스 IP 주소 변경

인터페이스 IP 주소 변경

변경 전 인터페이스 설정을 확인하세요. - Ubuntu Desktop은 GUI에서 IP 주소 변경이 가능합니다. 참조 : *Ubuntu Desktop* 네트워크 설정

Ubuntu 터미널창에서 ifconfig를 입력합니다.

```
root@geni:# ifconfig

docker0: ...

eth0: ...

lo: ...
```

인터페이스에 수동설정(IP / 게이트웨이) 및 자동설정(DHCP)이 동시에 활성화 되어있으면 기능이 올바르게 동작하지 않습니다.

인터페이스에 고정 IP 설정

인터페이스(eth0, eth1 등)의 IP 주소와 게이트웨이를 설정 하려면 다음을 수행합니다.

```
$ sudo su - root권한 획득
$ cd /etc/netplan - 네트워크 설정을 위해 netplan 디렉토리로 이동
$ vim *.yaml - netplan 하위의 네트워크 설정 파일을 에디터로 편집

# *.yaml
# network:
# version: 2
# renderer: NetworkManager
# ethernets:
#          eth0:
#                dhcp4: false
#                addresses: [IP address/CIDR]
#                gateway4: Gateway IP
#                nameservers:
#                        addresses: [IP address]

$ netplan apply - 설정 내용 적용
$ cd /usr/geni - DKNS 재부팅을 위해 디렉토리 이동
$ ./compose restart dkns - DKNS 리부트
```

yaml 파일 수정 예시 입니다.

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
          eth0:
                  dhcp4: false
                  addresses: [172.29.100.188/24]
                  gateway4: 172.29.100.254
                  nameservers:
                          addresses: [172.29.3.1]
```

인터페이스를 DHCP 클라이언트로 구성

인터페이스 또는 하위 인터페이스를 DHCP 클라이언트로 구성하려면 다음을 수행합니다.

```
.. code:: bash

   $ vim /etc/netplan/*.yaml - 에디터로 *.yaml 파일 수정

   # *.yaml
   # ...
   #           eth0:
   #                 dhcp4: false
   #                 addresses: []

  $ netplan apply - 수정한 *.yaml 파일을 적용
  $ cd /usr/geni - DKNS 재부팅을 위해 디렉토리 이동
  $ ./compose restart dkns - DKNS 리부트
```

11.5.2 센서 인터페이스에 Alias IP 추가

하나의 네트워크 인터페이스에 Secondary 네트워크가 존재하는 경우, 네트워크 센서의 인터페이스에 Alias IP를 설정하여 다수의 서브넷을 관리 할 수 있습니다.

Alias IP 추가

Alias IP는 Web콘솔에서만 설정 가능합니다.

1. 상단 패널에서 **시스템** 로 이동합니다.
2. 왼쪽 패널의 **시스템> 시스템관리** 로 이동합니다.
3. 설정할 네트워크센서 IP를 클릭합니다.
4. **센서설정** 탭을 클릭합니다.
5. Alias IP를 추가할 인터페이스의 **IP설정** 을 클릭합니다.
6. Sensor IP 우측의 **Alias IP 추가** 버튼을 클릭합니다.
7. Alias IP에 대해 다음 정보 입력합니다.
   - IP 주소 : 센서용 관리 IP

- 서브넷 마스크
- 게이트웨이
- 관리범위: IP패턴, 줄바꿈을 이용하여 미사용IP 관리영역을 제한합니다. (공란시 전체 서브넷 관리)

8. **수정** 을 클릭합니다.

Alias IP 삭제

1. 상단 패널에서 **시스템** 로 이동합니다.
2. 왼쪽 패널의 **시스템> 시스템관리** 로 이동합니다.
3. 설정할 네트워크센서 IP를 클릭합니다.
4. **센서설정** 탭을 클릭합니다.
5. Alias IP를 삭제할 인터페이스의 **IP설정** 을 클릭합니다.
6. Alias IP 우측의 **삭제** 버튼을 클릭합니다.

11.5.3 센서 인터페이스에 가상 IP 구성

Genian ZTNA는 위험감지를 위해 가상IP를 생성하고 관리하는 허니팟 기능을 제공합니다. 현재 네트워크에서 사용되지 않는 일부 IP를 네트워크센서가 서비스를 제공하는 것처럼 ARP 요청에 응답하여 알수없는 서비스 사용요청, 포트스캔 등 위험감지를 합니다. 가상IP주소는 자동 및 수동으로 할당할 수 있습니다.

가상IP 수동 추가 - 가상IP를 수동으로 직접 지정하여 추가할 수 있습니다.

가상IP 자동 추가 - 가상IP가 설정된 개수 만큼 미사용IP가 랜덤으로 가상IP으로 할당됩니다. - 가상IP 개수 변경 시, 기존의 가상IP 존재 여부 확인 후 가상IP를 할당합니다. - 기 사용중인 가상IP는 그대로 재할당하며, 추가된 개수만큼 미사용IP에 가상IP를 할당합니다.

가상IP 충돌방지 - 가상IP 자동 추가: 신규노드의 IP와 가상IP가 동일한 경우, 미사용IP로 가상IP가 자동으로 변경됩니다. - 가상IP 수동 추가: 신규노드의 IP와 가상IP가 동일한 경우, 신규노드가 등록되지 않습니다.

가상 IP 주소 보기

1. 상단 패널의 **시스템** 으로 이동합니다.
2. 좌측 패널에서 **시스템 > 시스템관리** 로 이동합니다.
3. 원하는 네트워크센서 IP를 클릭합니다.
4. **센서설정** 탭을 클릭합니다.
5. 원하는 인터페이스 우측의 **IP설정** 을 클릭합니다. 할당된 가상 IP 주소를 볼 수 있습니다.

가상 IP 주소 자동 추가/삭제

가상IP(자동) 설정 시, 미사용IP가 입력한 개수만큼 가상IP로 할당됩니다. 최대 128개를 설정할 수 있습니다.

1. 상단 패널의 **시스템** 으로 이동합니다.
2. 좌측 패널에서 **시스템 > 시스템관리** 로 이동합니다.
3. 원하는 네트워크센서 IP를 클릭합니다.
4. **센서설정** 탭을 클릭합니다.
5. 가상 IP를 추가할 인터페이스 우측의 **센서설정** 을 클릭합니다.
6. **가상 IP > 가상IP 개수** 에서 할당할 가상IP 개수를 입력합니다. 사용하지 않거나 삭제할 경우 "0" 을 입력합니다.
7. **수정** 버튼을 클릭합니다.

가상 IP 주소 수동 추가

1. 상단 패널의 시스템으로 이동합니다.
2. 좌측 패널에서 **시스템 > 시스템관리** 로 이동합니다.
3. 원하는 네트워크센서 IP를 클릭합니다.
4. **센서설정** 탭을 클릭합니다.
5. 가상 IP를 추가할 인터페이스 우측의 **IP설정** 을 클릭합니다.
6. 가상IP의 **추가** 버튼을 클릭하여 **IP주소** 와 **동작모드 > 설정함** 을 설정합니다.
7. **수정** 버튼을 클릭합니다.

가상 IP 주소 수동 제거

1. 상단 패널의 시스템으로 이동합니다.
2. 좌측 패널에서 **시스템 > 시스템관리** 로 이동합니다.
3. 원하는 네트워크센서 IP를 클릭합니다.
4. **센서설정** 탭을 클릭합니다.
5. 가상 IP를 추가할 인터페이스 우측의 **IP설정** 을 클릭합니다.
6. 삭제를 원하는 가상 IP 옆의 **삭제** 버튼을 클릭합니다.

11.5.4 네트워크센서 추가 및 삭제

네트워크가 변경되었을 때, 센서를 추가하거나 삭제할 수 있습니다.

- 원격지 관리대역이 추가되면 해당 원격지에 네트워크센서 장비를 설치해서 관리할 수 있습니다.
- 기존 네트워크센서에 관리대역이 추가될 경우, 기존 네트워크센서에 다른 인터페이스를 추가하여 이용할 수 있습니다.
- 단일 인터페이스인 경우 802.1Q 트렁크 포트를 통해 여러 VLAN을 관리할 수 있습니다.

신규 네트워크센서 추가

새 원격지 관리대역의 네트워크센서가 추가된 경우 정책서버에 연결하는 작업이 필요합니다. 신규 네트워크센서를 추가하는 방법은 네트워크센서 설치 를 참고해주시기바랍니다.

설치가 완료된 네트워크센서는 Web콘솔 메뉴 **시스템 > 시스템관리 > 센서관리** 에서 **네트워크센서** 에서 확인할 수 있습니다.

기존 네트워크센서 삭제

Note:

네트워크센서를 삭제하면 연결된 VLAN 및 모든 노드 정보가 함께 삭제됩니다.

1. **네트워크센서** 장비를 네트워크에서 분리하고 전원을 끕니다.
2. **정책 서버 Web콘솔** 에 접속합니다.
3. 상단 항목의 **시스템** 로 이동합니다.
4. 시스템 관리 항목에서 **시스템 > 시스템관리** 로 이동합니다.
5. 원하는 네트워크센서의 **체크 박스** 를 클릭합니다.
6. **작업선택 > 장비 삭제** 를 클릭합니다.
7. **확인** 을 클릭합니다.

기존 네트워크센서에 인터페이스 추가

이 옵션을 사용하면 트렁크 포트를 사용하지 않고도 단일 센서 어플라이언스에서 별도의 LAN 또는 VLAN을 모니터링할 수 있습니다. **각 네트워크마다 하나의 유선 인터페이스가 필요합니다.**

네트워크센서는 Web콘솔을 통해 추가할 수 없으며, CLI콘솔을 통해 기존 eth0 또는 eth1 인터페이스에 하위 인터페이스를 추가하여 구성해야합니다.

1. **SSH 클라이언트** 를 통해 네트워크센서에 연결합니다. 관리자 콘솔 의 CLI 접속 방법을 참고해주시기바랍니다.
2. 추가할 각 네트워크센서에 대해 아래 명령을 입력합니다.

   아래의 예시에서는 인터페이스 eth0이 이미 구성되어 있습니다. 인터페이스 eth1은 별도의 LAN을 모니터링하도록 구성됩니다.

```
$ sudo su - root권한 획득
$ cd /etc/netplan - 네트워크 설정을 위해 netplan 디렉토리로 이동
$ vim *.yaml - netplan 하위의 네트워크 설정 파일을 에디터로 편집

# *.yaml
# network:
# version: 2
# renderer: NetworkManager
# ethernets:
#          eth0:
#                dhcp4: false
#                addresses: [IP address/CIDR]
#                gateway4: Gateway IP
```

(continues on next page)

(continued from previous page)

```
#                 nameservers:
#                         addresses: [IP address]
#
#           eth1:
#                 dhcp4: false
#                 addresses: [IP address/CIDR]
#                 gateway4: Gateway IP
#                 nameservers:
#                         addresses: [IP address]


$ netplan apply - 수정한 *.yaml 파일을 적용
$ cd /usr/geni - DKNS 재부팅을 위해 디렉토리 이동
$ ./compose restart dkns - DKNS 리부트
```

yaml 파일 수정 예시 입니다.

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
          eth0:
                dhcp4: false
                addresses: [172.29.131.247/24]
                gateway4: 172.29.131.254
                nameservers:
                        addresses: [172.29.3.1]


          eth1:
                dhcp4: false
                addresses: [172.29.109.247/24]
                gateway4: 172.29.109.254
                nameservers:
                        addresses: [172.29.3.1]
```

고정 IP를 사용하지 않는 경우 DHCP를 설정합니다.

```
 $ vim /etc/netplan/*.yaml - 에디터로 *.yaml 파일 수정

 # *.yaml
 # ...
 #           eth0:
 #                 dhcp4: false
 #                 addresses: []

$ netplan apply - 수정한 *.yaml 파일을 적용
$ cd /usr/geni - DKNS 재부팅을 위해 디렉토리 이동
$ ./compose restart dkns - DKNS 리부트
```

기존 네트워크센서 인터페이스 삭제

Note:

이 기능은 단일 네트워크센서와 모든 노드, 노드정보를 삭제합니다.

1. **SSH 클라이언트** 를 통해 네트워크센서에 연결합니다. 관리자 콘솔 의 CLI 접속 방법을 참고해주시기바랍니다.
2. 삭제할 각 네트워크센서에 대해 아래 명령을 입력합니다.

```
$ sudo su - root권한 획득
$ cd /etc/netplan - 네트워크 설정을 위해 netplan 디렉토리로 이동
$ vim *.yaml - netplan 하위의 네트워크 설정 파일을 에디터로 편집
# *.yaml - 설정한 인터페이스 삭제
# ...
#          eth0:
#                dhcp4: false
#                addresses: [IP address/CIDR]
#                gateway4: Gateway IP
#                nameservers:
#                        addresses: [IP address]

$ netplan apply - 수정한 *.yaml 파일을 적용
```

3. Web콘솔 상단 항목의 **시스템** 으로 이동합니다.
4. 시스템 관리 패널에서 **시스템관리 > 센서관리** 로 이동합니다.
5. 변경할 네트워크센서의 **IP 주소** 를 클릭합니다.
6. **대상노드작업 > 삭제** 를 클릭합니다.
7. **확인** 버튼을 클릭합니다.

기존 트렁크 인터페이스에 VLAN 추가

이 옵션은 네트워크센서가 트렁크 포트 모드로 설치된 경우 사용됩니다. 장비당 최대 128개의 VLAN을 추가할 수 있으며, 64개의 VLAN을 사용하는 것을 권장합니다.

네트워크센서는 Web콘솔을 통해 추가할 수 없으며, CLI콘솔을 통해 기존 eth0 또는 eth1 인터페이스에 하위 인터페이스를 추가하여 구성해야합니다.

1. **SSH 클라이언트** 를 통해 네트워크센서가 구축된 Ubuntu 장비에 접속합니다. 관리자 콘솔 의 CLI 접속 방법을 참고해주시기바랍니다.
2. 모니터링할 모든 VLAN 인터페이스를 추가합니다.
3. 추가한 각 VLAN 인터페이스별 IP 및 Gateway를 설정합니다.

   eth0 이후의 각 VLAN 접미사는 VLAN ID에 의해 결정됩니다. 아래는 VLAN 109,114에 센서를 추가하는 예시입니다. 모니터링할 모든 VLAN에 대해 아래의 과정을 반복합니다.

```
$ sudo su - root 권한 획득
$ cd /etc/netplan - ubuntu 장비의 VLAN 설정을 위해 netplan 디렉토리로 이동
$ vim *.yaml - 에디터를 통해 네트워크 설정파일인 yaml를 수정

# *.yaml
```

(continues on next page)

(continued from previous page)

```
# network:
# version: 2
# renderer: NetworkManager
# ethernets:
#       eth0:
#               dhcp4: false
#               addresses: [IP address/CIDR]
#               gateway4: Gateway IP
#               nameservers:
#                       addresses: [IP address]
#
#
# vlans:
#
#       eth0.VLANID:
#                 id: VLANID
#                 link: eth0
#                 addresses: [IP address/CIDR]
#
#       eth0.VLANID:
#                 id: VLANID
#                 link: eth0
#                 addresses: [IP address/CIDR]

$ netplan apply - 수정한 *.yaml 파일을 적용
$ cd /usr/geni - DKNS 재부팅을 위해 디렉토리 이동
$ ./compose restart dkns - DKNS 리부트
```

yaml 파일 수정 예시 입니다.

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
          eth0:
                  dhcp4: false
                  addresses: [172.29.100.188/24]
                  gateway4: 172.29.100.254
                  nameservers:
                          addresses: [172.29.3.1]

  vlans:

        eth0.109:
                  id: 109
                  link: eth0
                  addresses: [172.29.109.200/24]




        eth0.114:
                  id: 114
                  link: eth0
                  addresses: [172.29.114.200/24]
```

고정 IP를 사용하지 않는 경우 DHCP를 설정합니다.

```
 $ vim /etc/netplan/*.yaml - 에디터로 *.yaml 파일 수정

 # *.yaml
 # ...
 #          eth0.VLANID:
 #                    dhcp4: false
 #                    addresses: []

$ netplan apply - 수정한 *.yaml 파일을 적용
$ cd /usr/geni - DKNS 재부팅을 위해 디렉토리 이동
$ ./compose restart dkns - DKNS 리부트
```

Note: **CISCO 스위치** 인 경우 Native VLAN을 파악하여 센서에 추가하지 않도록 주의하시기 바랍니다. **Native VLAN(default : VLAN 1)** 은 트렁크 포트에 구성된 센서로 모니터링할 수 없습니다.

기존 트렁크 인터페이스의 VLAN 삭제

Note:

이 기능은 단일 네트워크센서와 모든 노드, 노드정보를 삭제합니다.

1. **SSH 클라이언트** 를 통해 네트워크센서에 연결합니다. 관리자 콘솔 의 CLI 접속 방법을 참고해주시기바랍니다.
2. 설정 파일에서 기존 트렁크 VLAN 설정을 삭제합니다.
3. VLAN 센서 인터페이스를 제거하려면 아래의 명령어를 입력합니다.

```
$ sudo su - root권한 획득
$ cd /etc/netplan - 네트워크 설정을 위해 netplan 디렉토리로 이동
$ vim *.yaml - netplan 하위의 네트워크 설정 파일을 에디터로 편집
# *.yaml - 설정한 VLANS 설정 삭제
# ...
# vlans:
#
#       eth0.VLANID:
#                 id: VLANID
#                 link: eth0
#                 addresses: [IP address/CIDR]

$ netplan apply - 수정한 *.yaml 파일을 적용
```

4. Web콘솔 상단 항목의 **시스템** 으로 이동합니다.
5. 시스템 관리 패널에서 **시스템관리 > 센서관리** 로 이동합니다.
6. 변경할 네트워크센서의 **IP 주소** 를 클릭합니다.
7. **대상노드작업 > 삭제** 를 클릭합니다.
8. **확인** 버튼을 클릭합니다.

11.5.5 네트워크센서 인터페이스 유형 변경

네트워크 구성을 변경하면 네트워크센서의 인터페이스 유형이 액세스 포트에서 트렁크 포트로 또는 그 반대로 변경 될 수 있습니다. 이 장에서는 센서 인터페이스 유형을 변경하는 방법을 설명합니다.

Trunk Port 에 대한 액세스 포트

Note: 본 문서는 물리적 인터페이스가 eth0이라고 가정합니다.

기존 인터페이스 구성을 확인하고 저장합니다. 변경하려는 인터페이스에 IP 또는 게이트웨이 이외의 설정이 있는 경우 설정을 새 인터페이스로 전송해야합니다.

```
root@geni:# ifconfig

docker0: ...

eth0: ...
```

(continues on next page)

(continued from previous page)

```
lo: ...
```

물리적 인터페이스에 VLAN 인터페이스 생성 VLAN 인터페이스 및 게이트웨이의 고정 IP 설정

```
/etc/netplan/*.yaml
# *.yaml
# network:
# version: 2
# renderer: NetworkManager
# ethernets:
#       eth0:
#               dhcp4: false
#               addresses: [IP address/CIDR]
#               gateway4: Gateway IP
#               nameservers:
#                       addresses: [IP address]
#
#
# vlans:
#
#       eth0.VLANID:
#                 id: VLANID
#                 link: eth0
#                 addresses: [IP address/CIDR]
#
#       eth0.VLANID:
#                 id: VLANID
#                 link: eth0
#                 addresses: [IP address/CIDR]

$ netplan apply - 수정한 *.yaml 파일을 적용
```

yaml 파일 수정 예시 입니다.

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
          eth0:
                  dhcp4: false
                  addresses: [172.29.100.188/24]
                  gateway4: 172.29.100.254
                  nameservers:
                          addresses: [172.29.3.1]

  vlans:

        eth0.109:
                    id: 109
                    link: eth0
                    addresses: [172.29.109.200/24]




        eth0.114:
                    id: 114
                    link: eth0
                    addresses: [172.29.114.200/24]
```

또는 DHCP 설정 (고정 IP를 사용하지 않는 경우)

```
$ vim /etc/netplan/*.yaml - 에디터로 *.yaml 파일 수정

# *.yaml
# ...
#          eth0.VLANID:
#                    dhcp4: false
#                    addresses: []
```

모든 VLAN 인터페이스에 이더넷 고정 IP 또는 DHCP 를 제대로 설정되었는지 확인합니다.

VLAN 인터페이스에서 실행중인 네트워크센서를 구성하려면 다음을 수행합니다.

1. 관리자 웹 UI에 로그인하고 **시스템** 메뉴로 이동합니다.
2. 네트워크센서 IP를 클릭하고 **센서설정** 탭으로 이동합니다.
3. 인터페이스 이름을 클릭합니다.
4. **센서 동작모드** 를 **Inactive** 에서 **Monitoring** 로 변경합니다.
5. 하단의 **수정** 를 클릭합니다.

인터페이스가 CLI 설정에서 제거되면 관리 콘솔에 등록 된 모든 센서 또는 노드가 자동으로 삭제되지 않습니다. 더 이상 존재하지 않는 센서와 탐지 한 노드를 삭제하려면 다음 단계를 수행합니다.

1. **시스템** 메뉴로 이동합니다.
2. 왼쪽 패널에서 **시스템> 센서관리** 를 선택합니다.

3. 원하는 센서에서 **IP** 를 클릭합니다. (호스트명 열의 인터페이스 이름으로 식별 할 수 있습니다)
4. 하단의 **삭제** 를 클릭합니다.

Trunk Port 에서 액세스 포트로

모든 VLAN 인터페이스 설정 삭제

```
# *.yaml - 작성한 VLANS 설정 삭제
# vlans:
#
#       eth0.VLANID:
#                   id: VLANID
#                   link: eth0
#                   addresses: [IP address/CIDR]
#
#       eth0.VLANID:
#                   id: VLANID
#                   link: eth0
#                   addresses: [IP address/CIDR]

$ netplan apply - 수정한 *.yaml 파일을 적용
```

11.6 고 가용성 구성(HA구성)

ZTNA 시스템이 정상적인 서비스를 제공할 수 없게 되었을 때 이중화 구성을 통해 서비스 중단이 없도록 해주는 고가용성 기능을 제공합니다. 하나는 Active로 동작하면서 서비스를 제공하고, 나머지 하나는 Standby로 동작하면서 Active 장비의 동작상태를 모니터링합니다. 이를 위해서 표준 VRRP 프로토콜을 사용합니다.

- **Group** - VRRP 그룹 ID
- **Linkupdelay –** 인터페이스가 활성화 될 때까지 기다릴 시간
- **No-Virtual-Mac** – Master로 전환 할 때 인터페이스의 MAC 주소를 Virtual-MAC로 변환하지 않습니다.
- **Nopreempt** – 우선 순위에 관계없이 마스터가 우선 적용
- **Priority** – 우선 순위 값. 가장 높은 가치는 마스터
- **Timeout** – VRRP 패킷 손실 대기 시간
- **Virtual-IP** – 장치 및 UI 용 공유 IP

11.6.1 SSH가 설정되지 않은 경우 서버에 대한 시리얼콘솔 연결

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

11.6.2 HA구성을 위해 서버를 설정하는 방법

1. 준비된 장비를 네트워크에 연결합니다.
2. CLI(Command Line Interface)에 연결하여 각 서버에 연결합니다.
3. 현재 설정을 보려면 show 구성을 실행하십시오. (두대의 정책서버 *Device-ID*는 동일해야하므로 기록합니다.)
4. 전역 설정모드로 들어갑니다. (configure terminal)
5. 각 서버에서 다음 설정을 순서대로 입력합니다.

11.6.3 Primary 정책 서버

```
1. Interative Wizard
2. Manual Configration

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 ZTNA
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> enable
Password:
genian# configure terminal

genian(config)# hostname PRIMARY
PRIMARY(config)# interface eth0 address [IP address] [Subnetmask]
PRIMARY(config)# interface eth0 gateway [Gateway]
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]
PRIMARY(config)# data-server access-list [Secondary DB 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 [HA group ID]
PRIMARY(config)# interface eth0 ha linkupdelay 30
```

(continues on next page)

(continued from previous page)

```
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 [username]

device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (*두대의 정책서버의 Device-id는 동일해야합니다
*)

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

11.6.4 슬레이브 정책 서버

```
1. Interactive Wizard
2. Manual Configration

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 ZTNA
Username: [Admin ID]
Password:
```

(continues on next page)

(continued from previous page)

```
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# configure terminal

genian(config)# hostname SECONDARY
genian(config)# device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (Primary 정책서버의␣
↪Device-ID를 입력)
SECONDARY(config)# interface eth0 address [IP address] [Subnetmask]
SECONDARY(config)# interface eth0 gateway [Gateway IP]
SECONDARY(config)# ip default-gateway [Gateway IP]
SECONDARY(config)# ip name-server [DNS IP]
SECONDARY(config)# data-server username [username]
SECONDARY(config)# data-server enable
SECONDARY(config)# data-server password [password]
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


data-server enable
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 [Primary DB username]
data-server username [username]

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

hostname SECONDARY

interface eth0 address [IP address] [Subnetmask]
interface eth0 gateway [Gateway IP]
```

(continues on next page)

(continued from previous page)

```
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
```

11.6.5 Primary 네트워크센서

```
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 IP]
interface eth0.10 ha group [ha group id]
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]
```

11.6.6 SECONDARY 네트워크센서

```
device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx *(Primary network sensor Device-id)*

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

Primary와 Secondary 네트워크센서의 Device-id는 동일해야합니다.
Primary장비에 HA 설정된 인터페이스가 다운되거나 장비가 다운되는 경우에만 Failover가 진행됩니다.
모든 VLAN 인터페이스에 HA 설정을 하는 경우 하나의 인터페이스라도 다운이 되는경우 Failover가 진행됩니다.

11.6.7 장비 HA 확인하는 방법

```
-------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]
```

11.6.8 DB Replicatin 확인하는 방법

```
-------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 (Master DB의 현재 replication file)
Position                    : 123456 (Master DB의 현재 replication position)

==================== Secondary Replication Status ====================
Host                        : [Slave DB IP displayed]
Slave_IO_Running            : Yes (YES 라고 표시되어야 정상)
Slave_IO_State              : Waiting for master to send event
Slave_SQL_Running           : Yes (YES 라고 표시되어야 정상)
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 (Master DB의 현재 로그파일과 동일해야 정상)
Read_Master_Log_Pos         : 123456 (Master DB의 현재 로그포지션과 동일해야 정상)
Relay_Master_Log_File       : mysqld.000009
Exec_Master_Log_Pos         : 123456
```

(continues on next page)

(continued from previous page)

```
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.(이 메시지는 DB replication이 정상임을 나타냅니다.)

==================== Primary Replication Status ====================
Host                      : [Master DB IP displayed]
File                      : mysqld.000009 (Master DB의 현재 replication file)
Position                  : 123456 (Master DB의 현재 replication position)

==================== Secondary Replication Status ====================
Host                      : [Slave DB IP displayed]
Slave_IO_Running          : Yes (YES 라고 표시되어야 정상)
Slave_IO_State            : Waiting for master to send event
Slave_SQL_Running         : Yes (YES 라고 표시되어야 정상)
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 (Master DB의 현재 로그파일과 동일해야 정상)
Read_Master_Log_Pos       : 123456 (Master DB의 현재 로그포지션과 동일해야 정상)
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
```

Attention: Database 복제 확인 명령어는 Primary 와 Secondary 에서 각각 실행하여 확인 바랍니다.

11.6.9 Bonding 구성

Bonding은 물리적인 다수의 인터페이스를 논리적으로 하나의 인터페이스로 묶어서 사용하는 기술입니다.
bonding은 물리적으로 인터페이스가 다운되는경우를 대비할때 사용합니다.

- 케이블, 물리포트, 연결된 네트워크 장비 다운등의 상황에 서비스 가용성을 높이기 위하여 사용

Bonding 설정

Bonding 설정은 물리적인 포트가 2개 이상인 정책서버와 네트워크센서에서 사용할 수 있습니다.

정책서버 & 네트워크센서

```
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 (recommanded)
```

Note:

Bonding 설정을 하기전에 인터페이스에는 어떤 설정도 존재해서는 안됩니다.
Bonding parameters 설정 적용을 위해서 장비 리부팅이 필요합니다.
Bongding 인터페이스를 사용하는 경우 장비내 다른 인터페이스의 사용을 금지합니다.

Bonding 인터페이스 상태 확인

Bonding 인터페이스는 Active/Active, Active/Backup 형태의 상태변화가 발생합니다. 아래는 현재 상태를 확인하는 방법입니다.

```
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
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
```

11.7 백업 및 복원

자동백업을 예약하고, 장애 발생 시 복원할 수 있습니다.

Note: Cloud 버전에서는 이 기능을 사용할 수 없습니다.

11.7.1 백업 설정

특정 시간 백업 예약

1. 상단 패널의 **설정** 으로 이동합니다.
2. 왼쪽 환경 설정 패널에서 **환경설정 > 백업** 으로 이동합니다.
3. 백업 창에서 **백업수행여부** 을 찾습니다. 예약 백업을 위해 **On** 을 클릭합니다.
4. 백업을 반복하려면 **시간** 을 지정합니다.
5. 백업수행 시 여유공간보호를 위한 **임계치** 를 입력합니다.
6. **수정** 를 클릭합니다.

저장장치 유형 구성

저장장치 유형	설명 및 설정값
로컬디스크	정책서버 디스크에 백업을 수행합니다.(별도의 설정 필요없음)
외부 저장장치	정책서버에 USB Type으로 연결된 외장 디스크에 백업을 수행합니다.
CIFS 저장장치	윈도우 공유 기능을 이용하여 CIFS 사용 백업을 수행합니다.
NFS 저장장치	Unix나 Linux file system의 디렉토리를 mount하여 백업을 수행합니다.
FTP SERVER	FTP(File Transfer Protocol)을 통해 백업파일을 전송합니다. (보안상 비밀번호가 평문으로 전달됨으로 권장하지 않음)
SFTP SERVER	SFTP(Secure File transfer protocol)을 통해 백업파일을 전송합니다. (보안상 SSH 기반으로 암복호화를 수행함으로 권장함)

1. 상단 패널의 **설정** 으로 이동합니다.
2. 왼쪽 환경 설정 패널에서 **환경설정 > 백업** 으로 이동합니다.
3. 백업 창에서 **저장장치** 를 찾습니다. 목록에서 적절한 **유형** 을 선택합니다.
4. **수정** 를 클릭합니다.

Note: 백업파일에 저장장치를 **로컬디스크** 가 아닌 **다른 타입** 으로 지정할 경우 **백업파일 보존여부** 설정을 **ON** 으로 설정 시 백업파일 유실에 대응할 수 있습니다.

백업파일 다운로드

1. 상단 패널의 **설정** 으로 이동합니다.
2. 좌측 패널의 **환경설정 > 백업** 으로 이동합니다.
3. **백업파일 다운로드 > 백업목록** 버튼을 클릭합니다.
4. 목록에서 백업하려는 파일을 다운로드합니다.

11.7.2 시스템 복원

단일 구성인 경우

1. CLI를 통해 정책서버에 SSH 프로토콜로 연결합니다.
2. CLI 로그인 후 **enable** 및 **관리자 비밀번호** 를 입력하여 **EXEC Mode(#enable)** 로 변경합니다.
3. 백업을 복원하려면 "restore <filename> all" 을 입력합니다.

HA 구성인 경우

HA 구성이 되어있는 경우 Slack 으로 추가 문의 부탁드립니다.

Note: 복원을 수행하기 전에 서비스를 종료해야 합니다.

11.8 외부 전송 이메일 서버 설정

본 문서는 메일서버를 이용하여 외부로 메일을 전송하는 방법을 다루고 있습니다.

11.8.1 전자 메일 계정 설정

1. 상단 패널의 **설정** 으로 이동하십시오.
2. 왼쪽의 **환경설정> 기타설정** 으로 이동하십시오.
3. 메일서버 설정에 대하여 **SMTP** 또는 **구글메일서버** 를 선택하십시오.

SMTP

1. **서버주소** : 서버 주소 (예 : *smtp.gmail.com*)
2. **서버포트** : 포트 번호 (예 : *SMTP = 25, SSL = 465, TLS / STARTTLS = 587*) 를 입력하십시오.
3. **송신자주소** : 송신자의 주소 입력란 (전자메일 주소에 표시되는 주소)
4. **송신자이름** : 송신자 이름 입력 (전자메일 주소에 표시되는 이름)
5. **연결보안** : 위에서 지정한 서버포트에 맞는 보안방식을 선택합니다.
6. **인증사용자** : 인증사용자를 입력하십시오.
7. **인증비밀번호** : 비밀번호를 입력하고 확인란에 동일한 비밀번호를 입력합니다.

8. **수정** 을 클릭하십시오.
9. 설정테스트의 **발송** 을 클릭하여 해당 구성설정으로 메일이 정상 전송되는지 확인합니다.

구글메일서버

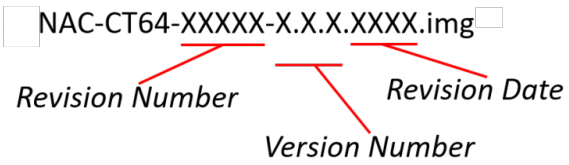
1. **송신자주소** : 송신자의 주소 입력란 (전자메일 주소에 표시되는 주소)
2. **송신자이름** : 송신자 이름 입력 (전자메일 주소에 표시되는 이름)
3. **코드발급** : 송신자 주소 계정으로 구글 로그인을 하여 인증코드를 발급 받습니다.
4. **구글 인증 코드** : 인증 팝업창에 표시된 코드를 복사해서 붙여넣습니다.
5. **수정** 을 클릭하십시오.
6. 설정테스트의 **발송** 을 클릭하여 해당 구성설정으로 메일이 정상 전송되는지 확인합니다.

11.9 시스템 업데이트 관리

11.9.1 소프트웨어 관리

시스템 소프트웨어 (정책서버, 네트워크센서 및 에이전트)를 관리 할 수 있습니다. 소프트웨어 패키지는 이름, 리비전 번호, 제품 버전 및 리비전 날짜 등 네 부분으로 구분됩니다.

- **ZTNA-CT** – 정책서버 이미지
- **ZTNA-SS** – 네트워크센서 이미지
- **ZTNA-AGENT** – 에이전트 이미지



정책서버 및 네트워크센서 업데이트

WebUI와 CLI를 통해 정책서버 및 네트워크센서를 업데이트할 수 있습니다.

Warning: 무분별한 업데이트는 ZTNA 시스템의 치명적인 오류의 원인이 될 수 있습니다. 파트너 엔지니어에게 문의 바랍니다.

업데이트 이미지 파일 준비하기

파트너 엔지니어에게 문의하여 소프트웨어 이미지 파일을 다운받습니다.

1. .iso 파일의 내용을 추출합니다.
2. .iso의 /images 디렉터리에서 원하는 소프트웨어 버전을 선택하십시오.
    - **정책서버** 의 경우 **ZTNA-CT** 로 시작하는 파일 (네트워크센서 파일 포함)
    - **네트워크센서** 의 경우 **ZTNA-SS** 로 시작하는 파일을 선택하십시오.

WEBUI를 통한 업데이트

1. 상단의 **시스템** 으로 이동하십시오.
2. 좌측 **업데이트 관리** 에서 **소프트웨어** 를 클릭하십시오.
3. 소프트웨어 창에서 **수동 업로드** 버튼을 클릭하십시오.
4. 업로드 창에서 **파일선택** 을 클릭하십시오.
5. 원하는 파일을 더블 클릭하십시오.
6. **업로드** 를 클릭하십시오.
7. 좌측의 **시스템 > 시스템관리** 로 이동하십시오.
8. 시스템 목록에서 **정책서버 / 네트워크센서** 를 찾습니다. **체크박스** 를 클릭하십시오.
9. **작업선택** 을 클릭하십시오.
10. **이미지선택 업그레이드** 를 클릭하십시오.
11. **이미지선택** 목록에서 이미지를 선택하고 **업그레이드** 를 클릭하십시오.
12. 자동으로 시스템 업데이트 및 재부팅이 진행됩니다.

CLI (Command Line Interface)를 통한 업데이트

CLI를 통해 정책서버 및 네트워크센서를 업데이트할 수 있습니다. 파트너 엔지니어에게 문의하여 소프트웨어 이미지 파일을 다운받습니다.

아래와 같은 경우는 CLI를 통한 업그레이드를 권장합니다.

- 정책서버 또는 DB서버와 같이 주요 서버를 업그레이드 하는 경우
- HA 구성으로 되어있는 경우

CLI update 명령어 : `geniup`

명령어 옵션

- `-h` : help
- `-f [image filename]` : 업데이트 파일 지정
- `-u [URL]` : 업데이트파일 URL 지정
- `-d` : 다운그레이드 수행 옵션
- `-c` : 이미지 종류를 체크하지 않는 옵션

1. Zmodem을 지원하는 터미널프로그램(secureCRT 등)으로 SSH접속을 합니다.
2. 쉘모드에서 rz 명령어를 사용하여 이미지 파일을 장비에 업로드 합니다.

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

3. geniup 명령어와 옵션을 사용하여 이미지 업그레이드를 진행합니다.

```
Genians$ geniup -cf [image filename]
System software upgrade from
Current Version :
Target Version  :
Do you want to upgrade this target version ? (y/N):
#해당 버전으로 업그레이드 여부 확인
Do you want to backup current database ? (Y/n):
#DB를 백업 여부 확인
Do you want to restart system after upgrade ? (Y/n):
#업그레이드 후 자동 재부팅 여부 확인
```

자세한 내용은 다음을 참조하세요. *CLI(Command Line Interface)*

Warning: geniup 명령어를 사용하여 정책서버 및 DB서버를 업그레이드하는 경우 백업을 수행하는 것을 권장합니다.

구성별 업그레이드 방법

정책서버/네트워크센서 구성 업그레이드 방법

정책서버와 네트워크센서의 버전이 다른 경우 비정상 동작하는 경우가 많습니다. 두 버전을 동일 버전으로 맞추어 업그레이드 진행하시기바랍니다.

1. 쉘모드 진입
2. 정책서버 서비스 중지

```
Genians$ alder stop
```

3. 정책서버 업그레이드 (재부팅 하지 않음)
4. 네트워크센서 업그레이드
5. 정책서버 재부팅

정책서버/DB서버 분리구성 시 업그레이드 방법

정책서버 업그레이드 중, DB서버 업그레이드가 되지 않도록 주의해야 합니다.

1. 쉘모드 진입
2. 정책서버 서비스 중지

```
Genians$ alder stop
```

3. DB서버 업그레이드
4. DB서버 재부팅 후, 정상 동작 확인
5. 정책서버 업그레이드

Note:

정책서버와 DB서버는 반드시 동일버전일 필요는 없습니다. 릴리즈 노트를 참조하여 DB서버 수정사항을 확인 후 업그레이드 진행해주시기 바랍니다.

HA구성 시 업그레이드 방법

업그레이드 과정에서 Master 시스템이 변경되지 않도록 주의해야 합니다.

1. Slave서버 업그레이드 (재부팅 하지 않음)
2. Slave서버 서비스 중지

```
Genians$ alder stop
```

3. Master서버 업그레이드
4. Master서버 재부팅 후, 정상 동작 확인
5. Slave서버 재부팅 후, 정상 동작 확인

에이전트 업데이트

Web UI를 통해 에이전트 파일을 업로드하여 업데이트할 수 있습니다.

에이전트 업데이트

1. 상단 패널의 **시스템** 로 이동하십시오.
2. 왼쪽 시스템 관리 패널에서 **업데이트 관리 > 소프트웨어** 로 이동하십시오.
3. **수동 업로드 > 파일선택** 을 클릭하여 에이전트 파일(.zip)을 업로드 하십시오.
4. **업로드** 를 클릭하십시오.

에이전트 플러그인 업데이트

Web UI를 통해 개별 에이전트 플러그인 파일을 업로드 하여 업데이트 할 수 있습니다.

Note: 개별 플러그인 파일은 지니언스 기술지원센터로 요청하시기 바랍니다.

1. 상단 패널에 **시스템** 으로 이동합니다.
2. 왼쪽 **업데이트 관리** 항목에 **소프트웨어 > 에이전트 플러그인** 을 선택합니다.
3. **작업선택** 항목에서 **플러그인 업로드** 를 선택합니다.
4. **파일선택** 버튼을 클릭하여 업로드할 플러그인 파일(확장자 : gpf)을 선택합니다.
5. **업로드** 를 클릭합니다.

에이전트 플러그인 버전 정보 확인하기

단말에 소프트웨어 정보를 통해 설치된 에이전트 플러그인 버전을 확인합니다.

Note: 에이전트 플러그인을 개별적으로 업로드 할 경우 소프트웨어 정보를 통해 업데이트가 정상적으로 수행되었는지 여부를 확인할 수 있습니다.

1. 상단 패널에 **관리 > 노드** 로 이동합니다.
2. 소프트웨어 정보를 확인할 **노드의 IP** 를 클릭합니다.
3. **소프트웨어 정보 탭** 을 선택합니다.
4. 소프트웨어 정보 창 우측 상단 **에이전트 정보 포함** 을 설정합니다.
5. 설치된 에이전트 및 플러그인 정보를 확인합니다.

정책서버 플러그인 업데이트

Web콘솔을 통해 정책서버 플러그인 파일을 업로드 하여 업데이트 할 수 있습니다.

정책서버 플러그인은 사이트에 국한된 기능이나 제한적 적용이 필요한 기능을 제품에 포함하지 않고 적용하기 위해 사용됩니다.

Note: Genian ZTNA 제품 이미지가 아닌 모듈 단위 형태로 동작하는 사항으로 기능 적용 시 버전 업그레이드가 필요하지 않습니다.

1. 상단 패널에 **시스템** 으로 이동합니다.
2. 왼쪽 **업데이트 관리** 항목에 **소프트웨어 > 정책서버 플러그인** 을 선택합니다.
3. **작업선택** 항목에서 **플러그인 업로드** 를 선택합니다.
4. **파일선택** 버튼을 클릭하여 업로드할 플러그인 파일(확장자 : gwp)을 선택합니다.
5. **업로드** 를 클릭합니다.

플러그인 키 별 구분 정의사항

Genian ZTNA에서 구분하는 정책서버의 플러그인은 다음과 같습니다.

모듈 구분	설명	예시
웹 모듈	팝업 페이지등 별도의 페이지를 표시하는 용도의 플러그인	OTP 인증 유틸리티
위젯모듈	지정된 항목으로 정의된 위젯 용도의 플러그인	RSS Reader 위젯 모듈
위젯정의모듈	데이터를 기반으로 관리자가 위젯을 정의할 수 있는 플러그인	
리포트모듈	지정된 항목으로 정의된 리포트 용도의 플러그인	쿼리리포트, 추이리포트, 노드그룹 리포트
리포트정의모듈	데이터를 기반으로 관리자가 리포트를 정의할 수 있는 플러그인	
서비스모듈	Rest API를 호출하는 용도의 플러그인	SSO Rest 서비스 모듈
외부연동모듈	타 시스템과 연동기능 관련 플러그인	CISCO ISE 연동 모듈
주기적 작업 모듈	주기적인 작업을 수행해야 하는 기능 관련 플러그인	AWS Connector

11.9.2 운영정보 데이터 관리

Genian Update Server 로부터 최신 데이터를 다운로드합니다.

- **CVE 업데이트 정보**, 디바이스 취약점에 대한 정보를 다운로드합니다.
- **PI 업데이트 정보**, 플랫폼 정보를 분류하기 위한 데이터를 다운로드합니다.
- **노드정보 감지 데이터**, 플랫폼 정보를 수집하기 위한 데이터를 다운로드합니다.
- **운영체제 감지 데이터**, 운영체제를 감지하기 위한 데이터를 다운로드합니다.
- **운영체제 업데이트 정보**, 운영체제 업데이트에 대한 정보를 다운로드합니다.

운영정보 데이터 자동 업데이트 설정하기

Genian Update Server 와 주기적인 버전 체크를 통해 최신 데이터를 자동으로 업데이트 하도록 설정합니다.

1. 상단 페널에 **설정** 으로 이동합니다.
2. 왼쪽 **환경설정** 항목에 **기타설정** 을 선택합니다.
3. **운영정보 데이터 설정** 에 **자동업데이트** 항목에 설정값을 **ON** 으로 변경합니다.
4. **수정** 버튼을 클릭합니다.

운영정보 데이터 수동 업데이트 하기

현재 시점을 기반으로 수동으로 운영정보 데이터를 최신 데이터로 업데이트 합니다.

1. 상단 패널에 **시스템** 으로 이동합니다.
2. 왼쪽 **업데이트 관리** 항목에 **운영정보 데이터** 를 선택합니다.
3. 상단에 **업데이트** 버튼을 클릭합니다.

11.10 모바일 앱 다운로드

Genian ZTNA Monitor는 관리자용 앱으로 노드들을 관리하고 사용자의 요청을 처리할 수 있습니다. iOS 및 Android를 모두 지원합니다.

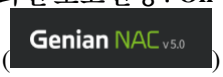
11.10.1 모바일 앱 설치방법

1. 상단 패널의 **시스템** 로 이동하십시오.
2. 왼쪽 시스템 관리 패널에서 **업데이트 관리> 소프트웨어** 로 이동하십시오.
3. **Genian ZTNA Monitor for Mobile** 을 찾아서 **iOS** 또는 **Android** 를 클릭하십시오.
4. **QR 코드** 를 스캔하여 소프트웨어를 다운로드하거나 링크를 클릭하여 App Store 또는 Play Store로 이동하여 다운로드하십시오.
5. **닫기** 를 클릭하십시오.

11.11 관리 콘솔의 환경 설정

관리자는 관리콘솔 페이지를 통하여 WEB 콘솔의 화면과 CLI 콘솔 접속 화면에 대한 설정을 할 수 있습니다.

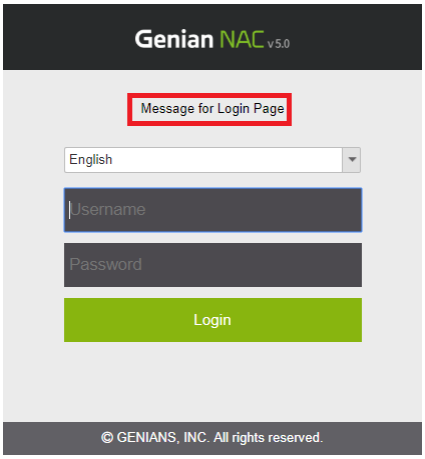
11.11.1 WEB 콘솔

1. 상단 패널의 **설정** 로 이동하십시오.
2. 왼쪽 패널의 **환경설정> 관리콘솔** 탭으로 이동하십시오.
   - **타이틀 문구** : 타이틀 이름을 설정할 수 있습니다. 이 이름은 브라우저 탭, Web콘솔 좌측 상단 탭과 트레이 메뉴의 아이콘 튤팁에 적용됩니다. (참고 : 로그아웃 후 재로그인해야 콘솔 이름의 변경 사항을 확인할 수 있고 에이전트 툴팁에 대한 에이전트를 실행해야 합니다.)
   - **관리화면 트리정렬** : **노드 관리**, **IP주소**, **스위치**, **무선랜 관리** 화면의 왼쪽 채널에 대한 트리 정렬 방식을 설정할 수 있습니다.
   - **노드수 미사용IP포함** : 관리메뉴의 트리화면에서 노드수 표시에 미사용IP포함여부를 설정할 수 있습니다. (참고 : 시스템 > 시스템관리 > 센서 선택 > 센서설정 > 미사용*IP*등록 >*ON* 설정 시 사용 가능합니다)
   - **관리화면 지원언어** : 관리화면에 대한 화면출력 지원언어를 설정할 수 있습니다.
   - **날짜패턴** : 날짜 패턴을 설정할 수 있습니다.
   - **시간패턴** : 시간 패턴을 설정할 수 있습니다.
   - **관리화면 로고변경** : **On** 옵션 선택 후 **헤더영역 배경색** 및 **로고이미지** 를 지정하여 왼쪽 상단에 기본 로고 (

) 가 사용자가 구성한 것으로 변경할 수 있습니다.
   - **페이지당 출력 열수** : 노드 관리의 단일 페이지에 표시되는 행 수의 기본값을 지정할 수 있습니다. (노드관리 페이지에서 검색 버튼 옆의 숫자 (

), 가 있는 오른쪽 상단 드롭 다운 메뉴의 설정이 최우선으로 적용됩니다.)
   - **세션 타임아웃** : Web콘솔의 세션 타임아웃 시간을 분 단위로 설정할 수 있습니다. 최소3분에서 최대 10분까지 설정가능합니다.

- **로그인화면 문구** : 로그인 페이지에 대한 텍스트, html (또는 일반 텍스트의 가능한 옵션)을 사용하여 메시지를 입력 할 수 있습니다. 이 메시지는 로그인 상자에 나타납니다.



- **2단계 인증 사용여부** : 관리자 인증으로 사용할 2단계 보안인증을 활성화할 수 있습니다. 해당 기능이 활성화되어 있는 경우에만 2단계인증을 사용할 수 있습니다. (관리자 2단계 사용을 위해서는 관리> 사용자> 관리자 탭> 로그인설정 > *2*단계인증 설정이 추가적으로 필요합니다.)
- **아이디/비밀번호 찾기** : 로그인 상자에 **사용자 이름 찾기 / 암호 재설정** 표시 여부를 결정할 수 있습니다. **사용** 을 선택하면 추가 옵션 **확인 방법** (문자 메시지 / 이메일), 찾기 / **재설정 옵션** (사용자 이름 / 비밀번호) 및 **보안 질문** 설정이 나타납니다.
- **인증코드 유효시간** : 인증코드 유효시간을 설정할 수 있습니다. 최소 30초에서 최대 5분까지 설정 가능합니다.
- **설정조건 출력수** : 정책, 그룹, 객체 관리화면에서 출력되는 설정조건의 출력수를 설정합니다. 최소 1에서 15까지 설정가능합니다.
- **로그인화면 헤더사용** : 로그인페이지 화면 헤더를 사용할지 여부를 선택할 수 있습니다. **On** 으로 변경하면 **헤더영역 배경색** 및 **헤더이미지** 를 설정할 수 있습니다.
- **대시보드 문서 제목** : 대시 보드를 내보낼 문서의 표시 제목을 설정할 수 있습니다. (*Dashboard* 오른쪽 상단의 내보내기 버튼을 클릭하여 *PDF, DOCX, PPTX* 로 저장가능합니다)

11.11.2 CLI 콘솔

CLI 배너 에서 CLI 접속시 표시될 배너를 설정할 수 있습니다.

11.12 SNMP로 정책 서버 관리

Genian ZTNA MIB 파일을 다운로드하여 NMS (Network Management System) 유형 솔루션에 사용할 수 있습니다.

11.12.1 Genian ZTNA MIB 파일 다운로드

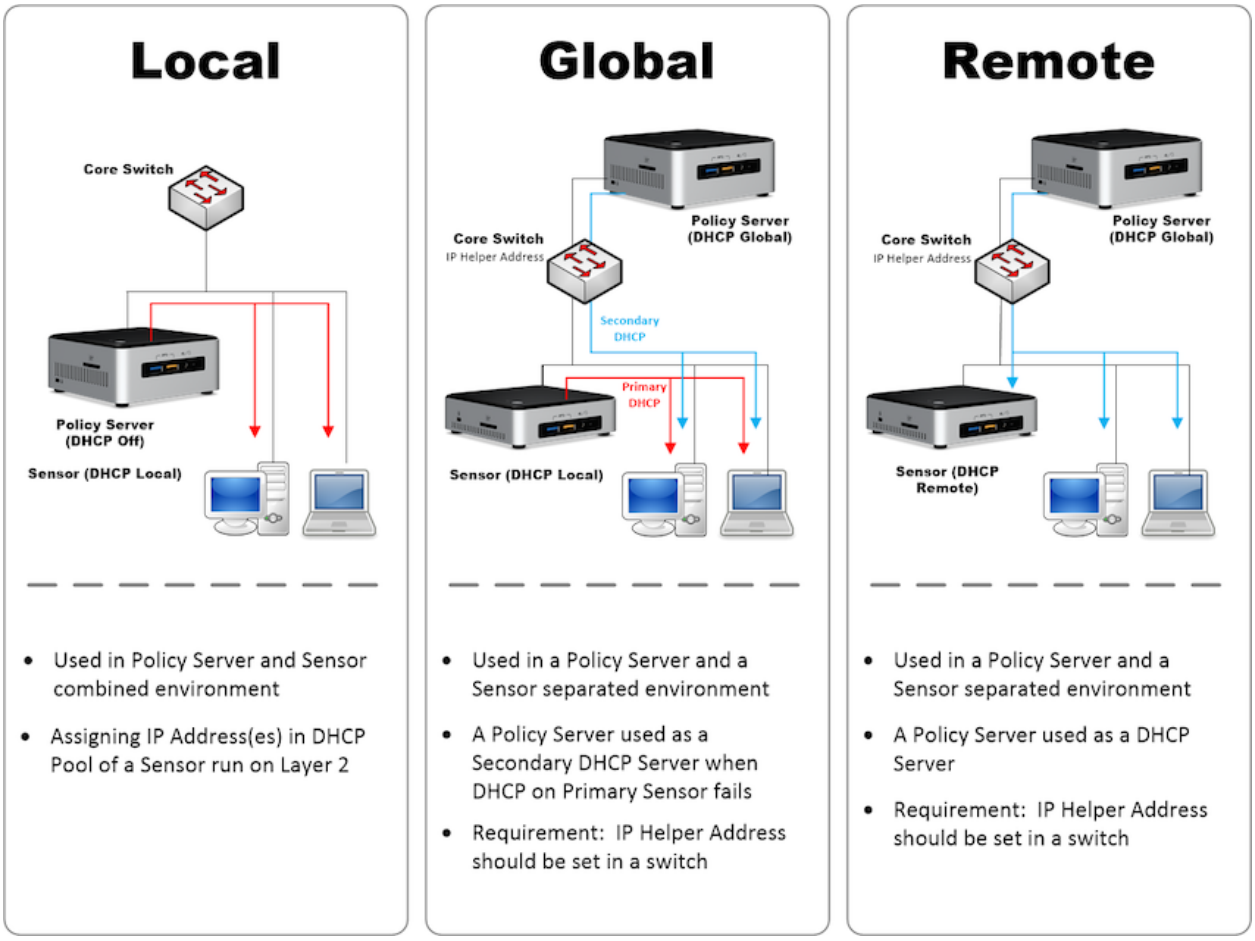
1. 상단 패널의 **설정** 으로 이동하십시오.
2. 왼쪽 환경 설정 패널에서 **환경설정> 감사기록** 으로 이동하십시오.
3. 기본 로그 창에서 **SNMP Trap 수신** 을 찾으십시오.
4. 사용여부를 **On** 으로 선택하십시오.
5. **커뮤니티 문자열** 입력하십시오.
6. **다운로드 GENIAN MIB** (*Zip* 파일이 로컬 시스템에 다운로드됩니다)
7. **업데이트** 를 클릭하십시오.
8. **GENIAN-MIB.zip** 파일의 압축을 풉니다.
9. **GENIAN-MIB.mib** 파일을 원하는 네트워크 관리 시스템에 추가하십시오.

11.13 네트워크센서 DHCP 서비스 설정하기

Genian ZTNA 네트워크 센서는 DHCP(Dynamic Host Configuration Protocol) 서비스 기능을 제공하여 관리 네트워크 대역에 IP를 자동으로 할당할 수 있습니다.

DHCP 서비스를 제공하는 항목은 아래와 같으며, 네트워크 환경에 따라서 선택적으로 사용합니다.

설정항목	기능설명	비고
로컬	네트워크 센서의 관리범위에 대해서 DHCP 서비스 제공	
리모트	네트워크 센서에서는 DHCP 서비스를 제공하지 않고, 리모트 서버에서 DHCP 서비스 제공	스위치에 DHCP Helper Address 설정 필요
로컬과 리모트	네트워크 센서의 관리범위 및 리모트로 설정된 네트워크 센서의 IP 대역에 DHCP 서비스 제공	



11.13.1 네트워크센서 로컬 DHCP 서비스 설정하기

1. 상단 페널에 **시스템** 으로 이동합니다.
2. 왼쪽 **시스템** 항목에 **센서관리** 를 선택합니다.
3. 설정할 **네트워크 센서** 에 체크박스를 선택합니다.
4. **작업선택** 항목에서 **센서 일괄 설정** 을 클릭합니다.
5. **DHCP** 관련 설정을 수행합니다
   - **DHCP 서비스** 설정값을 **ON** 으로 변경합니다.
   - **서비스 대상** 설정값을 **로컬** 로 설정합니다.
   - **노드 IP Pool** 설정값을 입력합니다.
   - **DNS 서버** 설정값을 입력합니다.
6. 저장 버튼을 클릭합니다.

11.13.2 네트워크센서 리모트 DHCP 서비스 설정하기

리모트 DHCP 서비스는 자체적으로 DHCP를 제공하지 않음으로 로컬과 리모트 설정된 정책서버가 필요합니다.

1. 상단 페널에 **시스템** 으로 이동합니다.
2. 왼쪽 **시스템** 항목에 **센서관리** 를 선택합니다.
3. 설정할 **네트워크 센서** 에 체크박스를 선택합니다.
4. **작업선택** 항목에서 **센서 일괄 설정** 을 클릭합니다.
5. **DHCP** 관련 설정을 수행합니다
    - **DHCP 서비스** 설정값을 **ON** 으로 변경합니다.
    - **서비스 대상** 설정값을 **리모트** 로 설정합니다.
6. 저장 버튼을 클릭합니다.

11.13.3 정책서버 로컬과 리모트 DHCP 서비스 설정하기

로컬과 리모트 DHCP 서비스 설정 시 리모트로 설정된 네트워크 센서 대역에 IP대역을 노드 IP Pool에 입력해야 합니다.

1. 상단 페널에 **시스템** 으로 이동합니다.
2. 왼쪽 **시스템** 항목에 **센서관리** 를 선택합니다.
3. 설정할 **네트워크 센서** 에 체크박스를 선택합니다.
4. **작업선택** 항목에서 **센서 일괄 설정** 을 클릭합니다.
5. **DHCP** 관련 설정을 수행합니다
    - **DHCP 서비스** 설정값을 **ON** 으로 변경합니다.
    - **서비스 대상** 설정값을 **로컬** 로 설정합니다.
    - **노드 IP Pool** 설정값을 입력합니다.(리모트로 설정된 네트워크센서 대역설정 필수)
    - **DNS 서버** 설정값을 입력합니다.
6. 저장 버튼을 클릭합니다.

11.13.4 정책서버에서만 DHCP 서비스하기

이 섹션은 네트워크환경이 DHCP 환경이고 DHCP 서버역할을 수행하는 주체가 정책서버이고 네트워크센서는 리모트로 동작하는 환경에서 사용됩니다.

1. 상단 항목에 있는 **시스템** 으로 이동합니다.
2. 정책서버 IP를 선택하고 **센서설정** 화면으로 이동합니다.
3. 하단 DHCP 항목에서 아래와 같이 설정합니다.

- DHCP서비스: On
- 서비스대상: 로컬과 리모트
- 노드 IP Pool: Client IP 대역 전체
- 기타 옵션들도 환경에 맞게 설정

4. 왼쪽 시스템 관리 항목에 있는 **시스템 초기설정 > 센서설정** 로 이동합니다.
5. 센서설정 창에서 아래와 같이 설정합니다.

- DHCP 서비스: On
- 서비스 대상: 리모트
  - **리모트** : 현재 센서는 DHCP서버 기능을 제공하지 않고 다른서버에서 DHCP 서비스 제공.

6. 이하 모든 **기타 설정** 들은 **옵션** 입니다.
7. 수정 을 클릭합니다.

11.14 SMS 서비스 알람 발신번호 변경하기

발신번호 변경기능은 Genian ZTNA에서 제공하는 SMS 서비스를 사용할 경우 설정이 가능합니다. Genian ZTNA에서 보내는 알람에 대해서 발신번호를 지정하여 사용할 경우 사용자와 관리자가 다수의 SMS 메시지에서 알람을 쉽게 인식을 할 수 있습니다.

Attention: 발신번호 변경은 국내 버전에 한하여 기능을 제공합니다.

11.14.1 SMS 발신번호 변경하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **환경설정** 항목에서 **기타설정** 을 선택합니다.
3. **SMS 설정** 에서 **기본 발신번호** 를 수정합니다.
4. **수정** 버튼을 클릭합니다.

11.15 추가필드 관리하기

Genian ZTNA에서는 **노드, 장비, 사용자, IP신청서, 장비 수명주기** 항목에 대해서 추가필드를 정의하여 정보를 입력할 수 있습니다.

추가필드를 통해 입력된 다양한 정보를 통해 관리자는 수집된 정보의 대상을 세부적으로 분류하여 관리할 수 있습니다.

추가필드는 다음과 같은 타입의 입력방법을 설정할 수 있습니다.

11.15.1 추가필드 정보 입력타입

입력타입	설명	사용가능 항목
문자열입력	입력 길이가 제한되지 않은 문자열 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
문자열입력(입력길이제한)	최대/최소 길이가 지정된 문자열 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
멀티라인 문자열입력	다중행이 지원되는 문자열 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
문자열패턴 입력	패턴에 매칭되는 문자열 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
멀티라인문자열패턴 입력	다중행이 지원되는 패턴에 매칭되는 문자열 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
날짜입력	기간/달력을 통한 날짜 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
날짜시각입력	기간/달력을 통한 날짜와 시각 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
IP 입력	IPv4 형태의 IP 정보 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
MAC 입력	':' 구분되는 MAC 정보 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
읽기전용	읽기 전용으로 표시되는 문자열 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
사용자 설정목록	관리자가 정의한 리스트 항목 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
사용자 설정목록(필수항목)	관리자가 정의한 리스트 항목 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
사용자 설정목록(체크박스)	관리자가 정의한 리스트 항목 체크 선택(다중선택)	노드, 장비, 사용자, IP신청서, 장비 수명주기
시스템 목록	부서명, 직급명으로 정의된 항목 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
시스템 목록(필수항목)	부서명, 직급명으로 정의된 항목 필수 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
시스템 목록(다중선택)	부서명, 직급명으로 정의된 항목 다중 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
시스템 목록(체크박스)	부서명, 직급명으로 정의된 항목 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
사용자 선택기	사용자 이름으로 검색된 사용자 계정 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
다중 사용자 선택기	사용자 이름으로 검색된 사용자 계정 다중 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
노드 선택기	IP와 인증사용자명 검색된 노드 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
부서 선택기	부서 이름으로 검색된 부서명 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
파일 업로드	업로드 파일 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
보안 질문입력	사용자 계정 보안 질문사항 답 입력	**사용자 추가필드에서만 가능**
국제 전화번호	국가 지정 전화번호를 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기

11.15.2 추가필드 정보 입력하기

추가 필드를 사용하여 노드에 추가정보 입력하기

노드에 추가필드를 설정하여 관리자가 추가필드에 정보를 입력하거나, 사용자에게 정보를 입력받을 수 있습니다.

관리자가 임의의 설정값을 입력하거나 사용자 인증 및 동의페이지에서 수집할 수 있는 정보로 추가필드를 설정할 수 있습니다. 추가필드를 통해 설정/입력된 다양한 정보를 통해 관리자는 노드 정보를 세부적으로 분류하여 관리할 수 있습니다.

Note: 노드를 대상으로는 추가필드를 20개 까지 설정할 수 있습니다.

추가필드 생성하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **추가필드관리 > 노드** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. 필드 설정값을 입력합니다.
5. **생성** 을 클릭합니다.

추가필드 정보 입력하기(관리자)

1. 상단 패널에 **관리 > 노드** 로 이동합니다.
2. 추가필드에 정보를 입력할 **노드의 IP** 를 클릭합니다.
3. **노드정보 탭** 하단 **부가정보** 항목에서 추가필드 정보를 입력합니다.
4. **노드정보 탭** 상단 **수정** 버튼을 클릭합니다.

추가필드 입력값 확인하기

관리뷰 편집기능을 사용하여 다수의 노드에 추가필드로 설정된 입력값을 뷰 화면에서 확인할 수 있습니다.

1. 상단 패널에 **관리 > 노드** 로 이동합니다.
2. 상단 **작업선택** 오른쪽  에서 **관리뷰 편집** 을 선택합니다.
3. **노드관리뷰 편집** 화면에서 **추가필드** 를 **선택창** 으로 이동합니다.
4. **수정** 버튼을 클릭합니다.

추가 필드를 사용하여 장비에 추가정보 입력하기

장비에 추가필드를 설정하여 관리자가 추가필드에 정보를 입력하거나, 사용자에게 정보를 입력받을 수 있습니다.

관리자가 임의의 설정값을 입력하거나 사용자 인증 및 동의페이지에서 수집할 수 있는 정보로 추가필드를 설정할 수 있습니다. 추가필드를 통해 설정/입력된 다양한 정보를 통해 관리자는 장비 정보를 세부적으로 분류하여 관리할 수 있습니다.

Note: 장비를 대상으로는 추가필드를 9개 까지 설정할 수 있습니다.

추가필드 생성하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **추가필드관리 > 장비** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. 필드 설정값을 입력합니다.
5. **생성** 을 클릭합니다.

추가필드 정보 입력하기(관리자)

1. 상단 패널에 **관리 > 노드** 로 이동합니다.
2. 추가필드에 정보를 입력할 **노드의 IP** 를 클릭합니다.
3. **장비정보 탭** 에서 추가필드 정보를 입력합니다.
4. **장비정보 탭** 상단 **수정** 버튼을 클릭합니다.

추가필드 입력값 확인하기

관리뷰 편집기능을 사용하여 다수의 장비에 추가필드로 설정된 입력값을 뷰 화면에서 확인할 수 있습니다.

1. 상단 패널에 **관리 > 노드** 로 이동합니다.
2. 상단 **작업선택** 오른쪽  에서 **관리뷰 편집** 을 선택합니다.
3. **노드관리뷰 편집** 화면에서 **추가필드** 를 **선택창** 으로 이동합니다.
4. **수정** 버튼을 클릭합니다.

추가 필드를 사용하여 사용자 계정에 추가정보 입력하기

사용자 계정에 추가필드를 설정하여 관리자가 추가필드에 정보를 입력하거나, 사용자에게 정보를 입력받을 수 있습니다.

추가필드를 통해 사용자 계정 신청서 작성 시 추가정보를 입력받거나, 동의페이지에서 수집할 수 있는 정보로 설정할 수 있습니다. 추가필드를 통해 설정/입력된 다양한 정보를 통해 관리자는 사용자 계정 정보를 세부적으로 분류하여 관리할 수 있습니다.

Note: 사용자 계정을 대상으로는 추가필드를 9개 까지 설정할 수 있습니다.

추가필드 생성하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **추가필드관리 > 사용자** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. 필드 설정값을 입력합니다.
5. **생성** 을 클릭합니다.
6. 상단 패널에 **설정** 으로 이동합니다.
7. 왼쪽 **속성관리** 항목에서 **용도관리 > 사용자용도** 로 이동합니다.
8. 위에서 생성한 추가필드를 적용할 사용자유형을 선택합니다.
9. **용도별 신청정보** 나 **용도별 계정정보** 항목에 생성한 추가필드를 할당합니다.
10. 하단 수정버튼 을 클릭합니다.

추가필드 정보 입력하기(관리자)

1. 상단 패널에 **관리 > 사용자** 로 이동합니다.
2. 왼쪽 항목에 **전체사용자** 를 선택합니다.
3. 추가필드에 정보를 입력할 **사용자 ID** 를 클릭합니다.
4. **기본정보** 하단 **추가정보 설정** 항목에서 추가필드 정보를 입력합니다.
5. **수정** 버튼을 클릭합니다.

추가필드 입력값 확인하기

관리뷰 편집기능을 사용하여 다수의 사용자 계정에 추가필드로 설정된 입력값을 뷰 화면에서 확인할 수 있습니다.

1. 상단 패널에 **관리 > 사용자** 로 이동합니다.
2. 상단 **작업선택** 에서 **관리뷰 편집** 을 선택합니다.
3. **관리뷰 편집** 화면에서 **추가필드** 를 **선택창** 으로 이동합니다.
4. **수정** 버튼을 클릭합니다.

추가 필드를 사용하여 IP 신청서에 추가정보 입력하기

IP 신청서 항목에 추가필드를 설정하여 사용자에게 추가적인 정보를 입력받을 수 있습니다.

IP 사용신청서 작성 시 추가정보를 입력받는 정보로 설정할 수 있습니다. 추가필드를 통해 입력된 다양한 정보를 통해 관리자는 IP 사용신청서 정보를 세부적으로 분류하여 관리할 수 있습니다.

Note: IP 신청서를 대상으로는 추가필드를 20개 까지 설정할 수 있습니다.

추가필드 생성하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **추가필드관리 > IP신청서** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. 필드 설정값을 입력합니다.
5. **생성** 을 클릭합니다.

추가필드 정보 입력하기(용도설정)

IP 사용신청서 작성 시 사용하는 용도 기능을 통해 용도별 추가필드를 입력을 다양하게 설정할 수 있습니다.

Note: 추가필드로 설정된 항목에 대한 입력을 사용자에게 받기 위해서는 IP사용신청서 기능을 사용해야 합니다.

---

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **용도관리 > IP용도 > IP신규** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. **용도별 신청정보** 항목에서 **할당** 버튼을 클릭합니다.
5. **신규 신청 입력 필드** 창에서 추가필드를 **Add** 합니다.
6. **확인** 버튼을 클릭합니다.
7. **생성** 버튼을 클릭합니다.

추가필드 입력값 확인하기

관리뷰 편집기능을 사용하여 신청된 IP사용신청서에 추가필드로 설정된 입력값을 뷰 화면에서 확인할 수 있습니다.

1. 상단 패널에 **관리 > 신청** 로 이동합니다.
2. 왼쪽 **IP사용신청서** 항목에 **IP신규/반납** 을 선택합니다.
3. 상단 **작업선택** 에서 **관리뷰 편집** 을 선택합니다.
4. **관리뷰 편집** 화면에서 **추가필드** 를 **선택창** 으로 이동합니다.
5. **수정** 버튼을 클릭합니다.

추가 필드를 사용하여 장비 수명주기에 추가정보 입력하기

장비 수명주기 항목에 추가필드를 설정하여 관리자가 추가필드에 정보를 입력하거나, 사용자에게 정보를 입력받을 수 있습니다.

관리자가 임의의 설정값을 입력하거나 사용자 인증 및 동의페이지에서 수집할 수 있는 정보로 추가필드를 설정할 수 있습니다. 추가필드를 통해 설정/입력된 다양한 정보를 통해 관리자는 장비 수명주기 정보를 세부적으로 분류하여 관리할 수 있습니다.

Note: 장비를 대상으로는 추가필드를 20개 까지 설정할 수 있습니다.

추가필드 생성하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **추가필드관리 > 장비 수명주기 관리** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. 필드 설정값을 입력합니다.
5. **생성** 을 클릭합니다.

추가필드 정보 입력하기(관리자)

1. 상단 패널에 **관리 > 노드** 로 이동합니다.
2. 추가필드에 정보를 입력할 **노드의 IP** 를 클릭합니다.
3. **장비정보 탭** 에서 **장비 수명주기 관리** 항목에 추가필드 정보를 입력합니다.
4. **장비정보 탭** 상단 **수정** 버튼을 클릭합니다.

추가필드 입력값 확인하기

관리뷰 편집기능을 사용하여 다수의 장비에 추가필드로 설정된 입력값을 뷰 화면에서 확인할 수 있습니다.

1. 상단 패널에 **관리 > 노드** 로 이동합니다.
2. 상단 **작업선택** 오른쪽  에서 **관리뷰 편집** 을 선택합니다.
3. **노드관리뷰 편집** 화면에서 **추가필드** 를 **선택창** 으로 이동합니다.
4. **수정** 버튼을 클릭합니다.

11.16 유형별 신청서 관리하기

Genian ZTNA에서 제공하는 신청서를 유형에 따라 다양한 형태에 용도를 설정할 수 있습니다. 용도에 따른 신청서 입력사항을 변경하거나, 관리자의 승인방법을 변경할 수 있어 사용자에게 부가적인 정보를 입력받거나 승인권한을 관리자가 아닌 대상에게 부여할 수 있습니다.

11.16.1 사용자 계정 용도별 속성값 설정하기

용도에 따른 신청서 입력사항을 변경하거나, 관리자의 승인방법을 변경할 수 있어 사용자에게 부가적인 정보를 입력받거나 승인권한을 관리자가 아닌 대상에게 부여할 수 있습니다.

사용자 용도에서 설정할 수 있는 항목은 신청서에 대한 처리옵션과, 신청서에 신청정보 입력과, 신청서에 계정정보 입력으로 나눠집니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **용도관리 > 사용자용도** 를 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.

사용자 신청서 처리옵션

신청서에 대한 처리옵션은 신청서에 대한 승인방식을 설정하는 사항입니다. **승인방식을 설정함에 관리자가 아닌 대상에 대해서 승인권한을 부여할 수 있는 기능을 적용합니다.** 승인메뉴를 사용한 승인, 이메일을 사용한 승인, 자동승인 항목 중 하나를 선택할 수 있으며 각 처리옵션은 다음과 같은 형식을 지원합니다.

항목	설명
승인 메뉴를 사용한 승인	승인권한을 가지고 있는 **관리자 계정** 만 승인처리 가능
이메일을 사용한 승인	승인권한을 **관리자** 와 **피신청자** (사용자 계정이 존재하는 대상)으로 세분화 가능
자동승인	별도의 신청서 승인을 수행하지 않음, 신청과 동시에 승인처리

사용자 신청서 신청정보 입력

신청정보는 Genian ZTNA에서 사전에 정의한 항목에 사용 유무를 설정할 수 있습니다. 신청정보 항목을 통해 사용목적과 사용기간을 신청자에게 받을 수 있으며, 신청서 승인결과를 전달받는 항목을 지정할 수 있습니다.

항목	설명
신청사유	사용자 계정 신청에 대한 목적을 입력받을 수 있습니다.
SMS문자통보	사용자 계정 신청 처리결과를 신청자에게 입력된 SMS 번호로 알려줄 수 있습니다.(SMS 설정 필요)
기간	사용자 계정에 유효한 기간을 신청자가 설정 할 수 있습니다.
전자우편	사용자 계정 신청 처리결과를 신청자에게 입력된 이메일을 통해 알려줄 수 있습니다.(메일서버 연동 필요)

사용자 신청서 계정정보 입력

계정정보로는 계정정보로 정의된 항목과 추가필드를 통해 정의된 값을 사용자에게 입력 받아 수집할 수 있습니다.

추가필드 관련 부분은 추가 필드를 사용하여 사용자 계정에 추가정보 입력하기 참고하시기 바랍니다.

11.16.2 IP신청서 용도별 속성값 설정하기

용도에 따른 신청서 입력사항을 변경하여 부가적인 정보를 입력받거나, 관리자의 승인방법을 변경하여 승인권한을 관리자가 아닌 대상에게 부여할 수 있습니다.

사용자 용도에서 설정할 수 있는 항목은 신청서에 대한 승인방식, 처리옵션, 신청정보 입력으로 나눠집니다.

IP 신청서는 IP신규, IP반납, 장비변경, 사용자변경 기능에 대해서 용도를 설정할 수 있으며, 각각 항목은 다음과 같은 기능을 제공합니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **속성관리** 항목에서 **용도관리 > IP용도** 를 선택합니다.
3. 생성 목적에 따라 **IP신규, IP반납, 장비변경, 사용자변경** 중 하나를 선택합니다.
4. **작업선택** 항목에서 **생성** 을 선택합니다.

항목	설명
IP신규	IP를 할당받기 위한 신청서로 다수의 용도로 설정할 수 있습니다.
IP반납	사용하고 있는 IP자원에 반납 신청서로 하나의 용도로 설정할 수 있습니다.
장비변경	사용하고 있는 IP자원에 MAC 변경 신청서로 하나의 용도로 설정할 수 있습니다.
사용자변경	IP를 사용할 수 있는 사용자 계정에 변경 신청서로 하나의 용도로 설정할 수 있습니다.

IP 신청서 용도별 승인방식 설정하기

IP 신청서에 대한 승인방식을 설정하는 사항입니다. **승인방식 설정을 통해 관리자가 아닌 대상에 대해서 승인권한을 부여합니다.** 승인 방법으로는 승인메뉴를 사용한 승인, 이메일을 사용한 승인, 자동승인 항목 중 하나를 선택할 수 있으며 각 항목들은 다음과 같은 형식을 지원합니다.

항목	설명
자동승인	신청과 동시에 승인 처리
승인자 이메일 승인 + 자동승인	이메일을 통한 승인 시 신청서 승인이 처리
승인자 이메일 승인	이메일을 통한 승인 시 신청서 등록 처리, 추가적인 관리자 승인 필요

IP 신청서 용도별 처리옵션 설정하기

IP 신청서의 용도에 따른 처리방법을 지정하는 항목으로 IP신규 용도의 처리옵션을 설정할 수 있습니다.

항목	설명
신청서처리 기본정책	IP 신규 용도의 신청서 승인시 IPM 정책설정
IP 호스트번호(처음)	IP 할당이 가능한 IP대역에 처음 IP 번호 설정
IP 호스트번호(마지막)	IP 할당이 가능한 IP대역에 마지막 IP 번호 설정
IP 사용자 인증제한여부	할당된 IP를 사용할 수 있는 사용자 제한 설정
호스트명 할당	할당된 IP를 사용할 수 있는 호스트명 제한 설정
IP소유부서 변경여부	부서기반에 IP 사용신청시 기존 IP에 할당된 소유부서 변경 설정
동일 MAC 노드 사용허용	신청서 승인 시 동일 MAC으로 등록된 기존 노드 삭제 설정
IP 할당 노드그룹 지정	IP를 할당할 수 있는 노드그룹 지정
용도 사용가능한 사용자 그룹	해당 용도를 사용할 수 있는 사용자 그룹 지정

IP 신청서 용도별 신청정보 설정하기

신청정보로는 추가필드로 생성한 항목과 IP신청서로 정의된 항목을 설정할 수 있습니다. 추가필드를 통해 정의된 IP신청서 입력정보가 아닌 임의의 값을 사용자에게 입력 받아 수집할 수 있습니다.

추가필드 관련 부분은 추가 필드를 사용하여 *IP* 신청서에 추가정보 입력하기 참고하시기 바랍니다.

11.16.3 단계별 승인 기능 사용하기

Genian ZTNA 신청시스템의 신청과 승인과정에서 승인과정을 세부적으로 분리하여 단계별로 사용할 수 있습니다.

단계별 승인이 가능한 용도	IP 신규
	IP 반납
	장비 변경
	사용자 변경
단계별 승인설정이 불가능한 용도	사용자 용도

용도의 설정 부분은 다음의 *IP*신청서 용도별 속성값 설정하기 참고하시기 바랍니다.

단계별 승인 처리하기

관리자 계정의 승인단계에 해당하는 신청서를 승인합니다.

1. 상단 패널에 **관리 > 신청** 으로 이동합니다.
2. 왼쪽 **IP사용신청서** 항목에서 **단계별승인** 을 선택합니다.
3. 승인할 **신청서 항목** 을 선택합니다. **(IP신규, IP반납, 장비변경, 사용자변경)**
4. 신청서 항목에 **승인** 버튼을 클릭합니다.

사전 승인 처리하기

관리자의 승인단계 이전 단계와 이후 단계에 대해서 우선 사용승인 기능을 사용하여 신청서를 승인합니다.

Note: 승인단계에 관리자의 부재로 인한 승인요청이 지연될 경우 우선 사용승인 기능을 활용할 수 있습니다.

1. 상단 패널에 **관리 > 신청** 으로 이동합니다.
2. 왼쪽 **IP 사용신청서** 항목에서 **단계별승인** 을 선택합니다.
3. 승인할 **신청서 항목** 을 선택합니다. **(IP 신규, IP 반납, 장비변경, 사용자변경)**
4. **구분** 항목을 선택합니다. **(이전단계, 이후단계)**
5. **작업선택** 메뉴에서 **우선사용승인** 을 선택합니다.

11.16.4 신청 시스템 결과 조회

사용자 / IP 사용 / 장비사용 신청시스템에서 등록된 신청서에 대한 처리결과를 확인할 수 있습니다.

사용자 신청 결과조회

등록된 사용자 신청서에 대한 처리결과(완료/거부)를 확인할 수 있습니다.

1. 상단 패널에 **관리 > 신청** 으로 이동합니다.
2. 왼쪽 **사용자 신청서** 항목에서 **결과조회** 를 선택합니다.

항목	설명
내보내기	신청서 처리결과 내용을 Excel 파일로 내려받을 수 있습니다.
관리뷰 편집	신청서 처리결과를 표시하는 관리뷰 항목을 수정할 수 있습니다.
빠른검색	신청서 처리결과를 검색할 수 있습니다.
신청일자	신청서 처리결과를 일자별로 검색할 수 있습니다.

IP 신청시스템 결과조회

IP 신청시스템을 통해 등록된 신청서(IP 신규, IP 반납, 장비변경, 사용자변경)에 대한 처리결과(완료/거부)를 확인할 수 있습니다.

1. 상단 패널에 **관리 > 신청** 으로 이동합니다.
2. 왼쪽 **IP 사용신청서** 항목에서 **결과조회** 를 선택합니다.

항목	설명
내보내기	신청서 처리결과 내용을 Excel 파일로 내려받을 수 있습니다.
관리뷰 편집	신청서 처리결과를 표시하는 관리뷰 항목을 수정할 수 있습니다.
구분	신청서 처리결과를 구분별(IP 신규, IP 반납, 장비변경, 사용자변경)로 검색할 수 있습니다.
빠른검색	신청서 처리결과를 검색할 수 있습니다.
조건검색	신청서 처리결과를 입력값으로 검색할 수 있습니다.

장비 사용신청 처리결과 확인하기

장치사용신청을 통해 등록된 신청서에 대한 처리결과(완료/거부)를 확인할 수 있습니다.

1. 상단 패널에 **관리 > 신청** 으로 이동합니다.
2. 왼쪽 **장치사용신청서** 항목에서 **결과조회** 를 선택합니다.

항목	설명
내보내기	신청서 처리결과 내용을 Excel 파일로 내려받을 수 있습니다.
일괄 사용종료 | 사용중인 장치에 대해서 일괄로 사용종료 할 수 있습니다.	
빠른검색	신청서 처리결과를 검색할 수 있습니다.
신청일자	신청서 처리결과를 신청일자로 검색할 수 있습니다.

11.16.5 신청서 처리하기

관리자가 사용자 / IP신청 / 장치신청 시스템에서 등록된 신청서에 대한 승인과 거부처리를 수행할 수 있습니다.

사용자 신청서 처리하기

사용자 신청서 관련 부분은 다음에 사용자 신청서를 통한 사용자 관리하기 참고하시기 바랍니다.

Note: 사용자신청 승인/거부사유 입력 기능을 사용 할 경우 승인과 거부 처리 시 사유입력창이 표시됩니다.

항목	설명
일괄승인	등록된 신청서를 일괄로 승인처리 합니다.
일괄거부	등록된 신청서를 일괄로 거부처리 합니다.
관리뷰 편집	등록된 신청서 정보 중 관리뷰로 표시할 항목을 선택합니다.
빠른검색	등록된 신청서를 검색합니다.

IP 사용신청서 처리하기

IP 사용 신청서 관련 부분은 다음에 *IP*신청서 용도별 속성값 설정하기 참고하시기 바랍니다.

1. 상단 패널에 **관리 > 신청** 으로 이동합니다.
2. 왼쪽 **IP사용신청서** 항목에 **하위메뉴(IP신규/반납, 장비변경, 사용자변경)** 을 선택합니다.
3. **신청서처리** 항목에서 **승인, 거부** 를 선택합니다.

Note: IP신청 승인/거부사유 입력 기능 사용 할 경우 승인과 거부 처리 시 사유입력창이 표시됩니다.

항목	설명
일괄승인	등록된 신청서를 일괄로 승인처리 합니다.
일괄거부	등록된 신청서를 일괄로 거부처리 합니다.
관리뷰 편집	등록된 신청서 정보 중 관리뷰로 표시할 항목을 선택합니다.
신청부서	등록된 신청서 정보 중 신청부서로 신청서를 검색합니다.
신청자명	등록된 신청서 정보 중 신청자 이름으로 신청서를 검색합니다.
사용자명	등록된 신청서 정보 중 사용자 이름으로 신청서를 검색합니다.
빠른검색	등록된 신청서를 검색합니다.

장치 사용신청서 처리하기

장치사용신청과 관련 부분은 다음에 장치 제어 참고하시기 바랍니다.

1. 상단 패널에 **관리 > 신청** 으로 이동합니다.
2. 왼쪽 **장치사용신청서** 항목에 **신규등록** 을 선택합니다.
3. **신청서처리** 항목에서 **승인, 거부** 를 선택합니다.

항목	설명
일괄승인	등록된 신청서를 일괄로 승인처리 합니다.
일괄거부	등록된 신청서를 일괄로 거부처리 합니다.
빠른검색	등록된 신청서를 검색합니다.
신청일자 검색	등록된 신청서 정보 중 등록날짜를 기준으로 검색합니다.

11.16.6 메일 승인대기 신청서 처리하기

이메일을 통한 승인기능을 사용할 경우 승인자가 승인/거부 처리하지 않을 경우 관리자가 강제로 신청서를 승인/거부 처리할 수 있습니다.

메일승인대기 항목에서 관리자가 수행할 수 있는 작업은 다음과 같습니다.

Note: 메일승인기능을 설정하는 부분은 다음에 사용자 계정 용도별 속성값 설정하기 참고하시기 바랍니다.

---

1. 다수 신청서 대상 작업

다수의 메일승인대기 신청서에 대해서는 **일괄승인** 을 할 수 없고, **승인메일 재전송** 기능을 사용하여 승인자에게 승인을 재요청해야 합니다.

항목	설명
승인메일 재전송	재전송 승인자에게 승인 이메일을 재전송 합니다.
일괄거부	승인대기 중인 신청서를 거부처리 합니다.
관리뷰 편집	등록된 신청서 정보 중 관리뷰로 표시할 항목을 선택합니다.
구분	등록된 신청서를 구분(IP신청, IP반납, 장비변경, 사용자변경)를 기준으로 표시합니다.
빠른검색	등록된 신청서를 검색합니다.
조건검색	검색된 결과값에 대해서 조건을 통한 추가검색을 수행합니다.

2. 개별 신청서 대상 작업

개별 메일승인대기 신청서에 대해서는 관리자가 승인/거부 처리를 할 수 있습니다.

항목	설명
승인	승인 대기중인 신청서를 승인처리 합니다.
거부	승인 대기중인 신청서를 거부처리 합니다.

11.17 서비스 제어

정책서버에서 제공하는 서비스에 관련하여 오류가 발생하거나 문제점이 있을경우 물리적인 조치를 수행하기 이전에 서비스를 재구동을 수행할 수 있습니다.

1. 상단 패널에 **시스템** 으로 이동합니다.
2. 왼쪽 **시스템 관리** 항목에 **서비스 제어** 를 선택합니다.

11.17.1 정책적용을 통한 정책 동기화 수행

이벤트에 누락 및 초기화로 인하여 정책서버와 네트워크 센서가 정책이 동일하지 않을 경우 강제로 현재시점을 기준으로 정책을 동기화 할 수 있습니다.

- 정책적용 항목에서 **적용** 버튼을 선택합니다.

11.17.2 제공중인 모든 서비스 중지 기능

일반적인 서비스에 대한 중지부분은 네트워크 센서의 동작모드를 Inactive로 변경하거나 운영모드를 Monitoring으로 변경할 경우 가능합니다. 서비스 중지 기능은 위 설정을 적용하지 못하는 긴급한 사항이 발생할 경우 모든 네트워크 센서를 대상으로 적용할 수 있습니다.

- "현재 서비스가 동작중 입니다." 항목에서 **중지** 버튼을 선택합니다.

Note: 서비스 중지 기능을 Genian ZTNA에서 제공하는 모든 기능이 제공되지 않음으로 변경 시 충분한 검토가 필요합니다.

11.17.3 제공중인 Web 서비스 재구동 기능

Genian ZTNA에서 제공하는 웹 관련 서비스에 대한 문제점이 발생하거나 재구동이 필요한 사항이 발생할 경우 웹어플리케이션 재구동 기능을 사용할 수 있습니다.

- 웹 어플리케이션 재구동에서 항목을 지정 후 **재구동** 버튼을 선택합니다.

항목	설명
관리콘솔	정책서버 Web 콘솔 페이지를 지칭합니다.(Ex. *https://정책서버IP/mc2*)
CWP	정책서버에서 제공하는 Captive Web Portal 페이지를 지칭합니다.(EX. *http://정책서버IP/cwp*)
IP신청시스템	정책서버에서 제공하는 IP신청시스템 페이지를 지칭합니다.(Ex. *https://정책서버IP/ipmgmt3*)

11.18 정책서버 Web 콘솔을 통한 네트워크 센서 디버그 설정하기

기존 네트워크 센서 CLI 모드에서 개별적으로 설정해야 하는 디버그 설정을 정책서버 Web 콘솔에서 일괄 설정을 할 수 있습니다.

디버그 설정과 관련한 부분은 네트워크 센서의 하드디스크 유무에 따라서 다음과 같이 동작합니다.

Note: 5.0.27 버전 이상부터 사용가능하며 기존 설정을 유지하고자 할 경우 저장위치를 **선택안함** 을 사용합니다.

---

1. 상단 패널에 **시스템** 으로 이동합니다.
2. 왼쪽 **시스템** 항목에 **시스템 관리** 를 선택합니다.
3. 디버그 설정을 변경할 **네트워크 센서** 장비의 **체크박스** 를 선택합니다.(다수의 네트워크 센서 변경 시 대상 체크박스 모두 선택)
4. **작업선택** 항목에서 **장비 일괄 설정** 을 선택합니다.
5. **기타설정** 항목에서 **센서 디버그로그 생성** 체크박스를 선택한 후 설정을 **ON** 으로 변경합니다.
6. **저장위치** 를 선택합니다.
7. **실행** 버튼을 클릭합니다.

저장위치	네트워크 센서 데이터 디스크 유무	설명
선택안함	O or X	네트워크 센서에 설정된 사항을 기반으로 동작합니다.
로컬	O	네트워크 센서에 데이터 디스크에 저장
	X	정책서버 데이터 디스크에 저장
정책서버	O	정책서버 데이터 디스크에 저장
	X	정책서버 데이터 디스크에 저장
로컬 및 정책서버	O	네트워크 센서에 데이터 디스크와 정책서버의 데이터 디스크에 모두 저장
	X	정책서버 데이터 디스크에 저장

11.19 디버그 설정하기

11.19.1 정책서버 디버그 설정하기

Genian ZTNA 장비의 센터디버그를 개별 장비의 CLI 콘솔에 접속하여 설정합니다. 디버그 설정을 통해 Genian ZTNA 장비의 문제점을 사전에 확인하거나, 문제가 발생할 경우 발생원인을 파악할 수 있습니다. 디버그를 CLI 콘솔에서 설정하는 경우는 다음과 같습니다.

정책서버 센터 디버그 설정하기

정책서버 디버그 설정은 웹콘솔에서 설정을 지원하지 않음으로, CLI 모드에서 설정을 해야 합니다.

디버그 설정을 통해 Genian ZTNA 장비의 문제점을 사전에 확인하거나, 문제가 발생할 경우 발생원인을 파악할 수 있습니다.

CLI 콘솔에서 디버그 설정하기

CLI 콘솔접속 방법은 *CLI 콘솔* 문서를 참고해주시기 바랍니다.

1. Username, Password를 입력하여 CLI 콘솔 접속을 수행합니다.
2. **enable** 명령어를 통해 글로벌 구성모드를 활성화 합니다.
3. **configure terminal** 명령어을 통해 설정모드에 진입합니다.
4. `debug centerd all` 명령어를 입력하여 디버그를 활성화 합니다.
5. **show configuration** 명령어를 입력하여 디버그가 설정됨을 확인합니다. 해당 명령어는 Configuration 모드가 아닌 Genian 일반 CLI에서도 사용할 수 있습니다.

```
genian> enable
Password :
genian# configure terminal
genian(config)# debug centerd all
genian(config)# show configuration

#디버그가 정상적으로 설정된 경우
debug centerd category 0xffffffff
debug centerd field 0x31d
```

HA 구성 디버그 설정하기

Genian ZTNA에서 고가용성 기능을 제공하는 VRRP 프로토콜에 대한 디버그를 설정하여 정상적인 상태를 확인하거나, 문제점이 발생할 경우 원인을 파악할 수 있습니다.

CLI 콘솔접속 방법은 *CLI 콘솔* 문서를 참고해주시기 바랍니다.

CLI 콘솔에서 디버그 설정하기

1. **Username, Password** 를 사용하여 SSH 접속을 수행합니다.
2. **enable** 명령어를 통해 글로벌 구성모드를 활성화 합니다.
3. **configure terminal** 명령어을 통해 설정모드에 진입합니다.
4. **debug vrrpd all** 명령어를 입력하여 디버그를 활성화 합니다.
5. **show configure** 명령어를 입력하여 디버그가 설정됨을 확인합니다.

```
genian> enable
Password :
genian# configure terminal
genian(config)# debug vrrpd all
genian(config)# show configuration

```

(continues on next page)

(continued from previous page)

```
#디버그가 정상적으로 설정된 경우
debug vrrpd category 0xffffffff
debug vrrpd field 0x31d
```

Note: 정책서버 디버그 설정은 웹콘솔에서 설정을 지원하지 않음으로, CLI 모드에서 설정을 해야 합니다.

CLI 콘솔에서 디버그를 설정할 수 있는 대상

항목	설명
centerd	정책서버에 디버그를 설정하는 항목입니다.
sensord	네트워크 센서에 디버그를 설정하는 항목입니다.
vrrpd	이중화 관련 VRRP 디버그를 설정하는 항목입니다.

11.19.2 네트워크센서 디버그 설정하기

디버그 설정을 통해 네트워크 센서의 정상동작 여부와 문제점이 발생할 경우 원인파악 수단으로 활용할 수 있습니다. 네트워크 센서의 디버그 설정은 정책서버 Web콘솔에서 설정할 수 있습니다.

Note: 네트워크센서의 디버그는 Web콘솔에서 설정하는 것이 최우선순위로 적용됩니다.

11.20 IP 신청시스템 공지사항 작성하기

Genian ZTNA에서 사용할 수 있는 신청서 항목중에 IP신청시스템에 공지사항을 등록할 수 있습니다.

IP신청서를 작성함에 사용자 고려사항 및 알림사항을 표시하여 신청시스템을 편하게 사용할 수 있도록 도움을 줄 수 있습니다.

11.20.1 공지사항 작성하기

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **환경설정** 항목에서 **IP관리 > IP신청시스템공지사항** 을 선택합니다.
3. **작업선택** 항목에서 **생성** 을 선택합니다.
4. 공지사항 항목을 입력 후 **생성** 버튼을 클릭합니다.

11.20.2 공지사항 최초 접속화면 설정하기

IP신청시스템에 접속할 경우 최초 표시되는 화면을 공지사항으로 설정하여 사용자가 신청서를 작성함에 유의해야 하는 사항을 사전에 확인하도록 합니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **환경설정** 항목에서 **IP관리** 를 선택합니다.
3. **IP신청시스템 화면설정** 항목에서 **최초접속화면** 을 **공지사항** 으로 선택합니다.
4. **수정** 버튼을 클릭합니다.

11.21 시스템에서 제공하는 메시지 변경하기

Genian ZTNA 시스템에서 표시되는 다국어(한글, 영어, 중국어) 메시지에 대한 변경 기능을 제공합니다.

메시지 변경 기능을 사용하여 고객사 환경에 맞는 단어와 문구를 삽입하거나, 전체 메시지 문구를 변경할 수 있습니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **접속인증페이지(CWP)** 항목에 **메시지관리** 를 선택합니다.
3. 변경하고자 하는 **메시지 ID** 를 클릭합니다.
4. 변경하고자 하는 **언어** 에 해당하는 **메시지 내용** 을 수정합니다.
5. **수정** 버튼을 클릭합니다.

11.21.1 메시지 분류 확인

메시지의 분류로는 시스템 메시지와 적용모드 설정 메시지로 나눌수 있으며 각각 다음과 같이 사용할 수 있습니다.

분류	설명
시스템 메시지	사용 여부를 선택할 수 없으며, 메시지 내용만 변경가능
적용모드 설정 메시지	사용 여부를 선택할 수 있으며, 메시지 내용도 변경가능

11.21.2 메시지 카테고리 확인

메시지를 구분하는 카테고리는 다음과 같습니다.

카테고리	설명
관리콘솔	Web 콘솔에서 제공하는 신청과 시스템 메시지입니다.
CWP	CWP 페이지에서 제공하는 노드 상태관련 메시지입니다.
에이전트	에이전트 팝업 알림창에서 제공하는 메시지입니다.
감사기록	정책서버 감사기록에서 제공하는 메시지입니다.
알림	사용자 인증과 관련된 알림 메시지입니다.

11.22 윈도우 업데이트 목록 자동 승인하기

Genian ZTNA에서 윈도우 업데이트 정책을 적용하기 위해서는 단말에 적용할 업데이트 목록 설정이 필요합니다.

윈도우 업데이트 목록 설정 이후 신규 업데이트 대상에 대해서 자동으로 승인되어 업데이트 목록에 추가되게 됩니다.

1. 상단 패널에 **정책** 으로 이동합니다.
2. 왼쪽 **정책** 항목에서 **Windows 업데이트 정책** 을 선택합니다.
3. **작업선택** 메뉴에서 **생성** 을 클릭합니다.
4. 업데이트 대상 **제품** 과 **분류** 항목에 **체크박스** 를 선택합니다. (다수 제품/분류 선택 가능)
5. **생성** 버튼을 클릭합니다.

Note: **승인유보기간** 설정은 신규 업데이트가 발생할 경우 자동으로 관리자 승인대상으로 변경할 대기기간을 이야기 합니다.(0 설정 시 즉시 관리자 승인으로 처리)

11.22.1 윈도우 업데이트 제품 목록

다음 항목에 제품에 대해서 업데이트 기능을 제공합니다.

항목	세부제품
오피스	Office 2003, Office 2007, Office 2010, Office 2013, Office 2016, Office XP
서버	Windows Server 2003, Windows Server 2003 Datacenter Edition, Windows Server 2008
	Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2
	Windows Server 2016, Windows Server 2019, Windows Server 2019 and later Servicing Drivers
	Windows Server 2019 and later Upgrade & Servicing Drivers
Windows 10 OS	Windows 10, Windows 10 LTSB, Windows 10 S and Later Servicing Drivers
	Windows 10 S Version 1803 and Later Servicing Drivers, Windows 10 S Version 1803 and Later Upgrade & Servicing Drivers
	Windows 10 S version 1809 and later Servicing Drivers, Windows 10 S version 1809 and later Upgrade & Servicing Drivers
	Windows 10 S version 1903 and later Servicing Drivers, Windows 10 S version 1903 and later Upgrade & Servicing Drivers
	Windows 10 version 1803 and Later Servicing Drivers, Windows 10 Version 1803 and Later Upgrade & Servicing Drivers
	Windows 10 version 1809 and later Servicing Drivers, Windows 10 version 1809 and later Upgrade & Servicing Drivers
	Windows 10 version 1903 and later, Windows 10 version 1903 and later Servicing Drivers
	Windows 10 version 1903 and later Upgrade & Servicing Drivers
Windows Other OS	Windows 2000, Windows 7, Windows 8, Windows 8.1
	Windows Vista, Windows Vista Dynamic Installer, Windows Vista Ultimate Language Packs
	Windows XP, Windows XP 64-Bit Edition 2003 버전, Windows XP x64 Edition
Other Tool	Microsoft Defender Antivirus, Windows Internet Explorer 7 Dynamic Installer
	Windows Internet Explorer 8 Dynamic Installer, Windows Media Dynamic Installer
	Windows Ultimate Extras

11.22.2 윈도우 업데이트 분류 목록

다음 항목으로 분류된 업데이트 기능을 제공합니다.

분류	설명
기능팩	제품 릴리스의 컨텍스트 외부에서 처음 배포되어 일반적으로 다음 전체 제품 릴리스에 포함된 새로운 제품 기능입니다.
도구	작업 또는 작업 집합을 완료하는 데 도움이 되는 유틸리티 또는 기능입니다.
보안 업데이트	제품별 보안 관련 취약점을 위해 널리 배포되는 수정 프로그램입니다. 보안취약성은 심각도에 의해 평가됩니다. 심각도 등급은 Microsoft 보안 공지에 중요, 중요, 보통 또는 낮음으로 나타냅니다.
서비스팩	모든 핫픽스, 보안 업데이트, 중요 업데이트 및 업데이트의 테스트된 누적 집합입니다. 또한 서비스 팩에는 제품 릴리스 이후 내부적으로 발견된 문제에 대한 추가 수정이 포함될 수 있습니다. 서비스 팩에는 고객이 요청한 제한된 수의 디자인 변경 또는 기능도 포함될 수 있습니다.
업데이트	특정 문제를 해결하기 위해 널리 릴리스된 수정입니다. 업데이트는 위험하지 않은 비보안 관련 버그를 해결합니다.
업데이트 롤업	간편한 배포를 위해 함께 패키지된 테스트된 누적 핫픽스, 보안 업데이트, 중요 업데이트 및 업데이트 집합입니다. 롤업은 일반적으로 특정 영역을 대상으로 합니다.
정의 업데이트	제품의 정의 데이터베이스에 대한 추가 기능을 포함하는 널리 출시되고 자주 사용되는 소프트웨어 업데이트입니다. 정의 데이터베이스는 종종 악성 코드, 피싱 웹 사이트 또는 정크 메일과 같은 특정 특성을 가지고 있는 개체를 검색하는 데 사용됩니다.
중요 업데이트	보안과 관련되지 않은 중요한 버그를 해결하는 특정 문제를 해결하기 위해 널리 릴리스된 수정입니다. |

11.23 윈도우 업데이트 목록 수동 설정하기

Genian ZTNA에서 윈도우 업데이트 정책을 적용하기 위해서는 단말에 적용할 업데이트 목록 설정이 필요합니다.

11.23.1 윈도우 업데이트 목록 수동 승인하기

윈도우 업데이트 목록 설정 이후 목록에 포함되지 않은 업데이트 항목에 대해서 수동으로 승인하여 업데이트 목록에 추가할 수 있습니다.

1. 상단 패널에 **정책** 으로 이동합니다.
2. 왼쪽 **정책** 항목에서 **Windows 업데이트 정책** 을 선택합니다.
3. 생성되어 있는 **업데이트 정책 ID** 를 클릭합니다.
4. **업데이트 설정** 탭을 클릭합니다.
5. **설치승인상태** 가 **설치미승인(자동)** 항목 중 업데이트 목록에 포함할 업데이트에 체크박스를 선택합니다.
6. **작업선택** 메뉴에서 **설치승인(관리자)** 를 선택합니다.
7. **설정 확인 팝업창** 에 **확인** 버튼을 클릭합니다.

11.23.2 윈도우 업데이트 목록 수동 미승인하기

윈도우 업데이트 목록 설정 이후 목록에 포함된 업데이트 항목에 대해서 수동으로 미승인하여 업데이트 목록에서 제거할 수 있습니다.

1. 상단 패널에 **정책** 으로 이동합니다.
2. 왼쪽 **정책** 항목에서 **Windows 업데이트 정책** 을 선택합니다.
3. 생성되어 있는 **업데이트 정책 ID** 를 클릭합니다.
4. **업데이트 설정** 탭을 클릭합니다.
5. **설치승인상태** 가 **설치승인(자동)** 항목 중 업데이트 목록에 포함할 업데이트에 체크박스를 선택합니다.
6. **작업선택** 메뉴에서 **설치미승인(관리자)** 를 선택합니다.
7. **설정 확인 팝업창** 에 **확인** 버튼을 클릭합니다.

11.24 기타 설정에서 외부 서버 접속 설정하기

정책서버에서 외부 서버(업데이트 서버, 메일서버, SMS 서버)로의 접속에 대한 기본설정을 수행할 수 있습니다.

항목	설명
인터넷 연결	시스템에 최신 데이터를 유지하기 위한 외부 업데이트 센터 접속 유무를 설정합니다.
센터 Domain Name	정책서버 관리자 페이지 접속 시 IP가 아닌 도메인으로 접속할 경우 설정합니다.
센터 NAT IP	정책서버가 NAT 로 설정되어 외부에서 정책서버로 접속할 수 있는 IP를 설정합니다.

11.24.1 메일서버 설정하기

관리자의 메일 알림이나 신청시스템에서 메일 알림 기능을 사용할 경우 전송할 수 있는 서버를 설정합니다.

Note: 메일서버 설정 부분은 다음에 외부 전송 이메일 서버 설정 참고하시기 바랍니다.

11.24.2 SMS 설정

관리자의 SMS 알림이나 신청시스템에서 SMS 알림 기능을 사용할 경우 전송할 SMS 서비스 항목을 설정합니다.

항목	설명
사용안함	SMS 서비스를 사용하지 않도록 설정합니다.
국내 SMS	1. ZTNA에서 제공하는 SMS 서비스를 사용하도록 설정합니다.(500건/월) 2. 국내 SMS 서비스일 경우 발신번호를 변경할 수 있습니다.
국제 SMS	해외에서 SMS 서비스(AWS SMS)를 사용하도록 설정합니다.(500건/월)

11.24.3 운영정보 데이터 설정

시스템에서 운영정보를 데이터에 최신 버전을 확인할 시간을 설정합니다.

Note: 운영정보 데이터 관련사항은 다음에 시스템 업데이트 관리 참고하시기 바랍니다.

11.24.4 구글 API 클라이언트 ID 및 인증키 설정

구글 메일서버를 사용하거나 정보동기화 시 구글 G Suite와 연동하기 위하여 API를 사용할 수 있는 계정과 인증코드를 설정합니다.

Note:

1. 구글 G Suite 연동 부분은 다음에 *Google G Suite* 참고하시기 바랍니다.
2. 구글 메일서버 연동 부분은 다음에 외부 전송 이메일 서버 설정 참고하시기 바랍니다.

11.25 컴플라이언스 정책 설정하기

컴플라이언스(compliance)는 통상 법규준수/ 준법감시/ 내부통제 등의 의미로 사용되며, ZTNA에서 컴플라이언스는 내부통제에 대상을 노드그룹으로 생성하여 해당 노드그룹에 포함된 대상을 표현하는 역할을 수행합니다.

Note: 컴플라이언스 정책은 단말 제어를 수행하지 않습니다. 제어와 관련한 부분은 다음에 접근제어 정책의 이해 참고하시기 바랍니다.

11.25.1 컴플라이언스 정책 생성하기

1. 상단 패널에 **정책** 으로 이동합니다.
2. **정책** 메뉴에서 **컴플라이언스 정책** 을 선택합니다.
3. **작업선택** 항목에서 **생성** 을 클릭합니다.

항목	설명
기본설정	정책을 구별하는 ID 및 설명을 설정합니다.
조건설정	내부통제와 관련된 노드그룹을 지정합니다.

노드그룹 생성 시 내부통제와 관련된 조건을 기반으로 노드그룹을 생성합니다.

Note: 노드그룹 생성과 조건 부분은 다음에 노드그룹 상세정보 부분을 참고하시기 바랍니다.

11.25.2 컴플라이언스 정책 현황 확인하기

컴플라이언스 정책에 해당 하는 대상에 정보(IP, MAC, 사용자, 만족현황, 조건)를 확인할 수 있습니다.

1. 상단 패널에 **관리>노드** 로 이동합니다.
2. 왼쪽 **현황 & 필터** 항목에 **컴플라이언스 정책** 을 선택합니다.

11.26 CWP 페이지 환경설정

다음에 환경을 설정하여 CWP 페이지를 사용할 수 있습니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **접속인증페이지(CWP)** 항목에서 **CWP설정** 을 선택합니다.
3. 변경하고자 하는 기능에 설정을 변경합니다.
4. **수정** 버튼을 클릭합니다.

항목	설명
IP관리 메시지 우선	IP관리 차단대상에 대한 별도의 메시지 표시 기능을 사용합니다.
지원언어	CWP 페이지에서 표시할 수 있는 언어를 설정합니다.
타임존 변경알림	ZTNA 시스템과 사용자 시스템의 타임존이 일치하지 않을 경우 알람 표시 기능을 사용합니다.
CWP 도메인 설정	CWP 페이지에 표시되는 URL을 도메인 형태로 변경합니다.
CWP SSL 사용	CWP 페이지를 HTTPS로 변경합니다.
세션 타임아웃	CWP 페이지의 세션 유지 시간을 설정합니다.
CWP 접근 허용그룹	CWP 페이지를 표시할 대상을 설정합니다.

11.26.1 1. CWP 페이지 SSL 사용 기능

HTTP의 보안 문제로 HTTPS를 사용해야 할 경우 다음과 같이 설정을 변경하여 적용할 수 있습니다.

Note:

1. ZTNA 서버의 SSL 인증서가 등록되지 않을 경우 신뢰되지 않은 연결과 관련한 보안 경고페이지가 우선 표시됩니다.
2. SSL 인증서 등록 부분은 다음에 *WEB 콘솔 접속 시 SSL 인증서 오류창 발생* 참고하시기 바랍니다.

11.26.2 2. IP관리 메시지 우선 표시 기능

IP관리 차단(IP차단, MAC차단, IP/MAC 차단, 변경금지 위반) 대상이 CWP 접속 시 IP관리 메시지를 우선적으로 표시하도록 합니다.

Note: IP관리 상태가 허용으로 변경된 이후에는 일반적인 CWP 페이지가 표시됩니다.

대상	설정값	표시메시지
IP관리 차단	ON	IP관리 메시지
	OFF	일반메시지 + IP관리 메시지
IP관리 허용	ON	일반메시지
	OFF	일반메시지

11.27 토큰기반 정책서버 접속 설정하기

11.27.1 토큰 미사용 센서 차단 기능

다음에 환경을 설정하여 정책서버에서 인가된 센서만 정책서버에 접속할 수 있게 만들 수 있습니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **환경설정** 항목에서 **노드 관리** 을 선택합니다.
3. **센서 토큰** 탭에서 **토큰 미사용 센서 차단** 을 **ON** 으로 변경합니다.
4. **수정** 버튼을 클릭합니다.

항목	설명
토큰	센서장비 CLI 에서 node-server token 명령에 사용하는 토큰값 입니다.
토큰(NAT)	센서가 NAT 예외대역에서 동작해야하는 경우 node-server token 명령에 사용하는 토큰값 입니다.

Note:

1. 토큰 미사용 센서 차단 기능을 사용하는 경우 정책서버에서 인증되지 않는 토큰을 사용하거나 토큰을 사용하지 않는 센서는 정책서버로 접속이 불가합니다.
2. 토큰정보에는 정책서버 접속정보가 들어가 있습니다.
3. 토큰 미사용 센서 차단 기능을 사용하지 않고 토큰을 센서에 설정하는 경우 센서는 토큰에 포함된 정책서버 접속주소를 이용하여 정책서버에 접속합니다.

11.27.2 토큰 미사용 에이전트 차단 기능

다음에 환경을 설정하여 정책서버에서 인가된 센서만 정책서버에 접속할 수 있게 만들 수 있습니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **환경설정** 항목에서 **에이전트** 을 선택합니다.
3. **기본설정** 탭에서 **토큰 미사용 에이전트 차단** 을 **ON** 으로 변경합니다.
4. **수정** 버튼을 클릭합니다.

항목	설명
토큰	에이전트 설치 시 사용하는 토큰값 입니다.
토큰(NAT)	에이전트가 NAT 예외대역에서 동작해야하는 경우 설치 시 사용하는 토큰값 입니다.

Note:

1. 토큰 미사용 에이전트 차단 기능을 사용하는 경우 정책서버에서 인증되지 않는 토큰을 사용하거나 토큰을 사용하지 않는 에이전트는 정책서버로 접속이 불가합니다.
2. 토큰정보에는 정책서버 접속정보가 들어가 있습니다.
3. 토큰 미사용 에이전트 차단 기능을 사용하지 않고 토큰을 에이전트에 설정하는 경우 에이전트는 토큰에 포함된 정책서버 접속주소를 이용하여 정책서버에 접속합니다.

11.28 관리자 Locale

- Locale은 Top 메뉴 영역에서 변경할 수 있습니다.
- 출력되는 Locale은 설정 > 환경설정 > 관리콘솔 > 관리화면 지원언어에서 설정할 수 있습니다.

CHAPTER

TWELVE

API 가이드

Genian ZTNA는 정책서버로 부터 원하는 정보를 얻거나 보안정책 및 각종 객체들을 설정하기 위한 REST API를 제공합니다. 외부에서 정책서버로 API를 호출하기 위해서는 API Key가 필요합니다. API Key는 각 관리자별로 생성되며 관리자에 부여된 권한에 따라 정보에 접근하거나 설정할 수 있게 됩니다.

관리자 API Key를 생성하거나 확인하기 위해서는 다음과 같이 합니다.

1. 상단 패널에서 **관리 > 사용자** 로 이동
2. 좌측 패널에서 **전체관리자** 를 선택
3. API Key를 생성할 **관리자명** 을 클릭
4. **로그인 설정 > API Key** 에서 **신규 키 생성** 버튼 클릭
5. **수정** 클릭

위 과정을 통해 설정된 API Key는 다음과 같이 Request URL의 파라메터로 전달되어야 합니다.

```
curl -X GET "https://nac.company.com/mc2/rest/logs?apiKey={API Key}"
```

좀 더 자세한 사용법은 *REST API* 활용 가이드 를 참고하시기 바랍니다.

Genian ZTNA에서 제공되는 API의 목록은 아래에서 확인할 수 있습니다.

- API Reference Guide for Enterprise Edition
- API Reference Guide for MSSP

12.1 REST API 활용 가이드

12.1.1 가이드 개요

Genian ZTNA는 타 장비 또는 타 시스템 등과의 연동을 위해 단말 정보의 제공, 정책/객체의 생성, 설정변경 등이 가능하도록 REST API를 제공합니다.

본 가이드는 V5.0 기준으로 작성되었으며, Genian ZTNA의 REST API를 활용하기 위한 요구사항, 인증 방법, 주요 API 등에 대한 안내를 목적으로 합니다.

유튜브를 통해 REST API 활용 가이드 동영상을 확인할 수 있습니다. 

12.1.2 사전 준비사항

Genian ZTNA 활용 사전 준비사항

외부 장비에서 Genian ZTNA로 REST API를 호출하기 위해서 인증이 필요하며, 인증을 위한 API 인증방식을 'API Key' 또는 'API 서비스 계정' 방식 중에서 선택하고, 그 값을 생성합니다.

API Key

- API Key방식은 연동을 위한 계정의 API키를 생성하여 Genian ZTNA의 API를 호출할 때 마다 API-Key를 첨부하여 활용하는 방식입니다.
- 각 계정 별로 별도로 생성하여 활용이 가능합니다. 호출의 권한은 해당 계정의 권한에 종속됩니다.
- 자세한 내용은 *API Key*를 이용한 상호 인증 방법 을 참고하시기 바랍니다.

API 서비스 계정

- API 서비스계정을 활용하는 방식은 연동을 위한 별도의 계정을 생성하여 활용하는 방식입니다.
- 호출 건 마다 API-Key를 첨부하여 활용하는 API-Key 방식과 달리 하나의 단위로 구현되어 API 서비스 계정으로 Genian ZTNA로 Log-in 후 기능을 수행합니다.
- 이 후 Log-off 절차까지 구현하는 방식으로 단순한 정보 확인 등을 위한 단편적인 기능 보다는 하나의 기능으로 구현하고자 할 때 유리한 방식입니다.
- API 서비스계정은 Web콘솔 접속용 계정으로는 활용할 수 없습니다.
- 자세한 내용은 *API* 서비스계정을 이용한 상호 인증 방법 을 참고하시기 바랍니다.

Networking 사전 준비사항

Genian ZTNA에서 제공하는 REST API는 https 프로토콜(TCP/8443)로 접속합니다.

TCP/8443 포트는 Web콘솔 접속용 포트와 동일합니다. 따라서, 방화벽 등에서 Genian ZTNA Web콘솔 접속을 위한 설정이 적용된 상태라면, 추가 작업은 하지 않으셔도 됩니다.

12.1.3 API 활용을 위한 상호 인증 방법

Genian ZTNA와 연동 대상 장비 간의 보안성이 확보된 상태에서 REST API를 활용하기 위해, 상호 인증 수행이 우선 진행되어야 합니다.

Genian ZTNA는 2가지의 인증 방식(API Key, API 서비스계정)을 제공하며, REST API를 활용하기 위해서는 Request URL 문이나 curl 명령이 필요합니다.

curl 생성 및 테스트 방법은 참고 - *API* 활용도구 제공: *Swagger* 를 참고하시기 바랍니다.

Note:

- curl 을 통한 API 호출은 Ubuntu Terminal, Windows Command 등 에서 가능합니다.
- curl 을 활용하여 API 호출 시, SSL 오류(신뢰되지 않은 인증서의 경우)가 발생하면 k 옵션(URL에 대한 SSL 검증을 하지 않도록 설정)을 추가하여 적용 하시기 바랍니다. (옵션 변경 : -X -> -kX)
  - 예시 : curl -X POST https://{정책서버IP}/mc2/rest/{API Path} **-->** curl -kX POST https://{정책서버IP}/mc2/rest/{API Path}

API Key를 이용한 상호 인증 방법

API Key를 이용한 방법은 사전에 상호간 합의된 Key값을 통해 API를 호출하여 사용할 수 있습니다.

API Key는 각 관리자 계정 별로 생성되며, 계정과 동일한 권한으로 API를 호출합니다.

Warning:

- **API Key 유출 시, 시스템의 정보가 노출될 수 있으니 주의하시기 바랍니다. 또한 보안을 위해 주기적으로 변경하는 것을 권장드립니다.**

1단계. API Key 생성

1. Genian ZTNA Web콘솔 접속 후 **관리 > 사용자** 메뉴 클릭
2. API Key를 사용할 **관리자 계정** 클릭
3. **기본정보 > 로그인 설정 > API 키** 항목으로 이동
4. **신규 키 생성** 버튼을 클릭하여 해당 계정의 API Key 생성

2단계. API Key를 활용한 인증

1. 사용하려는 curl에서 API Path가 끝나는 부분에 **?apiKey={003def2d-4326-4a40-8372-e7806ce5950f}** 와 같이 생성했던 API Key 입력
2. curl을 활용하여 API 호출 테스트 진행

- curl 예시

```
curl -kX POST "https://192.168.100.253:8443/mc2/rest/nodes?apiKey=
↪{003def2d-4326-4a40-8372-e7806ce5950f}"
-H "accept: application/json;charset=UTF-8" -H "Content-Type:␣
↪application/json;charset=UTF-8"
-d "[ { \"nl_ipstr\": \"100.100.100.101\", \"nl_mac\": \
↪"00:00:00:00:00:00\", \"nl_sensornid\": \"\", \"nl_genidev\": 0, \
↪"doNotDeleteNode\": true }]"
```

Note:

- REST API는 Request URL과 Get Parameter부분을 구분하기 위해 **"?"** 구분자를 사용합니다. Request URL이 끝난 부분 이후 구분자를 2개 이상 사용하게 되면 정상적으로 인식 되지 않습니다.
- REST API 사용 시 Get Parameter 에 다른 Parameter 값이 존재할 때, 값이 끝나는 부분에 **"&"** 를 이용하여 apiKey를 추가하면 정상적으로 동작됩니다.
  - 예 시 : curl -kX GET "https://192.168.100.253:8443/mc2/rest/tags?page=1&pageSize=30&apiKey={912fae69-b454-4608-bf4b-fa142353b463}" -H "accept: application/json;charset=UTF-8"

API 서비스계정을 이용한 상호 인증 방법

API 서비스계정을 이용한 인증방법은 API를 활용하기 위한 전용 계정을 추가하여 사용하는 방법입니다.

1단계. 서비스역할 생성

1. 서비스역할 생성 방법은 시스템 보안과 관련하여 별도의 관리가 필요하므로, **API 서비스역할(권한)** 생성을 요청해 주시면, 기술지원 담당자가 별도로 안내해 드리도록 하겠습니다.

2단계. API 서비스를 위한 계정에 서비스 역할 부여

1. Genian ZTNA Web콘솔 접속 후 **관리 > 사용자** 메뉴 클릭
2. API 서비스계정으로 사용할 **계정** 클릭
3. **기본정보 > 기본설정 > 관리역할** 항목으로 이동
4. 생성 요청을 통해 만들어 두었던 **API 서비스역할** 권한 부여

3단계. IP 패턴 또는 URL 패턴 설정

1. **API 서비스역할** 권한을 부여한 **계정** 클릭
2. **기본정보 > 관리역할별 설정 > 신뢰연결 설정** 항목으로 이동
3. API 호출을 허용할 **IP** 또는 **URL** 에 대해 패턴 설정

> **Warning:**
>
> - 보안상의 문제가 발생할 수 있으므로, IP 패턴 설정 시 **Subnet과 Range 설정은 불가합니다.**

4단계. API 서비스계정을 활용한 인증

1. curl을 활용하여 API 호출 테스트 진행 (API 서비스계정은 **API Key 없이 호출이 가능합니다.**)

- curl 예시

```
curl -kX POST "https://192.168.100.253:8443/mc2/rest/nodes"
-H "accept: application/json;charset=UTF-8" -H "Content-Type:␣
↪application/json;charset=UTF-8"
-d "[ { \"nl_ipstr\": \"100.100.100.102\", \"nl_mac\": \
↪"11:11:11:11:11:11\", \"nl_sensornid\": \"\", \"nl_genidev\": 0, \
↪"doNotDeleteNode\": true }]"
```

12.1.4 주요 API

Genian ZTNA와 연동을 위한 주요 API 항목은 NODES, TAGS, USERS, LOGS, NODEGROUPS, CVES 등이 있고, 각각의 내용은 다음과 같습니다.

NODES API

Genian ZTNA에서 노드(Node)란 IP 와 MAC 을 갖고 있는 장비 또는 엔드포인트를 말합니다.

노드는 ZTNA에서 관리하는 네트워크 대역대에 접속하거나 노드에 설치된 에이전트에 의해 자동으로 등록됩니다.

노드와 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
전체 노드 목록 및 정보 조회	GET	/nodes	특정 노드의 정보 조회 및 태그 할당, 제거를 수행하기 위해서 노드의 ip 및 nodeId를 얻기 위한 목적으로 전체 노드 목록 및 정보를 조회합니다.
특정 IP의 노드 정보 조회	GET	/nodes/{ip}/managementscope	특정 노드에 태그 할당 및 제거를 위해 전달받은 특정 IP에 대해서 nodeId 값을 얻기 위한 목적으로 사용됩니다.
특정 노드에 태그 할당	POST	/nodes/{nodeId}/tags	위협 노드로 판단되는 특정노드에 차단 태그를 할당하여 네트워크 격리를 수행하기 위한 목적으로 사용됩니다.
특정 노드에 태그 해제	DELETE	/nodes/{nodeId}/tags	안전하다고 판단되는 특정노드에 차단 태그를 제거하여 네트워크 진입을 허용하기 위한 목적으로 사용됩니다.
특정 노드의 상세 정보 조회	GET	/nodes/{nodeId}/information/{category}	IT 관리를 위해 특정 노드의 열린 포트 목록을 얻기 위한 목적으로 사용됩니다.

- 전체 노드 목록 및 정보 조회 예시

```
curl -kX GET "https://192.168.100.100:8443/mc2/rest/nodes?page=1&
↪pageSize=30&view=node&nid=All
&apiKey={912fae69-b454-4608-bf4b-fa142353b463}" -H "accept:␣
↪application/json;charset=UTF-8"
```

- 특정 IP의 노드 정보 조회 예시

```
curl -kX GET "https://192.168.100.100:8443/mc2/rest/nodes/192.168.
↪100.200/managementscope
?apiKey={912fae69-b454-4608-bf4b-fa142353b463}" -H "accept:␣
↪application/json;charset=UTF-8"
```

- 특정 노드에 태그 할당 예시

```
curl -kX POST "https://192.168.100.100:8443/mc2/rest/nodes/
↪974bc18c-2cf9-103a-8002-2cf05d0cf498-c0649e1c
/tags?apiKey={912fae69-b454-4608-bf4b-fa142353b463}" -H "accept:␣
↪application/json;charset=UTF-8"
-H "Content-Type: application/json;charset=UTF-8" -d "[ { \"id\":␣
↪\"\", \"name\": \"test_tag\",
\"description\": \"\", \"startDate\": \"\", \"expireDate\": \"\",␣
↪\"periodType\": \"\", \"expiryPeriod\": \"\" }]
```

- 특정 노드에 태그 해제 예시

```
curl -kX DELETE "https://192.168.100.100:8443/mc2/rest/nodes/
↪974bc18c-2cf9-103a-8002-2cf05d0cf498-c0649e1c
/tags?apiKey={912fae69-b454-4608-bf4b-fa142353b463}" -H "accept:␣
↪application/json;charset=UTF-8"
-H "Content-Type: application/json;charset=UTF-8" -d "[ \"5\"]"
```

- 특정 노드의 상세 정보 조회 예시

```
curl -kX GET "https://192.168.100.100:8443/mc2/rest/nodes/
↪974bc18c-2cf9-103a-8002-2cf05d0cf498-c0649e1c
/information/CAT_NETINFO?apiKey={912fae69-b454-4608-bf4b-
↪fa142353b463}" -H "accept: application/json;charset=UTF-8"
```

TAGS API

Genian ZTNA는 노드/사용자를 분류할 때 태그(Tag)를 사용할 수 있습니다. (디폴트 Tag로는 TRUSTED, THREAT, GUEST가 있고, 수정 및 추가가 가능합니다.)

외부장비에서 연동으로 ZTNA 제어정책 적용 시 노드그룹을 구분하기 위해 Tag가 사용됩니다.

태그와 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
태그 목록 조회	GET	/tags	노드, 사용자ID에 태그 할당 및 제거를 수행하기 위해 태그의 id값 혹은 name 정보를 얻기 위한 목적으로 태그의 정보를 조회합니다.
태그 생성	POST	/tags	관리자가 노드 혹은 사용자ID에 부여하려는 태그 항목이 Genian ZTNA에 존재하지 않을 시 태그 생성을 위한 목적으로 사용됩니다.

- 태그 목록 조회 예시

```
curl -kX GET "https://192.168.100.100:8443/mc2/rest/tags?page=1&
↪pageSize=30&apiKey={912fae69-b454-4608-bf4b-fa142353b463}"
-H "accept: application/json;charset=UTF-8"
```

- 태그 생성 예시

```
curl -kX POST "https://192.168.100.100:8443/mc2/rest/tags?apiKey=
↪{912fae69-b454-4608-bf4b-fa142353b463}"
-H "accept: application/json;charset=UTF-8" -H "Content-Type:␣
↪application/json;charset=UTF-8"
-d "{ \"np_idx\": 0, \"np_name\": \"test_tag\", \"np_desc\": \
↪"테스트 태그\",\"np_periodtype\": 0,
\"np_period\": \"\", \"np_periodexpire\": \"\", \"np_adminroles\
↪": \"\", \"np_color\": \"\", \"np_static\": 0}"
```

USERS API

Genian ZTNA의 사용자(User)는 관리자가 생성하거나 DB 동기화 등을 통하여 생성된 사용자 및 부서정보를 의미합니다.

사용자와 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
특정 사용자ID에 적용된 태그 목록 조회	GET	/users/{userId}/tags	특정 사용자ID에 적용된 태그의 목록을 조회하여 태그 할당 및 제거하기 위한 목적으로 tagid값 혹은 name 정보를 조회합니다.
특정 사용자ID에 태그 할당	POST	/users/{userId}/tags	인가되지 않은 특정 사용자ID에 차단 태그를 할당하여 네트워크 격리를 수행하기 위한 목적으로 사용됩니다.
특정 사용자ID에 태그 해제	DELETE	/users/{userId}/tags	인가된 특정 사용자ID에 차단 태그를 제거하여 네트워크 진입을 허용하기 위한 목적으로 사용됩니다.

- 특정 사용자ID에 적용된 태그 목록 조회 예시

```
curl -kX GET "https://192.168.100.100:8443/mc2/rest/users/test1/
```

(continues on next page)

(continued from previous page)

```
↪tags?apiKey={912fae69-b454-4608-bf4b-fa142353b463}"
-H "accept: application/json;charset=UTF-8"
```

- 특정 사용자ID에 태그 할당 예시

```
curl -kX POST "https://192.168.100.100:8443/mc2/rest/users/test1/
↪tags?apiKey={912fae69-b454-4608-bf4b-fa142353b463}"
-H "accept: application/json;charset=UTF-8" -H "Content-Type:␣
↪application/json;charset=UTF-8"
-d "[ { \"id\": \"\", \"name\": \"test_tag\", \"description\": \"\
↪", \"startDate\": \"\",
\"expireDate\": \"\", \"periodType\": \"\", \"expiryPeriod\": \"\
↪" }]"
```

- 특정 사용자ID에 태그 해제 예시

```
curl -kX DELETE "https://192.168.100.100:8443/mc2/rest/users/
↪test1/tags?apiKey={912fae69-b454-4608-bf4b-fa142353b463}"
-H "accept: application/json;charset=UTF-8" -H "Content-Type:␣
↪application/json;charset=UTF-8" -d "[ \"5\"]
```

LOGS API

Genian ZTNA에서 감사로그란 시스템, 장비 등에서 발생하는 이벤트에 대한 모든 로그를 뜻하며, 자체적으로 로그서버에 저장합니다.

로그와 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
감사로그 조회	GET	/logs	대시보드 및 이벤트 현황 작성에 활용하기 위한 목적으로 Genian ZTNA의 감사로그를 조회합니다.

- 감사로그 조회 예시

```
curl -kX GET "https://192.168.100.100:8443/mc2/rest/logs?page=1&
↪pageSize=30&logschema=auditlog&periodType=custom
&apiKey={912fae69-b454-4608-bf4bfa142353b463}"-H "accept:␣
↪application/json;charset=UTF-8"
```

NODEGROUPS API

Genian ZTNA의 정책(Policy)은 노드정책과 제어정책으로 구분되며 정책적용을 위해서는 노드그룹이 필요합니다.

노드그룹과 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
노드그룹 목록 조회	GET	/node-groups	대시보드 및 보안 운영 보고서 작성에 활용하기 위한 목적으로 Genian ZTNA에 생성되어 있는 노드그룹 목록을 조회합니다.

- 노드그룹 목록 조회 예시

```
curl -kX GET "https://192.168.100.100:8443/mc2/rest/nodegroups?
```

(continues on next page)

(continued from previous page)

```
↪page=1&pageSize=30&
apiKey={912fae69-b454-4608-bf4b-fa142353b463}" -H "accept:␣
↪application/json;charset=UTF-8"
```

CVES API

Genian ZTNA는 각 노드별로 공개적으로 알려진 정보 보안 취약성 및 노출에 대한 정보를 제공합니다.

CVES와 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
노드의 CVE 내역 조회	GET	/cves	위험노드에 네트워크 격리를 수행하기 위한 목적으로 Genian ZTNA에서 노드의 CVE 내역을 조회합니다.

- 노드의 CVE 내역 조회 예시

```
curl -kX GET "https://192.168.100.100:8443/mc2/rest/cves?page=1&
↪pageSize=30
&apiKey={912fae69-b454-4608-bf4b-fa142353b463}" -H "accept:␣
↪application/json;charset=UTF-8"
```

12.1.5 RESPONSES CODE

아래 표는 REST API에서 사용하는 HTTP Status Codes를 나타냅니다.

Code	Descriptions	Detailed Descriptions
200	Successful operation	요청 정상 처리
206	Partial Content	Range가 지정된 요청인 경우, 지정된 범위만큼의 요청을 받았다는 것을 알려줌.
400	Bad Request	클라이언트의 요청 구문이 잘못됨
401	Unauthorized	요청 처리를 위해 HTTP 인증 정보가 필요함을 알려줌. 접근 허용을 차단함.
403	Forbidden	접근 금지 응답. Directory Listing 요청 및 Web콘솔 접근 등을 차단하는 경우의 응답
404	Not Found	클라이언트가 요청한 리소스가 서버에 없음. 요청한 URL을 찾을 수 없음을 의미
406	Not Acceptable	클라이언트 요청에 대해 적절한 컨텐츠가 없음을 의미
412	Precondition Failed	클라이언트의 헤더에 있는 전제조건은 서버의 전제조건에 적절하지 않다고 알려줌
416	Range Not Satisfiable	Range 헤더 필드에 요청한 지정 범위를 만족시킬 수 없습니다.
500	Internal Server Error	서버에서 클라이언트 요청을 처리 중에 에러가 발생함

12.1.6 참고 - API 활용도구 제공: Swagger

Genian ZTNA는 API를 활용하는데 도움을 드리고자, Swagger(http://swagger.io/)를 제공합니다.

Swagger는 웹페이지를 통해서 REST API 정보와 테스트 도구를 제공합니다.

1단계. Swagger 접속

1. Genian ZTNA의 관리자 계정으로 Web콘솔 1차 접속
2. 로그인이 된 상태에서 주소창에 **https://{정책서버IP}:8443/mc2/swagger/index.html** 을 입력하여 2차 접속
3. Swagger 접속 확인

2단계. Swagger를 이용한 테스트

1. 활용하고자 하는 API를 선택한 후, 해당 API의 창 우측에 **Try It out** 버튼 클릭
2. Parameters 항목에서 **Description** 값 및 Body 의 **Example Value** 값 입력
3. 아래의 **Execute** 버튼 클릭
4. Responses 항목에서 **curl** 및 **Request URL** 값 확인 (Server response 항목에서 Code값이 **200** 일때 정상동작 됩니다.)

Note:

- Content Type은 JSON을 사용하며 'application/json;charset=UTF-8'을 표준으로 합니다. (포맷이 다른 경우, 폰트가 손상되어 보일 수 있습니다.)

CHAPTER

THIRTEEN

로그포맷

13.1 로그 타입별 로그 ID 정의

로그 ID	이름	내용
0	에러	
1	경고	
2	알림	
3	위험	

13.2 이벤트 항목 별 로그 ID 정의

로그 ID	이름	내용
100	노드관리	노드관리 시 발생되는 로그
101	GENIAN 장비	GENIAN 장비에서 발생되는 로그
102	동작상태변경	센서의 동작상태 변경 시 발생되는 로그
103	노드정보	노드의 상태 정보 변경 시 발생되는 로그
104	데이터베이스	백업 시 발생되는 로그
107	운영체제 업데이트 동기화	패치파일 업데이트 및 동기화 시 발생되는 로그
108	운영체제 업데이트 서비스	패치서비스 상태에 따른 이벤트 발생 로그
109	정책	정책 할당 및 변경에 대한 로그
110	그룹	그룹 할당 및 변경에 대한 로그
111	에이전트액션	에이전트 액션 수행 결과에 대한 로그
112	데이터무결성	중요 파일의 데이터 무결성 검사에 대한 수행 및 결과 로그
114	위험관리	위험관리 이벤트 발생 로그
116	인증	사용자 인증 수행 및 결과 로그
118	업데이트	패치 및 GENIAN 데이터 업데이트 로그
119	알람	SMS 전송 오류 로그
120	CLI	장비 CLI 접속 및 command 실행 히스토리 로그
121	데이터동기화	인사정보 동기화 이력 로그
122	네트워크제어	네트워크 접근제어 감사로그
123	무선랜 AP	무선랜 AP 감지 이벤트
124	DHCP	DHCP 할당 이력 로그
130	소프트웨어정보	해당 에이전트의 소프트웨어 정보 로그
131	시스템정보	시스템 정보 로그
132	네트워크정보	네트워크 정보 로그

continues on next page

Table 1 – continued from previous page

로그 ID	이름	내용
133	무선센서정보	무선랜 AP 정보 로그
134	무선랜관리	무선랜 AP 관리 로그
140	SYSLOG	SYSLOG 전송 시 발생되는 로그
300	비정상노드	IP 충돌 위반 대상 이벤트 로그
401	IP 사용시작	IP 사용시작 및 노드 동작상태 관련 로그
402	AGENT 사용시작	에이전트 사용 및 동작상태 관련 로그
451	IP 사용종료	IP 사용종료 및 노드 동작상태 관련 로그
452	AGENT 사용종료	에이전트 종료 및 동작상태 관련 로그
501	RADIUS 접속	RADIUS 인증 성공 관련 로그
551	RADIUS 해제	RADIUS 세션 만료 관련 로그
900	관리자접속	관리자 UI 접속 로그
902	정책변경	정책 할당 및 상태 변경 이벤트 로그
904	설정변경	ZTNA 설정 변경 이벤트 로그
906	시스템관리	ZTNA 에이전트 및 설정 파일 변경 로그
908	사용자관리	인증사용자 계정 이력 로그
910	IP 사용관리	IP 관리정책 이벤트 로그
912	리포트	감사기록 엑셀 출력 및 리포트 출력 이벤트 로그
920	매체사용관리	매체 사용 신청서 생성/수정/삭제 시 발생하는 로그
930	라이선스사용관리	라이선스 권한 적용 및 사용 이벤트 로그
1000	바이러스치료성공	백신 연동 시 바이러스 치료 성공 로그
1001	바이러스치료실패	백신 연동 시 바이러스 치료 실패 로그
1002	바이러스치료완료	백신 연동 시 바이러스 치료 완료 로그
1003	읽기차단	매체제어 읽기 접근 차단 관련 로그
1004	쓰기차단	매체제어 쓰기 접근 차단 관련 로그
1005	읽기허용	매체제어 읽기 접근 허용 관련 로그
1006	쓰기허용	매체제어 쓰기 접근 허용 관련 로그
1007	에이전트	에이전트 상태 및 정책 이벤트 발생 로그
1009	에이전트인증코드	에이전트인증코드 정보 로그

CHAPTER

FOURTEEN

FAQ

NAC와 무엇이 다른가요?

- 기존 NAC의 기능위에 Zero-Trust 보안정책을 구현하기 위해 다음과 같은 기능이 추가되었습니다.
- 센서 관리대상 노드간의 통신/내부망->Cloud/재택근무 접속에 대한 동적 목적지 접근제어 지원
- 재택 근무자에게 강화된 단말 보안과 안전한 통신환경을 제공하는 ZTNA Client 기능
- Cloud 서버 대역에 대한 가시성 및 Zero Trust 접근제어를 위한 Cloud 정보 수집기능
- Cloud 서버 대역 및 인터넷 억세스에 대한 동적 접근제어 제공을 위한 Cloud Gateway 기능
- Cloud 서버의 자동화된 보안정책 관리를 위한 Cloud Security Group 관리기능
- 네트워크 트레픽에 대한 가시성을 제공하는 Netflow(IPFIX) 기반 NTA 기능
- 최신 보안뉴스와 그에 관련된 노드를 알려주는 보안뉴스 피딩 서비스
- 새로워진 대시보드 / 확장된 노드타입 / 플랫폼 이미지 기반 그리드뷰

Zero Trust 보안정책이란 무었이며 ZT-NAC은 이것을 어떻게 제공 하는건가요?

- 네트워크에 접근하는 모든 장치는 그 장치에게 반드시 필요한 서비스/서버 이외에는 허용하지 않는 정책을 기본으로 가져가는 개념입니다.
- 이를 위해 출발지와 목적지가 그 역할에 따라 매우 정교하게 분류되어야 합니다. (Micro Segmentation)
- ZT-NAC는 그를 위해 500가지 이상의 조건식을 제공하는 노드그룹을 통해서 출발지와 Cloud를 포함한 목적지에 대한 노드그룹을 관리할 수 있습니다.
- 새로운 ZT-NAC에서는 세밀하게 분류된 사용자단말에게 허용되는 네트워크 접근권한을 설정할때 노드그룹을 사용할 수 있게 해줍니다.
- 노드그룹을 통한 목적지 제어를 사용하게 되면 기존 제품들이 제공하는 IP/Subnet 단위의 보안정책에서 벗어나 상태/속성/Tag등을 기반으로 보안정책이 자동으로 갱신됩니다.

동적 목적지 제어를 위해서 새로운 장비나 네트워크 구성이 필요한가요?

- 아니요. ZT-NAC을 기존에 센서가 설치된 환경에서 운영할 경우에는 새로운 장비나 네트워크 구성 변경이 필요하지 않습니다. 표준 VXLAN SGT를 통한 센서간의 통신을 통해서 구성변경 없이 동적 접근제어가 가능합니다.
- Genians의 특허받은 ARP기반 가상 Inline 접근제어방식을 통해서 Out-of-Band 방식으로 구성하거나 Inline Gateway방식의 센서를 구축하여 In-Band 접근제어를 할 수 있어 구축환경에 따라 적합한 방식을 선택할 수 있습니다.

클라우드에 존재하는 서버(워크로드)에 접근시 동적 목적지 제어는 어떻게 적용할 수 있나요?

- 클라우드 접근제어는 두가지 방식으로 적용할 수 있습니다.

- 첫번째 방법은 Cloud 에서 제공되는 Security Group 기능을 통해 서버에 접근가능한 단말의 IP목록을 노드그룹과 동기화시켜 관리할 수 있습니다.
- 두번째 방법은 Cloud Gateway를 구성해서 모든 통신을 Cloud Gateway를 거치도록 하여 접근제어를 수행할 수 있습니다. 이경우 특정 단말만을 위한 SSL-VPN기반의 G2C 방식이나 네트워크 단위의 접속을 위한 IPSec을 이용한 G2G 방식을 사용할 수 있습니다.

동적 접근제어 수행시 사용자의 네트워크 트레픽에 대한 가시성은 제공 되나요?

- 예, ZT-NAC는 센서/Gateway를 통과하는 접속에 대해서 표준 Netflow(IPFIX) 기반의 감사기록을 제공합니다. 이를 통해서 5 Tuples, Policy 정보에 더불어 GeoIP, BGP AS, HTTPS ETA(Encrypted Traffic Analysis), HTTP Request 정보등을 제공합니다.

ZT-NAC에서 제공되는 동적 접근제어는 컨트롤러 방식의 SDN과는 어떤 차이점이 있나요?

- 모든 접속에 대한 동적 접근제어를 하나의 중앙 컨트롤러에서 처리하는 SDN방식은 컨트롤러 장애시 모든 통신이 중단된다는 문제점을 가지고 있습니다.
- 이에 비해 Genian ZT-NAC의 동적 접근제어 방식은 표준 VXLAN SGT 방식을 사용하여 정책서버 장애시에도 기존에 인가된 단말의 동적 접근제어는 정상적으로 동작합니다.
- 아울러 Genian만의 ARP를 이용한 가상 Inline 방식을 통해 제공되므로 물리적인 네트워크 구성변경이나 네트워크 설정변경이 전혀 필요하지 않습니다.

동적 목적지 접근제어 사용시 ZT-NAC 센서 장애가 발생되면 어떻게 되나요?

- Out-of-Band 방식의 호스트센서 모드로 운영중인 경우라면 기존과 동일하게 센서장애시 네트워크 접근제어 기능이 해제 됩니다.
- Cloud Gateway를 통한 In-Band방식으로 운영중이라면 간단한 Instance 재구동/재생성으로 On-Prem Appliance 시스템 대비 빠른 복구가 가능합니다.

ZT-NAC에서 제공되는 ZTNA는 기존 VPN 대비 어떤 이점이 있나요?

- 기본적으로 ZT-NAC은 전통적인 VPN이 제공하는 IPSec, SSL-VPN 기능을 제공합니다.
- ZTNA Client가 NAC Agent내에 통합되어 있고 Zero Config를 지원합니다.
- 접속지점(PoP)을 Cloud에 위치시킬 수 있어 모든 트레픽이 사내로 들어오는 전통적인 VPN방식에 비해 WAN구간 트레픽을 획기적으로 감소시켜 주고 사용자에게 보다 빠른 네트워크 접속을 제공 합니다.
- 접속지점(PoP)을 다양한 국가/대륙별로 위치시킬 수 있어 글로벌기업에 적합합니다. (다중 PoP 및 Latency 기반 PoP 자동선택)
- NAC Agent에서 제공되는 단말 무결성 검사를 통과한 단말만 네트워크 접속이 가능하도록 통제할 수 있으며 네트워크 사용중에도 지속적인 단말 상태검사를 통해 접속을 통제합니다.

ZT-NAC은 Multi Cloud 환경을 지원하나요?

- 복잡해지는 Cloud 환경으로 인해 하나이상의 Cloud 서비스를 사용하는것이 보편화 되고 있습니다. ZT-NAC은 Cloud 사업자마다 다른 보안정책 수립을 단순화시키고 자동화 시키기 위한 간편한 방법을 제공합니다.
- Cloud 서버/서비스에 대한 보안정책을 ZT-NAC을 통해서 정의하면 개별 Cloud 서비스별로 별도의 UI / API / CLI 를 사용할 필요없이 업계표준인 Terraform을 통해 자동으로 Security Group을 적용시켜 줍니다.

Cloud Security Group 관리기능은 Public Cloud에만 적용할 수 있나요?

- 아니요. VMWare/Citrix와 같은 Private Cloud나 Nutanix와 같은 HCI, Hybrid Cloud에도 적용가능 합니다.
- 더 나아가 스위치, 보안장비, SaaS 서비스등 다양한 Provider를 지원 할 수 있습니다. 요청에 따른 순차적 지원을하고 있습니다.

ZT-NAC과 SASE는 어떤 차이점이 있나요?

- SASE의 서비스 방식은 모든 네트워크 접근제어를 Cloud Gateway를 통하여 이루어지도록 하여 보안시스템을 모두 Cloud에 위치시키는 개념 입니다. 이를 통해 On-Premises 중심의 보안체계를 Cloud중심으로 전환합니다.
- ZT-NAC은 이를위해 필요한 ZTNA와 Cloud Gateway를 제공합니다. Cloud Gateway는 다양한 지점 및 재택근무 사용자들이 안전한 통신 채널을 생성할 수 있도록 IPSec, SSL-VPN, GRE, VXLAN등 다양한 터널링 방법을 제공합니다.
- 사용자는 ZT-NAC을 통하여 자신만의 구축형 SASE 서비스를 만들 수 있습니다.

기존 V5.0 사용중 인 경우, ZTNA 도입시 따로 구매를 진행 해야 하나요?

- NAC의 내부/재택/Cloud까지 아우르는 ZTNA 개념의 NAC 확장 버전입니다. 만약 기존 V5.0을 사용하고 계신다면 업그레이드의 개념으로 생각하시면 될 것 같습니다.

NAC 인증 시 VPN 연결 할때도 인증없이 연결 가능하게 할 수 있나요?

- 현재는 NAC인증과 VPN 인증이 별도로 구분되어 있습니다. VPN 인증 시 ID,PW를 저장하여 자동 인증 처리할 수 있도록 기능제공 하고 있으며, 어느 곳에서든 항상 접속 가능하도록 Always ZTNA 기능을 지원하려고 합니다.

ZT-NAC은 Multi-Tenancy를 지원하나요?

- ZT-NAC은 기존과 같은 단일 테넌트를 위한 제품과 더불어 다수의 테넌트를 대상으로 서비스를 제공할 수 있는 Kubernetes 기반의 멀티테넌시 환경을 지원합니다.
- 이를 통해 고객사 내부에서 다수의 도메인에 대해 독립적인 관리형 서비스를 제공하는 시스템을 구축할 수 있습니다.

Cloud 환경에서만 사용이 가능한가요?

- Cloud 환경과 on-premise 환경 모두 구성 가능합니다.

IPSec VPN 기능이 있나요?

- IPSec HUB 용도의 서비스 제공 목적입니다. On-Perm 사이트는 IPSec 표준을 지원하는 자체 VPN 장비를 사용하시는 것을 권합니다.

사내에서도 VPN연결을 해야하나요?

- Zero Trust라는 개념에서 볼 때 어떠한 것도 신뢰하지 않습니다. 사내에서도 VPN 연결을 통해 안전한 연결을 유지하는 것이 ZTNA의 컨셉입니다.

Cloud의 자원을 보호하는 기능이 있나요?

- Cloud의 자원(인스턴스)를 수집하고 모니터링을 통한 Cloud Security Group을 설정하는 기능을 지원하고, Cloud의 CLI를 통해 다양한 활동을 하도록 변경할 수 있습니다.
- Cloud의 자원을 보호하는 역할은 지원하고 있지 않습니다.

VPN은 어느것을 사용하나요?

- 오픈 소스를 이용하여 자체 개발을 진행하였습니다.

Cloud ,on-premise 모두 이중화 지원이 가능한가요?

- 이중화 지원은 현재 개발 진행 중 입니다.

소프트웨어 버전을 다운그레이드할 수 있습니까?

- 아니요, 다운그레이드는 지원되지 않습니다. 원복을 위한 다운그레이드의 경우 업그레이드하기 전에 백업을 생성한 다음 소프트웨어를 다시 설치하고 백업 데이터를 복원해야 합니다. 잘못된 다운그레이드는 DB Migration에 의해 데이터베이스가 정상적으로 구성되지 못할 수 있기에 권고하지 않습니다.

각 구성 요소 간의 통신이 암호화되어 있습니까?

- 예, 각 구성 요소 간의 이벤트 및 정책 관련 통신은 TLS를 통해 암호화됩니다.

엔드포인트의 Windows 업데이트를 확인하려면 어떻게 해야 합니까?

- *Windows* 업데이트 의 1단계를 참고하세요.

에이전트 지원 운영체제는 어떻게 됩니까?

- Genian ZTNA는 *Windows*, *macOS*, *Linux* 운영체제에 대해서 에이전트를 제공합니다.

어떤 백신제품을 지원합니까? ?

- Genian ZTNA는 국내, 국외의 백신 제품들에 대해서 지속적인 연동을 통해 확대 범위를 넓혀가고 있습니다. *windows* 자세히 보기 , *macOS* 자세히 보기, *Linux* 자세히 보기

Genian ZTNA가 지원하는 무선어댑터는 어떻게 됩니까?

- Genian ZTNA 무센센서와 호환되는 무선 어댑터 리스트입니다. 무선 어댑터 호환성

네트워크 차단된 노드가 CWP 페이지가 표시되지 않는 이유는 무엇입니까?

- DNS 통신이 안되는 경우 차단페이지가 표시되지 않습니다, 그 외의 경우에는 HSTS, HPKP 등 브라우저의 보안 설정이 동작했을 가능성이 큽니다. 다음 문서를 참조 바랍니다. *HTTP* 통신을 시도하는 *PC*에 *CWP* 페이지를 표시하는 방식

Web콘솔 노드관리 화면의 에이전트 아이콘이 회색인 이유는 무엇입니까?

- Web콘솔 노드리스트에서 표시되는 에이전트 아이콘이 회색인 이유는 정책서버와 에이전트가 통신이 되지 않거나, 에이전트가 동작하고 있지 않을때 회색으로 표시됩니다.

Agentless 환경에서 도메인정보를 수집하지 못하는 이유가 무엇입니까?

- 네트워크센서가 단말의 netbios, remote WMI 등의 통신이 원활하지 않는 상태이면 수집이 되지 않습니다.

Agentless 환경에서 단말 호스트명이 수집되지 않는 이유가 무엇입니까?

- 네트워크센서는 단말의 호스트 명을 실시간으로 모니터링합니다. DHCP, netbios.ns, netbios-dgm, MDNS 서비스가 모니터링되지 않는 경우 호스트 명이 수집이 되지 않습니다.

Agentless 환경에서 단말 정보수집이 되지 않는 이유가 무엇입니까?

- 단말 OS Windows 10 2004 릴리즈에서 DCOM 버전 문제로 인하여 WMI 정보수집이 되지 않는 단말들이 있습니다. 기술지원센터를 통하여 임시조치를 받으실 수 있습니다.

감사로그에 데이터베이스 Duplicated 로그가 많이 보이는 이유가 무엇입니까?

- 데이터베이스에 존재하는 데이터를 다시 추가하려고 할 때 나타나는 DB 경고 로그입니다. 반복적으로 계속 나타나는 경우 기술지원센터를 통하여 지원받으실 수 있습니다.

Agentless 환경인데 제어정책에 Agent 미설치 차단 정책이 존재합니다.

- 기본 제어정책은 Agent를 설치하는 환경 기준으로 생성되어 있습니다. Agent를 설치하지 않는 환경에선 정책을 환경에 맞게 생성/삭제 후 사용하시면 됩니다.

운영정보 데이터(Genian data)의 업데이트 주기는 언제입니까?

- 운영정보 데이터는 **Web콘솔 > 설정 > 기타설정 > 운영정보 자동 업데이트 설정** 에서 검사 주기를 설정하고 하단 **자동업데이트** 항목을 `On` 으로 하게 되면 설정한 주기에 자동업데이트됩니다. 시스템 업데이트 관리

무선랜 AP SSID 수집은 어떻게 수집해야 되나요?

- 다음 문서를 참고 바랍니다. 무선랜 제어

단말 무선랜접속을 제어하는 방법은 무엇입니까?

- 단말 무선랜접속 제어는 2가지로 수행이 가능합니다. 무선네트워크 어댑터를 `Disable` 시키는 방법(인터페이스 제어)과 무선랜 제어 를 이용한 무선랜 AP 접속을 제한하는 방법이 있습니다.

유/무선을 사용하여 네트워크를 공유해서 사용하는 단말을 제어하는 방법은 무엇입니까?

- 위험감지 정책(위험감지의 이해)에 Adhoc 네트워크 연결 정책을 사용하여 제한할 수 있습니다.

불필요한 관리자 웹 접속을 제어하는 방법은 무엇입니까?

- 세션관리 기능(session-control)을 사용하여 불필요한 접속 세션을 강제로 종료할 수 있습니다.

노드에 네트워크 연결상태는 어떤 방법으로 확인하나요?

- 노드 상태체크 방식(node-updown-status)를 설정하여 확인할 수 있습니다.

CHAPTER

FIFTEEN

TROUBLESHOOTING

15.1 디버그 수집과 증상분석

15.1.1 ZTNA 디버그로그와 패킷 수집

ZTNA는 문제가 발생할 때 각 구성 요소에 대한 디버그로그 덤프를 지원한다. 각 덤프파일은 이슈 분석에 사용된다.

에이전트 디버그로그 수집 방법

WEB콘솔에서 수집

- WEB콘솔 관리 > 노드 메뉴로 이동
- 리스트에서 디버그로그를 수집할 노드를 체크
- **작업선택 > 노드 대상 명령 > 노드 대상 작업지시** 클릭
- **로그 수집 즉시수행(에이전트)** 선택 후 실행
- 상단 **감사 > 디버그로그** 메뉴로 이동
- 우측화면 **system > agent** 로 이동하여 **수집한 단말의 IP명 디렉토리** 클릭
- 수집날짜와 시간의 에이전트로그파일 클릭

> **Note:** 에이전트로그수집은 노드상세정보 **대상노드작업** 에서도 가능합니다.

단말에서 직접 수집

- PC Windows 우측하단 아이콘에서 우측버튼을 클릭
- 프로그램정보(A) 항목을 클릭한다.
- 팝업창의 좌측 하단 **오류 보고** 버튼을 클릭
- WINDOWS 단말의 디버그로그파일 저장위치는 **"C:"** 입니다.
- MAC 단말의 디버그로그파일 저장위치는 **"/Users/Shared/Genians"** 입니다.
- 파일명의 형태는 **"GnAgent_날짜시간.zip"** 입니다.

> **Note:**
>
> – ActiveDirectory 환경에서 로그수집을 위해서는 도메인관리자수준의 권한이 필요합니다.

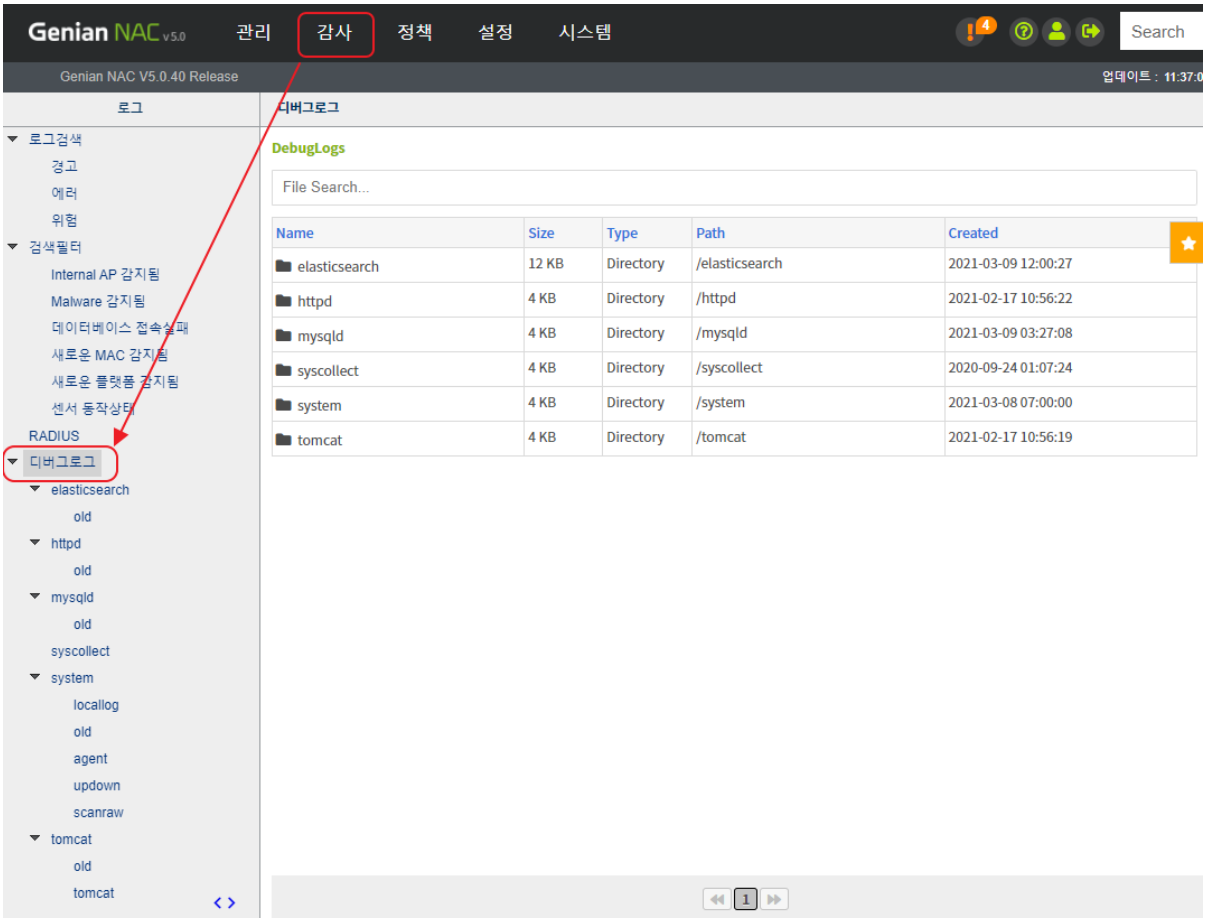
- LINUX 단말의 경우 직접 디버그 저장경로로 이동하여 수집하여야합니다. **"/var/log/genians"** 입니다.

정책서버/네트워크센서 디버그로그 확인 및 다운로드

WEB콘솔에서는 정책서버와 네트워크센서의 디버그로그를 실시간 확인 및 다운로드하는 기능을 제공합니다. 디버그로그는 시스템의 다양한 현재상황 및 문제해결에 사용됩니다.

아래를 참고하여 디버그로그를 확인하시기 바랍니다.

- WEB콘솔 접속
- 상단 **감사 > 디버그로그**
- 좌측 메뉴트리를 펼치거나 우측 창에서 확인하고자 하는 디버그로그파일을 선택
- 상단 아이콘을 클릭하여 다운로드(zip파일의 경우 클릭시 바로 다운로드)

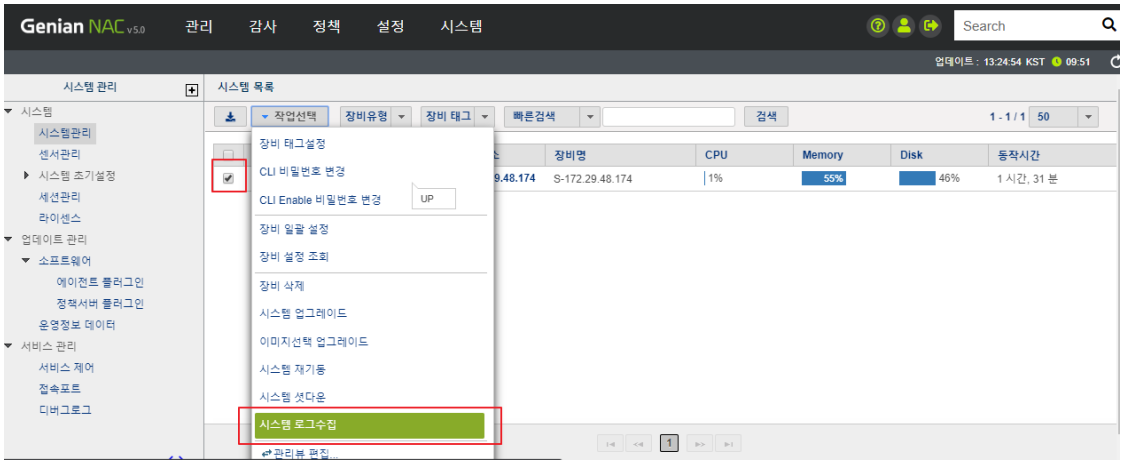


정책서버/네트워크센서 디버그로그 일괄 수집방법(syscollect)

WEB콘솔

아래를 참고하여 순서대로 수행합니다.:

- WEB콘솔 접속
- 상단 **시스템 > 시스템관리** 이동
- 리스트에서 수집하고자 하는 장비의 좌측 체크박스 체크
- 상단 **작업선택 > 시스템 로그수집** 클릭
- 상단 상태메시지 확인 시스템 로그수집 성공` 메시지 클릭
- **syscollect 디렉토리 하위에 생성된 .zip 파일 다운로드**
  - 시스템에 저장되어있는 디버그로그파일이 많은 경우 수분의 시간이 소요될 수 있습니다.



CLI콘솔

아래를 참고하여 순서대로 수행합니다.:

- Zmodem을 지원하는 터미널프로그램(secureCRT 등)으로 정책서버 SSH 접속
- Enable 모드로 진입
- 쉘모드 진입
- 프롬프트창에 *syscollect.sh* 입력
- 수집이 완료되면 명령어 `sz` 를 사용하여 결과에 생성된 파일의 위치를 입력하여 다운로드합니다.
  - 로그를 이슈관리시스템의 특정이슈에 업로드하려면 *Y* 를 입력하여 이슈번호를 입력합니다.
  - 주요데몬의 backtarace 정보를 추가로 수집하려면 *Y* 를 입력합니다.
  - 정책서버에 수집된 에이전트로그를 수집하려면 *Y* 를 입력합니다.

```
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)

Genians$sz [filename]
```

주요 구성요소간 전송되는 패킷 수집

정책서버와 네트워크센서, 에이전트와 통신에 사용되는 패킷을 수집할때 활용할 수 있습니다.

기본 명령어 예시

```
tcpdump -i eth0 port 80 and udp
- 인터페이스 eth0을 지나가는 UDP 포트 80을 사용하는 패킷 표시

tcpdump -i eth0 -e
- 인터페이스 eth0을 지나가는 모든패킷을 캡쳐하고 이더넷정보도 표시

tcpdump -i eth0 net 192.168.
- 인터페이스 eth0을 지나가는 192.168 네트워크의 패킷을 표시

tcpdump -i eth0 host [IP address] and arp[7] == 2
- 인터페이스 eth0을 지나가는 ARP Reply 패킷을 표시

tcpdump -i eth0 port 80 and udp -w /tmp/file1.pcap
- 인터페이스 eth0을 지나가는 UDP 포트 80 패킷을 /tmp/file1.pcap 으로 저장
```

옵션 상세

```
-v: 패킷캡쳐 결과를 상세하게 출력
-n: 주소(호스트주소, 포트번호)를 이름으로 변경하지 않고 출력
-e: 패킷캡쳐결과에 링크레이어 헤더를 출력 (이더넷 주소표시)
-w: 캡쳐한 패킷을 지정한 파일로 저장
-A: 각 패킷을 ASCII값으로 출력
-q: 출력결과를 짧게 출력
```

조건식

```
host : 패킷의 IP를 지정하여 결과 출력
dst host : 목적지 IP를 지정하여 결과 출력
src host : 출발지 IP를 지정하여 결과 출력
ether host : 패킷의 MAC주소를 지정하여 결과 출력
ether dst : 패킷의 목적지 MAC주소를 지정하여 결과 출력
ether src : 패킷의 출발지 MAC주소를 지정하여 결과 출력
net : 패킷의 네트워크주소 대역을 지정하여 결과 출력
dst net: 패킷의 목적지 네트워크주소 대역을 지정하여 결과 출력
src net: 패킷의 출발지 네트워크주소 대역을 지정하여 결과 출력
```

패킷수집의 다양한 예시

정책서버와 네트워크센서간 Keepalive 패킷 수집

```
tcpdump -i eth0 host [Network sensor IP] and port 3871
```

정책서버와 에이전트간 Keepalive 패킷 수집

```
tcpdump -i eth0 host [PC IP] and port 3871
```

네트워크센서에서 전송하는 ARP Reply 패킷 수집

```
tcpdump -nei eth0 ether src [NetworkSensor eth0 MAC] and arp[7] == 2
```

15.1.2 ZTNA 분석 방법

이 페이지에서는 Genian ZTNA에서 문제를 해결하기 위해 검사할 수 있는 주요 프로세스에 대한 개요를 제공한다.

ZTNA 프로세스 설명

정책서버 프로세스

```
centerd: 정책과 노드관리
sensord: 네트워크센서 프로세스
mysql: 데이터베이스에 노드와 정책정보를 저장
httpd: 웹서비스 데몬
java: WebUI를 실행하기 위한 JAVA프로세스로 웹과 데이터베이스 간의 연결작업 수행
procmond: ZTNA에서 사용하는 프로세스 모니터 데몬, 비정상 종료 모니터링 및 재실행 수행
sshd: SSH 원격접속 서비스를 제공하는 데몬
syslog-ng: SYSLOG 데몬
hbd: 하드웨어 또는 소프트웨어 오류가 발생한 경우 일정 시간 후 시스템을 정상화하는 작업(부팅 등)을 수행하는 데몬
mysqld_safe: mysqld 서버구동이 실패할 때 Mysqld_error에 재시작 및 런타임 정보를 저장하는 스크립트
gnlogin: CLI 명령 실행을 위한 서비스 제공
crond: 지정된 사이클에서 스크립트 및 명령을 수행하는 데몬
radiusd: 인증을 위한 RADIUS서버 데몬
```

네트워크센서 프로세스

```
sensord: 네트워크센서 프로세스
nmap: 노드의 네트워크 정보 검색 도구
procmond: ZTNA에서 사용하는 프로세스 모니터 데몬, 비정상 종료 모니터링 및 재실행 수행
sshd: SSH 원격접속 서비스를 제공하는 데몬
syslog-ng: SYSLOG 데몬
hbd: 하드웨어 또는 소프트웨어 오류가 발생한 경우 일정 시간 후 시스템을 정상화하는 작업(부팅 등)을 수행하는 데몬
```

에이전트 프로세스

프로세스명 : GnAgent.exe
설명 : Genian Agent
기능 : 에이전트 무경설 검사, 노드 정책 수신 및 GnPlugin 실행 관리
실행주기 : 항상
실행조건 : 윈도우즈 로그온 이후 항상

프로세스명: GnPlugin.exe
프로세스명: Genian Action Plugin
기능: 노드 정책의 작업 정책 수행 및 결과 전송
실행 주기: 항상
실행조건: 노드정책에 에이전트 액션이 있는 경우

프로세스명: GnStart.exe
프로세스명: Genian Starter
기능: 에이전트 무결성 검사, GnAgent 실행 관리, Keepalive 전송
실행 주기: 항상
실행조건: 항상

프로세스명: GnAccount.exe
프로세스명: Genian User Account Manager
기능: OS 로그온 계정 대신 특정 계정으로 GnAgent 프로세스를 실행하는 경우 사용
실행 주기: 이벤트가 발생한 경우
실행조건: 노드정책에 에이전트 실행계정 설정이 되어 있는 경우

프로세스명: GnDump.exe
프로세스명: Genian Agent Dump Utility
기능: 에이전트 디버그로그 수집
실행 주기: 없음
실행조건: 수동 실행 시에만 작동

프로세스명: GnExLib.exe
프로세스명: Genian External Module
기능: 외부 인증 모듈 등록(예:dll)
실행 주기: 없음
실행조건: 정책적으로 수동 실행시나 인증정보 갱신시

프로세스명: GnScript.exe
프로세스명: Genians Software Install Manager
기능: 에이전트 설치시
실행 주기: 없음
실행조건: 에이전트 설치 중에만 실행

프로세스명: GnUpdate.exe
프로세스명: Genian Updater
기능: 에이전트 자동 업데이트검사 및 업데이트
실행 주기: 6시간
실행조건: 없음

프로세스명: GnUtil.exe
프로세스명: Genian Agent Utility
Funcfiton: 특정 파일의 SHA1 해시 값 계산
실행 주기: 없음
실행조건: 수동으로 실행될 때만 작동함

시스템 디버그 프로세스명

정책서버 로그

Elasticsearch

```
GENIAN.log: Elasticsearch 프로세스 비정상 종료 및 재시작 오류 로그
```

httpd

```
Error_log: httpd 에러 로그
Mod_jk.log: Apache와 Tomcat은 Apache JServ Protocol(AJP)을 사용하여 통신하여 서로 통신하고 mod_
↪jk라는 모듈을 사용하여 구성한다.
- Apache 및 Tomcat 관련 오류 로그
```

mysqld

```
Initdb.log: 데이터베이스 초기화 중에 생성된 로그
구동시 테이블이 비정상인지 점검해야 한다.

Mysqld.error: mysql 작업 중 오류 로그
Slowquery.log: 장시간 실행된 작업에 대한 SQL 쿼리 로그
- ZTNA 작동 중 특정 작업이 오래 걸리는 경우 참조
```

system

```
Agent: PC에 저장된 에이전트 로그를 정책 서버에서 호출하여 저장

centerd: 정책서버에서 수행한 작업에 대한 로그
- 정책 서버 상태, 노드 Role 상태, 인증, 연동, 데이터 동기화 등

sensord: 네트워크센서가 수행한 작업 및 오류 로그
- 네트워크센서 상태, 노드 감지, UP/Down, 정책 수신 등

messages: dmesg와 같은 하드웨어 상태 관련 메시지

procmond: 프로세스가 비정상적으로 종료되고 다시 시작된 로그
scanraw: 노드의 플랫폼 탐지를 위한 노드의 네트워크 검색 정보
updown: 에이전트 Up/Down 상태 로그
authsync: 정보동기화 관련 로그
dbmigration: 데이터베이스 마이그레이션 로그
gnlogin: CLI 명령어 수행 이력 로그
radius.log: RADIUS 상태 및 노드 인증 로그
```

tomcat

```
Catalina.out: catalina.log 파일은 Tomcats "system.out" 및 "system.err" 스트림에 기록된 모든
로그 메시지를 포함한다
catalina.out에 포함된 내용:
- 미발견된 예외 사항 java.lang.ThreadGroup.uncaughtException(..)
- 시스템 신호를 통해 요청한 경우 시스템 덤프 제공
```

radius

```
Radiusd: 인증 및 오류 기록 포함(외부포함)
외부 서버에서 가져온 계정
```

시스템 검사

cli 명령어를 이용하여 ZTNA시스템의 상태를 확인합니다.

- 박스에 표시된 대로 다음 단계를 수행하십시오.
- 정책서버 콘솔에 직접 연결하거나 SSH통해 제품에 접속합니다.

```
genian> en

genian#
```

서버체크와 시스템 정보

- 시스템 이중화 여부 확인

```
genian# show ha status
```

- 데이터베이스 이중화체크, 복제상태 체크

```
genian# show replication status
```

- 시스템 구동된 시간, 시스템 부하

```
genian# show uptime
```

- 제품버전, H/W모델명 확인, 설치날짜

```
genian# show Version
```

- 사용중인 인터페이스 정보 확인

```
genian# show interface all
```

- 시스템 마운트 정보

```
genian# show filesystem
```

서비스 상태 체크

ZTNA에서 필요한 모든 프로세스가 실행 중인지 확인하십시오.

구성 요소별 필요한 프로세스:

```
정책서버:
Mysqld, elasticsearch, java, centerd, sensord, httpd, procmond, sshd, syslog-ng,␣
↪radius (Need confirmation if using RADIUS server), vrrpd (Need confirmation if␣
↪using HA configuration)

네트워크센서:
sensord, procmond, sshd

    명령어:
    genian# show processes
```

디스크사용량 체크와 메모리체크

서버의 하드 디스크 용량 및 메모리를 확인합니다. 하드 디스크가 꽉 찼거나 사용 가능한 메모리가 없는 경우 ZTNA는 다음과 같은 문제가 발생할 수 있습니다.

- ZTNA 동작이 느리거나 동작하지 않음
- 백업파일이 만들어 지지 않음

```
명령어:
genian# show Memory
genian# show filesystem
```

네트워크센서 확인 방법:

```
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
```

노드상태 확인 방법:

```
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 | Unauthorized Device(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
```

15.2 네트워크

15.2.1 네트워크센서가 웹콘솔에서 보이지 않음

증상

네트워크센서가 WebUI에 표시되지 않는 현상

원인

- 네트워크센서를 설치한 후 포트 443을 사용하여 정책 서버에 등록한다.
- 정책서버와 네트워크센서 간 등록통신이 실패하면 센서가 정책서버에서 등록되지 않는다. 그렇게 된다면 WebUI에 표시되지 않는다.

해결방법

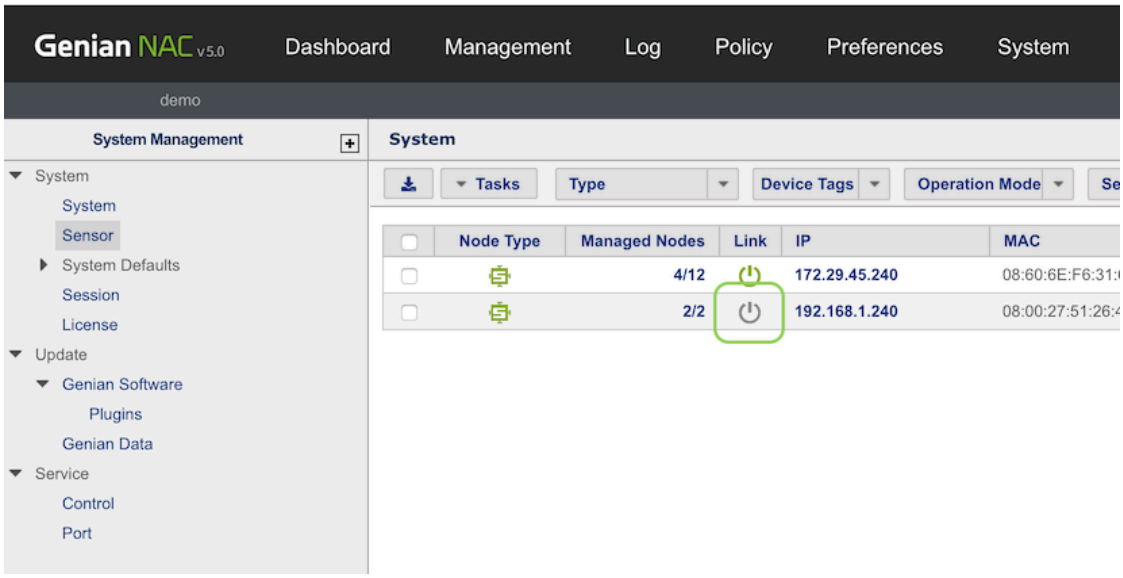
연결확인

- 포트 443의 정책서버와 네트워크센서 사이의 통신 경로를 확인. 방화벽 또는 기타 어플라이언스에서 필요한 정책예외를 확인. 방화벽 또는 기타 어플라이언스에서 정책서버와 네트워크센서간 통신패킷이 차단되는지 확인

15.2.2 센서 링크가 다운으로 표시되는 현상

증상

센서 링크상태 아이콘이 노드관리페이지나 센서관리페이지에서 다운으로 표시되는 증상



원인

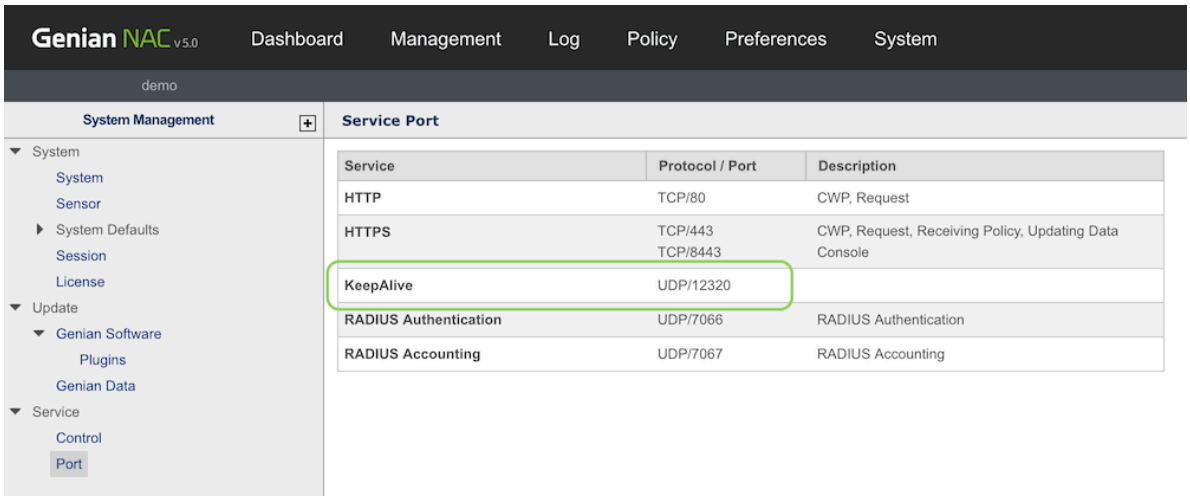
네트워크센서는 정상적인 작동상태를 정책서버에 알리기위해 주기적으로 keep-alive 패킷을 전송합니다.
이 패킷이 정책서버로 전송되지 않는 경우 WebUI에서 다운으로 표시될 수 있습니다.

Keep-alive를 위해 사용하는 통신 포트:

On-Premeses
: UDP / 3870 ports

Cloud-managed
: (변경가능)

메뉴위치는 **시스템> 서비스 관리 > 접속포트** 에서 **Keepalive** 항목에 적혀있는 포트를 허용



해결방법

이 경우 다음 사항을 확인해야 합니다:

1. 네트워크센서는 켜져있지만 다운으로 표시될때
2. 정책서버와 네트워크센서사이의 통신 경로 및 방화벽 또는 기타 네트워크/보안장비에서 예외처리가 되어있는지 확인한다. .

15.2.3 네트워크센서가 Failsafe 상태로 보일때

증상

네트워크센서가 노드관리/센서관리 화면에서 Failsafe 상태로 표시되는 현상

원인

네트워크센서는 정책서버와 주기적으로 UDP Keepalive 패킷을 주고 받습니다. 정책 업데이트가 있는경우 센서에게 알림이 가고 센서는 그에대한 응답을 수행합니다.

센서가 새로운 정책갱신이 필요한것을 인지하게 되면 TCP Port/443 HTTPS를 통하여 정책서버와의 TCP세션 연결시도를 합니다. 이 TCP 세션이 5번 연결 실패를 하게 되면 네트워크센서 상태가 Failsafe로 표시됩니다.

해결방법

통신연결상태 체크

- 정책서버와 네트워크센서사이에 TCP/443 HTTPS 통신이 정상적인지 확인합니다.
  - 방화벽 또는 기타 보안장비에서 필요한 예외처리가 되어있는지 확인합니다.

네트워크센서의 인터페이스 확인

- 네트워크센서의 SSH 접속하여 다음명령어를 수행합니다.: `show interface eth[#]`
  - 기본사용 인터페이스는 `[eth0]` 입니다.

정책서버와 네트워크센서 디버그 확인

WebUI에 접속 **시스템 > 서비스관리 > 디버그로그** :

`system/centerd` : `"ERRMSG=SOAP"` 관련 메시지가 있는지 확인, 디버그 용량이 큰 경우 다운로드하여 관련 메시지 검색

다음과 같은 `443` `Soap` 오류가 있는지 확인 ``[Policy Server or Network Sensor IP Address] 443``

15.2.4 ZTNA 에이전트 미동작

증상

노드 상태가 연결중 이고 에이전트가 실행 중이지만 관리WebUI에서는 에이전트가 다운으로 표시되는 증상

원인

에이전트는 정책서버로 2분에 한 번씩 Keep-alive 패킷을 전송하여 에이전트 동작 상태를 알려준다.

정책서버는 에이전트로부터 10분 동안 Keep-alive 패킷을 수신하지 못하였을 때 에이전트의 동작 상태를 미동작으로 변경한다.

다음과 같은 상황은 에이전트의 Keep-alive 동작을 방해하여 동작중이지만 다운상태로 표시된다:

1. 정책서버와 에이전트 사이 방화벽에서 패킷 차단
2. PC내 백신프로그램에서 Keep-alive 패킷전송을 방해
3. 하드디스크 변경으로 인한 에이전트 설치 불가

해결방법

정책서버와 에이전트간 통신 확인

- 정책서버와 에이전트 사이에 방화벽이나 타 보안솔루션에서 단말에서 발생하는 패킷이 존재하는지 확인

단말에서 발생한 패킷이 감지되지 않는 경우:

- 에이전트 설치가 정상적으로 설치되지 않았을 경우 발생 가능하며 에이전트를 재설치 하는 방법으로 조치
- 단말내 다른 보안제품으로 인하여 Keep-alive 동작을 할 수 없는 상태일 경우는 타 보안제품을 삭제하고 에이전트 재설치 방법으로 조치
- 기타 케이스에서는 로그를 수집하여 기술지원

참조: *ZTNA 디버그로그와 패킷 수집*

15.2.5 502 Proxy Error

증상

Web 콘솔에서 표시되는 정보가 최신이 아니며 오류메시지 `ERRMSG='Error 502 fault: SOAP-ENV:Server [no subcode] "HTTP/1.1 502 Proxy Error"'` 로그가 표시.

원인

대규모 네트워크에서는 센서에서 정책서버로 전송되는 정보가 많고 처리하는데 시간이 소요됩니다.

이와 같은 환경에서 데이터 전송에 대한 세션 타임아웃이 짧을경우 데이터전송을 하지 못하고 세션이 종료되버리며 에러로그가 발생됩니다.

조치

세션 타임아웃값을 길게 설정

1. 정책서버 CLI 접속
2. **show configuration** 명령을 이용하여 현재 타임아웃설정값을 확인
3. 설정모드로 진입
4. 세션 연결 타임아웃 설정과 데이터 타임아웃 설정

```
genian(config)# management-server connection-timeout [value in seconds]
genian(config)# management-server data-timeout [value in seconds]
```

15.2.6 스위치에서 mac flap 에러가 표시됨

증상

스위치 로그에 네트워크센서가 연결된 포트와 관련된 mac flap 로그를 표시하는 증상

원인

네트워크센서는 내부 AP 감지 메커니즘의 일부로 스푸핑된 가상 MAC을 전송하며 이로 인해 스위치에서 가끔 mac flap 이 발생할 수 있습니다.

해결방법

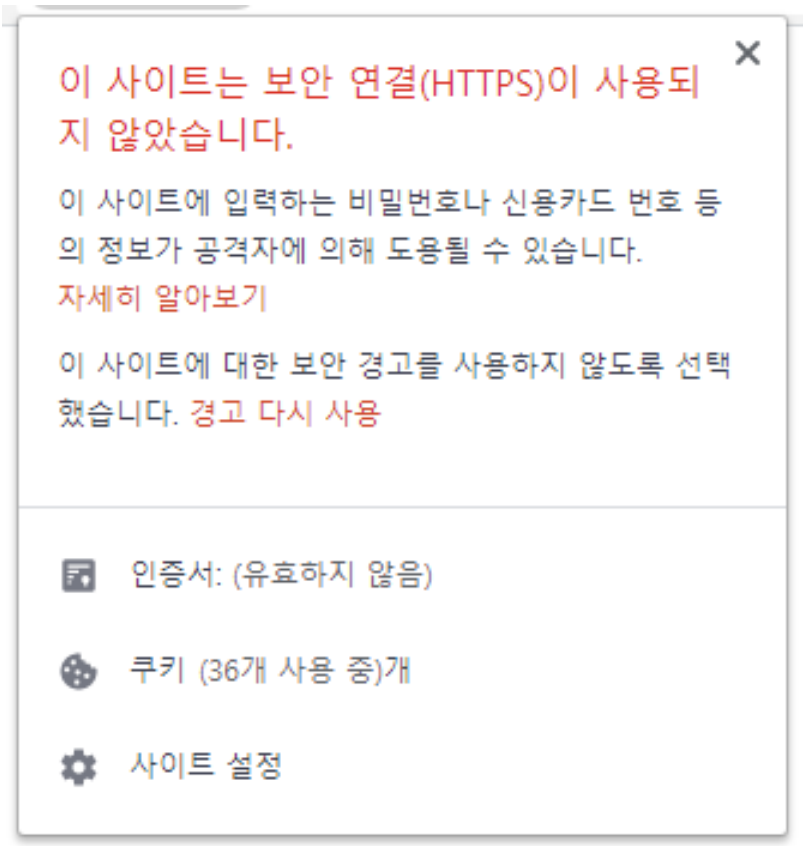
내부AP감지 기능 중지를 수행합니다.

1. WEB콘솔에 관리자로 로그인합니다.
2. 상단 설정메뉴로 이동합니다.
3. 좌측 메뉴트리에서 무선랜관리로 이동합니다.
4. 내부 AP 감지 항목에서 내부 AP 탐지용 가상 MAC 사용 옵션을 OFF 합니다.

15.2.7 웹 콘솔에서 SSL 인증서 오류 발생할때

증상

웹 콘솔 접속시에 "주의 요함 : 이 사이트는 보안 연결(HTTPS)이 사용되지 않았습니다." 인증서 오류 발생



원인

- 인증서가 만료되었거나 유효하지 않은 인증서로 인해 오류가 발생합니다.

해결방법

공인인증서 등록하여 인증서 오류를 해결할 수 있습니다.

인증서가 있는 경우:

- 관리WebUI 접속
- 다음 메뉴로 이동합니다. **설정 > 환경설정 > 인증서 관리**
- 인증서 파일을 업로드합니다.
- 다음 메뉴로 이동합니다. **시스템 > 서비스 관리 > 서비스 제어**
- 관리콘솔을 재구동합니다.

인증서가 없는 경우:

- 관리WebUI 접속
- 다음 메뉴로 이동합니다. **설정 > 환경설정 > 인증서 관리 > SSL 인증서**
- 호스트명, 국가코드, 회사/조직명, 이메일을 입력하여 CSR을 생성합니다.
- 생성된 CSR로 외부 인증서 발급기관에서 PEM 형식의 인증서를 발급 받습니다.
- 인증서를 등록합니다.

- 다음 메뉴로 이동합니다. **시스템 > 서비스 관리 > 서비스 제어**
- 관리콘솔을 재구동합니다.

Note: 인증서를 적용하려면 웹서비스(httpd)를 재시작해야 합니다.

15.3 설정

15.3.1 노드가 관리UI에 등록되지 않음

증상

네트워크센서를 제외한 모든 노드가 네트워크센서가 설치된 서브넷에서 표시되지 않음

원인

Genian ZTNA는 연결된 스위치포트의 설정과 네트워크센서 인터페이스 설정과 일치하지 않을 때 노드를 검색할 수 없다.

해결방법

스위치

- ZTNA가 연결되어 있는 포트가 모니터링하려는 VLAN에 엑세스하도록 올바르게 설정되어 있는지 확인하십시오.
- ZTNA는 표준 엑세스 포트 및 802.1q 트렁크포트만 지원합니다.

네트워크센서

- cli에서 `show interface eth[#]` 명령을 사용하여 인터페이스 설정을 확인하십시오.
- `eth0` 인터페이스는 스위치의 엑세스포트나 트렁크포트의 default vlan이 설정되어 있는 경우에만 작동합니다.
- 태깅된 모든 VLAN 트래픽은 해당 VLAN의 정의 된 하위 인터페이스에서만 볼 수 있습니다. 다음문서를 참조하십시오. 네트워크센서 추가 및 삭제
- 네트워크센서에서 통신이 되는지 서브넷으로 ICMP를 수행하십시오.

가상화 센서를 사용하는 경우

- 하이퍼 바이저의 인터페이스가 네트워크 스위치와 올바르게 통신이 되도록 설정되어 있는지 확인하십시오. 하이퍼바이저는 간혹 일반 통신이나 트렁크 인터페이스를 통한 통신을 할때 비표준 구성을 할때가 있습니다.
- 다음을 참조하십시오. 네트워크센서 설치

15.3.2 웹콘솔 로그인이 되지 않을 때

증상

인증이 실패하며 " 접속권한이 없는 위치 입니다." 라는 메시지가 표시되는 증상

원인

- 정책서버는 각 관리자계정에 대한 **접속허용 IP목록** 을 사용하여 관리WebUI에 대한 접속을 제어
- 접속허용 목록은 각 관리자 계정의 **기본정보탭 > 로그인 설정** 에서 변경 가능합니다.
- 관리자의 IP 주소가 **접속허용 IP** 에 존재하지 않을 경우 관리자는 관리WebUI에 접속할 수 없습니다.

해결방법

사용자 관리 수정 권한이 있는 관리자계정이 있는지 확인합니다.

다음:

- 관리WebUI 접속
- 다음위치로 이동 **관리 > 사용자 > 설정을 변경할 사용자ID 선택 > 로그인 설정**
- 접속하려는 IP가 관리WebUI 접속 IP1에 접속하는 관리자PC의 IP에 포함되는지 확인
- IP가 포함되지 않은 경우 접속하는 관리자 단말의 IP를 추가

15.3.3 SSH 로그인 실패

증상

SSH연결 시도가 실패하고 "Connection refused" 메시지 표시되는 증상

원인

- 보안상의 이유로 SSH 연결은 허용된 IP주소에서만 접속이 가능
- 설정에 접속하려는 IP가 존재하지 않으면 연결이 허용되지 않습니다.

해결방법

SSH 접속승인 IP 추가

1. 관리WebUI 상단 시스템메뉴 진입.
2. 접속할 장비의 IP를 선택.
3. 환경설정 탭을 선택.
4. CLI 콘솔 접속 IP1에 SSH접속을 허용할 IP입력
5. 하단 수정버튼 클릭
6. SSH 연결상태 확인

15.4 운영

15.4.1 Cisco 스위치 포트 정보가 표시되지 않음

증상

스위치는 표시되지만 노드 관리, 노드 정보 또는 스위치 관리 보기에는 노드의 스위치 포트 정보가 표시되지 않는 증상

원인

SNMPv3를 사용하는 경우 일부 Cisco IOS 버전에서는 모니터링하려는 모든 데이터를 볼 수 있도록 `snmp-server group`을 구성하여 권한 필요

해결 방법

아래 View contexts 예 에서 스위치 가시성을 얻기 위해 사용되는 SNMP GROUP은 스위치 포트에 할당된 VLAN을 볼 수 있는 권한이 없다. 스위치 포트의 가시성을 확보하기 위해서는 SNMP GROUP에 Context에 대한 할당이 필요하다.

View Contexts

```
switch>en
switch#>conf t
switch(Config)>show snmp context
vlan-1
vlan-2
vlan-3
```

접근허용 적용

```
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
```

Note: SNMP GROUP 에는 접속 클라이언트가 사용할 USER정보가 사전에 정의되어 있어야 한다. 참조 Cisco SNMP Configration

15.4.2 CLI 패스워드 분실

증상

CLI 콘솔 접속 패스워드 분실

원인

관리자는 다수의 솔루션을 관리하고 있으며 비밀번호 관리에 어려움을 가지고 있습니다.

해결방법

CLI 콘솔 패스워드는 관리UI에서 변경할 수 있습니다:

1. 관리권한의 계정으로 관리UI 접속을 합니다.
2. 상단 시스템메뉴로 이동 합니다.
3. 목록에서 패스워드를 분실한 장비의 좌측 체크박스를 선택합니다.
4. 상단 **작업선택 > CLI 비밀번호 변경** 팝업창에서 새로운 패스워드로 변경합니다.

15.4.3 웹콘솔에 접속하지 않고 센서동작모드 변경

상황

Web콘솔에 접속이 불가능한 상태에서 센서동작 상태를 비활성화 상태로 전환해야 하는 상황에서 사용

원인

다음과 같은 여러 가지 이유로 인해 위와 같은 문제가 발생할 수 있습니다.

- Genians 또는 다른 보안시스템에 의한 웹콘솔 접속 불가
- 웹콘솔이 동작하지 않음

해결방법

정책서버 CLI를 통하여 센서 제어

- 아래와 같이 정책서버 SSH로 접속하고 셀모드로 진입합니다.

```
genian> en

genian#

Genians$
```

- 센서 중지, 명령어 `centerd -dfS [SensorIP]`
  - 한대의 센서만 중지, 단일 센서 IP만 지정하는 명령어 : `centerd -dfS [1.1.1.1]`
  - 여러대의 센서를 중지, 여러 센서 IP를 지정하는 명령어 : `centerd -dfS [1.1.1.1,2.2.2.2]`
  - 전체 센서를 중지, 전체 센서를 대상으로 하는 명령어 : `centerd -dfS [all]`
- 센서 동작, 명령어 `centerd -dfR [SensorIP]`
  - 한대의 센서만 동작, 단일 센서 IP만 지정하는 명령어 : `centerd -dfR [1.1.1.1]`
  - 여러대의 센서를 동작, 여러 센서 IP를 지정하는 명령어 : `centerd -dfR [1.1.1.1,2.2.2.2]`
  - 전체 센서를 동작, 전체 센서를 대상으로하는 명령어 : `centerd -dfR [all]`

정책서버 CLI에서 센서 동작상태 확인

- 쉘모드를 종료하고 다시인증 하기위해 `exit` 입력
- 센서 상태 확인, 명령어 : `show sensor [옵션]`
  - 센서 동작 상태별로 결과를 필터링하기 위해서는 `all`, `active`, `passive`, `unknown` 을 옵션으로 사용합니다.

15.4.4 플랫폼 오탐으로 노드가 잘못된 정책을 할당받는 문제

증상

제어정책에서 감지된 노드타입 조건으로 네트워크 차단 예외를 받던 노드가 어느순간 차단정책에 할당되어 차단되는 현상

원인

조건 :

1. 제어정책에 예외처리를 위한 노드그룹의 조건을 감지된 노드타입으로 설정
2. 예외처리를 받던 노드의 보안설정이 변경되어 주기적으로 수행되는 노드 스캔정보가 변경됨

위 조건하에 예외정책을 할당받고 있던 노드가 네트워크센서에서 수행하는 주기적 노드 스캔으로 인하여 기존에 탐지된 정보보다 수집된 정보가 많거나 적은경우 아닌 다른 플랫폼으로 탐지.

플랫폼 오탐과 함께 노드타입도 예외처리된 노드타입이 아닌 차단정책을 할당받는 노드타입으로 변경되며 예외정책을 할당 받지 못하여 네트워크 차단.

해결 방법

감지된 노드타입,노드플랫폼은 간헐적으로 오탐이 발생할 수 있습니다. 그렇기 때문에 감지된 노드타입 이라는 조건은 예외처리 정책의 조건으로 적절하지 않습니다. 예외처리에 노드타입 조건을 사용하고자 하는 경우 노드타입-확인된 노드타입, 노드타입-감지방법-관리자지정 과 같은 조건을 사용해야 합니다.

방법1: 노드타입 - 확인된 노드타입 조건 으로 예외그룹 조건을 사용하는 방법 (권장)

1. **Web콘솔 > 관리 > 현황&필터 > 노드타입** 으로 이동하여 예외처리 할 노드타입을 선택합니다.
2. 우측 리스트화면 좌측 상단 체크박스를 선택하여 리스트에 표시된 모든 노드의 체크박스에 체크합니다.
3. **작업선택 > 노드 및 장비 > 노드 속성 변경** 을 선택합니다.
4. 관리자가 노드타입을 확인합니다. 항목과 관리자가 플랫폼을 확인합니다. 항목에 체크하고 하단 수정 버튼을 클릭합니다.
5. 예외처리 할 다른 노드타입도 동일한 작업을 수행합니다.
6. **설정 > 환경설정 > 노드관리 > 노드정보 검색** 항목에서 **최초플랫폼정보 자동확인** 옵션을 **On** 으로 변경합니다.
7. 제어정책 메뉴로 이동하여 예외처리 정책의 노드그룹 조건을 **노드타입 > 확인된 노드타입이 같으면** 조건을 선택하여 예외처리 할 노드타입을 추가합니다.

8. 노드타입을 모두 추가하였다면 수정 버튼을 클릭하고 화면 상단 변경정책 적용 버튼을 클릭하여 정책을 적용합니다.

> **Attention:** 확인된 노드타입과 플랫폼은 관리자가 확인한 정보라는 의미의 필드값으로 **현황&필터 > 변경관리** 항목에서 관리자가 직접 확인처리하여 변경하거나 **노드 상세정보** 화면에서 관리자가 변경하지 않는 경우 6번 설정으로 인하여 최초 탐지된 플랫폼과 노드타입이 확인된 정보로 유지됩니다.
>
> 노드의 플랫폼,타입이 기존과 다르게 탐지되는 정보는 **관리 > 현황&필터 > 변경관리** 메뉴와 대시보드 위젯 **노드 변경관리** 에서 모니터링 가능합니다.

방법2: 노드타입 – 감지방법 – 관리자지정 조건 으로 예외그룹 조건을 사용하는 방법

1. **Web콘솔 > 관리 > 현황&필터 > 노드타입** 으로 이동하여 예외처리 할 노드타입을 선택합니다.
2. 우측 리스트화면 좌측 상단 체크박스를 선택하여 리스트에 표시된 모든 노드의 체크박스에 체크합니다.
3. **작업선택 > 노드 및 장비 > 노드 속성 변경** 을 선택합니다.
4. 노드타입을 변경 (지정) 합니다. 항목을 체크, 지정할 노드타입을 선택하고 하단 저장 버튼을 클릭합니다.
5. 예외처리 할 다른 노드타입도 동일한 작업을 수행합니다.
6. 제어정책 메뉴로 이동하여 예외처리 정책의 노드그룹 조건을 **노드타입 > 감지방법 > 관리자지정** 조건을 추가하고 수정 버튼을 클릭, 화면 상단 변경정책 적용 버튼을 클릭하여 정책을 적용합니다.

> **Attention:** 감지방법을 관리자지정 조건을 사용할 경우 별도의 노드타입별로 지정이 되지 않아 만약 예외처리할 노드타입이 아닌 다른노드의 노드타입을 지정한 경우 해당 노드도 예외처리 정책에 포함될 수 있습니다.
>
> 노드타입을 변경(지정) 하는 경우, 스캐닝으로 인한 갱신시 다른 노드 타입으로 변경되지 않아 기존과 동일하게 감지된 노드타입 조건 으로도 정책설정이 가능합니다.
>
> 신규로 등록되는 예외처리 노드도 모니터링하여 노드타입을 변경(지정) 해야 예외처리 누락이 되지 않습니다.

방법3: 예외 노드그룹 조건을 기존대로 사용 + 노드스캐닝 검사 OFF

1. **Web콘솔 > 관리 > 현황&필터 > 노드타입** 으로 이동하여 예외처리 할 노드타입을 선택합니다.
2. 우측 리스트화면 좌측 상단 체크박스를 선택하여 리스트에 표시된 모든 노드의 체크박스에 체크합니다.
3. **작업선택 > 노드 및 장비 > 노드 관리 설정** 을 선택합니다.
4. **노드정보 검사** 항목을 체크하고 **Off** 옵션을 선택, 하단 저장버튼을 클릭합니다.

> **Attention:** 노드스캐닝 검사 OFF 설정을 하게 되면, 해당 노드로의 스캔작업이 수행되지 않습니다. 그로 인해 노드 탐지 정보 갱신이 이루어지지 않아 노드타입이 변경되는 문제가 발생하지 않습니다.
>
> 새로 추가된 예외노드에도 지속적으로 해당 설정을 수행해야합니다.

15.4.5 ZTNA로 인한 차단이 의심될때 확인 방법

Genian ZTNA를 운영하는 환경에서 간혹 단말의 네트워크 통신이 실패할 때 ZTNA와 관련이 있는지에 대한 부분을 확인하는 방법을 안내합니다.

Genian ZTNA는 크게 2가지 형태로 단말을 제어합니다.

- 네트워크센서를 통한 제어
- 에이전트를 통한 제어

각 제어 방법별로 확인하는 방법을 안내합니다.

1. 호스트 센서를 통한 제어

- 네트워크센서를 통하여 단말이 제어 되었을때 확인하는 방법

1) 단말 터미널 창을 열어 게이트웨이 IP로 PING 체크를 수행합니다.
2) 게이트웨이 IP로 PING이 정상 체크된다면 네트워크센서에서 제어하는 상황은 아닙니다.
3) 추가로 단말 터미널 창을 열어 ARP 캐시 테이블을 확인합니다.
4) 게이트웨이 IP 와 매칭된 MAC 주소가 네트워크센서의 MAC 주소로 변경되어있는지 반복 확인 합니다.
5) ARP 캐시 테이블 상에서 네트워크센서와 관련이 없는 IP 들이 네트워크센서의 MAC 으로 변경이 안 되어 있다면 ZTNA와 무관한 상황입니다.

2. 미러 센서를 통한 제어

- 미러센서를 통한 제어 시에는 게이트웨이와 ICMP 통신이 정상적으로 수행됩니다. 그래서 호스트센서를 통한 제어방법으로 판단하면 안됩니다.

1) 단말 웹브라우저 창을 열어 웹 접속시도를 합니다. (Google, Naver는 제외한 웹페이지를 권장합니다.)
2) 브라우저 화면에 CWP 페이지의 URL과 화면이 표시되는지 확인합니다.
3) ICMP 통신은 대부분의 구간에 체크가 정상이나 WEB 통신만 비정상일 때 확인하시기 바랍니다.

3. 에이전트를 통한 제어

- 에이전트를 통하여 단말을 제어하는 방법은 여러 가지가 있지만 본 상황에서는 네트워크 통신에 대한 부분만 확인합니다.

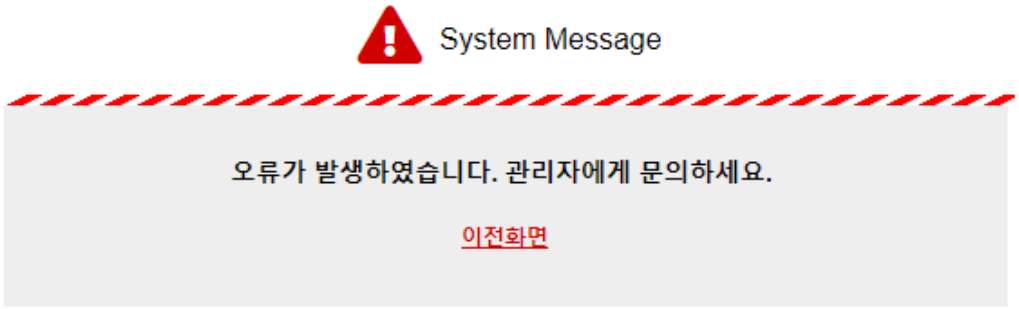
1) 시작버튼 > 설정 > 네트워크 및 인터넷 > 어댑터 옵션 변경 > 주 사용 네트워크 어댑터가 회색으로 사용 안 함 상태인지 확인합니다.
2) 사용 안 함 상태가 아니라면 에이전트 인터페이스 제어가 수행된 상태는 아닙니다.

15.5 시스템

15.5.1 웹콘솔 시스템 에러

증상

관리WebUI에서 특정 메뉴를 선택하였을 경우 아래와 같은 오류 메시지 표시:



원인

정책서버 데이터베이스와 WEB 프로세스 간의 연결을 지원하는 JAVA 프로세스에 오류가 있는 경우 발생할 수 있다.

해결 방법

- 다음 단계를 따르십시오.
- 관리UI에 접속.
- 상단 **시스템 > 서비스 관리 > 디버그로그** 로 이동.
- **tomcat > catalina.out** 을 선택합니다.
- 새로운 창을 실행하여 에러가 발생한 작업을 수행하여 오류 메시지를 합니다.
- 기술 지원 엔지니어와 디버그와 증상을 공유하여 기술 지원을 받습니다.

15.5.2 정상노드의 네트워크 차단

증상

제어정책에서 노드는 Perm-all 권한을 할당 받았지만 네트워크 통신은 차단되버린 증상 관리WebUI에서는 정책이 정상적으로 적용된 것으로 표시되지만 실제로는 정책이 적용되지 않는 증상

원인

노드에 할당된 제어정책이 변경되면 정책서버는 네트워크센서에게 노드의 정책 상태를 변경하도록 이벤트를 전송한다. 간혹 네트워크센서가 이 이벤트에 대해 수신해도 정책을 갱신하지 않을 수 있다.

해결 방법

통신연결상태 확인

- 정책서버와 네트워크센서사이에 TCP/443 HTTPS 통신이 정상적인지 확인합니다.
  - 방화벽 또는 기타 보안장비에서 필요한 예외처리가 되어있는지 확인합니다.

네트워크센서 정책 확인

네트워크센서 CLI 명령어를 이용하여 네트워크센서가 노드에 적용한 정책을 확인 할 수 있다.

- 센서 SSH에 접속하여 다음 명령어를 수행한다. `show nodeinfo filter [노드 IP 주소]`
  - 노드에 "제어정책"이 정상적으로 할당되었는지 확인합니다.

정책서버 네트워크센서 로그 확인

정책서버는 디버그파일을 **centerd** 라는 파일에 저장하고 네트워크센서는 **sensord** 파일에 저장한다. 이 디버그 파일에는 노드의 정책변경 내역이 작성되어 있다.

- 다음 단계를 따르십시오.
- 관리UI에 접속.
- 상단 **시스템 > 서비스 관리 > 디버그로그** 로 이동.
- **system > centerd OR sensord** 를 선택합니다.
- 새로운 창을 실행하여 노드의 정책변경을 수행합니다. .
- 디버그화면에 오류가 있는지 확인하고 기술 지원 엔지니어와 디버그와 증상을 공유하여 기술 지원을 받습니다.

정책서버 노드 정책 변경 예시:

```
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.
```

네트워크센서 노드 정책 변경 예시:

```
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
```

15.5.3 노드의 링크상태 오표시

증상

관리WebUI에 노드의 링크상태가 잘못 표기되는 증상

원인

- 네트워크센서는 항상 노드의 링크 상태를 확인합니다. 많은 노드가 센서에 의해 관리되고 있는 경우 노드 링크 상태를 업데이트 하는데 지연이 발생 할 수 있다.
- 노드와 네트워크센서 또는 정책서버와 네트워크센서 간에 통신에 장애가 있을 경우 이 프로세스에 영향을 끼칠 수 있다.

해결 방법

시스템로그 수집

- 정책서버와 네트워크센서간의 통신에 문제가 있는 경우 ZTNA 디버그/패킷 수집을 통해 문제를 해결합니다.
  - Syscollect 기능을 이용하여 기술지원 엔지니어와 증상과 로그를 공유하여 기술 지원을 받습니다.

참고: *ZTNA 디버그로그와 패킷 수집*

15.5.4 데이터베이스 크래시 발생 시 복구

Genian ZTNA는 시스템 설정, 정책, 수집정보들을 모두 데이터베이스에 저장하고 있습니다. H/W 오류나 S/W 오류로 인하여 데이터베이스에 문제가 발생한 경우 백업파일을 이용하여 데이터베이스를 복구 할 수 있습니다.

원인

데이터베이스는 다양한 문제로 인하여 크래시가 발생합니다. H/W문제 내부 데이터베이스 엔진 및 설정문제 등으로 발생하는데 본 문서는 데이터베이스 크래시 발생 시 복구하는 방법을 안내합니다.

증상

Web콘솔 로그인 실패, 정책할당 및 정책갱신 실패, 설정조회 실패 등

해결방법

백업파일에 있는 데이터베이스 정보를 이용하여 데이터베이스를 복구합니다.

```
Step 1 백업파일이 외부에 있다면 SecureCRT, lePutty, Xshell 등 Zmodem을 지원하는 터미널을 이용하여
백업파일을 업로드 합니다.
    백업파일이 복구할 장비내부에 있는경우 Step3로 이동합니다.
genian#
!!! WARNNING !!! - SHELL PROMPT IS JUST FOR MAINTENANCE.
!!! WARNNING !!! - USE AT YOUR OWN RISK.
Genians$ cd /disk/data/DBBACKUP
```

(continues on next page)

(continued from previous page)

```
Genians$ rz [백업파일]
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 gnlogin CLI에 접속합니다.
genian$ gnlogin

Step 3 복원할 시점의 백업파일을 확인합니다.
genian# show backup
Backup lists
--------------------------------
ALDER-93180-20210511-094236

Step 4 데이터베이스를 복원합니다.(옵션에서 데이터베이스만 선택합니다.)
genian# do restore [백업파일명]
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

Step 5 시스템이 재구동되고 데이터베이스 복원이 정상적으로 되었다면 모든 시스템이 정상적으로 동작합니다.
```

15.5.5 시스템 사용중인 네트워크 포트 확인 및 변경

증상

Genian ZTNA 시스템 서비스가 정상적으로 구동되지 않음

원인

서비스가 구동하기 위한 정상적인 통신이 실패하는 경우 문제점이 발생할 수 있다.

해결방법

네트워크 포트 확인

구축 시 해당 정보를 참고하여 각 구성간 통신이 정상적으로 수행되는지 확인할 수 있다.

1. 상단 패널에 **시스템** 으로 이동합니다.
2. 왼쪽 **서비스 관리** 항목에서 **접속포트** 를 선택합니다.

항목	설명	비고
HTTP	CWP와 신청시스템에서 사용하는 포트가 표시됩니다.	변경가능
HTTPS	CWP, 신청시스템, 정책수신, 정보 업데이트에서 사용하는 포트가 표시됩니다.	변경가능
HTTPS	관리콘솔에 사용하는 포트가 표시됩니다.	변경가능
KeepAlive	이벤트 송수신 및 장비 동작상태를 체크하는 서비스에 사용되는 포트가 표시됩니다.	변경불가
Syslog	syslog 수신 서비스에 사용되는 포트가 표시됩니다.	변경불가
Radius Authentication	Radius 사용자 인증에 사용되는 포트가 표시됩니다.	변경가능
Radius Accounting	Radius Accounting 수신에 사용되는 포트가 표시됩니다.	변경가능
Distribution Server	운영체제 업데이트 검색 및 다운로드, Agent 파일 배포에서 사용하는 포트가 표시됩니다.	변경불가
Data Server	Database 서비스에 사용하는 포트가 표시됩니다.	변경가능
Log Server	Log 검색과 HA구성에서의 클러스터 서비스에 사용하는 포트가 표시됩니다.	변경가능
SSH	제품 원격 CLI 접속 서비스에 사용되는 포트가 표시됩니다.	변경가능

네트워크 포트 변경

알려진 포트 사용이 문제점으로 판단될 경우 사용 포트를 변경할 수 있다.

HTTP 서비스에 대한 포트 변경하기

Genian ZTNA 시스템에서 HTTP 프로토콜을 통해 제공되는 서비스는 접속인증페이지(CWP)와 IP신청시스템이 있으며, 기본적으로 사용되는 알려진 포트 80을 통해 서비스가 제공됩니다.

사용중인 HTTP 포트는 다음에 과정을 통해 변경할 수 있습니다.

Note: HTTP 서비스는 정책서버에서만 제공합니다.

정책서버 포트 변경하기

1. 정책서버에 SSH를 사용하여 CLI Mode로 접속합니다. (SSH 접속방법은 *CLI 콘솔* 참고하시기 바랍니다.)
2. Globle configuration Mode로 전환합니다.

```
genian> enable
genian# configure terminal
```

3. *management-server http-port* 명령어를 사용하여 포트를 변경합니다.

```
genian(config)# management-server http-port 20000
```

HTTPS 서비스에 대한 포트 변경하기

Genian ZTNA 시스템에서 HTTPS 프로토콜을 통해 제공되는 서비스는 접속인증페이지(CWP), IP신청시스템, 정책수신, 정보업데이트가 있습니다. 기본적으로 알려진 포트 443을 통해 서비스가 제공되며 다음에 과정을 통해 포트를 변경할 수 있습니다.

Note: HTTPS 포트는 정책수신과 정보 업데이트 기능을 사용함으로 정책서버, 네트워크 센서, 에이전트에 적용됩니다.

정책서버 포트 변경하기

1. 정책서버에 SSH를 사용하여 CLI Mode로 접속합니다. (SSH 접속방법은 *CLI 콘솔* 참고하시기 바랍니다.)
2. Globle configuration Mode로 전환합니다.

```
genian> enable
genian# configure terminal
```

3. *management-server https-port* 명령어를 사용하여 포트를 변경합니다.

```
genian(config)# management-server https-port 22000
```

네트워크 센서 포트 변경하기

1. 네트워크 센서에 SSH를 사용하여 CLI Mode로 접속합니다. (SSH 접속방법은 *CLI 콘솔* 참고하시기 바랍니다.)
2. Globle configuration Mode로 전환합니다.

```
genian> enable
genian# configure terminal
```

3. *node-server port* 명령어를 사용하여 정책서버와 동일한 포트로 변경합니다.

```
genian(config)# node-server port 22000
```

Web콘솔 접속포트 변경하기

Genian ZTNA 시스템에서 별도의 HTTPS 프로토콜을 통해 관리자의 Web UI 접속을 지원합니다. 기본적으로 포트 8443을 통해 서비스가 제공되며 다음에 과정을 통해 포트를 변경할 수 있습니다.

정책서버 포트 변경하기

1. 정책서버에 SSH를 사용하여 CLI Mode로 접속합니다. (SSH 접속방법은 *CLI 콘솔* 참고하시기 바랍니다.)
2. Globle configuration Mode로 전환합니다.

```
genian> enable
genian# configure terminal
```

3. *management-server mgmt-port* 명령어를 사용하여 포트를 변경합니다.

```
genian(config)# management-server mgmt-port 28443
```

Radius Authentication 서비스에 대한 포트 변경하기

Genian ZTNA 장비를 Radius 서버로 사용할 경우 인증과 관련한 포트를 변경할 수 있습니다. 기본적으로 사용되는 알려진 포트 1812을 통해 서비스가 제공되며 다음에 과정을 통해 포트를 변경할 수 있습니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **서비스** 항목에서 **RADIUS서버** 를 선택합니다.
3. **RADIUS Authentication Server** 설정에서 **포트번호(Authentication)** 를 입력합니다.
4. **수정** 버튼을 클릭합니다.

Radius Accounting 서비스에 대한 포트 변경하기

Genian ZTNA 장비에서 Radius Accounting 연동을 통해 사용자 인증 정보를 수신하는 서비스에 대한 포트를 변경할 수 있습니다. 기본적으로 사용되는 알려진 포트 1813을 통해 서비스가 제공되며 다음에 과정을 통해 포트를 변경할 수 있습니다.

1. 상단 패널에 **설정** 으로 이동합니다.
2. 왼쪽 **서비스** 항목에서 **RADIUS서버** 를 선택합니다.
3. **RADIUS Accounting Server** 설정에서 **포트번호(Accounting)** 를 입력합니다.
4. **수정** 버튼을 클릭합니다.

Data Server 서비스에 대한 포트 변경하기

Genian ZTNA 장비에서 데이터를 저장하는 데이터베이스 서비스에 대한 포트를 변경할 수 있습니다. 기본적으로 사용되는 알려진 포트 3306을 통해 서비스가 제공되며 다음에 과정을 통해 포트를 변경할 수 있습니다.

Note: Database 분리구성과 Replication 구성 경우에는 개별 서버에 추가적으로 작업해야 합니다.

---

1. 정책서버에 SSH를 사용하여 CLI Mode로 접속합니다. (SSH 접속방법은 *CLI 콘솔* 참고하시기 바랍니다.)
2. Globle configuration Mode로 전환합니다.

```
genian> enable
genian# configure terminal
```

3. *data-server port* 명령어를 사용하여 포트를 변경합니다.

```
genian(config)# data-server port 23306
```

LOG Server 서비스에 대한 포트 변경하기

Genian ZTNA 장비에 Log Server를 사용할 경우 로그검색과 클러스터 구성에 대한 포트를 변경할 수 있습니다. 기본적으로 사용되는 알려진 포트 9200(로그검색), 9300(클러스터) 을 통해 서비스가 제공되며 다음의 과정을 통해 포트를 변경할 수 있습니다.

Note: Log Server 분리구성 및 클러스터 구성일 경우에는 개별 서버에 추가적으로 작업을 해야 합니다.

Log Server 검색 서비스 관련 포트 변경하기

1. 정책서버에 SSH를 사용하여 CLI Mode로 접속합니다. (SSH 접속방법은 *CLI 콘솔* 참고하시기 바랍니다.)
2. Globle configuration Mode로 전환합니다.

```
genian> enable
genian# configure terminal
```

3. *log-server http-port* 명령어를 사용하여 포트를 변경합니다.

```
genian(config)# log-server http-port 29200
```

Log Server 클러스터 서비스 관련 포트 변경하기

1. 정책서버에 SSH를 사용하여 CLI Mode로 접속합니다. (SSH 접속방법은 *CLI 콘솔* 참고하시기 바랍니다.)
2. Globle configuration Mode로 전환합니다.

```
genian> enable
genian# configure terminal
```

3. *log-server tcp-port* 명령어를 사용하여 포트를 변경합니다.

```
genian(config)# log-server tcp-port 29300
```

SSH 서비스에 대한 포트 변경하기

Genian ZTNA 장비에 CLI Mode 원격접속에 대한 포트를 변경할 수 있습니다. 기본적으로 사용되는 포트 3910를 통해 서비스가 제공되며 다음의 과정을 통해 포트를 변경할 수 있습니다.

1. 정책서버에 SSH를 사용하여 CLI Mode로 접속합니다. (SSH 접속방법은 *CLI 콘솔* 참고하시기 바랍니다.)
2. Globle configuration Mode로 전환합니다.

```
genian> enable
genian# configure terminal
```

3. *ssh port* 명령어를 사용하여 포트를 변경합니다.

```
genian(config)# ssh port 23910
```

15.5.6 WEB 콘솔 접속 시 SSL 인증서 오류창 발생

증상

Genian ZTNA Web콘솔 접속 시 인증서 오류창 발생

원인

공인된 인증기관에서 발급된 인증서를 사용하지 않아서 발생하는 문제점

해결방법

공인된 인증기관에서 발급된 인증서를 등록한다.

사전 발급된 공인 인증서 등록하기

보안 채널인 TLS 를 사용하여 HTTPS 접속을 수행하기 위한 공인된 기관에서 발급한 인증서를 등록하는 과정입니다.

1. 상단 패널에서 **설정 > 환경설정** 을 선택합니다.
2. 왼쪽 메뉴에서 **인증서관리** 로 이동하십시오.

항목	설명
CA 인증서	CA(Certificate Authority) 기관에 공개키 기반 인증서를 등록합니다.
서버 인증서	서버에 사용되는 공개키 기반 인증서를 등록합니다.
서버 키 파일	서버 인증서에 대칭되는 비밀키를 등록합니다.
서버 이름	서버를 지정하는 도메인을 입력합니다.

Note: 인증서 등록 후 서버에 적용되기 위해서는 서비스 재시작이 필요합니다. 서비스 제어 항목에 제공중인 Web 서비스 재구동을 참고하시기 바랍니다.

공인 인증서 발급받아 등록하기

1. 상단 패널에 설정으로 이동합니다.
2. 왼쪽 환경설정 항목에서 인증서관리 > SSL인증서 를 선택합니다.

서명요청서 작성하기

서명요청서(CSR)에 필요정보를 입력한 후 서버의 공개키를 포함한 서명요청서를 생성할 수 있습니다.

관리자는 Web 콘솔에서 서명요청서를 작성할 수 있으며 해당 서명요청서를 기반으로 인증기관에서 인증서를 요청할 수 있습니다.

1. 서병요청서(CSR) 필요정보를 입력합니다.
2. 서명요청서(CSR) 생성 버튼을 클릭합니다.

3. 서명요청서(CSR) 에 생성된 코드를 복사합니다.
4. 인증서 발급기관에 서명요청서(CSR)을 이용하여 인증서 발급을 요청합니다.

항목	설명
호스트명	사용자 단말에서 접속할 서버의 도메인을 입력합니다.
국가코드	국가를 지정하는 2자리의 국가코드를 입력합니다.
회사/조직명	인증서에 표시될 회사명 또는 조직명을 입력합니다.
이메일	인증서에 표시될 이메일을 입력합니다.

Note: 국내에서 공인인증기관으로 지정된 곳은 한국정보인증(주), (주)코스콤, 금융결제원, 한국정보사회진흥원, 한국전자인증(주), (주)한국무역정보통신 이 있습니다.

발급받은 인증서 등록하기

인증기관에 요청한 서명요청서를 통해 발급받은 인증서를 서버에 등록합니다.

1. 2단계 : 인증서등록 항목에서 발급받은 인증서 해쉬값을 입력합니다.
2. 등록 버튼을 클릭합니다.

Note: 인증서 등록 후 서버에 적용되기 위해서는 서비스 재시작이 필요합니다. 서비스 제어 항목에 제공중인 Web 서비스 재구동을 참고하시기 바랍니다.

15.6 연동

15.6.1 윈도우즈 업데이트 실패

증상

노드의 윈도우즈 업데이트가 되지 않는 증상

원인

- ZTNA는 다음과 같은 방법으로 윈도우 업데이트 서비스를 제공합니다.:
- 윈도우즈 업데이트 검색
- 스케줄링 업데이트
- 윈도우즈 패치검색 서버를 설정 (Genian ZTNA, Genian Proxy, or Microsoft Servers).
- 윈도우즈 패치 다운로드 서버를 설정 (Genian ZTNA, or Microsoft Servers).
- 위와 같은 설정과정이나 사용자 환경에 따라서 업데이트 실패가 발생할 수 있습니다.

해결 방법

윈도우즈 업데이트 로그 확인

업데이트 실패의 정확한 원인은 로그 파일에서 확인이 가능하다.

자세한 내용은 다음을 참조:

- https://docs.microsoft.com/en-us/windows/deployment/update/windows-update-logs
- https://docs.microsoft.com/en-us/windows/deployment/update/windows-update-errors

에이전트 업데이트 로그 확인

에이전트에서 윈도우즈 업데이트를 수행하는 프로세스는 **GnPMS.EXE** 프로세스이다.

디버그 파일은 다음과 같은 순서로 확인:

- 윈도우즈 탐색기를 실행한다.
- 위치 `C:\Program Files\Geni\Genian\Logs\` 위치 한다.
- 윈도우즈 업데이트 플러그인의 Debug 파일은 "UGnPMS[날짜].log" 파일이다.

15.6.2 LDAP 검색 실패 - 작업 오류

증상

LDAP search 수행시 다음과 같은 에러발생 `LDAP search failed. ERR=Operations error`

원인

LDAP 서버의 응답에 참조가 있는 경우 처리 오류 발생

해결 방법

제품 버전 업그레이드

15.6.3 외부 RADIUS 연동테스트시 secret key mismatched 발생

증상

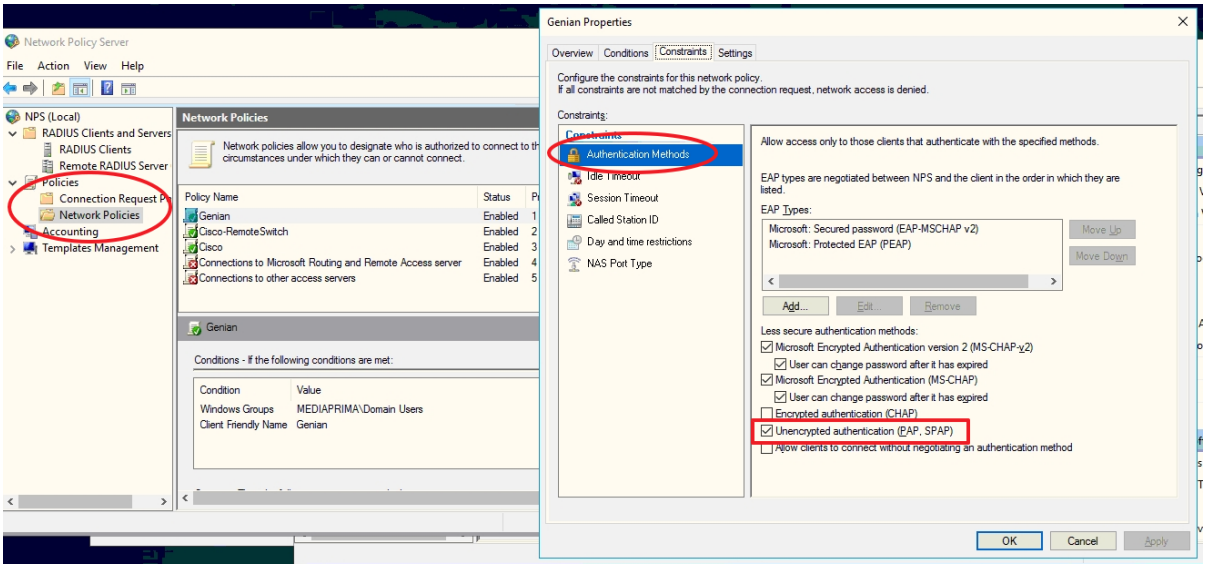
Genian ZTNA와 외부 RADIUS(Windows) 서버 연동 설정을 하고, Web콘솔에서 제공하는 인증 테스트 수행 시 `secret key mismached` 에러 발생

원인

Genian ZTNA 정책서버는 RADIUS 서버에 PAP(비암호화) 방식으로 인증을 요청. RADIUS서버에 비암호화 인증 요청이 허용되지 않은 경우, 인증테스트 창에 위와 같은 오류 메시지 표시되며 인증거부 발생.

해결방법

RADIUS서버에서 비암호화 방식의 인증요청도 허용하도록 설정



CHAPTER

SIXTEEN

RELEASE NOTES

16.1 Current Versions

16.1.1 Genian ZTNA 6.0.24 (R) Release Notes (2024-07-01)

Last Updated: 2024-07-01

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
127367	GN-28264	Windows Agent	무선연결관리자(WCM) 업그레이드 후 4버전 정리기능 추가	
127367	GN-28256	WebUI	관리자 본인의 비밀번호 변경시 현재 비밀번호를 입력하도록 개선	
127367	GN-28253	macOS Agent	macOS ZTNA 로그인 실패 메시지 세분화	
127367	GN-28179	Center	시스템정보의 마더보드 일련번호를 사용하는 노드그룹 조건 추가	
127367	GN-28177	WebUI	관리콘솔 Locale을 Top 메뉴 영역에서 설정할 수 있도록 개선	
127367	GN-28170	WebUI	태그 설정 팝업화면에서 기간선택의 (창)달력 위치가 잘못 표시되는 문제 수정	
127367	GN-28163	macOS Agent	macOS 파일배포 플러그인에 스크립트 실행 가능하도록 개선	
127367	GN-28135	Windows Agent	ZTNA 연결관리자에 의한 네트워크 연결 속도 개선	
127367	GN-28032	Linux Agent	Linux Agent, OSID 추가 작업	
127367	GN-27998	macOS Agent	macOS Agent 백신정보 수집 플러그인에 Apex one 및 비트디펜더 정보 수집 기능 추가	
127367	GN-27907		시스템 관리의 라이선스에서 라이선스 계약항목(EULA)을 확인할 수 있게 한다.	
127367	GN-27862	GenianOS	syscollect 압축파일에 비밀키 설정이 없어 중요 정보가 노출되는 문제	
127367	GN-27698	WebUI	취약점이 검출된 javascript 라이브러리 최신 버전으로 교체	
127367	GN-27552	WebUI	SAML IdP 설정시 IdP의 Metadata 이용해서 자동으로 설정값이 입력되도록 개선	
126780	GN-28021	WebUI	대시보드 리포트 내보내기시 용지 크기를 설정할 수 있도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
127367	GN-28301	Center, WebUI	신규 단말이 MAC 허용을 설정된 IP로 접근했음에도 차단아이콘이 표시되는 문제	4.0.8, 5.0.0, 6.0.0
127367	GN-28237	macOS Agent	macOS에서 슬립모드 해제 후 ZTNA연결시도 시 연결되지 않음	5.0.13, 6.0.0
127367	GN-28201	WebUI	Flow 로그의 Applications Detail 데이터가 깨져보이는 문제	
127367	GN-28157	Windows Agent	운영체제 정보 수집 플러그인을 통해 잘못된 업데이트 설정값 수집으로 '자동업데이트'항목에 빈값 표시	5.0.0, 6.0.0
127367	GN-28141	WebUI	IP신규신청(자동승인 사용)을 신청서추가로 여러건 신청 시 승인 완료 메일이 중복으로 발신되는 문제	5.0.42, 6.0.0
127367	GN-28013	WebUI	cwp2 디자인 템플릿(이미지 레이아웃) 사용시 SAML 로그인 버튼 및 메시지 위치 오류	5.0.30
127367	GN-27860		6.0 버전 신규위젯의 링크 오동작 및 미출력되는 항목 수정	

16.1.2 Genian ZTNA 6.0.16 (LTS) Release Notes (2023-07-21)

Last Updated: 2024-07-01

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
125678	GN-28063	WebUI	노드관리 검색바에 Blind Injection 가능한 문제		2.2
125405	GN-27107	WebUI	권한 없는 관리자로 인한 Tomcat 재구동 명령 수행으로 서비스 무력화	5.0.41	2.7
123782	GN-26393	WebUI	접근 권한 없는 페이지에 직접 URL을 입력하여 정보 수정이 가능한 취약점		3.1
123250	GN-26390	WebUI	감사로그 REST API를 통한 권한 없는 관리자의 파일 내보내기 권한 우회 취약점		3.1
122613	GN-27492	WebUI	Tomcat Version Upgrade (8.5.94 -> 8.5.96 / 9.0.81 -> 9.0.83)		7.5
121383	GN-26315	WebUI	2단계 인증에서 인증코드 입력값 횟수제한, 시간제한하도록 개선		4.3
120870	GN-27278	WebUI	Tomcat Version Upgrade (8.5.94 / 9.0.81)		7.5
120400	GN-27014	WebUI	권한이 없는 상태에서 Passkey 재등록 기능을 이용해서 Passkey를 등록할 수 있는 문제		3.9
120400	GN-26935	WebUI	부서명으로 출력된 html tag가 tree에서 실행되는 취약점	5.0.0	1.2
120400	GN-26835	Center	데이터 업데이트에 사용되는 SQL을 통한 Command Injection 취약점		6.6
120400	GN-26833	Sensor	센서의 NMDB 업데이트 과정에서 nmap 스크립트 변조 취약점		4.1
120400	GN-26696	Sensor	센서의 수신 이벤트에 대한 검증 미흡		6.3
120400	GN-26694	Center	다운로드 URL 검증 미흡으로 인한 Parameter Injection 취약점		6.6
120400	GN-26383	WebUI	html/script 코드 주입 가능한 취약점		5.3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
127333	GN-28368	macOS Agent	macOS 에이전트, 신규출시된 macOS 15(코드명 Sequoia) 지원	5.0.0, 6.0.0
125149	GN-27973	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 3.0.13, 1.1.1w 업그레이드 - X.509 정책 제약 조건을 확인하는 과정에서 과도한 리소스 사용	4.0.0, 5.0.0, 6.0.0
123470	GN-27625	Sensor	센서 운영모드 및 정책변경시 pubilc ip를 가져오지 못할 경우 반영되지 않는 문제 개선	
122931	GN-25063	WebUI	6.0 버전 위젯 추가	

continues on next page

Table 1 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122687	GN-27462	Windows Agent	파일 배포 V2 플러그인 설치할 때 운영체제(64/32비트)에 해당하는 cosign 파일만 다운로드하도록 개선	5.0.42, 4.0.155, 6.0.15, 5.0.55 (LTS), 5.0.56 (50 LTS), 5.0.57
122233	GN-27164	VRRPD	[범용OS] 이중화 구성 master 상태로 전환 후 인터페이스 상태검사 실패로 인해 slave 상태로 전환되는 문제	5.0.42
122171	GN-27390	Center, WebUI	리포트 보존개수 설정 시 /disk/data/report 디렉토리의 데이터도 삭제하도록 개선	
122168	GN-24332	WebUI	URL filter에 의한 차단시 출력페이지 변경	
121930	GN-27241	macOS Agent	macOS 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121903	GN-27248	Linux Agent	Linux Agent, 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121114	GN-27269	- Unknown/None-	apache / tomcat 관련 디렉토리 및 파일의 불필요한 권한 제거	
120400	GN-27402	WebUI	MAC 정책 수정 시 시작/종료 시각을 설정할 수 있도록 API 개선	
120400	GN-27207	Windows Agent	다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
120400	GN-27206	Center, Sensor	센터에서 신뢰할 수 있는 nodeid 를 센서와 에이전트로 내려보내는 기능 추가	
120400	GN-27146	Center	extauth 를 통한 외부인증연동 실패시 사용자가 입력한 패스워드가 센터디버그파일에 남는 문제	
120400	GN-27142	Windows Agent	알약 신규버전에 대응하는 연동 모듈 변경	
120400	GN-27121	Center, macOS Agent	macOS 에이전트 신규 OS 14.0 (Sonoma) 지원	
120400	GN-27046	WebUI	노드 등록, 노드 일괄등록, 노드 속성 가져오기에 IP/MAC 추가필드 항목을 추가	
120400	GN-27045	WebUI	노드관리 목록에 신규로 추가된 IP, MAC 추가필드 출력 기능 추가	
120400	GN-27038	WebUI	openssh 버전업 이후 webssh 접속되지 않는 문제 개선	
120400	GN-27031	Center, Sensor	[범용OS] Ubuntu OverlayFS 모듈에서 발생하는 로컬 권한 상승 취약점	
120400	GN-27013	WebUI	markdown으로 설정된 항목을 변환할 수 있도록 개선	
120400	GN-26988	macOS Agent	macOS 파일 배포 플러그인 V2 사용시 승인창 표시되지 않도록 기능개선	
120400	GN-26987	Linux Agent	Linux Agent, 파일 배포 플러그인 V2 사용시 승인창 표시되지 않도록 기능개선	

continues on next page

Table 1 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120400	GN-26981	Center, Linux Agent, macOS Agent, WebUI, Windows Agent	배포 플러그인 V2 사용시 승인창 표시 되지 않도록 기능 개선	
120400	GN-26879	WebUI	IP/MAC 추가필드 관리 기능 추가	
120400	GN-26838	Ubuntu(Debian)	[범용OS] ICMP Timestamp 지원 기능 제거	
120400	GN-26792	Center, Sensor	정책서버 수신 이벤트 검증 강화	
120400	GN-26791	WebUI	노드 일괄 등록시(csv 파일 업로드) 사용 가능한 커스텀필드 20개 까지 확장	
120400	GN-26789	Genian Syncer	지니안싱커로 동기화 되는 운영정보데이터의 전자서명 검증	
120400	GN-26778	Center	IP/MAC 추가필드 관련 노드그룹 조건 추가	
120400	GN-26766	Center, macOS Agent	macOS Sigstore 전자서명을 기반한 배포 플러그인 개발	
120400	GN-26730	macOS Agent	macOS 에이전트 ZTNA 신규 아이콘 적용 및 연결표시 변경	
120400	GN-26729	macOS Agent	macOS 에이전트 백신정보수집 플러그인 사용시 AhnLab V3 정보를 수집 못 하는 증상	
120400	GN-26724	Sensor	Axgate 80D, 200AX 모델 포팅 모듈 커널 업그레이드 (2.6.38->4.14.196) 개선	
120400	GN-26644	Windows Agent	센터 CA 인증서 설치 옵션을 기본 ON으로 변경 및 수행주기 변경	
120400	GN-26619	Sensor	NMAP 스캔 수행시 HNAP-NSE 사용 유무를 옵션으로 설정할수 있도록 개선	
120400	GN-26563	Sensor	센서 인터페이스에 Alias IP 설정없이 Alias IP대역을 센서가 관리할 수 있도록 개선	
120400	GN-26535	wsdump	DKNS 센서 구동시 WLAN 모니터링 기능 동작하도록 개선	
120400	GN-26479	Sensor	센서 reboot / poweroff 명령을 통해서 종료하는 경우 차단노드에 대해서 차단해제되도록 개선	
120400	GN-26450	WebUI	이력관리 목록에서 페이지 이동 시 스크롤이 상단으로 이동하도록 개선	
120400	GN-26442	GenianOS	[범용OS] ubuntu 타겟에 openvpn 패키지 추가	
120400	GN-26381	WebUI	사용자관리 목록에 조직명(USER_COMPANY) 컬럼 추가	
120400	GN-26330	Integretion	Keycloak 인증시 NAC 사용자DB를 사용할 수 있도록 provider 추가	
120400	GN-26300	WebUI	CWP 장치신청서 및 알람메시지 타임존 맞지 않는 문제	
120400	GN-26187	WebUI	사용자 등록 페이지의 피방문자 검색을 관리자의 이메일로 조회할 수 있도록 개선	

continues on next page

Table 1 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120400	GN-24976	WebUI	대시보드에 Flow Application Name 통계 위젯 추가	
120400	GN-23316	Center	정책서버 이미지에 센서/에이전트 포함하여 업그레이드 간편화	
120400	GN-19829	CLOUD	On-Prem 백업파일을 Cloud에 Restore 할 수 있도록 한다	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
127285	GN-27617	Windows Agent	운영체제 정보 수집 액션으로 AD서버에 빈암호 사용여부를 체크하여 AD계정이 잠기는 문제	4.0.109, 5.0.6, 6.0.0
127269	GN-28418	Windows Agent	윈도우 업데이트 액션에서 지정시각설치/검사 옵션이 적용되지 않는 문제	5.0.0, 6.0.0
127160	GN-28370	WebUI	센서 관리 > 센서설정 > IP설정의 인터페이스 설정 클릭시 설정항목 표시 되지 않는 문제	5.0.42, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS), 5.0.57
126840	GN-28306	Center, Sensor	시스템 명령 실행시 간헐적으로 실행결과를 가져오지 못해서 프로세스가 비정상적으로 동작하는 문제	5.0.42
126733	GN-28295	Center	정책서버 DB 연결 실패시 전체 감사로그가 삭제되는 문제	4.1.3
126397	GN-28228	Sensor	[범용OS] 센서가 업/다운상태를 반복하는 문제	5.0.42
126002	GN-28047	Sensor	[범용OS] 센서에서 snmp 데몬이 동작하지 않는 문제	6.0.15, 5.0.55 (LTS)
125368	GN-27983	Center	5.0/6.0 정책서버에서 보내는 이벤트패킷이 4.0.1 센서에서 처리 안되는 문제	5.0.42, 6.0.16 (LTS)
125293	GN-27972		SSL 인증서의 유효기간이 10년으로 생성되는 문제	6.0.15, 5.0.55 (LTS)
125276	GN-28003	Windows Agent	파일배포 플러그인 V2에서 배포파일 검증방법이 Sigstore Keyless Signing일 경우 실패하는 문제	5.0.42, 4.0.155, 6.0.15, 5.0.56 (50 LTS)
125167	GN-27994	Linux Agent	Linux Agent 파일배포 플러그인 V2에서 배포파일 검증방법이 Sigstore Keyless Signing일 경우 실패하는 문제	5.0.50, 5.0.53, 5.0.54, 6.0.15

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
125158	GN-28005	macOS Agent	macOS 파일배포 플러그인 V2에서 배포파일 검증방법이 Sigstore Keyless Signing일 경우 실패하는 문제	6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
125044	GN-27986	GenianOS	SLSA TUF 인증서 갱신에 따른 호환성 문제 해결	5.0.42, 5.0.50, 6.0.15, 4.0.156
124336	GN-27442	WebUI	노드관리 목록화면에서 마지막 동작시각 컬럼의 정렬이 동작하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
124083	GN-27749	WebUI	CWP의 사용자 정보 수정 페이지에 접속이 안되는 문제	6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS), 6.0.18, 5.0.58
123722	GN-27652	Center	센터에서 발급한 구글OTP 보안키가 에이전트로 전송 안되서 구글OTP 인증을 진행할 수 없는 문제	6.0.13
123436	GN-27641	WebUI	tomcat 로그에 by the following code has not been returned to the pool 가 다수 발생 후 웹 콘솔 접속 불가증상	5.0.20
123299	GN-27573	WebUI	사용자그룹별 현황에서 각 그룹 인원수 클릭시 목록이 출력되지 않는 문제	4.0.156, 6.0.16 (LTS), 5.0.57
123282	GN-27517	WebUI	Nodes REST API 에서 특정 항목이 수정되지 않는 오류	5.0.8, 4.0.111
123228	GN-27399	macOS Agent	macOS 내부/외부 상태에 맞지 않게 플러그인이 동작하는 문제	6.0.5, 5.0.48
123206	GN-27550	WebUI	트리구조의 데이터 컴포넌트가 출력되지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS), 6.0.17, 5.0.57
123146	GN-27460	GenianOS	[범용OS] 초기동작시 aes256 명령이 실행되지 않는 문제	5.0.42, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
123134	GN-27496	Linux Agent	Linux Agent, 간헐적으로 액션 시스템 정보 전송이 일부 누락되는 문제	5.0.50, 6.0.15

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
123122	GN-27401	Sensor	센서장비에서 동일한 이벤트를 받는 경우 센서프로세스가 비정상 종료 되는 문제	4.0.64
123118	GN-27541	Authsync	정보동기화 서버 접속 실패하면 삭제된 사용자로 처리 되어 전체 사용자가 삭제되는 문제	6.0.9
123056	GN-24708	Center	많은 센서 디버그를 센터로 전송하는 환경에서 센터 재부팅시 오래된 디버그 삭제 동작으로 부하가 발생할 수 있는 문제	5.0.0
123047	GN-27575	Center	ES 로그필터쿼리 결과가 2K보다 크면 로그필터액션이 동작하지 않는 문제	4.1.M6
122947	GN-27574	Center	ES로그 정리주기에 로그필터를 위한ES인덱스(nac-filter)가 삭제되는 문제	5.0.50, 6.0.11
122841	GN-27561	Center	[범용OS] LDAP 설정파일이 범용OS 에서 잘못된 파일에 설정되는 문제로 ldapsearch 명령 결과가 실패하는 문제	5.0.42
122588	GN-27502	Center	Keepalive 에 의한 에이전트/센서 다운 체크과정이 오래 걸리는 경우 에이전트 로그온 API 처리가 지연되는 문제	5.0.42
122557	GN-27480	WebUI	노드그룹 조건 중 부서선택 타입의 조건을 검색할 수 없는 문제	5.0.31, 6.0.0
122502	GN-27504	Center	KeepAlive 수신 시 NodeID 관련 DB 오류(Illegal mix of collations) 감사로그 발생되지 않도록 개선	
122482	GN-27451	WebUI	감사 > Flow 로그 목록에서 시간으로 정렬이 되지 않는 문제	6.0.1
122476	GN-27490	CWP	CWP에서 SAML 로그인 버튼 클릭시 Invalid settings: sp_cert_not_found_and_required 메세지 출력되는 문제	6.0.13
122445	GN-26487	WebUI	CVE 상세화면에서 값이 없을 경우 에러페이지 출력되는 문제 수정	5.0.24
122424	GN-27510	Center, Sensor	[범용OS] NAC패키지 업그레이드 후 추가된 라이브러리를 찾지 못하는 문제	5.0.42
122302	GN-27467	WebUI	노드액션 설명에 XSS를 추가하면 정책적용 팝업화면에서 XSS가 실행되는 문제	5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
122254	GN-27437	Center, macOS Agent	macOS Sonoma 단말의 OS정보가 unknown으로 분류되는 증상	6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS), 6.0.17, 5.0.57, 4.0.157

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122081	GN-27383	WebUI	parameter value is invalid 오류 발생하는 문제 및 한글이 입력가능한 입력폼에 모든 언어의 문자가 입력가능하도록 수정	5.0.42, 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
122069	GN-27385	GenianOS	iptables 명령이 동시 실행시 실패될 수 있는 문제 개선	5.0.0, 6.0.0
121997	GN-27417	WebUI	현황 & 필터 > 태그 > 노드 태그가 정상적으로 출력되지 않는 문제	6.0.16 (LTS)
121913	GN-27400	CWP	Agent에서 Passkeys 등록이 되지 않는 문제	6.0.16 (LTS)
121902	GN-27398	Linux Agent	Linux Agent, 조건만 검사 액션 수행 결과가 변경되어도 업데이트 안되는 문제	5.0.50, 6.0.15
121832	GN-27446	Center	외부인증연동(runauth) 이용시 빈 패스워드가 입력되는 경우 SOAP API 처리 프로세스 멈춤 및 CPU 100% 사용하는 문제	5.0.42, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS), 5.0.57, 4.0.157
121706	GN-27380	Windows Agent	액션검사조건에 에이전트가 지원하는 매크로 이외에 '%' 문자가 존재하면 비정상 종료되는 문제	5.0.0, 6.0.0
121592	GN-27393	WebUI	IP,MAC 추가필드 사용자선택기에서 설정된 맵핑 컬럼키가 동작하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
121505	GN-27382	WebUI	추가필드 - 사용자선택기에서 한글 및 일부 특수문자 포함시 parameter value is invalid 오류가 발생하는 문제	5.0.42, 5.0.50, 5.0.53, 4.0.155, 6.0.15
121461	GN-27394	Center	SFTP 저장장치 경로에 절대경로 설정 시 백업 실패하는 문제	5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
121448	GN-27291	WebUI	Alias 센서명에 *, · 등의 특수문자가 포함된 경우 parameter value is invalid 에러 발생	5.0.42, 4.0.156, 6.0.16 (LTS)
121419	GN-27209	WebUI	IP 신청 승인 완료 및 요청 Email 알림이 가지 않는 문제	5.0.46, 6.0.4
121394	GN-27388	Center	[범용OS] webssh 접속 안되는 문제	5.0.42
121368	GN-27203	Windows Agent	불특정하게 액션수행결과가 변경되어도 일정시간(5분) 후에 전송하는 문제	5.0.0, 6.0.0

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
121159	GN-27259	Linux Agent	Linux Agent, 특정 패키지로 에이전트 설치시 동작하지 않는 문제	5.0.45, 6.0.2
121154	GN-27221	Linux Agent	Linux Agent, 모니터 정보수집 플러그인에서 EDID값이 존재하지 않는 모니터를 수집할 경우 에이전트가 비정상적으로 종료되는 문제	6.0.12
121132	GN-27359	gnlogin, VR-RPD	이벤트재전송처리가 필요없는 프로세스에서도 이벤트큐 처리가 동작하여 Same event already exist in queue 디버그 로그가 발생하는 문제	5.0.42
121016	GN-27358	Center	centerd 실행 옵션의 센서 서비스 시작/중지 기능 동작하지 않는 문제	5.0.42, 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120716	GN-27290	WebUI	센서명에 '%' 가 포함되는 경우 센서트리가 정상적으로 표시되지 않는 문제	5.0.43, 6.0.0
120644	GN-27292	WebUI	노드상세에서 정책 설정 시 IP/MAC 목록을 선택하여도 선택항목이 입력되지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
120603	GN-27279	Center, Sensor	센터 장비에서 trust-nodeserver-id 설정시 센서 데몬을 재시작 해야지만 설정이 적용되는 문제	5.0.42, 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120534	GN-27091	Center, procmond	센서에서보내는 이벤트로그(procmond 프로세스)가 정책서버에서 unknown center did 에러 발생하면서 로그 저장안되는 문제	5.0.42
120519	GN-27113	Center	Slave 장비에서 전송되는 업데이트정보(sysinfo)를 unknown devid 로 업데이트 실패하는 문제	4.0.145, 5.0.42, 6.0.1
120506	GN-27200	Center	slave 센터에서 BadQuery=Illegal mix of collations 오류가 계속 발생하는 증상	5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120499	GN-27177	Backup	백업 파일에 에이전트 zip 파일이 포함되어 용량이 증가하는 문제	6.0.16 (LTS), 5.0.55 (LTS)
120420	GN-27210	Enforcer	Netflow 로그에 제어정책명이 안남는 문제	6.0.16 (LTS)
120412	GN-27224	Windows Agent	에이전트 인증창으로 화면이 잠겨있는 상태에서 입력대화상자 출력 안됨	5.0.49, 6.0.7

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120400	GN-27345	WebUI	페이지 준비(ready) 단계에서 markdown 변환되도록 수정	5.0.42, 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120400	GN-27237	Center, Sensor	관리콘솔에서 센서에 등록된 에이전트노드삭제시 센서에 의해서 노드가 즉시 재등록 안되는 문제	5.0.42
120400	GN-27198	Sensor	ZTNA NAT 예외대역 다중설정시 동작하지 않는 문제	6.0.12
120400	GN-27187	CLOUD	신규 Cloud 정책서버에서 agent 정보가 정상적으로 표시되지 않는 문제	5.0.45, 6.0.2
120400	GN-27183	Center, Sensor	정책서버에서 센서로 전송하는 재등록이벤트(REGISTER_REQ)가 센서에서 처리되지 않는 문제	5.0.42
120400	GN-27176	macOS Agent	macOS 업데이트 플러그인이 비정상 동작하는 문제	5.0.11
120400	GN-27162	Sensor	[범용OS] 장비 부팅후 gdcid 데몬이 구동되지 않는 문제	5.0.42
120400	GN-27158	WebUI	사용자 설정목록 타입의 IP 추가필드 변경 시 노드정보 업데이트 할 수 없는 오류	6.0.16 (LTS), 5.0.55 (LTS)
120400	GN-27154	WebUI	스위치 관리에서 스위치를 삭제하였으나 노드 목록에서 접속장치 컬럼의 링크가 동작하는 문제	5.0.38
120400	GN-27152	WebUI	동일 아이피의 여러 노드가 있을 경우 잘못된 노드가 매트릭스 뷰에 출력되는 문제	4.0.8
120400	GN-27151	geniup	마이그레이션 도중 명령어가 종료되어 마이그레이션이 정상 수행되지 않는 문제	5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120400	GN-27137	macOS Agent	macOS 메세지 팝업 내용이 보이지 않는 문제	5.0.42, 5.0.50, 5.0.53, 5.0.54, 6.0.14
120400	GN-27136	macOS Agent	macOS USB 차단 동작하지 않는 문제	5.0.50, 6.0.9
120400	GN-27132	gnlogin	mysql 패스워드에 % 문자열 존재시 센터 비정상 동작하는 문제	5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120400	GN-27127	Windows Agent	윈도우즈 업데이트 플러그인을 통한 Offline PMS 수행 실패	5.0.42, 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120400	GN-27106	Center	노드정책 즉시적용 시 일부 노드만 적용되는 문제	5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120400	GN-27089	macOS Agent	macOS Agent 관리콘솔에 의한 무결성 체크 명령시 Gn-Daemon재기동 되는 문제	5.0.42, 5.0.54, 6.0.15, 5.0.56 (50 LTS)
120400	GN-27088	Center	URL Filter기능 동작하지 않는 문제	6.0.4
120400	GN-27085	WebUI	SAML로 관리콘솔 로그인시 기존접속을 끊고 접속함(강제로그인) 기능이 동작하지 않는 문제	5.0.48, 6.0.6
120400	GN-27084	WebUI	XSS 검사로직에서 URLEncode처리된 파라미터에 대한 오탐으로 인해 감사로그가 남는 문제	5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120400	GN-27066	Windows Agent	파일배포V2에서 스크립트 수행시 CMD창 표시 오류 수정	5.0.42, 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120400	GN-27058	Windows Agent	PC 재시작시 내/외부 상태에 따라 수행 설정한 액션이 오동작하는 문제	5.0.43, 6.0.0
120400	GN-27053	WebUI	노드속성 가져오기 기능에서 AUTHUSER (인증사용자) 컬럼을 사용할 수 없는 문제	5.0.30
120400	GN-27047	WebUI	톰캣 구동시 Elastic 관련 초기화 중 오류가 발생하여 Elastic Percolate가 초기화 되지 않는 문제	5.0.53, 6.0.14
120400	GN-27037	MGMT	[범용OS] 관리콘솔 포트와 HTTPS 포트를 동일하게 설정하는 경우 apache 구동 안되는 문제	5.0.42
120400	GN-27016	Sensor	localconf의 서비스포트가 센서데몬에 의해서 불특정 값으로 변경되는 문제	NoVersion
120400	GN-27012	Center	ZTNA Client 연결시 다른 센서로 접근시도하는 문제	6.0.4

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120400	GN-27000	WebUI	노드관리목록 > 인증사용자 컬럼의 링크로 사용자 상세 화면 이동 시 유효하지 않은 파라미터 메시지 출력되는 문제	6.0.5, 5.0.50
120400	GN-26973	macOS Agent	macOS 사용자 알림메시지 주기적 수행시 팝업 되지않는 문제	5.0.42, 5.0.50, 5.0.53, 6.0.14
120400	GN-26972	Center	SLAVE 장비가 존재하는 경우 'BadQuery=Illegal mix of collations' 오류가 발생하는 문제	5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120400	GN-26970	Center	Push Notification 이벤트처리 개선버전 에이전트임에도 정책서버에서 과거 이벤트처리방식으로 이벤트처리하는 문제	5.0.42, 4.0.155
120400	GN-26969	WebUI	Get Parameter(QueryString) 관련 XSS 오탐 문제	5.0.42, 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120400	GN-26958	Center	ZTNA 고정아이피 할당시 신규 아이피가 할당되는 문제	6.0.13
120400	GN-26957	macOS Agent	macOS 플러그인 적용 범위와 무관하게 액션 즉시수행시 액션이 수행되는 문제	6.0.5, 5.0.48
120400	GN-26956	WebUI	인증연동 설정 수정시 Exception 오류 메세지가 출력되는 문제	6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120400	GN-26938	Linux Agent	Linux Agent, 로컬 네트워크 변경 감지 오류로 신규 노드 등록이 되지 않는 문제	5.0.51, 6.0.11
120400	GN-26934	Sensor	ZTNA Client 세션 모니터링 정보가 실제와 다른 문제	6.0.15
120400	GN-26931	Center	마더보드 정보(updateinfo)가 삭제되지 않는 문제	5.0.52, 6.0.13
120400	GN-26930	Center	알람 전송 실패 메시지 사용안함 설정 시 검색필터 관련 기능이 동작하지 않는 문제	5.0.39
120400	GN-26901	Sensor	[AXGATERALINK] 잘못된 엔디안으로 빌드하여 정책업데이트가 되지 않은 문제	6.0.5, 5.0.48
120400	GN-26898	WebUI	대시보드 라이선스 경고 메시지에 html이 텍스트로 표시되는 문제	6.0.15
120400	GN-26895	macOS Agent	macOS Mac mini M2 모델에서 소프트웨어 정보수집을 하지 못하는 현상	5.0.11
120400	GN-26887	WebUI	센서모드 전환시 노드목록의 제어정책 컬럼의 툴팁이 갱신되지 않는 문제	5.0.50, 6.0.11

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120400	GN-26886	Sensor	DKNS에서 ZTNA Client 연결오류 수정	6.0.15
120400	GN-26870	WebUI	EDR 에서 NAC 연동을 통한 대응 정책 설정시 NAC 노드에 태그가 할당되지 않는 문제	5.0.42, 5.0.45, 6.0.2
120400	GN-26840	WebUI	노드 상세정보의 수집정보 출력 시, 출력 설정과 다르게 출력되는 문제	6.0.4
120400	GN-26785	Center	장치제어 정책 사용 시, 다른 노드 그룹의 장치제어 정책을 수신할 수 있는 문제	5.0.23
120400	GN-26759	WebUI	RADIUS 정책의 조건추가 시 직접입력된 값 항목 수정시 값이 표시되지 않는 문제	6.0.11
120400	GN-26751	Sensor	sensord deadlock 감지시 잘못 데드락을 체크하는 문제	6.0.16 (LTS), 5.0.57
120400	GN-26687	WebUI	노드관리 마지막동작시각 컬럼의 시각이 관리자의 타임존이 적용되지 않고 출력되는 문제	4.1.M4
120400	GN-26674	WebUI	노드관리 제어정책 컬럼이 노드에 적용된 제어정책이 허용(PERM-ALL) 상태 임에도 차단된 상태처럼(주황색) 출력되는 문제	6.0.7
120400	GN-26643	Windows Agent	에이전트 자체인증창 액션정책을 제거해도 이전에 표시된 인증창이 계속 표시되는 문제	5.0.0, 6.0.0
120400	GN-26606	macOS Agent	macOS 인증창에서 엔터키 1회 입력시 로그인 수행되지 않는 문제	5.0.15
120400	GN-26566	WebUI	노드 정보 업데이트 후, 탭 이동 시 변경한 정보가 갱신되어 보여지지 않는 문제	5.0.50
120400	GN-26551	macOS Agent	macOS 에이전트 다수의 액션 수행 조건 검사 시 마지막 조건의 결과만 표시됨	5.0.21, 6.0.0
120400	GN-26511	WebUI	리포트 자동 생성 로그에 로그ID 잘못 입력되는 오류	6.0.1
120400	GN-26490	Center	Custom 서버 도메인을 설정한 경우 ZTNA 접속시 기본포트로 접속시도 하는 문제	6.0.15
120400	GN-26467	Windows Agent	비밀번호유효성검사 액션으로 검증 이후에도 간헐적으로 미검증 사유로 팝업창이 출력됨.	5.0.6, 6.0.0
120400	GN-26459	Sensor	아이피고정 옵션 사용시 ZTNA Client Split tunneling 동작하지 않는 문제	6.0.11
120400	GN-26432	Windows Agent	Windows 인증창,무선연결관리자에서 로고가 좌측 상단에 출력되는 문제	5.0.39, 6.0.0
120400	GN-26431	WebUI	관리콘솔 접속 IP 확인시 "x.x.x.x, x.x.x.x" 형태로 접속IP가 확인되는 경우 접속 가능 IP라도 접속이 되지 않는 문제	5.0.33
120400	GN-26408	Sensor	노드그룹에 노드그룹에 속하지 않는 조건을 넣을 때 간헐적으로 센서데몬이 죽는 문제	4.0.114, 5.0.11
120400	GN-26382	WebUI	사용자 인증 > 인증연동 > SAML2 인증연동에서 SAML IdP설정 또는 추가할때 Http Status 400 - Bad Request가 발생할 수 있는 문제	5.0.25
120400	GN-26380	WebUI	IPMGMT 에서 IP 신청서 양식 다운로드 되지 않는 문제	5.0.43, 6.0.0
120400	GN-26372	Center, Sensor	URL Filter 활성화후 ZTNA Client의 웹 접근이 SWG를 통해 통신되지 않는 문제	6.0.12
120400	GN-26354	Center	인증연동 시 연결되지 않은 로컬DB 계정정보 표시하는 문제	5.0.53

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120400	GN-26341	Authsync	Tibero/Altibase/DB2 정보동기화 시 ID를 제외한 정보가 동기화되지 않는 문제	6.0.8
120400	GN-26314	WebUI	IP 신청 목록 설정에서 부서명 등을 제거하면 IP 신청서에서 라벨이 보이지 않는 문제	4.0.11
120400	GN-26299	Center	인증연동 사용자도메인과 다른 도메인인 경우에도 인증 허용 문제	5.0.53
120400	GN-25831	WebUI	용도 관리의 필드 할당 추가/제거 시 입력타입이 변경되는 문제	4.0.11

16.2 Previous Versions

16.2.1 Genian ZTNA 6.0.23 (R) Release Notes (2024-06-03)

Last Updated: 2024-06-04

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
126762	GN-28125	WebUI	인증서 관리 메뉴의 Self-Signed 인증서 자동갱신 설정값이 변경될 경우 센서에 변경 이벤트 전송하도록 개선	
126762	GN-28100	WebUI	Cloud Provider에서 각 클라우드의 필수 입력 정보에 대한 UI 표시(*) 되도록 기능개선	
126762	GN-28023	WebUI	관리콘솔 SAML 인증 요청시 Signed Requests가 가능하도록 개선	
126762	GN-28020	Sensor	센서장비 SSL 서버인증서를 expire date 에 맞춰서 자동갱신할수 있도록 개선	
126762	GN-28002	CWP	CWP SAML 인증 요청시 Signed Requests가 가능하도록 개선	
126762	GN-27567	WebUI	센서에 alias IP 가 있을 경우, IP주소관리의 매트릭스 뷰에 IP 목록이 정렬되게 개선	
126762	GN-26639	Center	사용자이름 필드 길이가 짧아 이름이 일부 잘려서 저장되는 문제	
126762	GN-24948	macOS Agent	macOS 인증정보 외부연동 플러그인 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
126762	GN-28270	macOS Agent	macOS 에이전트, 도메인명에 하이픈(-)이 포함된 설치파일로 설치 시 에이전트 동작하지 않음	5.0.35, 6.0.0
126762	GN-28254	WebUI	감사로그 검색필터 수정 시 5초 간격으로 화면이 새로고침 되는 것처럼 보이는 문제	6.0.20
126762	GN-28210	WebUI	센서관리에서 dhcp서버가 on 상태인데도 off 로 보이는 문제	5.0.1
126762	GN-28181	Authsync	정보동기화 수행 시 데이터 소스에 존재하지 않는 부서의 삭제 감사로그가 남는 문제	4.0.128, 5.0.25
126762	GN-28122	Center	Genian Syncer를 통한 GenianData 업로드 이후 Windows 업데이트 정책을 생성할 수 없는 문제	6.0.19, 5.0.59
126762	GN-28035	WebUI	Auditor 관리자의 대시보드/로그 화면에서 수정 선택항목이 유지되지 않는 오류	
126762	GN-28000	WebUI	정책 > 그룹 > 노드 화면에서 상태그룹 부분에 이미지가 깨져 보이는 문제	6.0.0

16.2.2 Genian ZTNA 6.0.22 Release Notes (2024-05-07)

Last Updated: 2024-06-03

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
126175	GN-26723	WebUI	관리자의 권한 변경시 즉시 반영 안되는 취약점 수정		3.3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
126175	GN-28061	WebUI	IP 신청시스템 공지사항 본문에도 Markdown 이 적용 가능하도록 개선	
126175	GN-28012	gnlogin	CLI - show backup 명령 결과를 날짜순으로 정렬하도록 개선	
126175	GN-27995	WebUI	CWP SAML 설정 UI 사용자 생성 또는 갱신 용어를 JIT provisioning으로 변경	
126175	GN-27979	WebUI	CyclondeDX와 SPDX를 이용해 SBOM 생성	
126175	GN-27978	CWP	CWP SAML 인증연동시 Single Logout(SLO) 기능 추가	
126175	GN-27952	WebUI	감사로그 검색 조건으로 시간대를 자유롭게 설정할 수 있도록 개선	
126175	GN-27931	WebUI	SAML IdP 설정시 readonly 항목에 대해 복사 기능 추가	
126175	GN-27916	Linux Agent	Linux Agent, gncli 로그 기능 추가	
126175	GN-27887		Linux Agent, gncli 에이전트 삭제기능 추가	
126175	GN-27872	WebUI	IP신청시스템 신청서처리결과 화면에서 사용자도 결과를 확인할 수 있도록 기능 개선	
126175	GN-27849	WebUI	Genian ZTNA V6.0 SP1로 기본 로고 변경	
126175	GN-27846	WebUI	인증 정보의 재사용 시도를 탐지한 경우 인증 실패 및 인증 실패에 대한 감사로그 남기도록 개선	
126175	GN-27842	Windows Agent	Windows Agent, 데이터 암호화 방식 고도화	
126175	GN-27821		Linux Agent, gncli 다국어 지원을 위한 Resource Bundle 작업 (en, ko)	
126175	GN-27813	macOS Agent	macOS Agent, 데이터 암호화 방식 고도화	
126175	GN-27793	WebUI	관리콘솔 SAML 인증시 같은 사용자의 세션이 존재할 경우 강제 접속 하도록 개선	
126175	GN-27771	WebUI	Azure Cloud를 ZTNA Gateway에 추가되도록 기능개선	
126175	GN-27766	Linux Agent	Linux Agent, 데이터 암호화 방식 고도화	
126175	GN-27744	WebUI	국내 / 글로벌에 따라 다르게 EULA 출력하도록 개선	
126175	GN-27690	Windows Agent	웹브라우저 옵션제어 플러그인에 Edge, Chrome 의 보안 옵션 확장	
126175	GN-27683	Linux Agent	Linux Agent, gncli 자동 완성 기능 추가	
126175	GN-27644	macOS Agent	macOS 에이전트의 정책서버에 대한 식별 및 인증을 위한 SSL 인증서 검증 기능 추가	
126175	GN-27643	Linux Agent	Linux Agent, 정책서버에 대한 식별 및 인증을 위한 SSL 인증서 검증 기능 추가	
126175	GN-27539	WebUI	관리콘솔 SAML 인증연동 Single Logout(SLO) 기능 추가	
126175	GN-26926	macOS Agent	macOS 에이전트 무선랜제어 플러그인 사용 시 무선네트워크 정보 수집 주기 옵션화	
126175	GN-26435	WebUI	노드 상세화면에서 정책 탭의 제어정책 복수할당에 대한 내용이 출력이 될 수 있도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
126732	GN-28295	Center	정책서버 DB 연결 실패시 전체 감사로그가 삭제되는 문제	4.1.3
126677	GN-28288	WebUI	일부 타입의 노드명(센서명)을 수정할 수 없는 문제	6.0.21
126530	GN-27955		HA Slave 장비에 정책이 적용되지 않는 문제	5.0.42, 4.0.156, 6.0.16 (LTS)
126505	GN-28265	Sensor	SNMP Agent 기능을 설정했으나 외부에서 NAC장비의 SNMP 정보를 가져오지 못하는 문제	5.0.57
126466	GN-28271		4버전에서 신규(5.6)버전으로 에이전트업데이트 시 설치 토큰 입력 대화상자 출력되어 자동업데이트 안되는 문제	6.0.22, 5.0.62
126396	GN-28228	Sensor	[범용OS] 센서가 업/다운상태를 반복하는 문제	5.0.42
126330	GN-28231	Sensor	센서의 DHCP 서비스를 사용할 경우 센서가 재부팅되는 문제	4.0.158, 6.0.19, 5.0.59
126175	GN-28051	WebUI	노드 목록 화면의 검색바에서 IP 정책 관련 항목들이 중복으로 출력되는 문제	6.0.21, 5.0.61
126175	GN-28017	Windows Agent	하드웨어 정보 수집 플러그인에서 4TB 이상의 하드디스크에 대한 정보 수집 오류	5.0.0, 6.0.0
126175	GN-27999	Windows Agent	모양 및 개인설정 플러그인에서 화면보호기가 설정되어 있지 않지만 '사용함'으로 잘못 보고되는 문제	4.0.158, 6.0.19, 5.0.59
126175	GN-27963	WebUI	정렬 목록 태그로 마크업 된 항목이 숫자로 표시되지 않은 문제	6.0.1
126175	GN-27947	Sensor	무선감지 모드 실행 오류시 지속적으로 실패 오류가 발생하는 문제	6.0.22
126175	GN-27946	WebUI	라이센스 경고 메시지에 추가정보가 표시되지 않는 문제	5.0.22, 6.0.15
126175	GN-27939	WebUI	신규 설치할때 관리콘솔의 기본 테마(Green24)가 적용되지 않는 문제	6.0.5
126175	GN-27934	CWP	CWP 인증페이지에 사용자 등록 페이지 링크가 표시되지 않는 문제	6.0.18, 5.0.58
126175	GN-27908	WebUI	범용OS 관리콘솔에서 관리자 인증을 위한 Passkey 생성에 실패하는 문제	6.0.7
126175	GN-27884	WebUI	설정의 사용자인증 페이지에서 보안질문 설정 항목이 출력되지 않는 문제	6.0.19, 5.0.59
126175	GN-27858	CWP	CWP에서 SAML 인증을 사용할 경우 사용자 정보 수정페이지 접근시 사용자인증창이 반복 표시되는 문제	5.0.42, 5.0.50, 6.0.10
126175	GN-27856	WebUI	정보동기화 중 DB 타입을 Google G Suite 로 신규 생성시 동기화가 실패하는 문제	6.0.19, 5.0.59
126175	GN-27812	WebUI	에이전트 액션의 액션 수행 시각이 System Timezone으로 저장되지 않는 문제	5.0.45, 6.0.2
126175	GN-27790	WebUI	관리콘솔 SAML 인증 후 2차 인증이 설정되어 있는 경우 인증이 정상동작하지 않는 문제	5.0.48, 6.0.6
125885	GN-28010	Backup, CLOUD	[Cloud] 백업된 NAC Tenant 데이터로 Restore 되지 않는 문제	6.0.17, 5.0.57

16.2.3 Genian ZTNA 6.0.21 Release Notes (2024-04-01)

Last Updated: 2024-05-03

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
125554	GN-28063	WebUI	노드관리 검색바에 Blind Injection 가능한 문제		2.2

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
125514	GN-28027	WebUI	관리자 로그인 페이지 접속시 로컬호스트의 ip가 ipv6 일 경우에도 허용 가능하게 개선	
125410	GN-27711	RADIUSD	RADIUS 와 AD 인증연동 환경에서 사용자의 패스워드가 AD서버에서 변경되었을 경우 패스워드 prompt 가 나올수 있도록 개선	
125410	GN-27706	WebUI	WEBUI 2단계인증 시 1차 ID/PW 로그인 인증 실패 횟수가 포함되도록 개선	
125410	GN-27697	Center	Webhook 인증연동시 패스워드를 SHAxxx 결과로 전달할 수 있도록 추가	
125410	GN-27662	Windows Agent	Kaspersky 신규 백신 제품(Kaspersky Endpoint Security 12 for Windows) 에 대한 정보 수집기능 추가	
125410	GN-27499	Windows Agent	무선랜제어 플러그인에서 허용 무선랜 설정에 대한 설명 수정	
125410	GN-27335	Center	802.1x Account 패킷의 calling-station-id 에 단말의 IP가 들어가 있는 경우 Framed IP로 처리하도록 개선	
125410	GN-27294	IPMGMT, Sensor	IP 정책을 센서별로 생성할 수 있도록 개선	
125410	GN-26663	macOS Agent	macOS 비밀번호 유효성 검사 플러그인 추가	
125410	GN-26589	WebUI	CLI 비밀번호를 변경 할 수 없는 범용OS 및 클라우드 장비에 변경불가 안내메시지 표시되도록 개선	
125410	GN-25876	WebUI	관리자 2단계 인증 실패 시 감사로그 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
125634	GN-28024	Center, Sensor	ZTNA Client의 다수의 Split tunneling network 설정시 동작하지 않는 문제	6.0.5
125410	GN-28008	Center, IPMGMT	IP정책 센서대역 적용 설정을 ON에서 OFF 설정시 잘못된 제어정책으로 남는 문제	6.0.21, 5.0.61
125410	GN-27954	Center	RADIUS Account 패킷으로 노드의 IP를 업데이트하면서 IP/MAC이 동일한 노드가 복수개 만들어지는 문제	5.0.36
125410	GN-27944	WebUI	노드상세 화면에서 태그 UI가 다르게 적용되어 있는 문제	6.0.20
125410	GN-27911	WebUI	관리콘솔의 접근허용 IP 설정에서 Subnet 지원 옵션이 오동작하는 문제	6.0.21, 5.0.61
125410	GN-27895	Windows Agent	외부인증연동 플러그인에 등록된 프로그램이 계속 수행되는 문제.	6.0.18, 5.0.58
125410	GN-27894	Center	신규노드 호스트명제한 기능이 정상 동작하지 못하는 문제	6.0.21, 5.0.61
125410	GN-27848	GNOS, Sensor	[GNOS] 센서장비의 syslog 서비스가 외부로 OPEN 되어 동작하는 문제	
125410	GN-27808	Center	vpn 연결 실패도중에 vpn 기능을 off / on을 하면 불필요한 로그가 남는 문제	5.0.42, 6.0.0
125410	GN-27797	WebUI	IP정책을 센서 대역으로 적용한 경우 빠른검색 등에서 IP 검색시 다중으로 출력되는 문제	6.0.21, 5.0.61
125410	GN-27733	WebUI	노드 목록과 노드 상세 화면의 마지막 동작시각이 일치하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
125410	GN-27660	Windows Agent	펜타 솔루션(I-Sign+)가 로그인상태에서도 'Penta SSO 대체 인증' 플러그인으로 인증연동 안되는 문제.	5.0.51, 4.0.153, 6.0.11
125410	GN-27657	WebUI	감사로그 내보내기 한 엑셀 파일이 Windows Excel에서 정상적으로 열리지 않는 문제	6.0.11
125410	GN-27494	WebUI	관리자 확인창 및 순서일괄수정창 선택알림 및 여백, 버튼 UI 수정	6.0.18
125410	GN-27331	WebUI	목록페이지 헤더 영역의 페이징(Pagination) 부분 정렬 오류 및 select메뉴 일관성 있게 수정	6.0.5

16.2.4 Genian ZTNA 6.0.20 Release Notes (2024-03-04)

Last Updated: 2024-04-01

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
125406	GN-27107	WebUI	권한 없는 관리자로 인한 Tomcat 재구동 명령 수행으로 서비스 무력화	5.0.41	2.7

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
125148	GN-27973	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 3.0.13, 1.1.1w 업그레이드 - X.509 정책 제약 조건을 확인하는 과정에서 과도한 리소스 사용	4.0.0, 5.0.0, 6.0.0
124647	GN-27699	WebUI	WEBUI 2단계인증 인증코드 입력 시 마스킹 되어 표시되도록 개선	
124647	GN-27694	WebUI	WEBUI 관리접속 IP 설정시 xxx.xxx.xxx.1~254 만 가능하도록 개선	
124647	GN-27651	macOS Agent	macOS off-line 로그 (감사 기록) 전송 기능 개발	
124647	GN-27645	Center, Sensor	FTP/SFTP 백업시 서버연결timeout 시간을 설정할 수 있도록 개선	
124647	GN-27626	Center, procmond	프로세스검사데몬(procmond)에서 센터데몬 SOAP API HealthCheck 하도록 개선	
124647	GN-27620	Center, Sensor	파일 다운로드 수행 시 타임아웃 설정 가능하도록 개선	5.0.42 (LTS), 6.0.3
124647	GN-27551	WebUI	신규 로그인페이지 버튼 UI 개선	
124647	GN-27544	WebUI	신규 로그인 페이지에서 타임아웃 발생 시 출력되는 오류 메시지 변경	
124647	GN-27537	VRRPD	Multicast 패킷운영이 불가능한 환경에서 VRRP Unicast mode 를 통해서 HA 가능하도록 개선	
124647	GN-27524	macOS Agent	macOS 에이전트 비정상종료 원인분석을 위한 디버깅 정보 저장	
124647	GN-27518	WebUI	관리콘솔 SAML 인증 연동시 JIT provisioning 기능 지원	
124647	GN-27501	Center, Sensor	센서Inline 모드사용시 IP로 노드 등록되도록 기능 개선	
124647	GN-27487	Center, Sensor	어플리케이션 도메인 정규표현식/httpMethod 조건 추가	
124647	GN-27450	Linux Agent	Linux Agent, 프로그램 제거 플러그인 개발	
124647	GN-27444	Center, gnlogin	Docker Compose 정책서버에서 백업 파일 Restore 가능하도록 개선	
124647	GN-27441	WebUI	File Upload API 에서 Cert 파일인 경우 파일에 대한 Response 를 줄 수 있도록 개선	
124647	GN-27372	WebUI	노드그룹 목록의 적용 노드 수 가져오는 구조 개선	
124647	GN-27065	Center	인증코드 검증 실패시 감사로그 추가 및 비밀번호 수정시 by 정보 추가	
124647	GN-26946	WebUI	Azure Collector 추가	
124647	GN-26937	Linux Agent	Linux Agent, 개별 액션에 대한 로그를 분리하여 남길 수 있도록 기능 추가	
124647	GN-26877	Center	노드그룹 조건에서 매크로를 사용할 수 있도록 추가	
124647	GN-26847	WebUI	CWP설정 > 확인버튼 URL의 설명 보강	
124647	GN-26595	WebUI	정책 수정 시 적용된 노드의 수량을 포함한 경고 메시지 출력	
124647	GN-26182	Linux Agent	Linux Agent, 프로그램 정보 및 에이전트 삭제 UI를 ZTNA 신규 UI 디자인으로 개발	
124647	GN-25587	WebUI	5.0 to 6.0 업그레이드 시 관리자의 대시보드를 신규 대시보드에 맞게 migration 해주는 APP 개발	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
125366	GN-27983	Center	5.0/6.0 정책서버에서 보내는 이벤트패킷이 4.0.1 센서에서 처리 안되는 문제	5.0.42 (LTS), 6.0.16 (LTS)
125348	GN-27968	WebUI	설정의 인증서 관리에서 인증서 관련 업로드시 저장 및 수정이 안되는 문제	6.0.19, 5.0.59
125291	GN-27972		SSL 인증서의 유효기간이 10년으로 생성되는 문제	6.0.15, 5.0.55 (LTS)
125238	GN-28009	WebUI	서브넷마스크 입력 UI에서 255.255.255.0 처럼 입력시 마지막 값이 0이면 입력이 안되는 문제	6.0.20
125166	GN-27994	Linux Agent	Linux Agent 파일배포 플러그인 V2에서 배포파일 검증방법이 Sigstore Keyless Signing일 경우 실패하는 문제	5.0.50, 5.0.53, 5.0.54, 6.0.15
125157	GN-28005	macOS Agent	macOS 파일배포 플러그인 V2에서 배포파일 검증방법이 Sigstore Keyless Signing일 경우 실패하는 문제	6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
125040	GN-27989	Genian Syncer	지니안싱커로 GenianData를 동기화할 때 무결성 검증에 실패하는 문제	4.0.156, 6.0.16 (LTS), 5.0.55 (LTS)
124918	GN-27958	WebUI	frontend 페이지 내에서 참조하는 파일이 존재하지 않아, 감사로그에 오류경고가 발생하는 문제	6.0.20
124895	GN-27932	Center	센터 업그레이드 또는 재부팅할 때 다량의 Keep Alive 디버그 로그로 인한 부하 문제 개선	6.0.19, 5.0.59
124880	GN-27904	MySQL	SSD 사용 장비에서 MySQL 8.0 구동 실패하는 문제	6.0.18, 5.0.58
124870	GN-27936	RADIUSD	Radius 데몬 업그레이드 이후 TLS 1.0 으로 유/무선 연결시 인증실패로 연결안되는 문제	6.0.19, 5.0.59
124825	GN-27933	WebUI	태그 설정 팝업에서 태그해제시각 설정이 불가능한 문제	6.0.20
124647	GN-27726	WebUI	신규 로그인 페이지에서 유효하지 않은 경로로 접근 시 서비스를 사용 할 수 없는 문제	6.0.19
124647	GN-27722	macOS Agent	macOS 장치 차단시 로그에 차단 정책ID가 잘못 표시되는 문제	6.0.3, 5.0.46
124647	GN-27709	Windows Agent	신규로 파악된 백신의 엔진 업데이트 수행시 '실시간검사'가 미동작으로 보고되는 문제	6.0.19, 5.0.59
124647	GN-27682	Linux Agent	Linux Agent, System Dark 모드일 경우 일부 UI 글자가 보이지 않는 문제	6.0.17
124647	GN-27664	WebUI	IP관리센서 목록에서 한개의 센서에서만 DHCP Pool 사용현황이 출력되는 문제	5.0.42 (LTS)
124647	GN-27632	WebUI	로그인 한 관리콘솔 언어가 CWP 지원언어에 포함되어 있지 않은 경우 다국어입력기 출력 문제	5.0.31
124647	GN-27622	Sensor	권한정책의 earlyrole 매칭이 정상적으로 이루어지지 않는 문제	6.0.7

continues on next page

Table 3 – continued from previous page

Revision	Key	Components	Description	Affects Versions
124647	GN-27617	Windows Agent	운영체제 정보 수집 액션으로 AD서버에 빈암호 사용여부를 체크하여 AD계정이 잠기는 문제	4.0.109, 5.0.6, 6.0.0
124647	GN-27579	CWP	노드정책 > 비밀번호 사용 옵션을 off로 했을때 CWP 사용자 정보 확인 화면이 정상적으로 동작하지 않는 문제	4.0.M8
124647	GN-27576	WebUI	노드그룹 필터 설정 팝업영역이 화면을 벗어나는 오류	5.0.31, 6.0.0
124647	GN-27571	WebUI	노드뷰가 제한된 관리자로 새로운 노드뷰를 생성 후 사용시, 해당 뷰 항목이 증가되는 현상	5.0.42 (LTS)
124647	GN-27569	WebUI	대시보드 화면에서 출력되는 일부 다이얼로그 스타일이 다른 문제	6.0.15
124647	GN-27566	WebUI	에이전트 OS 아이콘이 잘못나오는 문제 수정	4.1.M5
124647	GN-27543	WebUI	CONF Update API 사용시 오류 발생되는 문제 수정	5.0.20
124647	GN-27536	dbmigration	레지스트리 설정의 데이터 마이그레이션시 값이 잘못 변환되는 문제	6.0.5, 5.0.48
124647	GN-27522	WebUI	노드액션의 플러그인 변경 후 정책적용 시 변경된 플러그인의 이름으로 출력되지 않는 문제	5.0.45, 6.0.2
124647	GN-27520	WebUI	CVE 상세화면 출력 시 데이터가 존재하지만 빈화면으로 출력되는 문제	5.0.50, 6.0.12, 5.0.53
124647	GN-27498	Windows Agent	인증상태 액션검사조건대로 플러그인이 동작하지 않는 문제	5.0.0, 6.0.0
124647	GN-27362	WebUI	사용자, IP 신청서의 추가필드를 패스워드 폼으로 지정하여도 일반 입력란 형식으로 나타나는 문제	5.0.34
124647	GN-27328	Elastic-Search, WebUI	Elasticsearch Export Utils에서 제거된 메소드 추가	6.0.11
124647	GN-26376	WebUI	일반용도의 IP사용신청 시 신청서에 처리결과 수신 정보를 입력해도 결과를 전송받지 못하는 문제	5.0.13
124647	GN-24361		hsecmod.sh 스크립트가 클라우드정책서버에서 동작안하는 문제	5.0.42 (LTS)

16.2.5 Genian ZTNA 6.0.19 Release Notes (2024-02-05)

Last Updated: 2024-02-29

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
124617	GN-27568	Windows Agent	유선 및 무선연결관리자의 802.1x 인증(GTC)에서 TLSv1.3 지원	
123976	GN-27612	WebUI	멀티라인 텍스트 입력형식의 추가필드에 읽기전용 옵션 추가	
123976	GN-27602	WebUI	멀티라인 입력 추가필드 항목에 READONLY 옵션 설정 추가	

continues on next page

Table 4 – continued from previous page

Revision	Key	Components	Description	Affects Versions
123976	GN-27473	Windows Agent	정책 재적용 할때마다 반복되는 액션 정책 로그 개선	
123976	GN-27465	macOS Agent	macOS 액션 플러그인 옵션 UX 개선	
123976	GN-27456	WebUI	ipmgmt 신청결과에 승인 사유 컬럼 추가	
123976	GN-27455	Windows Agent	하우리 바이로봇 API 변경 (VrInfo.dll ver 2023.11.10.0)	
123976	GN-27447	Linux Agent	Linux Agent, 소프트웨어 정보수집에서 Snap을 통해 설치된 소프트웨어도 수집되도록 개선	
123976	GN-27374	macOS Agent	macOS ZTNA 연결 시 연결창이 다른 창보다 하위에 있을 경우 최상위로 띄움	
123976	GN-27364	Sensor	ZTNA Client TLSv1.3 지원	
123976	GN-27357	WebUI	SAML idp의 IP-Port 출력형식에 대한 개선 및 관련 코드 정리	
123976	GN-27348	WebUI	오류 페이지 출력 개선	
123976	GN-27315	WebUI	대시보드 '센터/센서 장비상태 현황' 위젯 기능 개선	
123976	GN-27313	WebUI	어플리케이션 관리 목록에서 설정된 조건까지 확인 가능하도록 개선	
123976	GN-27260	Linux Agent	Linux Agent, 전자 서명을 실행 가능한 상태로 서명되도록 개선	
123976	GN-27229	WebUI	임시사용자 IP 신청서 비밀번호 입력란에 필수입력 표시 추가	
123976	GN-27225	Windows Agent	하우리 Virobot Security 1.0 백신 정보 수집	
123976	GN-27214	WebUI	시스템 기본설정의 Timezone 기본값을 Browser Timezone으로 변경	
123976	GN-27212	WebUI	Cloud 환경에서 정책서버 Timezone 설정 가능하도록 개선	
123976	GN-27199	WebUI	IP/MAC 추가필드 빠른검색 조건에 추가	
123976	GN-27197	Linux Agent	Linux Agent, 네트워크 공유폴더 플러그인 개발	
123976	GN-27163	Sensor	센서데몬의 주기적으로 데드락 여부를 검사하는 기능 추가	
123976	GN-27133	WebUI	대시보드 센서맵에 센서 상태에 따라 마커의 색상이 구분되도록 개선	
123976	GN-27109	macOS Agent	macOS 에이전트 잠자기 모드 해제 후 ZTNA 접속 실패시 재접속을 위한 ZTNA 연결창 표시	
123976	GN-27108	macOS Agent	macOS 에이전트 ZTNA 사용자 접속정보 저장 기능개선	
123976	GN-26667	WebUI	정책에 액션 일괄적용 기능 추가	
123976	GN-26539	WebUI	관리 상세 페이지 수정 버튼 위치 변경	

continues on next page

Table 4 – continued from previous page

Revision	Key	Components	Description	Affects Versions
123976	GN-26389	macOS Agent	macOS용 네트워크 커널 모듈 개발	
123976	GN-26311	WebUI	ZTNA 신규 로그인페이지 개발 (Frontend)	
123976	GN-26251	WebUI	사이트 생성시 사이트 명을 사용 가능 문자만 허용하도록 변경	
123976	GN-26189	macOS Agent	macOS 에이전트 ZTNA DNS 설정 기능	
123976	GN-25991	macOS Agent	macOS 에이전트 Internet Kill Switch를 위한 방화벽 제어 플러그인	
123976	GN-25989	Kubernetes	K8s Kata container 기반 DKNS 지원작업	
123976	GN-25751	WebUI	IP/장비 소유자 설정에서 사용자 이름 검색 시 검색결과 출력 형태 수정	
123976	GN-25552	Linux Agent	Linux Agent, CLI 를 통한 사용자 인증 관리 기능 개발	
123976	GN-25545	Linux Agent	Linux Agent, 장치 제어 기능 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
124617	GN-27464	Windows Agent	Openssl3.0 적용된 무선연결관리자를 통해 GTC 인증실패 &무선연결안됨 (임시조치)	6.0.19, 5.0.59
124316	GN-27648	WebUI	감사로그에 An error occurred when requesting the page. StatusCode=404, 403 Warning 로그가 남는 문제	6.0.19, 5.0.59
124082	GN-27749	WebUI	CWP의 사용자 정보 수정 페이지에 접속이 안되는 문제	6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS), 6.0.18, 5.0.58
124025	GN-27742	Center	Cloud NAC에서 메일전송 실패하는 문제	6.0.19, 5.0.59
123976	GN-27678	Windows Agent	모양 및 개인설정 플러그인에서 화면보호기 정보 수집안되는 문제	5.0.59
123976	GN-27623	WebUI	로그인 세션이 없는 경우 리다이렉트 되는 페이지가 잘못 설정되어 있는 문제	6.0.19
123976	GN-27619	Center	GNOS 센터에 Ubuntu NAC 센서 소프트웨어 업로드 안되는 문제	5.0.42 (LTS)
123976	GN-27593	WebUI	신규 로그인페이지의 OTP 안내화면이 깨져보이는 문제	6.0.19
123976	GN-27590	WebUI	노드그룹의 백신정보 관련 조건에 백신명을 직접입력할 수 없는 문제	6.0.6, 5.0.49

continues on next page

Table 5 – continued from previous page

Revision	Key	Components	Description	Affects Versions
123976	GN-27580	CWP	SAML 인증연동(CWP)시 사용자 생성 또는 갱신을 off 설정된 상태인데 SAML Attribute 설정이 잘못되었습니다. 감사로그가 남는 문제	6.0.17, 5.0.57
123976	GN-27572	Backup	[범용OS] 백업 파일에 에이전트 zip 파일이 포함되어 용량이 증가하는 문제	5.0.31
123976	GN-27521	ulogd	DKNS > ULOGD로그가 logrotate 에 포함 안되어있어 로그파일 사이즈가 증가 문제	6.0.15
123976	GN-27514	Center	노드정책의 인증방식 순서에 따라 일부 인증방식의 실패 로그가 남지 않는 문제	5.0.16
123976	GN-27508	Windows Agent	모양및개인설정 액션에 액션즉시적용 명령으로 설정되어있는 화면보호기 동작하지 않는 문제.	4.1.M8, 5.0.0, 6.0.0
123976	GN-27482	WebUI	무선랜 그룹 복사 시 오류 발생하는 문제	4.1.4
123976	GN-27458	Center	CLOUD 버전 에이전트 로그 수집되지 않는 문제	5.0.42 (LTS)
123976	GN-27445	Sensor	URL path로 어플리케이션 제어되지 않는 문제	6.0.14
123976	GN-27443	Windows Agent	PC부팅시 백신 실시간 감시상태가 미동작으로 보고되는 문제	5.0.0, 6.0.0
123976	GN-27442	WebUI	노드관리 목록화면에서 마지막 동작시각 컬럼의 정렬이 동작하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
123976	GN-27439	WebUI	아이디가 영문이 아닌 관리자의 대시보드가 출력되지 않는 문제	6.0.0
123976	GN-27435	WebUI	어플리케이션 객체 > 어플리케이션 설정의 추가 버튼이 브라우져 사이즈가 작은 경우 클릭되지 않는 문제	6.0.11
123976	GN-27433	Sensor	어플리케이션 객체 수정한 경우 적용되지 않는 문제	6.0.7
123976	GN-27429	Center	Openssl 3.0을 사용 할 때 라이센스정보를 읽어오지 못하는 문제	6.0.19
123976	GN-27426	WebUI	ColorPicker 컴포넌트에서 이미지 선택이 정상출력되지 않는 문제	6.0.7
123976	GN-27420	WebUI	노드 관리범위 제한이 걸린 센서그룹에 센서를 추가하는 경우 해당 관리자의 트리에 즉시 반영되지 않는 문제	5.0.31
123976	GN-27413	WebUI	다국어 메세지 컴포넌트에서 국문항목만 수정시 타언어 설정값이 반영안되는 문제	4.1.M3, 4.0.17
123976	GN-27409	Sensor	AD 서버에 최신 업데이트 설치 시 Agentless AD SSO 기능이 동작하지 않는 문제	
123976	GN-27405	WebUI	무선랜 정책복사 후 수정이 안되는 문제	4.0.8
123976	GN-27396	WebUI	노드목록 내보내기 시 마지막동작시각 컬럼의 내용이 잘못출력되는 문제	6.0.16 (LTS), 5.0.55 (LTS)
123976	GN-27371	WebUI	적용범위가 없는 같은 단독 플러그인이 정책에 다중 할당 가능한 문제	5.0.43, 6.0.0
123976	GN-27308	Elastic-Search, Ubuntu(Debian)	[범용OS] 로그서버가 싱글모드일 때, elasticsearch의 nac_nodegrptreesnapshot 인덱스의 복제본이 생기는 문제	

continues on next page

Table 5 – continued from previous page

Revision	Key	Components	Description	Affects Versions
123976	GN-27285	WebUI	password 타입의 입력란이 상위 옵션과 관계없이 빈 값일 경우, 저장이 안되는 문제	6.0.17, 5.0.57
123976	GN-27247	WebUI	WMI 수집정보 위젯의 링크를 통해 노드 목록 이동 시 결과 출력되지 않는 문제	5.0.33
123976	GN-27238	WebUI	영문 ID/비밀번호 찾기 문구에 클라우드 버전 ID/비밀번호 찾기 문구가 무조건 출력되는 문제	5.0.31
123976	GN-27236	WebUI	CWP 세션 만료 페이지의 문구가 시스템 로케일로 출력되는 문제	5.0.14
123976	GN-27227	WebUI	관리콘솔 로그인 페이지에서 자바스크립트 콘솔 오류 로그 출력 문제	6.0.7
123976	GN-27220	Genian Mobile	패스워드에 '%' 포함된 경우 NAC Monitor (mobile) 로그인 되지 않는 문제	6.0.14
123976	GN-27218	Database	운영체제 정보수집 액션에 의한 정책서버의 "Unknown CODEMAP" 디버그 발생	5.0.48, 6.0.6
123976	GN-27179	Sensor	DKNS 사용시 IPM정책 수신 실패가 발생하면서 센서가 정상 구동되지 않는 문제	5.0.42 (LTS)
123976	GN-27173	Center	스위치 삭제 시 노드의 접속장치/접속포트 정보가 삭제되지 않는 문제	
123976	GN-27125	GenianOS	[범용OS] 이미지 업그레이드 이후 서비스 구동되지 않도록 개선	
123976	GN-27120	WebUI	노드정책의 노드액션 할당에서 할당항목을 취소하게되면 할당가능한 목록에 보이지 않는 문제	6.0.17, 5.0.57
123976	GN-27099	Sensor	글로벌 DHCP 환경으로 DHCP IP 할당 시 노드의 Active 상태를 확인하도록 개선	
123976	GN-27080	WebUI	권한 제어정책의 노드수가 제어정책 위젯의 카운트와 맞지 않는 문제	6.0.7
123976	GN-27064	Windows Agent	안전모드 부팅 후 장치제어 플러그인 버전이 변경되면 이전 정책으로만 제어되는 문제	5.0.0, 6.0.0
123976	GN-26900	Sensor	사용 중인 IP를 DHCP IP로 할당하는 문제	4.0.149
123976	GN-26559	WebUI	사용자 등록 페이지의 기간 설정 처리 시 관리자의 타임존에 맞게 설정되도록 개선	4.1.M4
123976	GN-26180	WebUI	관리 화면에서 선택된 항목이 없는 경우에도 돌아가기 버튼 활성화	6.0.10
123133	GN-27496	Linux Agent	Linux Agent, 간헐적으로 액션 시스템 정보 전송이 일부 누락되는 문제	5.0.50, 6.0.15

16.2.6 Genian ZTNA 6.0.18 Release Notes (2023-12-19)

Last Updated: 2024-02-01

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
123781	GN-26393	WebUI	접근 권한 없는 페이지에 직접 URL을 입력하여 정보 수정이 가능한 취약점		3.1
123284	GN-26390	WebUI	감사로그 REST API를 통한 권한 없는 관리자의 파일 내보내기 권한 우회 취약점		3.1

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
123464	GN-27625	Sensor	센서 운영모드 및 정책변경시 pubilc ip를 가져오지 못할 경우 반영되지 않는 문제 개선	
122922	GN-25063	WebUI	6.0 버전 위젯 추가	
122821	GN-27491	WebUI	SAML 인증 연동시 IdP-initiated SSO 인증 요청에 대해 인증 가능하도록 개선	
122708	GN-27476	WebUI	SAML 로그인시 기존 로그인 버튼과 구분하기 위해 구분선을 추가와, 다중 IdP 설정시 로그인 버튼 출력 개선	
122708	GN-27344	Center	Secondary Webhook 인증연동을 할 수 있도록 기능 개선	
122708	GN-27320	WebUI	외부 접근 허용 시 출력되는 알람에 대한 개선	
122708	GN-27249	Linux Agent	Linux Agent, ZTNA Client 연결실패할 경우 서버에서 전송한 에러메시지 표시하도록 수정	
122708	GN-27243	Authsync	응답헤더에 포함된 페이징파라미터를 이용할 수 있도록 REST API Server 타입 정보동기화 개선	
122708	GN-27201	WebUI	노드 속성 변경에 IP / MAC 추가필드 항목 추가	
122708	GN-27140	Sensor	ZTNA Gateway 서버인증서 센터 CA로 서명하도록 개선	
122708	GN-27100	Center	ZTNA 클라이언트 고정 아이피 할당 실패 메시지를 클라이언트에 전달	
122708	GN-27090	Center	ZTNA 고정아이피 할당 실패시 감사기록이 남지 않는 문제	
122708	GN-27077	Sensor	이벤트 소켓 생성시 event socket not configured 로그 발생에 대한 예외처리 개선	
122708	GN-27068	WebUI	노드그룹 조건필터 목록을 탐색 할 수 있도록 개선	
122708	GN-27052	WebUI	어플리케이션 정의화면에서 Domain 입력시 path 경로를 추가로 입력할 수 있게 개선	
122708	GN-26955	- Unknown/None	ES 계정 변경 시 sysinspect 스크립트가 변경된 ES 계정으로 동작하도록 개선	
122708	GN-26942	WebUI	장비 수정 API 호출 시 오류 로그 남는 문제 개선	
122708	GN-26929	Database	'USB 정보' 추가/삭제 감사로그에 장치정보 추가	

continues on next page

Table 6 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122708	GN-26921	Windows Agent	에이전트를 통한 외부인증연동 플러그인 개발	
122708	GN-26913	Windows Agent	엑소스피어 백신 정보 수집	
122708	GN-26909	Zero Trust Security	[ZTNA]Client 접속시 생성되는 RADIUS accounting Attribute 추가	
122708	GN-26907	Center	검색필터 Webhook 설정 시 복수의 URL 설정이 가능하도록 개선	
122708	GN-26889	Sensor	ZTNA GW(Global-line) 사용시 트래픽 정보가 출력되지 않는 문제	
122708	GN-26873	WebUI	Top 메뉴의 빠른검색에서 (IP/장비)소유자, 소유부서 검색이 되도록 개선	
122708	GN-26860	WebUI	클라우드 수집기에서 프로세스의 상태 정보 조회 기능	
122708	GN-26855	MySQL	[범용OS] mysql 비밀번호 재사용 방지하도록 개선	
122708	GN-26842	Center	CLOUD GPDB 갱신시 mysqldump 수행오류	
122708	GN-26575	IPMGMT	ipmgmt 페이지 기능 사용하지 않을 시 접근 불가 설정	
122708	GN-26545	GenianOS	GNOS 커널 버전 업그레이드 (5.15.0)	
122708	GN-26482	Authsync, Database	부서코드 저장 시, 사이즈 초과를 방지하기 위해 해시 함수로 압축	5.0.45, 6.0.2
122708	GN-26325	GNOS	httpd 구동 스크립트 실행 시 procmond에 의해 중복 실행되는 문제 개선	
122708	GN-26284	Center	제품내 self-sign 인증서 자동 갱신 기능	
122708	GN-26021	Sensor	APP DB를 이용한 Application 탐지 시 URL+pathPattern, UserAgent Rule 적용	
122708	GN-25674	WebUI	ZTNA 비밀번호 변경 시 비밀번호 규칙 가이드 문구 영역 벗어나는 오류	
122708	GN-25533	Center	Proxy 서비스설정시 cache 삭제 옵션 추가	
104536	GN-22567	Database	GNOS MySQL 8.0 업그레이드	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
123883	GN-27681	WebUI	시스템>시스템관리>이미지선택 업그레이드 팝업창 에러	6.0.18
123767	GN-27674	MySQL	SSD가 있는 장비에서 mysql 8.0버전 이미지로 업그레이드 후 데몬이 실행되지 못하는 문제	6.0.18, 5.0.58
123721	GN-27652	Center	센터에서 발급한 구글OTP 보안키가 에이전트로 전송 안되서 구글OTP 인증을 진행할 수 없는 문제	6.0.13

continues on next page

Table 7 – continued from previous page

Revision	Key	Components	Description	Affects Versions
123497	GN-27646	Authsync	정보동기화의 사용자 부서ID컬럼명에 MySQL함수사용하는 경우, 부서 동기화 실패하여 잘못된 정책이 할당될 수 있는 문제	6.0.18, 5.0.58
123435	GN-27641	WebUI	tomcat 로그에 by the following code has not been returned to the pool 가 다수 발생 후 웹 콘솔 접속 불가증상	5.0.20
123340	GN-27399	macOS Agent	macOS 내부/외부 상태에 맞지 않게 플러그인이 동작하는 문제	6.0.5, 5.0.48
123298	GN-27573	WebUI	사용자그룹별 현황에서 각 그룹 인원수 클릭시 목록이 출력되지 않는 문제	4.0.156, 6.0.16 (LTS), 5.0.57
123293	GN-27401	Sensor	센서장비에서 동일한 이벤트를 받는 경우 센서프로세스가 비정상 종료 되는 문제	4.0.64
123291	GN-27541	Authsync	정보동기화 서버 접속 실패하면 삭제된 사용자로 처리되어 전체 사용자가 삭제되는 문제	6.0.9
123281	GN-27517	WebUI	Nodes REST API 에서 특정 항목이 수정되지 않는 오류	5.0.8, 4.0.111
123274	GN-27550	WebUI	트리구조의 데이터 컴포넌트가 출력되지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS), 6.0.17, 5.0.57
123268	GN-27460	GenianOS	[범용OS] 초기동작시 aes256 명령이 실행되지 않는 문제	5.0.42 (LTS), 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
123266	GN-26993	WebUI	감사로그, 노드상세 이력관리 화면에서 ip, mac에 툴팁으로 표시되는 정보표기 오류	6.0.4, 5.0.47
123166	GN-27519	Sensor	지속적으로 센서모드 변경시 데드락이 발생하여 센서 시스템이 멈추는 증상	5.0.57, 4.0.157, 6.0.19 (R)
123133	GN-27496	Linux Agent	Linux Agent, 간헐적으로 액션 시스템 정보 전송이 일부 누락되는 문제	5.0.50, 6.0.15
123055	GN-24708	Center	많은 센서 디버그를 센터로 전송하는 환경에서 센터 재부팅시 오래된 디버그 삭제 동작으로 부하가 발생할 수 있는 문제	5.0.0
123046	GN-27575	Center	ES 로그필터쿼리 결과가 2K보다 크면 로그필터액션이 동작하지 않는 문제	4.1.M6
122946	GN-27574	Center	ES로그 정리주기에 로그필터를 위한ES인덱스(nac-filter)가 삭제되는 문제	5.0.50, 6.0.11
122840	GN-27561	Center	[범용OS] LDAP 설정파일이 범용OS 에서 잘못된 파일에 설정되는 문제로 ldapsearch 명령 결과가 실패하는 문제	5.0.42 (LTS)
122708	GN-27500	Windows Agent	"외부인증연동(레지스트리)" 액션 최초적용시 인증해제 안되는 문제	4.0.0, 5.0.0, 6.0.0

continues on next page

Table 7 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122708	GN-27438	WebUI	노드 상세정보에서 태그 추가 시 기존에 존재하던 태그가 해제되는 문제	6.0.18
122708	GN-27424	WebUI	대시보드 태그 클라우드 타입 위젯의 로딩상태가 계속되는 문제	6.0.14
122708	GN-27419	WebUI	Flow 로그에서 유효하지 않은 조건으로 검색하는 경우 데이터 영역이 출력되지 않는 문제	6.0.0
122708	GN-27397	WebUI	operator 계정으로 RADIUS정책 생성 수정 못하는 오류	5.0.30
122708	GN-27389	Center, CLOUD	CLOUD 정책서버 업그레이드 시 범용OS 센서 자동 업그레이드 수행되지 않는 문제	
122708	GN-27368	WebUI	관리범위에 따른 관리자별 일일리포트 생성시 집계가 잘못된 문제	6.0.17, 5.0.57
122708	GN-27356	Sensor	패치 Proxy 서비스설정 on 설정임에도 cache 서비스가 구동되지 않는 문제	5.0.55 (LTS), 4.0.157
122708	GN-27321	WebUI	노드/제어 정책 수정되지 않는 문제	4.0.157, 6.0.18, 5.0.58
122708	GN-27293	WebUI	노드그룹 필터 설정 팝업에서 오류메시지가 관련없는 위치에 표시되는 문제	6.0.14
122708	GN-27268	Sensor	정책서버와 통신할 인터페이스가 지정되어도 RADIUS 인증요청이 default gateway로 전송되는 문제	6.0.14
122708	GN-27148	WebUI	2차인증 사용하여 관리콘솔 로그인 시 로그인 성공 후 로그인 실패 카운트 초기화 되지 않는 문제	4.0.10
122708	GN-27119	Windows Agent	에이전트인증창 URL버튼에서 정의된 이름값 출력이 모두 출력되지 않는 문제	5.0.42 (LTS), 6.0.0
122708	GN-27111	Authsync	직급동기화 시 로컬DB에 직급정보가 없을 때 직급동기화가 실패하는 문제	6.0.6, 5.0.49
122708	GN-27110	WebUI	CWP 사용자 등록 신청결과조회 화면에서 사용자 정보 수정 후 다시 신청결과조회 화면 접근시 인증이 안되는 문제	5.0.32
122708	GN-27059	WebUI	태그명을 공백(Space)으로 입력이 가능한 문제	4.0.M7
122708	GN-27057	procmond	tomcat 재시작시 tomcat9 버전이 아님에도 감사기록에 tomcat9 라고 남는 문제	5.0.53, 6.0.15
122708	GN-27048	WebUI	로그인화면 3줄 이상 입력 시, 레이어 세로 영역 겹치는 문제	6.0.8
122708	GN-27040	Center	에이전트에서 수집된 '알수없음', '정보없음' 날짜 정보가 '1970-01-01'로 표시되는 문제	
122708	GN-27017	Elastic-Search, gnlogin	로그서버 구동 전 로그서버 인증 정보 변경 시 감사로그 저장되지 않는 문제	
122708	GN-27006	WebUI	CLOUD 버전에서 서비스 제어 메뉴 제거했으나 상단 메뉴에서 접근이 가능한 문제	5.0.29
122708	GN-26992	Center	에이전트 플러그인이 정책서버의 타임존 기준으로 동작하는 문제	
122708	GN-26953	WebUI	감사로그 실시간모드에서 필드정렬을 하지 않은 경우 데이터 연동 값이 잘못 전달되는 문제	6.0.2

continues on next page

Table 7 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122708	GN-26951	Windows Agent	백신정보수집 플러그인으로 바이러스 치료 감사기록이 되지 않는 문제	4.0.144, 5.0.41
122708	GN-26941	WebUI	ConfEngine 의 AddRemove 컴포넌트 내 항목 수정시 잘못 수정되는 문제	5.0.18
122708	GN-26933	WebUI	일부 날짜 입력필드에 사용되는 달력 컴포넌트가 영문으로만 표시되는 문제	5.0.20, 6.0.0
122708	GN-26904	WebUI	노드관리 > 위험 컬럼의 아이콘 미출력 문제	5.0.53, 6.0.13
122708	GN-26864	Windows Agent	간헐적으로 정보수집플러그인의 최신정보가 업데이트되지 않는 문제	5.0.0, 6.0.0
122708	GN-26859	Linux Agent	Linux Agent, 파티션이 나눠져 있지 않은 저장 장치 정보가 수집되지 않는 문제	5.0.41, 6.0.0
122708	GN-26777	WebUI	노드/제어정책의 노드그룹 수정 시 갱신시각 업데이트 되지 않는 문제	6.0.18
122708	GN-26742	Sensor	센서 노드정보 검사 설정의 "NMAP TCP SCAN" 사용안함 적용되지 않는 문제	5.0.40
122708	GN-26415	WebUI	보안그룹정책의 조건 수정 시 정책 업데이트 실패되는 문제	6.0.3
122708	GN-26032	WebUI	dialog 창 세로 스크롤 발생 시 하단 버튼 영역 만큼 컨텐츠 안보이는 문제	6.0.1
122708	GN-25805	WebUI	IP Matrix View 에서 IP 변경금지 (지정 IP 대역) - 단일 IP 위반됨 아이콘 표시되지 않는 문제	4.0.8

16.2.7 Genian ZTNA 6.0.17 Release Notes (2023-10-11)

Last Updated: 2023-12-19

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
122609	GN-27492	WebUI	Tomcat Version Upgrade (8.5.94 -> 8.5.96 / 9.0.81 -> 9.0.83)		7.5
121382	GN-26315	WebUI	2단계 인증에서 인증코드 입력값 횟수제한, 시간제한하도록 개선		4.3
120862	GN-27278	WebUI	Tomcat Version Upgrade (8.5.94 / 9.0.81)		7.5
120382	GN-26600	WebUI	비정상 api 호출 후 로그인 되지 않는 문제	5.0.42 (LTS), 5.0.49, 6.0.7, 4.0.156, 5.0.56 (50 LTS)	5.3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
122686	GN-27462	Windows Agent	파일 배포 V2 플러그인 설치할 때 운영체제(64/32비트)에 해당하는 cosign 파일만 다운로드하도록 개선	5.0.42 (LTS), 4.0.155, 6.0.15, 5.0.55 (LTS), 5.0.56 (50 LTS), 5.0.57
122678	GN-27340	Sensor	SSL 터널을 통한 정보동기화 및 인증연동 기능을 DKNS에서도 제공하도록 개선	
122661	GN-25714	WebUI	보안서약 만료일 설정 옵션 추가	
122232	GN-27164	VRRPD	[범용OS] 이중화 구성 master 상태로 전환 후 인터페이스 상태검사 실패로 인해 slave 상태로 전환되는 문제	5.0.42 (LTS)
122211	GN-27402	WebUI	MAC 정책 수정 시 시작/종료 시각을 설정할 수 있도록 API 개선	
122163	GN-27390	Center, WebUI	리포트 보존개수 설정 시 /disk/data/report 디렉토리의 데이터도 삭제하도록 개선	
121924	GN-27241	macOS Agent	macOS 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121886	GN-27248	Linux Agent	Linux Agent, 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121740	GN-26627	WebUI	CWP 웹 페이지 출력 상태에서 에이전트 인증 후 CWP 웹에서 인증 화면이 다시 출력되지 않도록 개선	
121113	GN-27269	-Unknown/None-	apache / tomcat 관련 디렉토리 및 파일의 불필요한 권한 제거	
120834	GN-27319	WebUI	Tomcat 구동시 jdbc 연결에 serverTimezone 설정 추가	
120399	GN-27146	Center	extauth 를 통한 외부인증연동 실패시 사용자가 입력한 패스워드가 센터디버그파일에 남는 문제	
120324	GN-27174	WebUI	ConfEngine File (40) 타입에서 기본 출력되는 콤보박스의 데이터 선택할 수 있도록 개선	
120324	GN-27160	Center	인증 연동 시 사용자 도메인을 사용할 때 로컬DB 계정 연결 방식 수정	
120324	GN-27049		macOS 파일배포 폴더 정규식 지원하도록 개선	
120324	GN-26875	WebUI	호스트명 제한시 CWP에 출력되는 메시지 수정	
120324	GN-26843	Center	센터데몬 초기 구동시 에이전트 패키지를 두번 생성하는 문제	
120324	GN-26827	WebUI	백업수행 지금시작 버튼의 팝업 메시지 수정	
120324	GN-26803	Windows Agent	플러그인을 통한 공유폴더제어에 대한 감사기록 추가	
120324	GN-26801	WebUI	WEBUI 의 primefaces 기본 시스템 오류가 출력되는 문제 개선	

continues on next page

Table 8 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120324	GN-26775	Linux Agent	Linux Agent, Popup 메시지 전체 내용 확인 기능 추가	
120324	GN-26763	WebUI	데일리 리포트 내 전일 동안 추가된 항목을 선택할 수 있도록 개선	
120324	GN-26760	WebUI	데일리 리포트 생성 및 발송 시 관리자 별로 (관리범위에 따른) 관리되도록 개선	
120324	GN-26753	WebUI	쿼리리포트에 쿼리 문자열 끝에 세미콜론 입력시 오류 메시지 출력하도록 개선	
120324	GN-26734	WebUI	관리>노드>장비속성 에서 내용연수 시작일/만료일 잘못된 날짜를 입력시 오류메시지 개선	
120324	GN-26681	WebUI	노드 관리 그리드 모드에서 상세화면 분할 기능 적용	
120324	GN-26668	CWP	CWP SSL 사용 기본 설정을 On으로 변경	
120324	GN-26665	WebUI	정책 생성시 에이전트 액션 할당시 "사용가능 OS 종류"의 드랍다운 UI 를 추가	
120324	GN-26653	WebUI	노드관리목록>노드속성변경 시 같은 카테고리의 항목은 하나만 선택할 수 있도록 개선	
120324	GN-26640	WebUI	노드그룹 조건 계속추가 시 이전 항목이 선택되어 있도록 변경	
120324	GN-26612	WebUI	대시보드 센서맵에서 현재 위치 포인트를 토글하여 표시할 수 있도록 개선	
120324	GN-26611	WebUI	Keycloak 로그인시 Agent 설치를 강제하는 Authentication Flow 추가	
120324	GN-26610	Center	사용자 기본 로케일 설정과 상관없이 에이전트 설치 시 영문으로 표시되는 문제	
120324	GN-26564	GNOS	NanoPI 센서 하드웨어 지원	
120324	GN-26555	Sensor	네트워크객체에서 FQDN을 사용시 센서에 캐시된 IP 정보를 확인하는 gnlogin 명령 추가	
120324	GN-26547	WebUI	신청관리 > IP신규/반납 > 신청서 처리 (승인/거부) 사유 입력 팝업창 UI 개선	
120324	GN-26544	GNOS	GNOS 커널 최신패치 적용 (5.10.181)	
120324	GN-26538	WebUI	대시보드 위젯 애니메이션 제거	
120324	GN-26524	WebUI	CommonData(confui, codemap, customdata) Rest API 호출시 헤더의 Accept-Language 의 값으로 로케일 처리하도록 개선	
120324	GN-26491	WebUI	노드 관리 설명 컬럼의 내용이 컬럼 사이즈만큼 출력되도록 개선	
120324	GN-26488	Windows Agent	윈도우 바탕화면에 에이전트 바로가기 아이콘 생성 옵션 추가	
120324	GN-26473	Sensor	입력한 SNMP Agent의 버전분리 및 Community와 Passwd를 정규식 검사하도록 개선	
120324	GN-26468	WebUI	노드상세의 소프트웨어/이력관리 목록의 페이지당 목록 출력 갯수를 변경 가능하도록 개선	
120324	GN-26464	WebUI	설정 > 공지사항에서 이미지 업로드 및 미리보기 시 이미지가 깨져보이는 문제 개선	

continues on next page

Table 8 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120324	GN-26412	WebUI	관리자 세션 강제종료시 로그인 화면으로 전환되도록 수정	
120324	GN-26410	CWP, WebUI	SAML 인증연동시 IdP 인증 후 SP에서 오류가 발생시 아무런 메세지가 출력되지 않는 문제	
120324	GN-26407	WebUI	IP 관리 매트릭스 뷰에서 정책서버 표시될 수 있도록 수정	
120324	GN-26360	Linux Agent, Zero Trust Security	Linux Agent, ZTNA 연결관리자 2단계 인증 기능 추가	
120324	GN-26344	WebUI	Keycloak 로그인 페이지 Genians 테마 추가	
120324	GN-26312	WebUI	노드 일괄 등록시 csv 중복노드 존재하면 이후 작업이 진행되지 않는 문제	
120324	GN-26263	WebUI	노드 상세정보 내 다이어그램 출력개선	
120324	GN-26152	Center, DKNS, Sensor	compose 환경 SWG를 통한 HTTPS 웹기반 Application 감지	
120324	GN-26133	Linux Agent	Linux Agent, Linux 보안설정 플러그인 개발	
120324	GN-25759	WebUI	캘린더에 양식에 맞지 않는 값 입력시, 영문 메세지가 출력되는 문제	
120178	GN-27207	Windows Agent	다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
122586	GN-27502	Center	Keepalive 에 의한 에이전트/센서 다운 체크과정이 오래 걸리는 경우 에이전트 로그온 API 처리가 지연되는 문제	5.0.42 (LTS)
122548	GN-27495	WebUI	서비스 제어 > 정책적용 다이얼로그에서 닫기 버튼 클릭시 정책 적용 이벤트가 호출되지 않도록 수정	6.0.17, 5.0.57
122534	GN-27480	WebUI	노드그룹 조건 중 부서선택 타입의 조건을 검색할 수 없는 문제	5.0.31, 6.0.0
122501	GN-27504	Center	KeepAlive 수신 시 NodeID 관련 DB 오류(Illegal mix of collations) 감사로그 발생되지 않도록 개선	
122481	GN-27451	WebUI	감사 > Flow 로그 목록에서 시간으로 정렬이 되지 않는 문제	6.0.1
122475	GN-27490	CWP	CWP에서 SAML 로그인 버튼 클릭시 Invalid settings: sp_cert_not_found_and_required 메세지 출력되는 문제	6.0.13

continues on next page

Table 9 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122451	GN-27345	WebUI	페이지 준비(ready) 단계에서 markdown 변환되도록 수정	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
122423	GN-27510	Center, Sensor	[범용OS] NAC패키지 업그레이드 후 추가된 라이브러리를 찾지 못하는 문제	5.0.42 (LTS)
122374	GN-27404	Center, macOS Agent	macOS 업데이트 플러그인의 설치모드 사용시 정상적으로 설치되지 않는 문제	5.0.11
122301	GN-27467	WebUI	노드액션 설명에 XSS를 추가하면 정책적용 팝업화면에서 XSS가 실행되는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
122253	GN-27437	Center, macOS Agent	macOS Sonoma 단말의 OS정보가 unknown으로 분류되는 증상	6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS), 6.0.17, 5.0.57, 4.0.157
122080	GN-27383	WebUI	parameter value is invalid 오류 발생하는 문제 및 한글이 입력가능한 입력폼에 모든 언어의 문자가 입력가능하도록 수정	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
122068	GN-27385	GenianOS	iptables 명령이 동시 실행시 실패될 수 있는 문제 개선	5.0.0, 6.0.0
121995	GN-27417	WebUI	현황 & 필터 > 태그 > 노드 태그가 정상적으로 출력되지 않는 문제	6.0.16 (LTS)
121910	GN-27400	CWP	Agent에서 Passkeys 등록이 되지 않는 문제	6.0.16 (LTS)
121877	GN-27398	Linux Agent	Linux Agent, 조건만 검사 액션 수행 결과가 변경되어도 업데이트 안되는 문제	5.0.50, 6.0.15

continues on next page

Table 9 – continued from previous page

Revision	Key	Components	Description	Affects Versions
121831	GN-27446	Center	외부인증연동(runauth) 이용시 빈 패스워드가 입력되는 경우 SOAP API 처리 프로세스 멈춤 및 CPU 100% 사용하는 문제	5.0.42 (LTS), 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS), 5.0.57, 4.0.157
121705	GN-27380	Windows Agent	액션검사조건에 에이전트가 지원하는 매크로 이외에 '%' 문자가 존재하면 비정상 종료되는 문제	5.0.0, 6.0.0
121652	GN-27387	WebUI	OpenPort 현황 화면에서 내보내기 기능 동작하지 않는 문제	5.0.6
121591	GN-27393	WebUI	IP,MAC 추가필드 사용자선택기에서 설정된 맵핑 컬럼키가 동작하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
121525	GN-27270	macOS Agent	macOS AD 대체인증시 허용 도메인명에 .com 생략시 인증되지 않는 문제	4.0.108, 5.0.5
121504	GN-27382	WebUI	추가필드 - 사용자선택기에서 한글 및 일부 특수문자 포함시 parameter value is invalid 오류가 발생하는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 4.0.155, 6.0.15
121454	GN-27394	Center	SFTP 저장장치 경로에 절대경로 설정 시 백업 실패하는 문제	5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
121442	GN-27291	WebUI	Alias 센서명에 , * · 등의 특수문자가 포함된 경우 parameter value is invalid 에러 발생	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS)
121393	GN-27388	Center	[범용OS] webssh 접속 안되는 문제	5.0.42 (LTS)
121197	GN-27322	Center, Sensor	[범용OS] 시스템관리 > 환경설정 > 타임존 설정이 우분투 NAC 에서 동작 안하는 문제	5.0.50
121158	GN-27259	Linux Agent	Linux Agent, 특정 패키지로 에이전트 설치시 동작하지 않는 문제	5.0.45, 6.0.2
121153	GN-27221	Linux Agent	Linux Agent, 모니터 정보수집 플러그인에서 EDID값이 존재하지 않는 모니터를 수집할 경우 에이전트가 비정상적으로 종료되는 문제	6.0.12
121131	GN-27359	gnlogin, VRRPD	이벤트재전송처리가 필요없는 프로세스에서도 이벤트큐 처리가 동작하여 Same event already exist in queue 디버그 로그가 발생하는 문제	5.0.42 (LTS)
121074	GN-27289	WebUI	사용자정의 리포트 생성시 리포트 파일이 생성되지 않는 문제	6.0.17, 5.0.57

continues on next page

Table 9 – continued from previous page

Revision	Key	Components	Description	Affects Versions
121015	GN-27358	Center	centerd 실행 옵션의 센서 서비스 시작/중지 기능 동작하지 않는 문제	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120814	GN-27262	Center	정책서버와 DB서버의 Timezone 설정이 다른경우 노드의 변경된 제어정책이 센서로 전달 안되는 문제	6.0.17, 5.0.57
120771	GN-24372	CLOUD	Docker compose 정책서버에서 백업 동작안하는 문제	5.0.42 (LTS)
120763	GN-27211	Sensor	권한제어 정책을 통해 다중의 접근 권한을 부여받을 경우 적용되지 않는 문제	6.0.7
120693	GN-27290	WebUI	센서명에 '%' 가 포함되는 경우 센서트리가 정상적으로 표시되지 않는 문제	5.0.43, 6.0.0
120602	GN-27279	Center, Sensor	센터 장비에서 trust-nodeserver-id 설정시 센서 데몬을 재시작 해야지만 설정이 적용되는 문제	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120533	GN-27091	Center, procmond	센서에서보내는 이벤트로그(procmond 프로세스)가 정책서버에서 unknown center did 에러 발생하면서 로그 저장 안되는 문제	5.0.42 (LTS)
120518	GN-27113	Center	Slave 장비에서 전송되는 업데이트정보(sysinfo)를 unknown devid 로 업데이트 실패하는 문제	4.0.145, 5.0.42 (LTS), 6.0.1
120505	GN-27200	Center	slave 센터에서 BadQuery=Illegal mix of collations 오류가 계속 발생하는 증상	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120494	GN-27177	Backup	백업 파일에 에이전트 zip 파일이 포함되어 용량이 증가하는 문제	6.0.16 (LTS), 5.0.55 (LTS)
120457	GN-27153	WebUI	관리자 노드관리범위 제한을 센서그룹으로 설정하고 노드 등록 시 관리센서 선택할 수 없는 문제	5.0.31
120418	GN-27210	Enforcer	Netflow 로그에 제어정책명이 안남는 문제	6.0.16 (LTS)
120357	GN-27191	WebUI	감사로그 화면에서 브라우저가 멈추는 문제	5.0.54, 6.0.15

continues on next page

Table 9 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120324	GN-26976	Center	[범용OS] 업데이트 실패 시, 장비가 제대로 동작하지 못하는 문제	5.0.56 (50 LTS), 6.0.17
120324	GN-26899	Center	Self-Signed 인증서 재발급 되지 않는 문제	5.0.45, 6.0.2
120324	GN-26845	WebUI	윈도우즈 업데이트 액션이 할당되어 있을 경우 에이전트를 삭제했지만 노드목록에서 에이전트 존재하는것처럼 출력되는 문제	4.0.M1, 5.0.0, 6.0.0
120324	GN-26836	WebUI	태그가 포함된 부서명이 존재하면 노드그룹 조건에 부서정보 검색 오류	5.0.42 (LTS), 6.0.0
120324	GN-26815	WebUI	감사 > 리포트 > 노드 리포트 > 노드그룹 선택 > 내용 출력되지 않는 문제	5.0.24
120324	GN-26771	Center	gnlogin 을 통해서 정책서버 Enable(node-server enable) 후 센터데몬 프로세스가 정상 구동되지 않는 문제	5.0.42 (LTS)
120324	GN-26746	WebUI	RADIUS 정책의 2단계 인증 유예시간의 설명이 잘못된 문제	6.0.11
120324	GN-26740	WebUI	어플리케이션 수정정보 반영 안되는 오류	6.0.13
120324	GN-26721	WebUI	Agent 업로드시 검증 성공 로그가 Error 로그로 남는 문제	6.0.1
120324	GN-26692	WebUI	시스템관리의 소프트웨어에서 파일 선택없이 업로드 처리시 프로그레스가 종료되지 않는 현상	5.0.2
120324	GN-26689	Center	변경금지 설정 제거 디버그에 노드 IP 잘못 출력되는 문제	5.0.43, 6.0.0
120324	GN-26680	Center	비밀번호 Blacklist 파일의 마지막 라인 단어가 사용금지(제한)되지 않는 문제	4.0.106
120324	GN-26676	gnlogin	[범용OS] gnlogin 명령시 감사기록에 ADMIN, ADMINIP가 남지 않는 문제	5.0.23
120324	GN-26673	Center	신규노드 정책: MAC차단 인 경우 변경금지(지정IP대역) 설정된 노드의 IP 사용시간 만료 시 MAC허용 노드가 차단되는 문제	4.1.M5
120324	GN-26652	WebUI	노드관리 목록 > 노드속성 가져오기 수행시 IP시작/종료 시각이 입력한 값과 9시간 차이나는 문제	4.1.M4
120324	GN-26605	Center	새로운 무선랜 AP 감지, 무선랜AP정보변경 감사로그 형식 수정	6.0.0
120324	GN-26588	WebUI	대시보드 새탭 추가 시, 탭 목록의 마지막에 정렬되도록 수정	6.0.0
120324	GN-26586	WebUI	노드그룹 복사 시 '변경 정책 적용' 버튼이 출력되지 않고 즉시 적용되는 문제	5.0.31
120324	GN-26581	WebUI	간헐적으로 로딩바가 출력되지 않는 오류	6.0.17
120324	GN-26578	WebUI	IP사용신청서 결과조회에서 사용자ID, 부서명 컬럼이 공백으로 출력되는 문제	4.1.4
120324	GN-26573	WebUI	관리콘솔 설정값 확인 연동변경 및 언어설정 파라메터 변경	6.0.0
120324	GN-26560	WebUI	노드관리 화면에서 검색어에 AND가 존재할 경우 검색되지 않는 문제	5.0.38
120324	GN-26558	WebUI	네트워크 객체의 네트워크 주소 중 FQDN 옵션의 TTL 값만 수정 시 수정되지 않는 문제	5.0.19

continues on next page

Table 9 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120324	GN-26529	WebUI	센서 IP사용률 Top 현황(구버전) 위젯에서 잘못된 센서의 IP/Mask 설정으로 인한 오류 페이지 출력 개선	4.1.4
120324	GN-26489	Center	우분투/클라우드 버전에서 디버그 파일의 스레드 ID가 정상적으로 남지 않는 문제	6.0.0
120324	GN-26487	WebUI	CVE 상세화면에서 값이 없을 경우 에러페이지 출력되는 문제 수정	5.0.24
120324	GN-26476	WebUI	액션별 수행결과 현황 페이지 오류 수정	5.0.50
120324	GN-26463	GenianOS	syscollect 정상 동작하지 않을 수 있는 문제	5.0.0
120324	GN-26439	Center, Sensor	어플리케이션객체의 Application Category조건인 경우 SWG에서 허용되지 않는 문제	6.0.14
120324	GN-26369	WebUI	노드/로그/무선랜 리포트에서 전년도 검색시 날짜 표시가 잘못 출력되는 문제	5.0.34
120324	GN-26235	macOS Agent	macOS 에이전트 신규 모델 mac의 메인보드 정보를 얻어오지 못하는 문제	5.0.41, 6.0.0
120324	GN-25815	WebUI	IP 신규/반납 신청서의 승인/거부 팝업이 활성화 되어있는 상태에서 승인/거부시 대기상태가 되는 문제	4.1.3
120324	GN-24713	procmond	정책서버를 센서전용 이미지로 변경시 데몬구동 오류가 발생되는 문제	5.0.0
120142	GN-27237	Center, Sensor	관리콘솔에서 센서에 등록된 에이전트노드삭제시 센서에 의해서 노드가 즉시 재등록 안되는 문제	5.0.42 (LTS)
114063	GN-26566	WebUI	노드 정보 업데이트 후, 탭 이동 시 변경한 정보가 갱신되어 보여지지 않는 문제	5.0.50

16.2.8 Genian ZTNA 6.0.15 Release Notes (2023-05-17)

Last Updated: 2023-07-20

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
115659	GN-26725	Linux Agent, macOS Agent, Windows Agent	[Agent] 센터 및 센서에서 전송된 이벤트에 대한 유효성 검사 추가		6.3
114716	GN-26368	WebUI	관리자의 API 키가 다른 관리자에게 노출되는 취약점		5.3
114205	GN-26392	WebUI	권한 없는 관리자가 디버그 로그 다운로드 가능한 취약점		2.9
113812	GN-26222	WebUI	관리콘솔 내 페이지 이동시 사용하는 returnUrl 파라미터를 변조하여 리다이렉트 할 수 있는 문제		1.9

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
117753	GN-26702	WebUI	정책서버에서 외부로 접근이 허용되면 경고를 출력하는 기능	
117445	GN-26769	Linux Agent	Linux Agent, Sigstore 전자서명을 기반한 배포 플러그인 개발	
117369	GN-26755	Center, Linux Agent, macOS Agent, WebUI, Windows Agent	Sigstore 전자서명을 기반한 배포 플러그인 개발	
116763	GN-26826	geniup	UEFI 시스템에서 geniup 수행시 디스크부족 발생하는 문제	
116385	GN-26844	Center, Sensor	센서에서 외부로 접근가능여부를 센서정보(공인IP)에 표시	
116215	GN-26705	Center	SLSA를 통한 업데이트서버 배포 데이터 전자서명 검증	
115882	GN-26786	Center	업데이트서버로 부터 받은 WSUSSCN2.CAB 에 대한 전자서명 검증	
115309	GN-26336	Center	ExtSvc 를 이용해서 RADIUS 2차 인증 연동이 가능하도록 개선	
114491	GN-26631	Docker	nftables를 사용하는 Linux 시스템에서 DKNS동작할 수 있도록 개선	
114376	GN-26043	Sensor	SNMP Agent 구동시 인증 및 암호화 알고리즘 선택가능하도록 개선	
114251	GN-26328	WebUI	노드그룹 엑셀다운로드시 노드 그룹명이 포함되게 개선	
114195	GN-26568	WebUI	노드그룹 조건의 소프트웨어 명 포함/미포함 설정 시, 직접 입력 가능하도록 개선	
113890	GN-26359	Windows Agent	윈도우의 'Wi-Fi 임의 하드웨어 주소 옵션'을 사용하지 않도록 강제화하는 기능 추가	
113812	GN-26515	Enforcer	DKNS Ubuntu 22.04 지원	
113812	GN-26462	WebUI	관리UI 로그인 화면에서 고객정보가 노출되지 않도록 개선	
113812	GN-26348	WebUI	제어정책 목록에 출력되는 노드차단비율현황 위젯의 타이틀 개선	
113812	GN-26329	Windows Agent	화면보호기 제어시 Windows 로그온 화면 표시 설정을 강제로 해제할 수 있는 기능 추가	
113812	GN-26321	WebUI	장치그룹화면의 OS 종류 콤보박스가 빈값으로 출력되는 문제	
113812	GN-26301	WebUI	접속허용IP 설정창 info 메시지 style 개선	
113812	GN-26279	WebUI	대시보드 위젯추가 다이얼로그 UI/UX 개선	
113812	GN-26254	WebUI	이중화 환경에서 ZTNA client 정보가 정상적으로 표시되도록 개선	

continues on next page

Table 10 – continued from previous page

Revision	Key	Components	Description	Affects Versions
113812	GN-26207	Center, DKNS	ZTNAClient/URLFilter 동적 서비스포트 적용	
113812	GN-26192	WebUI	SAML Service Provider Metadata 생성 기능	
113812	GN-26186	Center	event key 불일치로 인한 감사로그 타입이 맞지 않는 부분 개선	5.0.33
113812	GN-26183	WebUI	IP신청시스템의 IP신청시 사용종료일이 당일로 기본 출력되지 않도록 수정	
113812	GN-26171	CWP	CWP 공지사항에 관리자의 아이디가 노출되지 않도록 개선	
113812	GN-26148	Center	에이전트 로그온 시 기존 노드와 다른 장비로 판단되면 노드 정보를 즉시 업데이트할 수 있도록 개선	
113812	GN-26139	Sensor	정책서버 이중화시 ZTNA Client 세션 관리 동작하도록 개선	
113812	GN-26123	WebUI	사용자 계정신청 후 전송된 메일의 DateTime 값에 밀리세컨드 값이 출력되는 부분 개선	
113812	GN-26104	Center	[범용OS] Flow Log 수집 기능 동작하도록 개선 (Filebeat 추가)	
113812	GN-26037	WebUI	사용자신청서 상세페이지에서 승인/거부처리시 사유입력 팝업창이 나타나도록 개선	
113812	GN-26031	Center, Database	Agent에 의해 수집된 시스템정보(마더보드)를 이용한 노드그룹 조건 추가	
113812	GN-25782	Linux Agent	Linux Agent, 비밀번호 유효성 검사 액션 기능 추가	
113812	GN-25540	GenianOS	CA 인증서 유효기간 10년으로 변경	
113812	GN-25196	Sensor	ZTNA 게이트웨이(센서)간 VXLAN 연결 기능 구현	
113812	GN-24116	WebUI	외부 서비스 연동 API 기능 추가	
113812	GN-22197	Center	OAUTH 2.0 ROPC 인증연동 가능하도록 기능 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
117409	GN-26213	WebUI	노드정책 생성 후 노드그룹을 할당시에 변경하지 않는 옵션값이 변경된 것으로 나타나는 문제	5.0.44
117204	GN-26852	Center, Genian Syncer	Syncer 를 통한 지니데이터 업로드시 Mobilebrowser 데이터가 업데이트 안되는 문제 및 CVE 데이터 버전 갱신 안되는 문제	4.1.0
117179	GN-26770	Center, Sensor	[범용OS] 센서가 배포서버로 동작하지 않는 문제	5.0.29
116850	GN-26839	Center, Sensor	정책서버/센서 메모리 릭(지니업데이트 및 노드스캔(https)) 발생 문제	4.0.14

continues on next page

Table 11 – continued from previous page

Revision	Key	Components	Description	Affects Versions
116693	GN-26768	WebUI	노드 추가필드 - 사용자 선택기 설정 옵션이 반영되지 않는 오류	5.0.22
116649	GN-26767	WebUI	라이선스 및 알림 메시지 표시 누락	6.0.0
116622	GN-26816	WebUI	노드그룹의 CWP 메세지에 태그가 있는 경우, 출력이 깨지는 오류	5.0.37
116612	GN-26779	WebUI	로그서버(elasticsearch) 정상상태 임에도 경고 메시지 출력되는 문제	5.0.23
116606	GN-26773	WebUI	노드 목록 조회 API에서 노드그룹 조건이 동작하지 않는 문제	5.0.54, 6.0.14
116577	GN-26758	Windows Agent	에이전트가 로컬시스템으로 동작하면 프로그램제거 플러그인을 통하여 Store앱 삭제 실패	5.0.42 (LTS), 6.0.0
115782	GN-26749	Elastic-Search	[범용OS] Elastic과 통신이 Iptables 정책에 의해서 차단되어 간헐적으로 ES가 정상 구동 안하는 문제	5.0.31
115635	GN-26727	Sensor	[범용OS] 센서와 동일한 DNS를 할당하는 DHCP 서버가 비정상적인 DHCP서버로 감지되는 문제	
115608	GN-26706	WebUI	'노드 추가필드 - 사용자선택기' 텍스트 입력 불가 옵션인 경우 검색팝업 동작하도록 수정	5.0.22
115567	GN-26748	WebUI	감사 > Flow 목록 화면에서 Application Detail 클릭시 자바스크립트 오류가 발생하여 로딩 이미지가 사라지지 않는 문제	6.0.8
115370	GN-26719	WebUI	정책 > 객체 > 시간 메뉴에서 시간 객체 생성시 System Timezone과 관리자 Timezone이 다른 경우 날짜가 잘못 저장되는 문제	5.0.34
115297	GN-26601	WebUI	관리자의 관리범위를 센서그룹으로 설정 시 매트릭스뷰에서 미사용 IP 선택하지 못하는 문제	4.0.117, 5.0.14
115246	GN-26739	CWP	Google OTP 2단계 인증에서 사용자 등록 후 최초 인증 시 CWP에서 보안키 발급 과정에서 Your security key has already been generated. 라는 문구가 표시되는 현상	6.0.13
115118	GN-26428	Center	콘솔UI를 통한 deb 이미지 업그레이드시 OS 종류에 따라 실패할 수 있는 문제	5.0.42 (LTS), 6.0.12
115105	GN-26571	Enforcer	CWP사용안함으로 설정해도 센서에서 SYN-ACK 응답이 발생하여 차단 노드가 통신되는 것처럼 보이는 문제	5.0.0
115040	GN-26660	Docker, Sensor	DKNS 센서 IP 변경시마다 새로운 센서로 등록되는 문제	6.0.0
115019	GN-26607	GenianOS	관리WEBUI 접속 허용 IP에서 Genian Monitor 프로그램 접속되지 않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 6.0.13
114878	GN-26654	macOS Agent	macOS 화면보호기 설정을 사용자가 수동으로 변경시 강제화 안됨	5.0.45, 6.0.2
114830	GN-26409	Linux Agent	Linux Agent, 로그인 사용자 정보 수집 실패로 인한 Agent 관련 UI 동작 오류(트레이 아이콘 등)	6.0.15, 5.0.55 (LTS)
114819	GN-26647	WebUI	시스템 관리화면에 Disk 컬럼 내용 출력되지 않는 문제 개선	5.0.23
114639	GN-25626	WebUI	피방문자 이메일 승인 대상이 관리자임에도 일반 사용자가 검색되는 문제	4.0.M8

continues on next page

Table 11 – continued from previous page

Revision	Key	Components	Description	Affects Versions
114611	GN-26629	WebUI	빠른검색을 통해 노드관리 화면 이동, 전체 노드 선택 후 일괄 작업 수행 시 선택한 노드 없다는 메시지 출력되는 문제	4.0.114, 5.0.11
114555	GN-25887	WebUI	현황&필터의 노드그룹 내에 다단계의 카테고리 구조에서 하위 카테고리가 표시되지 않음	5.0.42 (LTS), 5.0.45, 6.0.2
114516	GN-26620	Enforcer	IP충돌보호 unknown mac 설정 시 정상 mac이 더라도 충돌보호가 걸리는 문제	4.0.17
114498	GN-26402	Center, Sensor	RADIUS 설정 변경시 PROCMON 데몬이 hang 걸릴수 있는 문제	6.0.3
114309	GN-26597	WebUI	DB/Log 서버 분리구성 일 경우 쿼리리포트 생성되지 않는 문제	5.0.37
114297	GN-26532	WebUI	NIC 벤더별 현황의 수량 맞지 않는 문제 개선	
114258	GN-26609	WebUI	노드추가필드(사용자선택기-맵핑컬럼명) 사용하여 노드 등록 시 오류 발생되는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
114230	GN-26430	WebUI	클라우드 환경에서 장치사용신청서의 부서트리가 나타나지 않는 문제	5.0.52, 6.0.13
114195	GN-26465	WebUI	노드그룹 조건의 에이전트 액션 수정 시, 기존 설정 값이 기본값으로 선택되지 않는 문제	5.0.45
114195	GN-26440	WebUI	태그의 변동사항이 없는데 노드 상세정보 수정 시 함께 업데이트 처리 되는 문제	5.0.22, 6.0.4
114195	GN-26425	WebUI	노드그룹 조건의 사용자 부서 선택 시 데이터에 상위부서가 포함되지 않는 문제	5.0.35
114150	GN-26280	Center	멀티 센서 장비 삭제 이후 재등록될때 센서 승인 상태로 등록되는 문제	6.0.8, 5.0.50
114063	GN-26566	WebUI	노드 정보 업데이트 후, 탭 이동 시 변경한 정보가 갱신되어 보여지지 않는 문제	5.0.50
114007	GN-26531	WebUI	전체사용자의 부서별의 트리목록이 나타나지 않는 문제	6.0.7
113966	GN-26587	WebUI	노드관리 부서명 컬럼의 내용이 정상 출력되지 않는 문제 개선	6.0.5, 5.0.50
113812	GN-26677	Center	권한정책 내 제어액션 수행 불가 및 윈도우 방화벽 제어 불가 오류	6.0.13
113812	GN-26655	WebUI	Compose 버전에서 노드관리 엑셀 export 시 오류 페이지 발생	5.0.48, 6.0.6
113812	GN-26549	Sensor	간헐적 dnsmasq 데몬 재시작 증상	6.0.12, 5.0.53
113812	GN-26497	Windows Agent	무선연결관리자에서 무선프로파일(EAP-TTLS)의 서버 인증서 검증을 끄면 연결안됨	5.0.49, 6.0.7
113812	GN-26411	ulogd	ULOGD 디버그로그에 대해서 logrotate 동작 안하는 문제로 인해서 디스크용량이 부족해지는 문제	6.0.0
113812	GN-26377	WebUI	센서 일괄설정 및 운영모드 적용되지 않는 문제 수정	6.0.8

continues on next page

Table 11 – continued from previous page

Revision	Key	Components	Description	Affects Versions
113812	GN-26363	WebUI	CWP 접속 시 세션 만료 페이지 출력 및 정상적으로 노드 정보가 표시되지 않는 문제	6.0.15
113812	GN-26350	Center	범용OS ZTNA client 사용시 센서가 RADIUS 자동허용되지 않아 인증되지 않는 문제	6.0.10
113812	GN-26335	Windows Agent	PC 원격 접속시 에이전트 트레이 아이콘 미표시 문제	5.0.0, 6.0.0
113812	GN-26317	WebUI	방문자 용도의 용도 설정에서 사용자/신규신청 옵션에 동일 조건 추가시 오류 발생	4.0.11
113812	GN-26288	WebUI	사용자 정의 필드 수정후 목록 출력이 이상해지는 오류	4.0.11
113812	GN-26272	Center	SMTP인증연동 - [계정]@[도메인] ID형식인 경우 사용자 인증 비정상 문제	5.0.53
113812	GN-26250	Linux Agent	Linux Agent, 일부 Network interface 정보 수집이 누락되는 문제	5.0.51, 6.0.12
113812	GN-26236	WebUI	노드상세 소프트웨어정보탭 Pagination ui 통일	6.0.4, 6.0.9
113812	GN-26204	Center	정책서버 설치시에 "File read failed. ERRMSG=Is a directory" 디버그가 발생하는 문제	5.0.42 (LTS), 4.0.152
113812	GN-26194	Sensor	http / https 포트 설정변경시 중복으로 IPTABLES가 생성되는 문제	4.0.17
113812	GN-26190	Sensor	2중화 환경에서 TCP패킷이 차단되는 문제	6.0.15
113812	GN-26181	Linux Agent	Linux Agent, 이미 로그인된 사용자로 전환시 트레이 아이콘 표시 안되는 문제	5.0.41, 6.0.0
113812	GN-26097	WebUI	노드관리 엑셀 Export 시 진행되지 않는 문제	4.0.2
113812	GN-25916	Center	ZTNA 인증대체 실패 이후 할당가능 아이피 갯수가 줄어드는 문제	6.0.14
113812	GN-25148	WebUI	WebUI 스마트도움말 설정이 표기되지 않는 오류	5.0.49, 6.0.7
113318	GN-26444	WebUI	노드그룹 조건의 소프트웨어 설정 창에서 한글검색이 안되는 증상	5.0.35

16.2.9 Genian ZTNA 6.0.14 Release Notes (2023-04-12)

Last Updated: 2023-05-16

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
113417	GN-26391	WebUI	권한 없는 관리자가 디버그로그 실시간 보기 가능한 취약점	5.0.0, 6.0.0	2.9
113217	GN-26460	Windows Agent	에이전트를 통해 일반 사용자가 PC 관리자 권한을 획득할 수 있는 취약점	5.0.0, 6.0.0	4.6

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
113565	GN-26098	WebUI	대시보드 화면 출력시 브라우저가 멈춰있는 상태(Freezing)로 있는 현상 개선	
113517	GN-26494	WebUI	대시보드 위젯에 데이터 로딩표시 추가	
113466	GN-26493	WebUI	관리콘솔 로그인 시간 검증방식 개선	
112778	GN-26167	Authsync	SCRAM-SHA-256 인증방식 지원을 위한 postgresql 패키지 업그레이드	
112778	GN-26138	Center	ZTNA 인증시 비밀번호변경 강제 설정이 되어있는 사용자는 클라이언트 인증이 실패로 인해서 비밀번호변경 페이지로 접속할 수 없는 문제	
112778	GN-26105	WebUI	노드관리 동작상태차트의 너비(width)의 개선	
112778	GN-26073	Sensor	NAT예외대역에 대해서만 MASQUERDE하지 않도록 변경	6.0.5
112778	GN-25993	Center	GPDB/NMDB 업데이트 이전 버전 원복 기능	
112778	GN-25990	WebUI	SAML Assertion Attribute(사용자정보)를 통한 사용자 추가/갱신 기능	
112778	GN-25959	Center	자동반납 시 감사로그를 남기도록 개선	
112778	GN-25940	Linux Agent	Linux Agent, Offline 설치 패키지 제작 툴 개발	
112778	GN-25921	Linux Agent	Linux Agent, Log 정리 기능 추가	
112778	GN-25882	Linux Agent	Linux Agent, 액션 플러그인 정책 옵션 UX 개선	
112778	GN-25704	Sensor	PROXY 를 통한 연결시에도 CWP 리다이렉트 동작하도록 수정	
112778	GN-25630	Center	감사로그검색필터 WEBHOOK 외부연동기능시 BULK전송 가능하도록 개선	
112778	GN-25613	Linux Agent	Linux Agent, 백신 정보 수집 데이터화 작업	
112778	GN-25517	WebUI	노드목록에서 컨버터 적용으로 인해 정렬이 불가능한 컬럼에 대한 개선	
112778	GN-25337	WebUI	매일 특정 시간대에 발생한 감사로그를 검색필터로 설정 가능하도록 개선	
112778	GN-25204	Center, Sensor	SWG를 통한 Web 접근시 Flow감사기록에 Application 정보 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
113764	GN-25776	Center	패스워드가 없는 사용자 및 동기화된사용자(READ ONLY) 에 대해서 비밀번호 변경 만료 알림메시지가 나오지 않도록 개선	4.0.18
113658	GN-26554	Sensor	우분투NAC 센터/센서장비에서 Too many open file 에러 발생 및 센서 상태 Down 되는 문제	5.0.51, 6.0.11
113558	GN-26448	WebUI	Compose 방식 설치후 시스템 목록에서 정책서버 정보가 출력되지 않는 오류	5.0.6
113539	GN-26540	Windows Agent	영문관리콘솔의 플러그인 '적용OS' 선택에서 Windows 11이 Windows 10으로 잘못 표시됨.	5.0.42 (LTS), 6.0.0
113484	GN-26267	WebUI	감사 > 로그에서 KST 기준 9시 이전에는 오늘의 감사로그가 출력되지 않는 문제	4.0.17
113398	GN-26357	WebUI	신규 노드그룹 상세화면의 대상노드리스트에서 기본현황으로 돌아갈때 구 버전 상세화면 출력되는 문제	5.0.35
113369	GN-26518	Center	에이전트가 수집한 정보(updateinfo)가 삭제될수 있는 문제	5.0.52, 6.0.13
113354	GN-26322	macOS Agent	macOS 알림메세지 수신시 CPU 점유율 높아지는 문제	5.0.27
113340	GN-26446	Center	LDAP 연결 실패 시 center 데몬의 fd가 증가하는 문제	5.0.41, 4.0.145, 6.0.0
113318	GN-26444	WebUI	노드그룹 조건의 소프트웨어 설정 창에서 한글검색이 안되는 증상	5.0.35
113230	GN-26496	CLOUD	Cloud site 최초 생성시 로그 통계 데이터가 보이지 않는 문제	5.0.50, 6.0.12
113147	GN-26296	Windows Agent	장치 제어 정책에 많은 수의 USB 예외 정책이 존재할 때 다른 액션 정책들이 오동작하는 문제	5.0.0, 6.0.0
113128	GN-26353	Authsync	Google G Suite 정보 동기화 시 고정값 설정되지 않는 문제	
113042	GN-26414	Windows Agent	비밀번호 검증창의 고정옵션이 off 임에도 주기적으로 화면 중앙으로 위치되는 문제	5.0.42 (LTS), 6.0.12, 5.0.53
113035	GN-26454	Sensor	센서HA구성, Slave 센서에서 디폴트 어플리케이션목록을 생성하지 않아 비정상 종료되는 문제	6.0.14
113027	GN-26433	Sensor	게이트웨이 IP추가시 IP Rule 이 잘못생성되어 센서 통신이 안될 수 있는 문제	5.0.42 (LTS)
112970	GN-26367	WebUI	RADIUS 정책에서 2단계 인증설정의 설명문구가 다국어 변경시 한글로 나오는 문제	6.0.11
112778	GN-26331	WebUI	대시보드 위젯 설정에서 다국어처리 및 차트 타임존 설정 추가	
112778	GN-26320	WebUI	보안그룹 정책 생성 시 In/OutBound 조건에 따라 오류가 발생되는 문제	6.0.3
112778	GN-26233	Windows Agent	ZTNAClient을 통한 VPN 연결시 인터페이스 이름에 한글이 존재할 경우 감사로그가 깨지는 문제	6.0.0
112778	GN-26132	Center	ZTNA Client의 기존 센서IP를 동일네트워크의 다른 IP로 지정한 경우 적용되지 않는 문제	6.0.4
112778	GN-26102	WebUI	노드 설정 시 세로 뷰가 작을 때 캘린더 화면이 메뉴 탭에 가려지는 문제	6.0.4
112778	GN-26099	Center	"IP+사용자ID" 노드 수동 등록시, 사전 등록한 IP가 할당되지 않는 문제	6.0.11
112778	GN-26027	Center	미사용IP에 대해 변경금지를 설정한 노드등록시 IPM 아이콘이 출력되지 않는 문제	4.0.8
112778	GN-26026	Sensor	센서장비 구동시 센터와 시간차이로 인해서 스케쥴러가 비정상 동작하면서 센서가 다운상태로 표시되는 문제	5.0.50
112778	GN-	Center	custom 인증서 만료로 로그가 정상적으로 남지 않는 문제	5.0.0

16.2.10 Genian ZTNA 6.0.13 Release Notes (2023-03-13)

Last Updated: 2023-04-14

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
112768	GN-26286	WebUI	Google OTP 2단계 인증에서 보안키를 신규로 발급받아 2단계 인증을 통과할 수 있는 문제		6.5

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
112639	GN-26337	macOS Agent	macOS 액션 수행 조건에 사용자 경로에 대한 매크로 추가	
112190	GN-26255	WebUI	OTP 입력길이를 32자까지 확대	
111909	GN-26039	Center	ZTNA 클라이언트 인증시 인증허용IP에 의해서 클라이언트 대체인증이 실패하는 문제	
111909	GN-25874	Center	센터 api status 로깅 주기 변경 (1일->10분)	
111909	GN-25860	WebUI	태그 추가 시 감사로그에 설명이 저장될 수 있도록 개선	
111909	GN-25710	Center	procmod에서 syslog-ng를 모니터링하도록 추가	
111909	GN-25550	WebUI	노드/제어 액션의 상세화면에서 사용처에 대한 목록 출력 및 삭제 가능하도록 개선	
111909	GN-25501	WebUI	Passkeys 인증을 1차 인증으로 지원 - 관리콘솔(MC)	
111909	GN-25035	CWP	Passkeys 인증을 1차 인증으로 지원 - 사용자(CWP)	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
112765	GN-26160	Authsync, Center	CSV를 다운로드 받아 사용자정보 동기화 진행할 때 실패할 수 있는 문제	5.0.0
112751	GN-26385	Packaging	C30G,C50G장비 모니터 출력 안되는 문제	5.0.44, 6.0.1
112679	GN-26339	dbmigration	6.0 제품에서 버전정보가 5.0 버전으로 잘못 출력되는 문제	6.0.5
112671	GN-26259	Elastic-Search	Advance 페이지의 Elasticsearch 관리툴에서 샤드 정보표시 오류	5.0.17

continues on next page

Table 12 – continued from previous page

Revision	Key	Components	Description	Affects Versions
112654	GN-26319	WebUI	감사로그 화면에서 관리장비명 클릭시 노드관리 검색되지 않고 모두 출력되는 문제	5.0.38
112637	GN-26223	WebUI	노드 상세화면에서 태그할당 시 태그가 50개만 출력되는 문제	5.0.22
112631	GN-26276	Elastic-Search	Elasticsearch 이중화 구성 되지 않는 문제	5.0.51, 6.0.11
112600	GN-26242	WebUI	구름OS(Linux)에 설치 된 에이전트가 관리콘솔의 노드목록에 Windows 아이콘으로 표시 되는 문제	6.0.8, 5.0.50
112529	GN-26316	Center	과거 비밀번호 재사용 방지 기능 사용 시에도 최근 사용 비밀번호로 변경 가능한 문제	3.0_1007
112507	GN-26227	Center	[범용OS] 서버인증서에 Subject Alternative Names 이 없어서 INVALID COMMON NAME 인증서 오류 발생하는 문제	5.0.23
112382	GN-26208	WebUI	검색창에 < 문자가 포함된 검색어를 입력할 경우 XSS 감지로그가 남는 문제	6.0.7, 5.0.50, 4.0.152
112366	GN-26178	WebUI	상세 감사로그 메세지에 포함된 -&gt로 인해 XSS 발견 로그가 남는 문제	6.0.7, 5.0.50, 4.0.152
112312	GN-26198	macOS Agent	macOS 에이전트 두번째 ZTNA 네트워크 연결시 2차 인증 오류	6.0.2
112119	GN-25936	WebUI	관리역할 권한설정에 상관없이 동작하는 노드 작업명령이 동작하지 않는 문제	5.0.44, 6.0.1
112097	GN-26219	WebUI	정책 복사 시 액션에 라벨이 존재할 경우 오류가 발생되는 문제	4.0.113, 5.0.10
112062	GN-26170	WebUI	영문 관리콘솔의 CWP 디자인 템플렛의 컴포넌트 추가/삭제가 정상동작하지 않는 문제	5.0.48, 6.0.7
111951	GN-26200	Center	ZTNA 및 NAC 최신버전에서 CVE 목록 갱신되지 않는 문제	5.0.50, 6.0.12, 5.0.53
111909	GN-26119	Windows Agent	무선랜제어에서 대소문자 비교 오류로 인한 연결허용된 AP가 차단되는 문제	4.0.0, 5.0.0, 6.0.0
111909	GN-26118	Windows Agent	프린터정보 수집에서 가상 프린터 수집 제외 설정시 일부 프린터가 제외되는 문제	4.0.0, 5.0.0, 6.0.0
111909	GN-26095	Center	ZTNA Client 접속 옵션이 간헐적 비활성화되는 문제	6.0.6
111909	GN-26053	Sensor	센서 Inline Global 모드에서 ARP Poisoning 동작하는 문제	5.0.37
111909	GN-26020	Windows Agent	내용이 없는 프린터 정보 수집으로 대시보드에서 빈정보 출력	4.1.0, 5.0.0, 6.0.0
111909	GN-26019	Center	검색필터 알람전송 SMS 내용에 {_FULLMSG} 포함 시 국제 SMS 전송 실패하는 문제	5.0.19
111909	GN-26009	Elastic-Search	6.0 ES(7.17.7) 클러스터 구성 안되는 문제	6.0.11
111909	GN-26008	WebUI	노드그룹 상세화면에서 정책복사 기능 동작 하지 않는 문제	5.0.31
111909	GN-26005	Genian Syncer	지니안싱커로 한글경로의 파일이 업로드되지 않는 문제	4.0.0, 5.0.0, 6.0.0

continues on next page

Table 12 – continued from previous page

Revision	Key	Components	Description	Affects Versions
111909	GN-25999	Windows Agent	인터페이스 제어 액션으로 무선인터페이스가 유선으로 오탐하여 차단되는 문제	5.0.0, 6.0.0
111909	GN-25996	WebUI	사이트 정보수정시 클라우드 VPC로 인한 내부오류 발생	6.0.2
111909	GN-25927	Ubuntu(Debian)	[범용OS] 웹서버 상태 모니터링(FTSS) 할 수 있도록 개선	5.0.23
111909	GN-25926	Sensor	ARM 플랫폼 DKNS가 WebUI를 통하여 업그레이드 되지 않는 문제	6.0.12
111909	GN-25908	Center	[범용OS] CENTERD STAT - HTTPD가 아닌 APACHE2를 Count 하도록 수정	5.0.50
111909	GN-25893	WebUI	5.0 노드상세정보에서 노드선택 후 작업선택의 노드대상 작업지시 명령이 수행안되는 문제.	5.0.44, 6.0.1
111909	GN-25846	Database	Ad hoc 네트워크 연결 위험감지의 "알려진 네트워크 자동 포함" 설정 적용되지 않는 문제	5.0.21
111909	GN-25817	WebUI	에이전트 버전현황 위젯에서 노드목록으로 이동 후 페이지 이동 및 작업 수행 시 잘못된 검색조건이 추가되는 문제	5.0.26
111909	GN-24674	WebUI	장치사용신청서에서 부서 할당시 부서 출력 화면에 error: 문구 표시	5.0.42 (LTS), 6.0.0

16.2.11 Genian ZTNA 6.0.12 Release Notes (2023-02-10)

Last Updated: 2023-03-17

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
111883	GN-26150	WebUI	Tomcat version upgrade (9.0.68 -> 9.0.72, 8.5.78 -> 8.5.86)		
111842	GN-26205	Database	mysql 버전 업그레이드 5.7.40 -> 5.7.41		
111646	GN-25869	CWP	IP관리 메시지 우선 On 일때 에이전트 사용자 인증 메뉴로 CWP 인증 시 계정(ID)으로만 인증되는 문제	6.0.3, 5.0.46	3.4
111295	GN-26000	MySQL	mysql 버전 업그레이드 5.7.33 -> 5.7.40		
111254	GN-26062	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 1.1.1t 업그레이드 - 임의 포인터를 memcmp 호출에 전달하여 메모리 내용을 읽거나 서비스 거부를 유발할 수 있음		7.4

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
111631	GN-26135	macOS Agent	macOS 파일배포 옵션 추가 및 파일 실행 관련 로직 개선	5.0.35
111205	GN-25739	WebUI	사용자 일괄등록시 관리역할 추가	
111186	GN-25994	macOS Agent	macOS 하드웨어 정보 수집 플러그인에 USB 장치 정보 추가	
111033	GN-26163	Sensor	Dnsmasq Cache 기능을 사용하도록 변경	
111033	GN-25933	Center, Database	ZTNA Client 다중 서버도메인 설정 가능하도록 개선	
111033	GN-25928	Genian Syncer	지니안싱커에 불필요하게 출력되는 패치모음 설정 항목 제거	
111033	GN-25914	Sensor	ARM 환경에서 ZTNA Client동작하지 않는 문제	
111033	GN-25911	Zero Trust Security	ZTNA 고정아이피 사용 설정시 Secondary DNS 설정 반영	
111033	GN-25866	Center	ZTNA RADIUS secret설정이 RADIUS 클라이언트 설정보다 우선되도록 개선	
111033	GN-25762	Center, Sensor	ZTNA Client 연결시 Physical Interface 사용할 수 있도록 개선	
111033	GN-25752	WebUI	메모리 위젯 출력의 세분화 및 동작방식 개선	
111033	GN-25748	Linux Agent	Linux Agent 모니터 정보수집 플러그인 개발	
111033	GN-25726	Sensor	사이트 NAT 예외대역 설정	
111033	GN-25718	Center	ZTNA 사이트 다중센서에 대한 동일 네트워크 할당 지원	
111033	GN-25622	build	실시간 네트워크 인터페이스 트래픽량을 확인할 수 있는 스크립트 추가	
111033	GN-25440	Center	장비 인증 사용 시 미사용노드 자동로그아웃에 의해 일부 노드가 인증해제되는 문제 개선	
111033	GN-25049	Linux Agent	Linux Agent, Popup 모듈 개발 및 사용자 알림 메시지 액션 기능 추가	
111033	GN-24094	Sensor	센서 업그레이드 실패 감사기록 상세화	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
113135	GN-26130	macOS Agent	macOS 하드웨어 정보수집 플러그인 사용시 크래시 발생하는 문제	5.0.38
113080	GN-26040	WebUI	변경노드관리 전체 노드 선택 시 관리자 확인 기능 동작 않는 문제	5.0.26
111889	GN-26072	Linux Agent	Linux Agent, GUI Module 미사용으로 동작시 행걸리는 문제	6.0.12
111835	GN-26188	IPMGMT	IP신청시스템 임시사용자 자동로그인 되지 않는 문제	5.0.50, 4.0.153, 6.0.11
111735	GN-25998	Windows Agent	(비밀번호 검증 플러그인) 계정의 비밀번호 변경시각이 계속 변경되어 보고되는 문제	4.0.M5, 5.0.0, 6.0.0
111726	GN-25565	Center	Syslog TLS 전송시 센터데몬 비정상 종료	4.1.M7
111667	GN-26175	Center	GDPI를 사용하는 Cloud 서비스에서 GPDB를 계속 다운로드 하는 현상	5.0.41
111618	GN-26106	Windows Agent	네트워크 공유폴더제어에서 공유허용시간 설정시 공유 해제되지 않는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
111584	GN-26137	WebUI	CWP 디자인 템플릿 설정 페이지에서 CWP 페이지 미리보기 화면이 보이지 않는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
111581	GN-26124	WebUI	FLOW 로그 기간이 전체일때 차트가 출력되지 않는 문제	6.0.0
111571	GN-26161	GenianOS	procmond에서 sshd 재구동 오류 수정	5.0.23
111408	GN-26125	ulogd	FlowLog에 제어정책 ID 가 저장 안되는 문제	6.0.1
111211	GN-26035	WebUI	IP 사용 신청서 상세보기에서 다운로드 이미지 클릭지 오류 페이지 발생	5.0.42 (LTS), 5.0.50, 6.0.10
111161	GN-26063	IPMGMT	CWP에서 IP사용신청 자동로그인 기능이 동작하지 않는 문제	5.0.50, 4.0.153, 6.0.11
111033	GN-26006	Center	[범용OS] 정책서버에서 ZTNA Client 동작하지 않는 문제	6.0.11
111033	GN-25979	Center	RADIUS 정책을 여러번 변경시 정책적용 큐가 정상동작하지 않는 문제	5.0.23
111033	GN-25978	WebUI	스위치 상세화면에서 수정시 패스워드 변경을 하지 않았는데 패스워드 길이 오류 출력되는 문제	5.0.17
111033	GN-25888	Center	메일서버 및 정보동기화 시, 구글 인증 코드 발급이 안되는 증상	5.0.16, 6.0.0
111033	GN-25859	Enforcer, Sensor	[범용OS] ubuntu 커널 버전에 대한 nac.ko 모듈 생성 실패로 인한 센서 오작동	5.0.39, 6.0.0
111033	GN-25830	Sensor	노드 상세 정보 수집시 snmp 수집이 정상적으로 수행되지 않는 문제	6.0.4
111033	GN-25801	WebUI	전체사용자 목록 화면에 2단계 인증 설정 화면이 출력되는 문제	6.0.7
111033	GN-25756	Windows Agent	로컬시스템으로 에이전트 동작 시 수동 프록시 설정 않는 문제	4.0.0, 5.0.0, 6.0.0
111033	GN-25675	Center	LDAP 인증연동 설정값이 없으면 Agentless AD SSO 기능 동작하지 않는 문제	5.0.44, 6.0.1
111033	GN-	Center	NAT IP 노드등록 기능으로 등록된 노드의 플래폼 및 타	4.0.27

16.2.12 Genian ZTNA 6.0.11 Release Notes (2023-01-10)

Last Updated: 2023-02-10

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
111015	GN-25982	WebUI	WebUI Response Header에 CSP, HSTS Header 추가		
110942	GN-25849	WebUI	WebUI lib 취약점 항목 점검		
110495	GN-25875	Windows Agent	에이전트가 웹브라우저 실행할 때 High권한 가지는 문제	4.0.0, 5.0.0, 6.0.0	3.3
110354	GN-25811	IPMGMT	IP 신청시스템에서 frontpage를 통해 사용자ID만으로 로그인 가능한 문제		4.9

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
110821	GN-25891	Windows Agent	수집되는 오픈포트의 개수 제한기능 추가	
110801	GN-25280	WebUI	사용자 생성 wizard 기능 추가	
110619	GN-24938	WebUI	이메일 발송의 즉시수행시 수행시점의 노드그룹 데이터로 메일을 발송하도록 수정	
110535	GN-25579	Center	노드 스냅샷 정리기능 누락	
110495	GN-25865	Windows Agent	에이전트에서 수집된 정보 전송에 실패할 때 짧은 시간에 무한반복전송으로 인한 센터 부하 문제 개선	4.0.0, 5.0.0, 6.0.0
110215	GN-25741	Center, WebUI	노드 등록시 인증사용자 항목 추가	
110215	GN-25735	WebUI	라이선스 현황 화면에서 라이선스에 에이전트 제한 수량이 있을 경우 출력	
110215	GN-25731	WebUI	노드상세의 장비 항목 선택시 선택한 센서에서 검색이 아닌 전체노드에서 검색되도록 개선	
110215	GN-25727	Ubuntu(Debian)	[범용OS] history 이력에 timestamp 출력	5.0.0, 6.0.0
110215	GN-25666	Center	[RADIUS] 감사로그를 로그필터를 통해서 외부 전송할 수 있도록 개선	
110215	GN-25656	RADIUSD	[RADIUS] AD 인증연동시 실패감사로그를 상세하게 출력하도록 변경	
110215	GN-25623	Center, DKNS	동일 ZTNA Client 설정으로 다중센서에서 동작가능하도록 개선	
110215	GN-25604	Center	CWP 에이전트설치 메시지 삭제 시 에이전트설치 아이콘 출력되지 않는 문제	3.0_0910
110215	GN-25592	Center	ZTNA 사용자에 대한 고정 아이피할당 기능 지원	6.0.11
110215	GN-25576	Windows Agent	Always on ZTNA 기능 개발	
110215	GN-25564	Linux Agent	Linux Agent, 로컬 네트워크 변경시 감지 및 관련 추가작업 개발	
110215	GN-25480	Sensor	[범용OS] 디스크 정보 수집시 블록 디바이스 정보가 수집되도록 개선	
110215	GN-25269	Center	RADIUS 정책 추가속성에 USER 매크로를 사용가능 하도록 개선	
110215	GN-25232	WebUI	제어정책 CLI 도구명령의 할당 파라메터 항목 Macro 설정 도움말 추가	
110215	GN-24836	Center	ZTNA 클라이언트 Access 2차인증 유예시간 기능 추가	
110215	GN-24755	Center	geniupdate 를 통한 BP 공지사항을 NAC 에 적용	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
114610	GN-25945	Center	[ZTNA] 권한정책 내 제어액션 수행 불가 및 윈도우 방화벽 제어 불가 오류	6.0.7
111461	GN-26028	Windows Agent	프로세스 강제종료 액션정책이 여러 개 존재할 경우 강제종료 미동작 문제 수정	5.0.25
110993	GN-26042	Linux Agent	Linux Agent, dbus connection 에러로 인한 권한 문제	6.0.6
110979	GN-26029	CLOUD	Cloud NAC 사용자정보 동기화 안되는 문제	6.0.3, 5.0.50
110971	GN-26045	CLOUD	신규 Cloud Site 생성시 GDPI API를 사용하도록 설정이 되지 않는 문제	5.0.50, 6.0.10
110966	GN-25749	WebUI	보안그룹 설정시 nhn cloud와 naver cloud에서 서비스 객체 tcp-all, udp-all 적용시 오류	6.0.9
110790	GN-26018	WebUI	IP신규/반납 신청서의 상세보기 화면에서 승인시 오류 발생	5.0.49, 6.0.8
110778	GN-25964	Windows Agent	에이전트 인증창 업그레이드 후 인증 후 실행 옵션이 사라지는 문제	5.0.42 (LTS), 6.0.3, 5.0.46
110736	GN-25832	WebUI	PC 시간 변경시 관리콘솔 세션타임이 변경되는 문제	5.0.48, 6.0.7
110566	GN-25965	Center	ZTNA 센서 터널링 시 event 이름이 다른 문제	6.0.0
110440	GN-25880	Center	[범용OS] favicon 출력 안되는 문제	5.0.37
110376	GN-25861	WebUI	사용자 정의 리포트 파일 생성되지 않는 문제	6.0.4
110373	GN-25889	WebUI	스위치 관리에서 삭제 기능 동작하지 않는 문제	6.0.4
110346	GN-25931	CWP	On Premise에서 Domain을 사용하는 경우 SAML 인증시 IP주소로 인증요청이 발생하여 인증이 되지 않는 문제	5.0.48
110215	GN-25797	WebUI	선택 노드바구니 비우기 기능 오동작 문제 수정	5.0.44, 6.0.1
110215	GN-25763	WebUI	ZTNA-Client 설정시 클라이언트 할당 네트워크 수정시 항목 출력 안되는 오류	6.0.0
110215	GN-25760	WebUI	노드의 IP 정책이 정상적으로 반영되지 않는 문제	4.0.116, 5.0.13
110215	GN-25730	WebUI	노드상세화면에서 ZTNA VPN 으로 등록된 노드 동작방식 잘못출력되는 문제	5.0.32
110215	GN-25712	Windows Agent	DNS제어 플러그인을 통한 Hosts 파일 제어시 한글이 포함되어있으면 오동작하는 문제	4.1.0, 5.0.0, 6.0.0
110215	GN-25694	WebUI	노드의 관리센서를 센서 Alias 로 설정할 수 있는 문제 수정	4.0.119, 5.0.16
110215	GN-25686	Windows Agent	무선연결관리자 OFF 상태에서 트레이아이콘에 무선관련 메뉴 표시 오류	5.0.0, 6.0.0
110215	GN-25677	CWP	SAML 인증연동 환경에서 CWP 사용자정보 수정화면 이동시 사용자 재인증 화면에서 SAML 로그인 버튼이 출력되지 않는 문제	5.0.45, 6.0.2
110215	GN-25507	WebUI	노드 액션의 조건설정에서 조건컬럼에 나타나는 아이콘에 툴팁이 표시되지 않음	4.0.M1
110215	GN-25489	WebUI	노드 관리의 노드 삭제 명령 전송 건수에 상관 없이 '(1건)'으로 표시되는 문제	5.0.44

16.2.13 Genian ZTNA 6.0.10 Release Notes (2022-12-05)

Last Updated: 2023-01-10

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
110207	GN-25925	IPMGMT, WebUI	IP 신청시스템 > IP신청 화면 XSS 가능한 문제		5.4
109988	GN-25847	WebUI	CWP 화면에서 사용자 정보 수정 페이지 접근시 재인증 절차 추가		4.2
109886	GN-25740	WebUI	감사 > 로그 > 로그검색바에서 XSS가 가능한 문제		5.6

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
109570	GN-25657	WebUI	임시사용신청의 신청서처리결과를 IP 관리에서 메뉴 추가 삭제 가능하도록 수정	
109570	GN-25639	CLI/gnlogin, Database	ssh port 변경시 DB에 즉시 반영되도록 개선	
109570	GN-25625	WebUI	필수항목으로 사용자 추가 필드를 생성하는 경우 필수항목임을 표시하도록 수정	
109570	GN-25567	Linux Agent	Linux Agent, 네트워크 정보 수집시 다중 IP, DNS 설정 정보(IPv4, IPv6) 수집 가능하도록 개선	
109570	GN-25513	Linux Agent	Linux Agent, 소프트웨어 정보수집 액션 적용유무와 상관없이 에이전트 버전정보를 센터에 전송하도록 기능 추가	
109570	GN-25494	Windows Agent	비밀번호 유효성검사에서 비밀번호 변경감지하여 검증창이 자동으로 종료 될 수 있도록 수정	
109570	GN-25470	WebUI	노드관리 동작상태차트 클릭시 화면전환없이 노드상세화면의 이력관리탭 출력될 수 있도록 개선	
109570	GN-25278	Windows Agent	Microsoft store에 에이전트 설치패키지 게시	
109570	GN-25186	Center	Netflow 로그 Start/Close/Update/Deny 선택 옵션 추가	
109570	GN-24968	WebUI	다른 화면에서 노드 상세 정보페이지로 이동시에 상세 페이지에 뒤로가기 버튼 추가	
109570	GN-24820	WebUI	감사 > 로그 화면에 로그데이터 사용량 표기 기능 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
110912	GN-25900	Linux Agent	Linux Agent 장기 사용시 서버로부터 정책을 받는 횟수가 증가하는 문제	5.0.41, 6.0.0
110215	GN-25616	WebUI	클라우드 사이트 생성시 신규 대시보드의 디폴트 위젯들이 추가되지 않는 문제	6.0.1
110209	GN-25903	macOS Agent	macOS 파일배포 플러그인 파일 미업로드시 에이전트 오동작하는 문제	5.0.31, 6.0.0
110173	GN-25796	Center	에이전트에 의한 신규노드 등록 시 노드타입이 지정된 경우에도 노드타입 변경되는 문제	5.0.33
110152	GN-25885	Sensor	스위치 포트정보가 수집 안되는 문제	6.0.4, 5.0.47
110059	GN-25863	WebUI	노드관리 검색어에 &가 있을 경우 동작하지 않는 문제	5.0.42 (LTS), 5.0.49, 6.0.8
109972	GN-25868	Center	간헐적으로 노드(에이전트) 업다운 로그가 남지 않는 문제	5.0.49
109939	GN-25699	WebUI	현황&필터 의 에이전트 액션의 필터 결과가 상세조회 내역과 다른 문제 및 엑셀다운로드가 안되는 현상	6.0.4, 5.0.48
109915	GN-25819	WebUI	소프트웨어 현황을 통한 노드관리 검색이 정상동작하지 않는 문제	6.0.7
109766	GN-25488	WebUI	관리콘솔 세션 타임아웃이 60분을 넘어가는 경우 남은 시간이 정상적이지 않는 문제	6.0.1
109752	GN-25818	WebUI	에이전트 파일업로드 시 메모리가 낮은 장비에서 out of memory 오류 발생되며 업로드가 되지 않는 문제	6.0.8, 5.0.50, 4.0.152
109720	GN-25750	Windows Agent	인증창에서 잘못된 URL으로 웹브라우저가 열리는 문제	5.0.0, 4.0.123
109570	GN-25864	Genian Mobile	Genian NAC Monitor 에서 센터에 접속되지 않는 문제	5.0.49, 6.0.9
109570	GN-25745	Linux Agent	Linux Agent, "파일 배포" 플러그인에서 Root 권한으로 파일 실행이 안되는 문제	6.0.8, 5.0.50
109570	GN-25734	Windows Agent	에이전트 알림메세지에서 하이퍼링크 클릭시 IE가 표시되는 현상	6.0.4, 5.0.47
109570	GN-25723	Sensor	ZTNA IPSec 비활성화후 iptables rule 제거되지 않는 문제	6.0.1
109570	GN-25652	WebUI	대시보드의 CVE 현황 위젯에서 플랫폼 수량을 클릭하여 이동됐을 때, 목록 버튼 클릭시 오류 발생	5.0.43, 6.0.0
109570	GN-25621	WebUI	로그인 페이지에서 헤더 이미지를 추가했지만 출력되지 않는 문제	6.0.7
109570	GN-25608	Windows Agent	유선인증관리자로 GTC인증 후 다시 인증정보 받지 않고 자동 인증 되는 문제	5.0.17, 6.0.0
109570	GN-25575	WebUI	노드리포트 검색바에서 달력에 날짜를 선택하면 선택한 날짜와 다른 날짜가 선택되는 문제	5.0.8
109570	GN-25553	WebUI	감사로그 Excel Exporter시 상세정보의 내용이 깨지는 현상	5.0.21
109570	GN-25549	dbmigration	CLOUD 고객사 사이트 생성후 RADIUS Accounting 동작하지 않는 문제	5.0.33
109570	GN-25543	WebUI	SAML2로 사용자 인증 후 노드목록 인증사용자 컬럼에 아이콘 미출력 문제 수정	5.0.19
109570	GN-25430	WebUI	노드 관리의 검색바에서 에이전트 액션 조건(AgentActionName) 으로 조회되지 않는 문제	6.0.7

16.2.14 Genian ZTNA 6.0.9 Release Notes (2022-11-11)

Last Updated: 2022-12-05

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
109583	GN-25753	WebUI	CWP 에서 PAGEFW 파라미터를 통한 불법 경로로 리다이렉트 하지 않도록 개선		4.2
109400	GN-25746	Center, Sensor	시큐어코딩 점검결과 취약점 패치		
108915	GN-25438	Center, Sensor	_filelist.html 파일을 센터마다 다르게 생성하도록 개선		3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
109642	GN-25446	Linux Agent	Linux Agent, Sophos Linux 백신 정보 추가 수집 기능 개발	
109174	GN-25570	Center, WebUI, Windows Agent	Google OTP 2차인증 사용시 보안키 등록할 때 CWP에 의한 중복 로그인 과정이 필요한 문제 개선	6.0.2
109081	GN-25601	WebUI	IP 사용 신청서 수정화면에서 신청정보 비활성화 되는 문제	
109071	GN-25640	WebUI	사용자정의 리포트 트리 메뉴에 내가생성한 리포트만 출력되도록 수정	
108915	GN-25510	WebUI	ZTNA 게이트웨이 추가시 지원되지 않는 사이트 선택시 오류 메시지 출력	
108915	GN-25496	macOS Agent	macOS 에이전트 자동업데이트 부하 분산 가능하도록 체크 주기 변경	
108915	GN-25479	WebUI	장치 사용 신청서 처리 알림 메세지의 html 구문 제거	
108915	GN-25477	macOS Agent	macOS 잠자기 모드에서 무선랜제어 플러그인 사용시 Popup 메시지 중복처리	
108915	GN-25457	WebUI	REST API를 통한 '인스턴스 메세지' 전송	
108915	GN-25450	Linux Agent	Linux Agent, 에이전트 삭제시 액션 정리작업 수행되도록 기능 추가	
108915	GN-25416	Linux Agent	Linux Agent, 정책서버에서 서로다른 표준시간대 사용에 대한 예외처리	
108915	GN-25407	WebUI	calendar 현재 일자와 선택 일자 UI 구분	
108915	GN-25388	Windows Agent	무선랜제어 플러그인에 "허용SSID-정규식"옵션에 대한 도움말 추가	
108915	GN-25333	RADIUSD	RADIUS EAP-TTLS 지원 (MSCHAPv2, PAP)	
108915	GN-25322	WebUI	사용자 관리뷰에 마지막 인증해제시각 컬럼 추가	
108915	GN-25321	Windows Agent	액션 정책 CONF설정 UX개선	
108915	GN-25312	Linux Agent	Linux Agent, Always on ZTNA 기능 개발	
108915	GN-25231	WebUI	노드그룹 조건 중 MAC 주소 조건 클릭시 로딩이 오래 걸리는 문제 개선	
108915	GN-25212	WebUI	CWP 신규 사용자 등록 화면의 기간(날짜시각입력 형태) 입력 항목 출력 개선	
108915	GN-25134	Linux Agent	Linux Agent, CLI를 통한 필수동작 관리 기본 구조 및 VPN 접속 관리 기능 개발	
108915	GN-25096	Center	RADIUS MAC인증 노드그룹검사를 Calling-Station-Id 를 가지고 비교할 수 있도록 개선	
108915	GN-25077	WebUI	Passkeys 대체인증 수단 추가	
108915	GN-24841	Linux Agent, WebUI, Windows Agent	Windows 방화벽 제어 플러그인의 커스텀 규칙 내 설정을 '모두'로 변경하는 경우 하위 항목에 설정된 내용 삭제 기능 추가	
108915	GN-24705	Windows Agent	Captive Portal Detection을 통한 차단페이지 표시 기능	
108915	GN-24504	WebUI	Naver CLOUD (NCP) 지원	
108915	GN-	Windows	에이전트 자동업데이트 부하 분산 가능하도록 체크 주기	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
109403	GN-25671	WebUI	Hub-Branch 간의 ZTNA - IPSec Pre-Shared Key 설정 오류	6.0.1
109323	GN-25708	macOS Agent	macOS 에이전트 크래시 발생하는 문제	5.0.45, 6.0.2
109233	GN-25663	macOS Agent	인터넷연결 차단 환경에서 macOS 에이전트 설치 시 IP입력창 출력	5.0.27, 6.0.0
109217	GN-25720	IPMGMT	임시사용자 IP신규신청이 안되는 문제	4.0.149, 6.0.6, 5.0.49
109158	GN-25645	Center	DHCP노드IP변경시 변경전IP로 만들어진 플랫폼탐지데이터파일(scanraw)이 정리 안되는 문제	4.0.M7
109150	GN-25589	Center	IP변경노드 삭제에 의해서 노드 삭제시 Bad type conversion 에러 발생	5.0.46, 6.0.5
108989	GN-25698	WebUI	수집기 데이터 전송시 메시지 사이즈 오류	6.0.0
108938	GN-25669	WebUI	노드목록에서 컬럼 사이즈 조절 후 갱신했을때 조절한 사이즈로 출력되지 않는 문제	6.0.7
108915	GN-25574	macOS Agent	macOS 에이전트 내의 메세지 관련 ID를 정상적으로 가져오지 못하는 문제	5.0.50, 6.0.9
108915	GN-25568	WebUI	노드 정책에서 전체 선택후 즉시 적용 수행 시, 항목들이 해제되는 현상	6.0.4
108915	GN-25559	Windows Agent	무선연결관리자를 통하여 한글 SSID 프로파일이 잘못 등록되어 연결못하는 문제	4.0.5, 5.0.0, 6.0.0
108915	GN-25498	macOS Agent	macOS 모양 및 개인설정 플러그인의 화면보호기 옵션이 적용되지 않는 문제	5.0.15, 5.0.45, 6.0.2
108915	GN-25462	Genian Monitor	윈도우용 Genian Monitor에서 상세항목 클릭시 웹페이지 오류 표시 문제	5.0.19, 6.0.0
108915	GN-25443	Center	custom 인증서 사용중에도 인증서 만료로그가 장비인증서 기준으로 남는 문제	5.0.0
108915	GN-25439	Center	GPDB 수동 업데이트 시 에이전트 설치 노드의 플랫폼이 Unknown으로 변경되는 문제	
108915	GN-25428	Ubuntu(Debian)	[범용OS] 에이전트 파일 restore 후, 에이전트 설치 파일 업로드 및 다운로드 안되는 문제	5.0.23, 6.0.0
108915	GN-25418	GenianOS	[범용OS] 파일 내보내기(Excel Export) 기능이 동작하지 않는 문제	
108915	GN-25400	WebUI	에이전트 버전별 현황 위젯을 통해 노드목록 이동 후 재검색 또는 페이지 이동 시 정상출력 되지 않는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
108915	GN-25399	Center, Database	Windows 업데이트 액션 라벨 할당 시 Windows 업데이트 현황의 노드 수가 잘못 표시되는 문제	4.0.113, 5.0.10
108915	GN-25390	Sensor	FQDN 네트워크 객체 사용시 권한이 정상동작하지 않는 문제	5.0.27
108915	GN-25381	Center, CLOUD	CLOUD 버전에서 인증서 재발급 버튼으로 인증서가 재발급되지 않는 증상	5.0.45, 6.0.2
108915	GN-25364	WebUI	CONF On/Off 버튼을 부모로 설정했을 때 자식 설정의 visible 처리가 정상적으로 처리되지 않는 문제	5.0.16

continues on next page

Table 13 – continued from previous page

Revision	Key	Components	Description	Affects Versions
108915	GN-25350	WebUI	IP신규신청의 이메일 승인/거부 후 로그인 되어 있는 관리자 UI 세션이 종료 되는 문제	4.1.0
108915	GN-25345	Center	[범용OS] 정책서버 업그레이드시 센서 자동 업그레이드 기능 동작하지 않는 문제	5.0.43, 6.0.0
108915	GN-25340	macOS Agent	macOS 운영체제 정보수집 플러그인에서 설치 날짜를 가져오지 못하는 문제	6.0.4, 5.0.47
108915	GN-25317	Center	노드그룹 조건의 시간객체 종료시각 이후에도 노드그룹에서 해제되지 않는 문제	4.1.3
108915	GN-25289	macOS Agent	macOS 장치제어 플러그인 동작 오류 및 로그 개선	6.0.3, 5.0.46
108915	GN-25219	Center	[범용OS] HA 이중화 구성에서 Master 파일이 Slave로 동기화되지 않는 문제	
108915	GN-25159	WebUI	URL 호출에서 설정된 헤더 목록이 모두 삭제되지 않는 문제	5.0.15
108915	GN-25117	WebUI	에이전트 관련 위젯에서 노드목록 이동시 검색되지 않는 문제	5.0.33
108915	GN-25081	WebUI	IP 신청서 REST API에서 장비변경 승인이 처리되지 않는 문제	5.0.7, 4.0.110

16.2.15 Genian ZTNA 6.0.8 Release Notes (2022-10-11)

Last Updated: 2022-11-08

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
109188	GN-25561	WebUI	노드검색바 Blind SQL Injection 취약점		5.3
108509	GN-25184	Sensor	DNS Cache Poisoning 공격방어를 위해서 Dnsmasq 에서 쿼리 결과를 캐쉬하지 않도록 수정		3.7
108074	GN-23677	Center, Sensor	센서 정책서버 등록시 보안성 강화를 위한 관리자 승인 시스템		7.9

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
108806	GN-25615	Linux Agent	NAC 설치 및 업그레이드 시 리눅스 에이전트 등록 및 업그레이드 누락 추가	
108767	GN-25468	WebUI	액션조건 설정시 레지스트리 값에 공백 허용	
108676	GN-25266	Windows Agent	비밀번호 검증 플러그인 시작 시 디버그로그에 빈암호 사용 여부 표시	
108630	GN-25075	WebUI	공지사항 이미지 업로드 기능 추가	
108274	GN-24693	Windows Agent	인증창 잠금화면에 배경이미지 지원	
108074	GN-25509	Database	ZTNA를 위한 최초 Popup 페이지 변경	
108074	GN-25417	macOS Agent	macOS 에이전트 인증창 종료 금지	
108074	GN-25411	WebUI	Cloud Sensor 생성 후 로딩바는 출력되었지만 Sensor 생성 후에도 화면 갱신이 이뤄지지 않는 문제	
108074	GN-25316	GNOS	"잘못된 DHCP서버 수집 정보"관련 위험 감사로그 항상 출력 옵션 추가	
108074	GN-25223	Linux Agent	Linux Agent, 트레이 아이콘을 통한 웹 브라우저 접속 시, snap에서 다운받은 웹 브라우저 연동 추가	
108074	GN-25205	WebUI	노드상세 - 운영체제 업데이트 정보탭의 최근 수행결과 출력 개선	
108074	GN-25191	WebUI	'에이전트 서비스 중지'시 변경된 상태를 Image Icon으로 확인 할 수 있게 제공	
108074	GN-25189	CLI/gnlogin	mgmt-port CLI 입력시 mgmt-local-port 가 적용되도록 개선	5.0.44, 6.0.2
108074	GN-25176	WebUI	File Upload 컴포넌트 파일명 저장 방식 및 다운로드 개선	
108074	GN-25161	Center	제어정책을 통한 Switch Port VLAN 변경시 Port Bounce 처리	
108074	GN-25027	WebUI	감사로그 필터의 입력항목 글자수 제한 확대	
108074	GN-25015	Linux Agent	Linux Agent, Genian Linux PAM(Pluggable Authentication Modules) 개발	
108074	GN-25006	WebUI	Flow Log 화면에 Application Name 통계 Pie Chart 추가	
107302	GN-25095	Linux Agent	Linux Agent, 파일 배포 액션 플러그인 개발	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
108774	GN-25482	WebUI	정책 그룹의 조건설정을 수정하는 경우, 신규 추가되는 문제	6.0.6, 5.0.49
108771	GN-25481	dbmigration	액션조건 중 레지스트리 설정 관련 데이터 마이그레이션 오류 발생	5.0.48
108770	GN-25032	WebUI	태그해제시각을 무제한으로 설정했음에도 태그에 설정된 기간설정이 적용되는 문제 수정	5.0.21
108730	GN-25086	WebUI	카테고리 미지정에 속하는 리포트 항목 클릭시 오류 발생	5.0.38, 6.0.0
108538	GN-25560	WebUI	노드관리 화면에서 검색 수행 후 정책탭 이동 시 스크립트 오류 문제	6.0.4
108173	GN-25532	WebUI	CWP 에서 사용자 패스워드 변경 시 USER_LASTPWCHANGE 값이 갱신되지 않는 문제	6.0.6, 5.0.49, 4.0.151
108074	GN-25456	macOS Agent	macOS 에이전트 업로드시 Duplicate entry 로그 발생하는 문제	5.0.45, 6.0.2
108074	GN-25402	macOS Agent	macOS 호스트명 변경 플러그인 성공여부 오류	5.0.34, 6.0.0
108074	GN-25386	macOS Agent	macOS 프로세스 강제종료 플러그인 동작하지 않음	5.0.0, 6.0.0
108074	GN-25361	Windows Agent	허용된 AP의 SSID가 한글일 때 무선랜제어 플러그인 동작오류	5.0.0, 6.0.0
108074	GN-25357	WebUI	IP신규/반납 신청서의 상세보기 화면에서 승인시 오류 발생	5.0.13
108074	GN-25354	macOS Agent	macOS 공유폴더명에 마침표가 포함되면 정보 수집하지 못하는 문제	6.0.4, 5.0.47
108074	GN-25339	WebUI	로그검색 및 검색필터의 수정상태에서 새로고침 버튼 클릭 시 분석차트페이지로 전환되는 현상	5.0.22
108074	GN-25319	WebUI	노드목록에서 NodeType 조건을 여러개 입력해서 조회할 때 오류 페이지 출력되는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
108074	GN-25279	WebUI	노드타입 위젯에서 일부 노드타입의 링크로 이동된 노드 목록에서 결과가 잘못출력되는 문제	5.0.43, 6.0.0
108074	GN-25271	Center	기본/보조DNS 조건 정책 적용시 링크 UP 된 인터페이스만 정책검사되도록 수정	5.0.0
108074	GN-25259	Windows Agent	노드정책의 에이전트 사용여부를 OFF으로 변경해도 이전 액션수행결과가 남아있는 문제	5.0.0, 6.0.0
108074	GN-25253	Windows Agent	장치제어 차단 후 감사로그에 'ID=숫자' 형태로 출력되어 정책 이름으로 수정	5.0.25, 6.0.0
108074	GN-25238	WebUI	노드그룹 조건 추가 UI에서 부서검색 팝업에 X버튼이 없으며, 부서 정보가 없는 경우 두번째 부서검색 팝업에서 취소버튼 보이지 않는 문제	5.0.20
108074	GN-25216	WebUI	REST API 를 통한 파일 업로드 수행 시 정상적으로 파일이 업로드 되지 않는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
108074	GN-25152	IPMGMT	IP관리정책위반인 상태에서 IP사용신청 시 페이지 오류	5.0.11
108074	GN-25147	WebUI	디폴트 노드그룹를 모두 업데이트 했는데 업데이트 가능 수량이 있다고 표시될 수 있는 문제	5.0.27
108074	GN-25144	Center	인증연동 서버주소에 공백이 포함된 경우 서버 연결에 실패하는 문제	

16.2.16 Genian ZTNA 6.0.7 Release Notes (2022-09-06)

Last Updated: 2022-10-11

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
107755	GN-25237	WebUI	CSAP(SaaS) 보안인증 심사 소스코드 취약점 조치		0
107447	GN-25387	Database, WebUI	정책 > 클라우드 보안그룹 정책에 대한 관리역할 미적용 문제		3.5
107144	GN-25309	Center, Sensor	CSAP(SaaS) 보안인증 심사 소스코드 취약점 조치 - C/C++		7.5
107144	GN-25250	WebUI	HTML Tag 문자열 뒤에 /를 붙이는 경우 XSS가 가능한 문제		4.9
107144	GN-25239	WebUI	Tomcat version upgrade (8.5.78 -> 9.0.65)		7.5
107144	GN-25193	WebUI	[범용OS Ubuntu] 관리콘솔 > CWP Design Template 목록 페이지 'X-Frame-Options' Header 가 allowall로 표시되는 문제		6.5
107144	GN-25119	macOS Agent	macOS Agent, OpenVPN(2.5.7) 및 OpenSSL(1.1.1q) 최신 버전으로 업그레이드		5.3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
108044	GN-25409	WebUI	디버그로그 화면의 접근권한 설정 개선	
107868	GN-24699	Windows Agent	에이전트 인증창의 2차인증에 Passkeys(생체 인증) 기능 추가	
107717	GN-24803	WebUI	리포트 이메일 폼, 설정, 목록 조회 관련 기능 개선	
107144	GN-25273	GenianOS	[범용OS] apache2 설정을 custom 하게 사용할 수 있도록 개선	6.0.3
107144	GN-25201	macOS Agent	macOS 에이전트 상태 재검사 기능	
107144	GN-25164	GenianOS	인증시마다 소유자를 재설정 시 정보가 갱신된 경우에만 감사로그를 남기도록 개선	
107144	GN-25160	Windows Agent	Sophos Endpoint Agent 백신정보 업데이트	
107144	GN-25138	Windows Agent	GnPMS 수행결과를 윈도우즈 업데이트 액션의 결과메시지로 제공	
107144	GN-25137	Linux Agent	Linux Agent, ARP 관리 액션 플러그인 개발	
107144	GN-25125	WebUI	사용자 생성 화면의 출력 순서 변경	
107144	GN-25112	Linux Agent	Linux Agent, 에이전트 삭제 방식 옵션에 따른 동작 기능 개발	
107144	GN-25078	Windows Agent	에이전트 인증창으로 화면잠금을 사용중에 모니터 확장에 대한 고려	
107144	GN-25025	Windows Agent	무선연결관리자를 통하여 "EAP-TTLS" 인증방법 제공	
107144	GN-24950	Windows Agent	유선인증관리자를 통하여 "EAP-TTLS" 인증방법 제공	
107144	GN-24929	Enforcer, Sensor	Application 식별을 통한 네트워크 제어(차단) 기능	
107144	GN-24913	Windows Agent	ZTNA 연결관리자에 Passkeys 기반 2차 인증 기능 추가	
107144	GN-24814	CWP, WebUI	Passkeys(FIDO2 - 생체 인증) 관련 REST API	
107144	GN-24745	CWP	Passkeys 인증을 2차인증으로 지원 - 사용자(CWP)	
107144	GN-24744	CWP, WebUI	Passkeys 인증을 2차 인증으로 지원 - 관리콘솔(MC)	
107144	GN-22592	CWP	CWP 디자인템플릿 컴포넌트 설정을 off 했다가 on 할 경우 컴포넌트 위치가 최하단으로 떨어지는 문제	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
108688	GN-25129	CWP, WebUI	AWS에 AMI 이미지로 운영되는 정책서버에서 SAML 인증연동이 안되는 문제	5.0.19
107849	GN-25478	WebUI	IPMGMT 폰트어썸 아이콘 출력되지 않는 문제 수정	6.0.7
107708	GN-25308	WebUI	관리콘솔이 유휴 상태에서 깨어난 후 세션 타임 아웃 시간이 지나도 세션이 유지되는 문제	5.0.42 (LTS), 6.0.0
107422	GN-25380	Sensor	SNMP v2 Community 설정값에 특수문자 포함 시 스위치 등록에 실패하는 문제	6.0.4, 5.0.47
107221	GN-25099	WebUI	사용자등록신청서의 메일 승인시 사용만료일이 반영되지 않는 문제	4.0.M8, 5.0.41
107144	GN-25343	Windows Agent	PC부팅시마다 관리폴더에 대한 공유제어 알림팝업이 띄워지는 문제	5.0.0, 6.0.0
107144	GN-25318	Windows Agent	취약한 비밀번호 사용에도 비밀번호유효성검사 팝업창을 닫을 수 있는 문제	5.0.13, 6.0.0
107144	GN-25301	macOS Agent	macOS 네트워크 공유폴더 해제 오작동 및 글자 깨지는 문제	6.0.4, 5.0.47
107144	GN-25296	Windows Agent	영문윈도우에서 에이전트 인증창의 기본로고가 한글로 표시됨.	5.0.8, 6.0.0
107144	GN-25222	Linux Agent	Linux Agent, 장기 사용시 간헐적으로 Database Access 오류	6.0.4, 5.0.47
107144	GN-25218	WebUI	fontawesome 아이콘 클릭시 로딩바 출력 문제	6.0.3, 5.0.46
107144	GN-25211	WebUI	설정 > 환경설정 > 관리콘솔 > 인증 > 세션 타임아웃 설정 오류	6.0.1
107144	GN-25209	WebUI	에이전트 미설치노드 시 상세뷰에서 '알림 메시지' 탭메뉴 아래로 가려지는 문제	6.0.5
107144	GN-25181	Windows Agent	최초 Google OTP를 통한 2단계 인증시 발생하는 오류 수정	6.0.2
107144	GN-25163	Windows Agent	노드가 삭제되고 신규로 다시 등록된 노드에 백신정보수집이 바로 되지 않는 문제	5.0.0, 6.0.0
107144	GN-25151	Center	동일한 이름을 가지는 소프트웨어가 여러개 있는 경우 소프트웨어 버전이 같으면/다르면 노드그룹 매칭이 안되는 문제	5.0.37
107144	GN-25136	WebUI	노드 관리 화면에서 만족함/만족안함 컬럼의 카운트가 잘못 출력되는 문제	5.0.33
107144	GN-25130	Genian Monitor	윈도우용 Genian Monitor에서 항목 및 설정 등을 수정 할 수 없음	5.0.0, 6.0.0
107144	GN-25115	WebUI	관리콘솔에서 IP 관리의 신청결과 목록의 컬럼에서 IP주소 컬럼을 제거했으나 반영되지 않는 문제	5.0.10
107144	GN-25103	Sensor	모바일 OpenVPN앱 ZTNA 연결시 노드등록되지 않는 문제	6.0.0
107144	GN-25080	Authsync, Center	관리콘솔에서 설정 변경 시 정보동기화 수행주기 시점에 동기화 수행되지 않는 문제	
107144	GN-25074	Center	폐쇄망에서 이미지 업그레이드시 GPDB를 이용한 신규 기능이 정상동작 하지 않을 수 있는 문제	5.0.0, 6.0.0
107144	GN-25029	macOS Agent	macOS Agent에서 무선랜제어 차단시 메시지 팝업되지 않음	5.0.27, 6.0.0
107144	GN-24914	Genian Syncer	지니안싱커를 통하여 업로드된 패치파일을 다운로드 받지 못하는 문제	5.0.44, 6.0.1
107144	GN-24676	WebUI	REST-API 서비스 이용시에 관리자 세션이 유지되는 오류	5.0.14
107144	GN-24287	Center	RADIUS Google OTP 인증을 통해서 secret key 를 생성할 수 없는 문제	6.0.7

16.2.17 Genian ZTNA 6.0.6 Release Notes (2022-08-08)

Last Updated: 2022-09-06

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
106934	GN-25306	WebUI	사용하지 않는 HTTP-Method를 통해 사용가능 method 정보가 출력되는 문제		5.3
106611	GN-25110	Linux Agent	Linux Agent, OpenVPN(2.5.7) 및 OpenSSL(1.1.1q) 최신 버전으로 업그레이드		5.3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
106673	GN-24961	WebUI	노드 목록 내보내기(다운로드)시에 진행률 표시	
106611	GN-25206	macOS Agent	macOS 에이전트 데몬동작 중단시 프로세스 완전종료	
106611	GN-25149	Windows Agent	윈도우 게스트 계정에 대한 정보수집 가능하도록 개선	
106611	GN-25100	Database	mysql이 활성화 되지 않은 서버에서 mysql client 동작시 Port 관련 경고 제거	
106611	GN-25089	WebUI	메뉴얼 링크 개선	
106611	GN-25082	WebUI	Cloud Sensor 추가 UX 개선	
106611	GN-25071	Linux Agent	Linux Agent, 노드 재등록 시 액션이 다시 수행되도록 기능 추가	
106611	GN-25054	Linux Agent	Linux Agent, 오류 보고를 위한 Agent 전체 로그 압축 기능 추가	
106611	GN-25047	WebUI	노드 등록 API 에 노드 커스텀필드 수정 기능 추가	
106611	GN-25046	Enforcer	kernel debug 기능에 권한정보도 출력할 수 있도록 개선	
106611	GN-25033	RADIUSD	RADIUS 인증서 등록 개선 및 Windows 11 단말에서 EAP-TLS 연결 실패하는 문제	5.0.42 (LTS)
106611	GN-25030	WebUI	Cloud Sensor 추가시 저장용량 선택 옵션 추가	
106611	GN-25001	WebUI	사용자 화면에서 부서명으로 사용자 검색 기능 추가	
106611	GN-24980	Center, Database, Sensor	ZTNA 연결할 서버도메인 설정 추가	
106611	GN-24978	WebUI	대시보드 빅넘버 위젯에서 쿼리로 데이터 가져올때 선택한 순서대로 출력할 수 있도록 개선	
106611	GN-24975	WebUI	엑셀 내보내기 된 파일의 로딩 속도 개선	
106611	GN-24970	Sensor	Softether Virtual-Hub Real interface 지원	
106611	GN-24966	WebUI	정책 관리화면에서 링크를 통한 노드목록 이동시 노드관점으로 출력될 수 있도록 파라미터 추가	
106611	GN-24935	WebUI	감사 메뉴 하위에 검색필터, RADIUS, Flow 메뉴 추가	
106611	GN-24930	Sensor	ZTNA 단말의 IP가 NAC WEBUI에서 누락되어 출력이 되는 경우가 발생하는 문제	
106611	GN-24925	WebUI	REST API 사용시 인증에 대한 설명 수정	
106611	GN-24903	WebUI	노드그룹 상세화면 조건 목록에 검색기능 추가	
106611	GN-24884	Linux Agent	Linux Agent 모양 및 개인설정 플러그인 개발	
106611	GN-24847	WebUI	관리콘솔 인증을 SAML 방식으로 인증하도록 기능 개발	
106611	GN-24791	WebUI	매트릭스 뷰에서 관리IP제어범위 설정시 설정된 범위의 내역만 확인하도록 기능 개선	
106611	GN-24698	macOS Agent	macOS에서 ZTNA 네트워크에 항상 연결 옵션 구현	6.0.0
106611	GN-24691	Zero Trust Security	Proxy를 통한 Web 접속 감사기록	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
107108	GN-24990	WebUI	IP 다중신청서 업로드시 용도 설정이 되지 않은 경우 동일의 검증 메세지가 출력되는 문제	4.0.106, 4.0.148
106968	GN-25287	WebUI	노드상세 정책 > MAC 정책 > 변경금지의 IP LIST 수정시 IPMChange Event 호출이 되지 않는 문제	5.0.41
106954	GN-25298	macOS Agent	macOS 에이전트에서 '주기적 수행'주기의 액션 수행시 수행결과가 '수행전 만족'으로 유지	5.0.11, 6.0.0
106864	GN-25242	CLOUD	cloud ztna site 삭제시 elasticsearch index가 삭제되지 않는 문제	6.0.5
106664	GN-25257	WebUI	리포트 메뉴에서 노드 리포트의 필터 메뉴에서 Excel 다운로드 시도 시 오류 발생	5.0.36
106636	GN-25277	Windows Agent	에이전트 빌드시 전자서명 검증 오류 수정	4.0.0, 5.0.0, 6.0.0
106611	GN-25225	Windows Agent	모니터 정보수집 플러그인으로 인한 GnPlugin.exe 비정상 종료	5.0.0, 6.0.0
106611	GN-25215	Windows Agent	운영체제정보수집 플러그인으로 인한 GnPlugin 미동작 문제	5.0.37, 6.0.0
106611	GN-25200	WebUI	영문UI에서 관리역할 메뉴제한 항목내에 특정항목 한글로 출력되는 오류	4.1.0
106611	GN-25127	Zero Trust Security	ZTNA isolation 기능이 정상 동작하지 않는 문제	6.0.6
106611	GN-25094	macOS Agent	macOS 에이전트에서 AD계정 대체인증시 반복하여 재인증	5.0.7, 6.0.0
106611	GN-25091	WebUI	특정 관리역할 할당 후 감사로그 IP, MAC 클릭시 노드 목록 검색 필터가 안되는 증상	4.1.M1
106611	GN-25083	WebUI	쿼리리포트 타입의 사용자정의 리포트가 생성되지 않는 문제	6.0.1
106611	GN-25048	Linux Agent	Linux Agent, Tray Icon 간헐적으로 표시 안되는 문제	5.0.42 (LTS), 6.0.0
106611	GN-25044	WebUI	Genian Software 파일업로드시 문제	5.0.2
106611	GN-25039	Center	ZTNA Profile 다운로드시 무한로딩 문제	6.0.0
106611	GN-25018	WebUI	멀티 사이트 생성시 수집기에 잘못된 메시지 출력되는 오류	6.0.3
106611	GN-25016	WebUI	신규 노드그룹의 백신정보의 조건 출력 오동작 수정	5.0.31
106611	GN-24998	Authsync	부서정보, 직급정보 동기화시 데이터소스 구분값 설정이 변경되면 동기화가 정상수행되지 않는 문제	4.0.0
106611	GN-24947	WebUI	사용자 수정 API 호출 시 비밀번호 마지막 변경시각 컬럼이 수정되지 않는 문제	5.0.43, 6.0.0, 4.0.146
106611	GN-24835	Center	에이전트로 인해 등록되는 노드등록시 MAC정보가 소문자로 저장될 수 있는 문제	6.0.4
106611	GN-24675	Ubuntu(Debian)	[범용OS] NAC deb 파일 생성시각이 관리콘솔에서 잘못 표시되는 문제	5.0.41

16.2.18 Genian ZTNA 6.0.5 Release Notes (2022-07-11)

Last Updated: 2022-08-16

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
106029	GN-25104	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1q)		5.3
105858	GN-24782	WebUI	취약점 점검에 따른 라이브러리 업그레이드		9.8

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
107045	GN-21428	macOS Agent	macOS Agent 단말 네트워크의 내/외부 상태에 따른 액션 정책 적용	
105858	GN-24983	Linux Agent	Linux Agent, Sophos server protection 정보 수집 기능 추가	
105858	GN-24962	WebUI	노드 등록시에 설명을 입력할 수 있는 UI 추가	
105858	GN-24945	WebUI	노드 목록의 엑셀 출력시 IP소유자/IP소유부서 출력 형태 수정	
105858	GN-24942	WebUI	미사용 IP에 MAC 태그 설정시 모든 미사용 IP 노드에 MAC태그가 할당되는 문제 및 현황&필터 화면 문제 개선	
105858	GN-24924	WebUI	노드목록 가져오기(GET /nodes) API 에 인증사용자 아이디 파라미터 추가	
105858	GN-24922	WebUI	Flow log 검색창에서 검색필드 자동완성 기능이 목록UI에 표시되는 컬럼 먼저 표시되도록 개선	
105858	GN-24921	Center	ldap 인증연동 및 ldap 정보동기화에서 인증서를 이용한 LDAP서버 연결이 가능하도록 수정	
105858	GN-24910	Sensor	ZTNA Isolation 옵션 변경시 설정 변경이 즉시 반영되지 않는 문제	
105858	GN-24900	Center	ZTNA Client OpenVPN 호환 옵션 추가	
105858	GN-24899	Database	App 데이터 베이스 Rule 추가	6.0.4
105858	GN-24894	Enforcer	NAC 커널(Enforcer) 에서 udp 이벤트패킷 전송시 패킷사이즈가 mtu 사이즈보다 크면 정책서버로 패킷전송 안되는 문제	
105858	GN-24879	Linux Agent	Linux Agent, 최신 플랫폼 버전 정보 추가	
105858	GN-24876	WebUI	사용자 신청서 용도에 MAC/장비 인증제한 처리옵션 추가	

continues on next page

Table 14 – continued from previous page

Revision	Key	Components	Description	Affects Versions
105858	GN-24871	WebUI	사이트 관리기능 설정 UX 변경	
105858	GN-24865	Center, DKNS, Sensor	ZTNA Client Split tunneling	
105858	GN-24862	WebUI	IP/장비 소유자 설정에서 사용자 이름 검색 가능하도록 기능 추가	
105858	GN-24858	Sensor	SoftetherVPN Foreground 실행시 디버그 메시지가 표준출력으로 나오도록 개선	
105858	GN-24850	Sensor	ZTNA Client 단말간 격리 동작시 동일 사용자간 통신 허용처리	
105858	GN-24832	WebUI	관리 > 노드 목록 화면에 트리의 전체노드 선택시 미사용 아이피 출력될 수 있도록 개선	
105858	GN-24825	Center	ZTNA 클라이언트가 아니면 조건을 가지는 기본 RADIUS 정책 추가	
105858	GN-24818	Zero Trust Security	동일 사이트 ZTNA Client 단말간 격리	
105858	GN-24816	Windows Agent	에이전트 인증창에 비밀번호 입력 자동 전환 기능 추가	
105858	GN-24787	Center	동작상태관련 감사로그의 관리장비명이 센서이름으로 표시도록 수정	
105858	GN-24786	WebUI	local.conf의 data-server username 앞뒤에 공백이 있는 경우 웹 콘솔 구동되지 않는 문제 개선	
105858	GN-24768	Linux Agent	Linux Agent 프로세스 강제 종료 플러그인 개발	
105858	GN-24753	WebUI	노드목록의 컨버터가 ajax 호출할때 단일건이 아닌 여러건을 묶어서 호출하도록 개선	
105858	GN-24672	CLOUD	ZTNA Client 사용시 DHCP IP 고정가능하도록 개선	
105858	GN-24671	WebUI	ZTNA Client Sessions 목록 화면의 할당IP에 노드목록으로 연결되는 링크 추가	
105858	GN-24664	Linux Agent	Linux Agent package 전자서명 기능 추가	
105858	GN-24655	RADIUSD	RADIUS 서버 외부인증연동에 RADIUS 인증연동 추가	
105858	GN-24600	Center	사용자 계정 시작 시각 기능 추가	
105858	GN-24330	Windows Agent	KB국민은행 PentaSSO 지속적으로 인증연동가능하도록 수정	
105858	GN-24183	Sensor	엑스게이트 MIPS-ralink 장비에 센서 모듈 포팅	
105858	GN-23901	WebUI	UI화면 출력 성능 개선	
105858	GN-17371	Windows Agent	에이전트 디버그 로그 영문화	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
106536	GN-25228	WebUI	on-premises 사이트에 수집기 설정이 동작하는 오류	6.0.0
106390	GN-24967	WebUI	상위 부서의 정보 변경시 부서에 속한 하위 부서 정보가 변경되지 않는 문제	4.0.M9
106370	GN-25220	Backup	백업 시 비밀번호가 암호화되어 실패하는 문제	6.0.3, 5.0.46
106363	GN-25179	Center	첨부파일메일전송시 MIME 형식이 잘못되어서 첨부파일 사이즈가 0kB 로 표시되고 읽을수 없는 문제	5.0.16
106305	GN-25153	WebUI	신규 노드 상세화면에서 변경된 항목이 화면 갱신이 없으면 반영되지 않아 보이는 문제	6.0.1
106275	GN-24904	WebUI	관리 (노드/스위치/무선랜/사용자) Left 메뉴에서 수정모드(on/off) 오류 문제	6.0.5
106046	GN-25090	Sensor	호스트명 변경 실시간 감지기능 사용시 메모리 할당 실패에 대한 예외처리 누락으로 센서 죽는 문제	4.0.114, 5.0.11
106009	GN-25135	Database	DB 백업 파일이 정상 생성되지 않는 문제	6.0.3
105959	GN-25132	WebUI	범용OS 우분투 버전에서 '에이전트상태'로 분류된 항목으로 노드그룹 조건추가시 에러 발생	5.0.42 (LTS), 5.0.43, 6.0.1
105858	GN-25043	MGMT	등록된 외부인증서로 웹서버(httpd) 구동 안되는 문제	5.0.42 (LTS)
105858	GN-24984	Sensor	Secondary IP 가 설정된 인터페이스에 대해서 마지막 Secondary IP 대역만 서브넷스캔 동작하는 문제	5.0.42 (LTS)
105858	GN-24981	Windows Agent	PC에 Teredo Tunneling Pseudo-Interface가 존재할 경우 MAC/IP Clone 탐지 오류	5.0.0, 6.0.0
105858	GN-24977	Zero Trust Security	OpenVPN앱에서 프로파일 Import되지 않는 문제	6.0.0
105858	GN-24946	WebUI	Radius 정책 수정시 오류 메시지 출력 및 변경정책 적용이 정상적으로 되지 않는 문제 수정	5.0.30
105858	GN-24939	Authsync	REST API Server 를 통해서 정보동기화시 Pageing 파라미터값이 잘못적용되어 API 를 호출하는 문제	5.0.38
105858	GN-24919	WebUI	상세리포트 타입으로 정의된 이메일 즉시수행시 오류 발생	5.0.43, 6.0.0
105858	GN-24906	Center	백신정보/서약동의정보의 시간관련 노드그룹 조건이 경과하더라도 노드그룹이 변경되지 못하는 증상	3.0_0910
105858	GN-24896	WebUI	IP 다중 신청 목록이 용도에 설정된 IP 처리 대역보다 많은 경우 서브넷을 변경하여 할당하지 않는 문제	4.1.0
105858	GN-24891	DKNS	Ubuntu 20.04 DKNS에 대하여 WEBUI를 통해 업그레이드 수행시 실패하는 문제	6.0.5
105858	GN-24867	Windows Agent	프린터 공유폴더에 대한 공유제어가 안되는 문제	4.0.125, 5.0.22, 6.0.0
105858	GN-24846	WebUI	IP 사용 신청서의 IP 리스트가 용도에 설정된 IP 할당 대역으로 표시되지 않는 문제	5.0.13
105858	GN-24845	WebUI	IP신청시스템 자동거부처리 API 에서 에러가 나타나는 문제	5.0.14
105858	GN-24839	WebUI	IP/MAC 현황에서 엑셀 내보내기 시 오류 페이지 발생되는 문제	4.0.M7

continues on next page

Table 15 – continued from previous page

Revision	Key	Components	Description	Affects Versions
105858	GN-24811	Windows Agent	무선연결관리자에서 사용자ID/PW 저장 해제 후 값이 다시 채워지는 문제	5.0.0, 6.0.0
105858	GN-24798	Center	Google G Suite 정보동기화 및 SAML 인증연동 시 노드의 인증사용자가 검색되지 않는 문제	5.0.19
105858	GN-24792	Linux Agent	Linux Agent, 인증 허용 MAC 정책 기능 동작하지 않는 문제	5.0.41, 6.0.0
105858	GN-24784	IPMGMT	IP사용신청서 결과조회시에 locale값이 변경되는 오류	4.0.114, 5.0.11
105858	GN-24741	WebUI	노드 상세에서 장비내 노드의 다른 노드 이동시 해당 노드의 상세화면이 출력되지 않는 문제	5.0.38
105858	GN-24725	Linux Agent	Linux Agent Debian11 기반 플랫폼에서 트레이 아이콘 표시 안되는 문제	5.0.0, 6.0.0
105858	GN-24663	Center, Linux Agent, macOS Agent, WebUI, Windows Agent	노드액션의 조건설정에 콤마(',')가 존재할 경우 조건설정이 오동작하는 문제	5.0.0, 6.0.0
105858	GN-24625	Center	에이전트버전 업그레이드시 에이전트소프트웨어 신규 추가로 처리 되어 대시보드에 업그레이드 현황이 잘못나오는 문제	4.0.M8
105858	GN-24580	Windows Agent	문서검색&삭제 커스텀 플러그인에서 삭제 실패시 사용자에게 표시되는 메시지 없음	5.0.42 (LTS)
105858	GN-24551	Sensor	범용OS에서 센서관련 기능이 정상적으로 동작하지 않는 문제	6.0.4
105341	GN-25000	Linux Agent	Linux Agent, 액션 수행 결과 메시지가 잘못 표시되는 문제	5.0.42 (LTS), 6.0.0

16.2.19 Genian ZTNA 6.0.4 Release Notes (2022-06-10)

Last Updated: 2022-07-11

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
105837	GN-25064	WebUI	웹서비스 취약점 Apache WAS 정보를 노출하지 않도록 개선	4.0.119, 5.0.16	2.5
105203	GN-23947	Windows Agent	윈도우 에이전트 시큐어코딩 점검결과 취약점 패치	5.0.0, 6.0.0	
103600	GN-24583	WebUI	WebUI에서 사용하는 java lib 중 취약점이 발견된 lib 업그레이드		9.8

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
105730	GN-25062	macOS Agent	macOS 에이전트의 macOS Ventura 지원	
105203	GN-24918	WebUI	IP할당 시 관리IP 제어범위 옵션에 따라 IP가 제한되게 출력되도록 개선	6.0.4, 5.0.47
105203	GN-24728	IPMGMT, WebUI	IP사용 신청서에서 Email 승인/거부 버튼링크 파라미터 암호화	
105203	GN-24718	WebUI	ZTNAC 버전 대시보드 위젯 팔렛트에 미리보기 이미지 추가	
105203	GN-24656	WebUI	Flow log UI 검색기간 default값을 1주 -> 최근24시간으로 변경	
105203	GN-24643	WebUI	위젯 데이터 기준 관점(노드/장비)으로 노드목록을 출력하도록 개선	
105203	GN-24639	WebUI	보안위반 탐지 로그를 기본 필터로 제공	
105203	GN-24636	CLOUD	IPsecVPN 암호화방식 Hub별 적용	
105203	GN-24633	WebUI	노드그룹 조건 설정시 '특정시간내에~' 조건의 경우 시간 단위 이외의 단위를 설정 못하는 문제	
105203	GN-24616	Linux Agent	Linux Agent, 정책 및 관리 서버 정보에 대한 무결성 검증 기능 개발	
105203	GN-24614	WebUI	Hub 사이트의 경우 IPSec의 Advance 설정기능 추가	
105203	GN-24613	WebUI	클라우드 센서 추가시 이미지 선택 항목 개선	
105203	GN-24602	WebUI	노드관리 검색바 스타일 수정	
105203	GN-24599	WebUI	정책 > 객체 > Web Access UI 추가	
105203	GN-24594	WebUI	노드 정책 즉시 적용시 선택된 항목의 상태 초기화 및 나타나는 팝업을 모달창으로 개선	
105203	GN-24572	WebUI	네트워크주소 입력시 설명 입력이 가능하도록 기능 추가	
105203	GN-24562	Windows Agent	에이전트에서 사용되는 웹브라우저 기본값을 "기본 웹브라우저"로 변경	
105203	GN-24548	WebUI	감사 > 로그 > IP 링크에 노드 정보가 tooltip으로 표시되도록 개선	
105203	GN-24545	WebUI	IP 신청 REST API에 센서의 서브넷 파라미터를 추가하여 해당 서브넷의 미사용 IP로 자동할당 될 수 있도록 개선	
105203	GN-24543	WebUI	Flow 로그 목적지 IP 컬럼 값 정렬이 맞지 않는 문제 개선	
105203	GN-24507	Linux Agent	[CC] Linux Agent, 신규 플랫폼 (한컴 구름) 정보 추가	
105203	GN-24501	WebUI	사이트 목록에 URLFilter 설정 여부 컬럼 추가	
105203	GN-24486	WebUI	노드 목록화면에 컬럼 사이즈 조절 옵션 추가	

continues on next page

Table 16 – continued from previous page

Revision	Key	Components	Description	Affects Versions
105203	GN-24471	WebUI	노드목록에서 부서, 직급, 태그에 관련된 항목을 converter로 출력하도록 개선	
105203	GN-24468	Zero Trust Security	Webfilter 객체 및 파일형태별 제어 구현	
105203	GN-24464	macOS Agent	macOS Agent 운영체제 정보수집 플러그인에 설치시각 정보 추가	
105203	GN-24463	Linux Agent	[CC] Linux Agent, TLS 통신시 Cipher Suite 고정되도록 개선	
105203	GN-24451	macOS Agent	macOS 네트워크 공유폴더 플러그인 개발	
105203	GN-24450	Linux Agent	[CC]Linux Agent, 인증코드를 통한 에이전트 삭제 기능 추가	
105203	GN-24433	Linux Agent	Linux Agent, OS 최신 업데이트 체크를 버전이 아닌 업데이트 항목으로 검사하도록 개선	
105203	GN-24373	Zero Trust Security	URL Filter 제어정책 적용	
105203	GN-24333	WebUI	Web Filter의 Rule 객체화	
105203	GN-24328	macOS Agent	macOS PC에 Auto Proxy Configuration 설정 기능 추가	
105203	GN-24156	WebUI	노드 일괄 등록 시 MAC허용 - 변경금지(지정IP) 설정 가능하도록 개선	
105203	GN-24024	WebUI	노드관리 목록과 상세화면의 통합 관리화면 개발	
105203	GN-24008		URL filtering 기능 추가	
105203	GN-22495	Windows Agent	Internet Kill Switch 관련 기능 개발	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
105827	GN-25085	Center	노드생성시 등록일자/업다운상태 노드그룹 조건에 잘못 매칭되는 문제	4.0.0
105671	GN-24936	WebUI	노드그룹 생성 조건에 출력되는 컴포넌트 항목 수정	5.0.31
105637	GN-25060	Center	장기간 다운에 의한 에이전트 정보 삭제 후 에이전트 재설치 및 로그온 이후에도 에이전트 플랫폼 정보가 업데이트 안되는 문제	5.0.0, 4.0.61
105629	GN-25067	Center, Sensor	[범용OS] 디버그로그가 복수개의 파일에 중복으로 쌓이는 문제	5.0.42 (LTS)
105624	GN-25003	Sensor	센서에서 수집된 노드의 DHCP 정보 전송 실패 이후 센터 재구동되는 문제	4.0.114, 5.0.11
105616	GN-25068	macOS Agent	macOS 모양 및 개인설정 액션 사용시 플러그인 종료되는 문제	5.0.15, 6.0.0

continues on next page

Table 17 – continued from previous page

Revision	Key	Components	Description	Affects Versions
105529	GN-25037	WebUI	노드관리 화면에서 현황 및 필터의 노드그룹 메뉴를 통해 목록 확인 후 재검색 시 오류 발생	5.0.38
105514	GN-25050	Enforcer	Enforcer 커널 모듈에서 메모리 할당 실패 문제	5.0.40
105410	GN-24885	WebUI	사용자 정의 버튼에서 이미지 업로드 시 목차 페이지가 넘어가지 않는 문제	5.0.12
105390	GN-24999	Sensor	가상센서 32개까지만 추가되는 문제	5.0.32
105203	GN-24971	Sensor	센서데몬 hang 증상 문제	4.0.117
105203	GN-24905	Center	스위치 ARP 테이블 정보를 이용해서 노드를등록하는 환경에서 에이전트가 Down상태인데 노드는 UP 상태로 변경되는 문제	6.0.4, 5.0.47
105203	GN-24897	macOS Agent	macOS 모양 및 개인설정 액션 관련 데이터베이스 오류 발생하는 문제	5.0.45, 6.0.2
105203	GN-24817	WebUI	하위 부서별 사용자 목록이 출력이 되지 않는 문제	5.0.45, 6.0.4
105203	GN-24802	Windows Agent	V3 백신에 대한 실시간 감시 강제화 제어 옵션이 동작안함.	5.0.0, 6.0.0
105203	GN-24797	Sensor	SNMP 정보수집시 잘못된 데이터형식으로 인한 수집오류	4.1.4
105203	GN-24785	Center	구글 API 클라이언트 ID 변경 이후 G Suite 동기화 설정의 구글 인증 코드 발급 오류	6.0.4
105203	GN-24767	Sensor	NETBIOS 스캔에 의해서 노드의 도메인정보가 업데이트 되지 않는 문제	4.0.M3
105203	GN-24733	Windows Agent	스크립트 수행플러그인에서 수행할 스크립트 내용이 많을 경우 액션정책이 수행안됨.	4.0.16, 5.0.0, 6.0.0
105203	GN-24729	IPMGMT, WebUI	IP사용신청서 Email 승인시 다중신청항목 일괄승인시 오류	4.0.113, 5.0.10
105203	GN-24707	WebUI	관리 > 노드 > 현황및필터 > 액션 > 노드목록 이동 시 결과 출력되지 않는 문제	5.0.33
105203	GN-24701	Windows Agent	외부인증연동 기능 사용시 BASE64 암호화 방식을 사용할 경우 인증연동 미동작 문제	5.0.0, 6.0.0
105203	GN-24665	Backup	외부저장장치를 통해서 백업을 수행하는 경우 로컬디스크에 대한 여유공간확보가 동작 안하는 문제	4.0.19
105203	GN-24652	WebUI	대시보드 에이전트 설치현황의 수행날짜 라벨 출력되지 않는 문제	6.0.0
105203	GN-24649	Center, Windows Agent	제어정책에 권한객체가 다중등록되어있으면 윈도우 방화벽 제어 플러그인에 의한 차단 오동작	5.0.28, 6.0.0
105203	GN-24645	WebUI	현황&필터 태그 화면에서 관리뷰 편집이 반영되지 않는 문제	5.0.9
105203	GN-24637	WebUI	시스템 > 사이트에서 인프라를 Cloud -> On-Premises 로 변경시 오류 발생 문제	6.0.0
105203	GN-24630	WebUI	센터에 등록된 노드의 제어정책 컬럼 툴팁이 잘못 출력되는 문제 수정	5.0.27
105203	GN-24628	macOS Agent	macOS Agent에서 무결성 검사 기능이 정상동작하지 않는 문제	5.0.27, 6.0.0
105203	GN-24626	WebUI	노드상세화면에서 목록 닫기 버튼 클릭시 오류 로그 출력되는 문제	5.0.38

continues on next page

Table 17 – continued from previous page

Revision	Key	Components	Description	Affects Versions
105203	GN-24620	WebUI	노드관리 트리의 노드바구니 클릭 후 필터 및 현황의 메뉴 조회시 노드목록 출력되지 않는 문제	5.0.42 (LTS), 6.0.0
105203	GN-24592	WebUI	시스템 로그수집완료시 생성되는 버튼으로 이동된 페이지에 관련 데이터가 나타나지 않는 문제	5.0.40
105203	GN-24568	Windows Agent	무선랜제어로 허용된AP 가 차단되는 문제	
105203	GN-24560	Windows Agent	에이전트 인증창의 실행옵션에 "%ProgramFiles%" 사용시 "C:Program Files (x86)" 경로의 파일 수행 안됨.	5.0.0, 6.0.0
105203	GN-24554	WebUI	구(舊) 노드그룹 상세화면에서 조건 삭제 시 페이징 출력 옵션이 원복되는 문제 (255 설정시 50으로 변경)	5.0.12
105203	GN-24523	WebUI	사용자 내보내기시 특정 컬럼 누락 현상(엑셀 형식)	4.0.7
105203	GN-24502	WebUI	노드정책 복사 후 정책 수정시 변경안한 옵션의 값이 수정되는 문제	5.0.44
105203	GN-24449	Windows Agent	프로그램제거 플러그인에서 '선택삭제' 버튼 무반응 문제	5.0.42 (LTS), 6.0.0
105203	GN-24192	WebUI	사용자 태그부여 시 사용자 목록에서 태그가 인증된 노드의 개수 만큼 표기되는 증상	4.0.138, 5.0.35
105203	GN-21894	Center	노드타입: 미분류 노드가 IP/MAC 사용시간 만료시 삭제되지 않는 문제	5.0.31
103937	GN-24685	WebUI	차단된 IP 허용옵션을 사용시, 사용예정으로 설정된 차단IP가 할당되는 문제	4.0.12

16.2.20 Genian ZTNA 6.0.3 Release Notes (2022-04-12)

Last Updated: 2022-06-10

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
104957	GN-24908	WebUI	Tomcat version upgrade (8.5.78)		8.6
104926	GN-24917	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1o)		9.8
104654	GN-24851	Center	Apache HTTP Server 2.4.53 업그레이드		9.8

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
104355	GN-24852	WebUI	노드 관리화면의 노드그룹 트리 출력 쿼리 개선	
103851	GN-24546	WebUI	관리콘솔의 IP관리에서 할당대상 IP가 차단된IP할당을 허용할 때 차단된 IP를 할당가능하게 개선	
103851	GN-24493	macOS Agent	macOS 백신정보 수집 플러그인에 ESET Endpoint Security 정보 추가	
103851	GN-24469	Center	센서 DHCP노드 IP갱신 기능을 스위치를 통한 노드등록 시에서 적용할 수 있도록 개선	
103851	GN-24458	Windows Agent	연결할 수 있는 AP가 없으면 무선연결관리자 출력되지 않도록 수정	
103851	GN-24367	WebUI	[CC] 관리콘솔에서 센터/센서 reboot 명령 숨김 처리	
103851	GN-24319	Linux Agent	Linux Agent, 노드 삭제시 재 등록 이벤트 처리 기능 추가	
103851	GN-24316	Windows Agent	DNS제어 플러그인에서 IP주소와 Host를 매칭되는 설정 값을 제거 할 수 있도록 수정.	
103851	GN-24312	syslog	syslog TLS 사용시 TLS 1.0 사용하지 않도록 syslog-ng 설정 수정	
103851	GN-24281	WebUI	노드명령 REST API 개선	
103851	GN-24278	WebUI	상태그룹에서 '노드액션'의 플러그인이 할당되었을 때, 노드 액션에서 플러그인을 변경할 수 있도록 개선	
103851	GN-24272	WebUI	클라우드 보안그룹 정책 화면 개선	
103851	GN-24267	Center	Agentless AD SSO - 3개 이상의 서버 설정 가능하도록 개선	
103851	GN-24263	Center	SMTP 인증시 인증 사용자 ID 를 도메인까지 포함해서 표시 하도록 개선 및 인증 감사로그에 인증소스 추가	
103851	GN-24262	IPMGMT, WebUI	IP 신청서 작성시 승인자를 설정하지 않은 경우 모두전달 옵션에 따라 모든 사용자에게 메일이 전달되는 문제 개선	
103851	GN-24243	WebUI	사이트 관리에서 On-Premises hub의 경우 제한된 IPSec, ZTNA Client 기능 활성화	
103851	GN-24229	WebUI	노드상세 페이지 FlowData 탭 제거	
103851	GN-24212	WebUI	대시보드 ZTNA Client Session 현황, IPsec 터널 현황 BigNumber 위젯에서 사이트를 설정할 수 있도록 개선	
103851	GN-24204	WebUI	NHN CLOUD 지원	
103851	GN-24178	Linux Agent	[CC] Linux Agent Clam antivirus 정보 수집 기능 추가	
103851	GN-24044	Center	백업을 위한 sftp 설정 시 패스워드가 평문으로 저장되는 문제	
103851	GN-24000	WebUI	사이트 관리 화면 - 모니터링 기능 추가	
103851	GN-23766	WebUI	CONF 설정 UX 개선	
103851	GN-23716	WebUI	REST API Event 연동 서비스 (Java용 버전) 개발	
103851	GN-17595	macOS Agent	macOS 에이전트 장치 제어 플러그인 제작	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
105188	GN-24989	Sensor	DHCP 서버포트(UDP/목적지포트 67)로 dhcp 가 아닌 패킷을 센서가 수신하는 경우에 센서데몬 메모리 증가하는 문제	4.0.11
105167	GN-24956	WebUI	사이트 관리의 ZTNA-Client에서 접속하는 Sensor의 NAT IP가 설정되어 있지 않을때 관련UI가 정상동작하지 않는 문제	6.0.0
104926	GN-24941	Windows Agent	특정 PC에서 4.0에서 5.0으로 에이전트 업데이트할 때 다량의 파일복사로 인한 설치 실패	4.1.2, 5.0.0, 6.0.0
104904	GN-24789	Sensor	에이전트설치 단말의 FQDN 정보가 센서 NETBIOS 스캔에 의해서 변경되는 문제	4.0.146
104778	GN-24920	WebUI	정보동기화 조건문에 "%" 입력시 에러페이지뜨는 현상	5.0.42 (LTS), 5.0.45, 6.0.2
104597	GN-24829	WebUI	정상적인 정책 적용 데이터 인데 XSS 발견 감사로그가 남는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
104576	GN-24838	macOS Agent	macOS monterey환경에서 '모니터 정보 수집' 플러그인 사용 시 GnPlugin 프로세스 실행 안됨	5.0.17
104567	GN-24837	macOS Agent	macOS monterey환경에서 '파일배포' 액션동작시 pkg설치파일 실행불가	5.0.45
104270	GN-24696	macOS Agent	macOS Agent 트레이 메뉴의 ZTNA 연결상태가 불특정하게 잘못 표시되는 문제	6.0.0
104208	GN-24819	Windows Agent	불특정하게 액션정책 무결성 체크 실패로 액션정책이 수행안됨.	5.0.0, 6.0.0
104208	GN-24695	Windows Agent	불특정하게 에이전트 트레이 메뉴의 ZTNA 연결상태가 잘못표시되는 문제	6.0.0
104160	GN-24661	WebUI	백신 관련 노드그룹 필수항목값 누락으로 인한 그룹조건 즉시 수정 안되는 오류	5.0.23
104125	GN-24806	Center	RADIUS 이중화 구성에서 Account 패킷 요청 목적지 IP 와 응답 출발지 IP가 다른 문제	6.0.3, 5.0.46, 4.0.149
104017	GN-24673	VRRPD	[범용OS] HA 환경에서 M->S 전환시 인터페이스 MAC주소가 변경되는 문제	5.0.42 (LTS), 6.0.0
103976	GN-24430	Center	IP관리 메시지 우선: On 설정 시 노드정책에 설정된 CWP 디자인 템플릿이 적용되지 않는 문제	5.0.14
103851	GN-24668	Center	수동등록된 스위치를 통해서 등록된 노드의 UP/DOWN 상태가 센서와 동기화 안되는 문제	5.0.36
103851	GN-24660	Center	노드의 플랫폼정보가 Microsoft Windows 에서 Unknown Platform 으로 변경되는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
103851	GN-24631	WebUI	IP신규신청 일괄승인시 미할당IP가 있음에도 할당IP가 없다고 나타나는 문제	6.0.3, 5.0.46
103851	GN-24577	macOS Agent	macOS 액션조건이 불만족인데도 주기가 항상수행인 일부 플러그인이 동작하는 문제	5.0.0, 6.0.0
103851	GN-24563	Windows Agent	액션조건이 불만족인데도 주기가 항상수행인 일부 플러그인이 동작하는 문제	5.0.0, 6.0.0

continues on next page

Table 18 – continued from previous page

Revision	Key	Components	Description	Affects Versions
103851	GN-24496	Center	노드정보 호스트명(NL_FQDN)이 센서 노드정보검사 후 변경되는 문제	4.0.25
103851	GN-24434	WebUI	노드 상세화면에서 노드타입을 지정 체크박스를 선택했지만 해당 내용이 저장되지 않는 문제	5.0.44, 6.0.1
103851	GN-24424	WebUI	노드그룹 상세화면의 대상노드리스트 탭에서 노드 상세화면으로 이동 후 돌아가기 버튼의 오동작 문제	5.0.31
103851	GN-24418	Windows Agent	인증창 종료금지상태에서 외부 프로그램에 의하여 종료될 수 있는 문제	4.1.0, 5.0.0, 6.0.0
103851	GN-24410	CWP	CWP 템플릿 사용시 IP관리메세지 우선 설정 이후 사용자 인증 컴포넌트 사용하면 정상 동작 안하는 오류	4.0.143, 5.0.40
103851	GN-24407	IPMGMT, WebUI	IP 신규신청 일괄 승인 시 할당 가능한 IP 주소가 부족함에도 동일 IP 주소로 일괄 승인되는 문제	4.1.4
103851	GN-24406	IPMGMT, WebUI	REST API 를 통한 IP 신규 신청 시 자동승인 미동작	5.0.8
103851	GN-24360	Windows Agent	에이전트 설치 노드가 에이전트 센서 설치후에도 센터 관리 대역에 계속 존재하는 문제	5.0.40, 6.0.0
103851	GN-24338	Windows Agent	Windows 보안설정 액션에 대한 반복적인 디버그로그 남는 문제 수정	4.0.109, 5.0.6, 6.0.0
103851	GN-24329	Windows Agent	알림메시지 및 공지사항 표시할 때 태그 표시 오류	5.0.42 (LTS), 6.0.0
103851	GN-24327	WebUI	대시보드 위젯 감사로그 필터 추가 시 오류 페이지 발생	4.0.13
103851	GN-24318	Docker	DKNS설치시 호스트머신의 네트워크 인터페이스가 사라지는 문제	6.0.1
103851	GN-24314	WebUI	대상노드작업의 접속인증페이지(CWP) 조회 시 내 정보 IP 표기 오류	5.0.40
103851	GN-24307	Center, Sensor	IP 로만 구성된 노드그룹의 IP들이 변경 될때 노드롤이 센서로 전달되지 않는 증상 발생	5.0.11, 6.0.0
103851	GN-24303	WebUI	노드그룹 IP/MAC 정보 CSV 일괄 설정시 항목에 조건항목이 출력되는 오류	5.0.43, 6.0.0
103851	GN-24301	Center	SFTP 백업시 LOG는 SFTP 전송이 되지 않는 문제	5.0.45, 6.0.2
103851	GN-24300	Windows Agent	에이전트 인증창에서 " 인증 후 실행" 옵션 동작 안하는 문제	5.0.0, 6.0.0
103851	GN-24290	GenianOS	NAC 점검 스크립트(sysinspect) 'Check Setup Config' 수행시 Warning 발생	4.0.120, 5.0.17
103851	GN-24245	Windows Agent	정책서버와 통신되지 않는 상황에서 내부네트워크로 표시되는 문제	5.0.43, 6.0.0
103851	GN-24244	Center	이중화 설정되어있는 장비에서 백업시 오류 메시지가 화면에 표시되는 문제	4.0.119, 5.0.16
103851	GN-24241	Center	동일 대역에 여러대의 센서가 존재하는 경우 노드타입과 플랫폼이 일반 노드로 등록되는 문제	6.0.0
103851	GN-24200	WebUI	센서 서브넷 23비트로 설정 후 IP신청서에서 할당 시 2번째 대역 목록 표시가 안되는 문제	5.0.13
103851	GN-24187	Windows Agent	무선연결관리자의 '유선 사용시 숨김'옵션이 동작하지 않는 문제	5.0.0
103851	GN-24181	macOS Agent	macOS Agent '에이전트 삭제방식' 적용되지 않는 문제	5.0.41, 6.0.0

continues on next page

Table 18 – continued from previous page

Revision	Key	Components	Description	Affects Versions
103851	GN-23710	macOS Agent	macOS 에이전트 인증창에서 인증 제한 기능을 사용할 경우 인증 해제 되지 않는 이슈	5.0.17, 6.0.1
103851	GN-23285	Windows Agent	윈도우쉘이 explorer가 아닐 경우 에이전트가 동작하지 않는 문제	4.0.0, 5.0.0, 6.0.0
103851	GN-22689	WebUI	CLI(conf terminal)에서 hostname 변경시 시스템관리 > 시스템 목록에 장비명(System Name)이 변경되지 않는 문제	5.0.33

16.2.21 Genian ZTNA 6.0.2 Release Notes (2022-02-09)

Last Updated: 2022-04-12

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
103842	GN-24689	WebUI	감사 > 로그 > 로그검색에서 XSS가 가능한 문제		4.3
103670	GN-24651	Center, macOS Agent, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1n)	4.0.0, 5.0.0, 6.0.0	7.5
103638	GN-24687	WebUI	디버그로그 화면에서 상대경로로 파일 접근 가능한 문제		3.83
102685	GN-24535	WebUI	logstash 제거		5.9

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
103413	GN-24648	WebUI	노드목록에서 IP소유자 컬럼이 있을 경우 검색 결과가 느려지는 문제 개선	
103066	GN-24302	Center	Webhook 인증 연동 암호화방식 MD5(MD5B64) 가능하도록 매크로 추가 및 응답메세지 캡쳐기능 제공	
103058	GN-24257	Center	LDAP 인증연동 시 서버 연결 타임아웃 설정 가능하도록 개선	
103053	GN-24198	WebUI	네트워크 객체의 네트워크주소에 특정 도메인이 등록되지 않는 문제	
102920	GN-24557	Center, RADIUSD	RADIUS 인증시 노드등록 기능을 옵션설정 기능으로 제공	
102892	GN-24151	WebUI	IP신청시스템 용도별 사용 가능 센서 설정 및 조회 API 추가	
102436	GN-24246	macOS Agent	macOS ZTNA 연결 관리자 2차 인증 관련 기능구현	6.0.2

continues on next page

Table 19 – continued from previous page

Revision	Key	Components	Description	Affects Versions
102436	GN-24172	WebUI	Bad Request(400) 발생 시 톰캣 버전 정보 출력하지 않도록 수정	
102436	GN-24165	WebUI	인스턴스메시지 내용 입력시 html 태그를 변환하지 않도록 수정	
102436	GN-24130	macOS Agent	macOS ZTNA 연결 관리자에 다중 VPN 접속을 위한 구조 개선	6.0.2
102436	GN-24082	WebUI	/nodes/{nodeId}/tags API를 통해 노드 태그 외 다른 태그도 추가로 조회할 수 있도록 개선	
102436	GN-24077	WebUI	mysql 인증 플러그인을 sha256_password로 변경해도 웹 접속 가능하도록 수정	
102436	GN-24068	WebUI	신규 대시보드 차트 위젯 툴팁에 표시되는 날짜형식 지정 가능하도록 개선	
102436	GN-24059	WebUI	IP신청시 역순 할당 기능 추가	
102436	GN-24045	DKNS	ZTNA Client설정시 DHCP Pool 설정가능하도록 개선	
102436	GN-24029	Center	에이전트인증 및 RADIUS 인증시 Google OTP 2차 인증 및 웹훅을 통한 인증코드 전송기능	
102436	GN-24020	WebUI	Applications REST API 에 추가된 기능에 대한 파라미터 추가	
102436	GN-24010	WebUI	센서명 변경시 해당 센서에 속한 노드들의 센서명이 즉시 변경되도록 수정	
102436	GN-23980	Center	쿼리리포트 메일 전송 시 다중 메일 계정으로 메일이 전송되도록 개선	
102436	GN-23964	WebUI, Windows Agent	노드정보-인터페이스 정보에서 연결방식에 가상타입 표시	
102436	GN-23953	WebUI	Self-Sign 인증서 재생성 및 외부에서 생성된 SSL 인증서 등록기능	
102436	GN-23943	Center	영문 감사로그 생성시 한글이 표기되는 부분 개선	
102436	GN-23930	WebUI	Custom 암호화 알고리즘 방식 지원	
102436	GN-23918	WebUI	하나의 노드정책에 동일한 단독플러그인액션이 둘 이상 들어갈 수 있는 문제	
102436	GN-23896	WebUI	노드 상세화면의 목록쿼리 조회시 JOIN 쿼리 제거 등의 성능 개선	
102436	GN-23895	Authsync	Oracle Database 19c까지 연동 가능하도록 개선	
102436	GN-23880	Linux Agent	Linux Agent, OS 로그인 사용자 변경 또는 로그아웃 & 재로그인시 에이전트 비정상 동작하는 문제	
102436	GN-23869	Windows Agent	5.0 버전 "http URL 인증" 커스텀 플러그인 추가	
102436	GN-23865	Windows Agent	5.0 버전 호스트명 인증 커스텀 플러그인 추가	
102436	GN-23861	WebUI	Cloud Sensor 등록기능 개선	
102436	GN-23852	WebUI	CWP에서 Google OTP 2차 인증 가능하도록 개선	

continues on next page

Table 19 – continued from previous page

Revision	Key	Components	Description	Affects Versions
102436	GN-23833	WebUI	Security Group 상세화면에 템플릿 수정 기능 추가	
102436	GN-23831	WebUI	flow 로그 위젯에 기간 설정이 서브타이틀 출력되도록 수정	
102436	GN-23825	Linux Agent	Linux Agent, 센터 접속이 안될 경우 이전 정책으로 액션이 동작하도록 기능 추가	
102436	GN-23817	IPMGMT, WebUI	IP신청시스템 Email 단계별 승인 방식 개선	
102436	GN-23802	WebUI	소프트웨어 업데이트 안내 방식 개선 - 패치 및 업그레이드 분리 제공	
102436	GN-23752	Linux Agent	Linux Agent, 신규 배포판 및 버전 정보 추가	
102436	GN-23749	Linux Agent	Linux Agent, TmaxOS 최신 업데이트 체크 기능 개발	
102436	GN-23731	WebUI	Security Group Terraform tf 파일 다운로드 기능	
102436	GN-23724	WebUI	CONF엔진의 선택 항목에 따른 기본 초기값 반영되는 CONF_OPTIONS 항목 추가	
102436	GN-23722	Linux Agent	Linux Agent, 인터페이스 제어 액션 개발	
102436	GN-23698	WebUI	위젯 스키마에 링크 Target 설정을 위해 관련 내용 추가	
102436	GN-23644	GenianOS	부팅시 일부 파일시스템 검사 누락된것 추가	
102436	GN-23468	Center	Webhook API 호출 결과를 이용해서 다른 Webhook API 호출가능하도록 개선	
102436	GN-23221	Windows Agent	IE보안옵션제어 플러그인에 Chrome,Edge 옵션 제어 추가	
102436	GN-23212	Ubuntu(Debian)	[범용OS] genian-nac 버전 별 설치를 위한 레포지토리 분리 작업	
102436	GN-23210	macOS Agent	macOS ZTNA 연결 관리자 플러그인 추가	
102436	GN-23189	macOS Agent	macOS Agent 모양 및 개인설정 플러그인 - 화면보호기, 바탕화면 제어 추가	
102436	GN-22690	WebUI	감사로그 제한 기능 - 노드 관리 범위 제한이 걸려 있어도 감사로그는 모든 로그가 표시되는 문제	
102436	GN-22074	WebUI	SAML 인증연동을 2개 이상의 IdP(인증 정보 제공자)를 지원 가능하도록 개선	
102436	GN-21279	CLOUD	AWS SES를 통한 Email 전송시 파일첨부 가능하도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
103817	GN-24691	Center	스위치를 통해서 등록된 노드가 센서에 의해서 등록됨 으로 로그가 생성되는 문제	5.0.43, 6.0.0
103760	GN-24683	Sensor	센서데몬이 dhcp scan 시작 후 잘못된 메모리 참조로 비정상 종료되는 문제	4.0.2
103726	GN-24724	Windows Agent	외부에서 내부 네트워크 상태로 전환된 후 에이전트 액션 정책이 늦게 적용되는 문제	5.0.40, 6.0.0
103639	GN-24284	WebUI	IP 신청서 승인화면에서 직접할당시 관리센서를 변경한 후 승인을 할 경우 오류 발생문제	5.0.13
103620	GN-24682	WebUI	IP 용도 용도별 승인방식이 자동승인인 경우 역순으로 IP 할당되지 않는 문제	5.0.44, 6.0.2
103614	GN-24684	WebUI	라이선스 화면에서 계정(genians.com) 로그인시 반응이 없는 문제	5.0.20
103517	GN-24617	WebUI	추가된 노드타입(가상센서, Agent센서)이 노드그룹의 설정리스트와 노드목록의 검색필드 조건 항목에서 누락된 문제	5.0.40
103488	GN-24597	Center	에이전트 버전비교 조건대로 노드그룹이 포함되지 못하는 문제	5.0.16, 6.0.0
103432	GN-24485	macOS Agent	macOS Agent 메모리가 지속적으로 증가하는 문제	4.0.0, 5.0.0, 6.0.1
103404	GN-24644	Center	ARP관리 플러그인 정보 갱신시 간헐적으로 센터데몬이 죽는 문제	5.0.43, 6.0.0, 4.0.146
103399	GN-24658	OpenVPN	9자리 이상의 ID로 ZTNA Client 연결시 인증사용자가 잘못 표시되는 문제	6.0.0
103384	GN-24678	Sensor	SNMP v3 스위치정보 수집시 일부 정보가 누락되는 문제	5.0.44, 6.0.1
103342	GN-23923	Windows Agent	정보수집 플러그인에서 빈정보 수집하여 노드정보가 삭제되는 문제	5.0.0
103247	GN-24619	Center	수동등록스위치의 노드타입이 노드정보스캔에 의해서 네트워크장비로 변경되는 문제	5.0.14
103224	GN-24582	Center	미러센서에서 제어정책 복사 시 권한객체가 동작하지 않는 증상	4.0.116, 5.0.13
103213	GN-24622	Enforcer	노드정보갱신과정에서 잘못된 쓰레기값으로 인해서 Enforcer 커널모듈에서 패닉 발생하는 문제	6.0.1
103093	GN-24586	Windows Agent	소프트웨어정보수집 플러그인으로 일부SW가 수집되지 않고 DB에러 발생	5.0.43, 6.0.0
103048	GN-24603	Center	신규제어정책 추가 또는 제어정책 사용함/안함 변경시 제어정책권한 cache를 업데이트 안하는 문제	4.0.M2
102987	GN-24593	Enforcer	가상센서에 등록된 노드에 대해서 healthcheck 를 수행해서 노드상태가 down으로 변경되는 문제	5.0.32
102950	GN-24358	Center	가상센서가 아닌 일반 노드에도 가상센서와 IP가 동일하면 에이전트센서로 설정되는 문제	5.0.40
102867	GN-24544	Sensor	WOL 패킷이 잘못된 인터페이스로 전송되는 문제	5.0.40
102836	GN-24375		ES 백업(Snapshot) 정리 안되는 문제	5.0.42 (LTS)

continues on next page

Table 20 – continued from previous page

Revision	Key	Components	Description	Affects Versions
102798	GN-24350	WebUI	사용중인 노드액션의 설정 변경 시 설정 UI가 정상적으로 출력되지 않는 문제	5.0.45, 6.0.2
102557	GN-24364	WebUI	IP충돌보호 - 다중 MAC 설정되지 않는 문제	5.0.42 (LTS), 6.0.0
102509	GN-24467	WebUI	노드관리 목록에서 직급컬럼 추가시 목록 출력이 되지 않는 문제	5.0.33
102500	GN-24479	WebUI	라이선스가 초과되지 않았는데 NAC 라이선스초과 문구가 출력 될 수 있는 문제	4.1.M3
102436	GN-24598	Enforcer, Sensor	노드그룹 조건에서 '속하지 않으면' AND '속하지 않으면' 설정 시 earlyrole 비정상 동작 수정	4.0.114, 5.0.11
102436	GN-24415	Authsync	Cloud NAC Oracle 정보동기화 시 라이브러리 경로 오류	5.0.45, 6.0.2
102436	GN-24346	Authsync	[CLOUD] 정보 동기화 수행 완료시까지 오랜 시간이 소요되는 문제	5.0.23
102436	GN-24307	Center, Sensor	IP 로만 구성된 노드그룹의 IP들이 변경 될때 노드롤이 센서로 전달되지 않는 증상 발생	5.0.11, 6.0.0
102436	GN-24273		ZTNA Client 접속시 사용자 인증되지 않는 문제	6.0.1
102436	GN-24268	WebUI	노드 스냅샷 리포트 자동생성 실패하는 문제	6.0.0
102436	GN-24261	Center	HA VIP 노드의 Device Type 이 NODE 로 등록되는 문제	5.0.40
102436	GN-24254	RADIUSD	RADIUS 데몬 STOP시 winbindd 데몬은 STOP 안되고 계속 남아 있는 문제	5.0.35
102436	GN-24194	Center	사용자 패스워드 업데이트시 사용자 그룹 재적용 안되는 문제	5.0.44
102436	GN-24188	WebUI	메일승인대기 항목의 신청서 우선사용승인 처리 후 화면 이동이 없는 문제	5.0.13
102436	GN-24153	WebUI	IP관리 > 매트릭스 뷰에서 정상적으로 출력되지 않는 매트릭스 존재	4.0.12
102436	GN-24147	WebUI	감사로그 설명 컬럼 툴팁의 태그 표시 문제 수정	5.0.22
102436	GN-24139	Windows Agent	저장장치 정보 수집에 Storage 총용량 잘못수집되는 문제	4.1.0, 5.0.0, 6.0.0
102436	GN-24136	WebUI	노드 액션명에 ,(comma) 가 존재하는 경우 노드그룹 설정값에 이미지 경로가 표시되는 문제	5.0.14
102436	GN-24120	WebUI	관리역할 관리화면 > 서비스역할 생성시 오류 발생	5.0.42 (LTS)
102436	GN-24113	WebUI	관리역할 수정시 메뉴제한 설정 disabled 처리 안되는 오류	5.0.0
102436	GN-24110	Windows Agent	Smart NAC 대체 인증 플러그인으로 잘못된 인증값이 연동되는 문제	5.0.41
102436	GN-24092	WebUI	노드그룹 조건 설정 시, 선택항목에 따라 입력항목이 변경되지 않는 문제	5.0.20
102436	GN-24085	WebUI	사용자 관리화면에서 사용자 가져오기 시 패스워드 입력되지 않는 문제	5.0.40
102436	GN-24071	WebUI	CWP 신규 사용자 등록 화면에 본인인증 항목이 출력되지 않는 문제	5.0.42 (LTS), 6.0.0

continues on next page

Table 20 – continued from previous page

Revision	Key	Components	Description	Affects Versions
102436	GN-24011	RADIUSD	RADIUS Attribute 의 갯수가 많은 경우 RADIUS 인증이 실패하는 문제	5.0.24
102436	GN-24005	Center	파일배포 플러그인 https URL 사용시 다운로드하지 못하는 문제	4.0.0, 5.0.0
102436	GN-24002	Linux Agent	Linux Agent, 트레이 아이콘 표시 안되는 문제	5.0.42 (LTS), 6.0.0
102436	GN-23997	WebUI	권한객체의 조건설정에서 객체에 대한 수정 버튼 클릭시 에러 메세지 출력되는 문제	5.0.25
102436	GN-23962	WebUI	권한 객체 ID에 특수문자가 포함된 경우 제어정책에 할당되지 않는 문제	4.0.M8
102436	GN-23952	IPMGMT	http 사용시 IP신청시스템에서 자동로그인 및 로그인이 안되는 문제	5.0.27
102436	GN-23950	Authsync	https를 사용해 csv 정보동기화 시 동기화 되지 않는 문제	4.0.5
102436	GN-23949	CWP	신규 사용자 등록 시 피방문자 이메일 승인을 사용 안함에도 승인 요청 메일이 발송되는 문제	4.0.M8
102436	GN-23925	Sensor	Alias IP 로 추가된 인터페이스에 대한 로컬네트워크패킷이 Default Gateway 로 전달 되는 문제	5.0.42 (LTS)
102436	GN-23917	Sensor	가상IP 수동 추가 시 등록되지 않는 문제	5.0.41, 6.0.0
102436	GN-23891		LDAP 인증연동시 Primary Server 에서 연결실패하는 경우에도 인증시도 하는 문제	5.0.15, 4.0.137
102436	GN-23855	Center	스위치 수동 등록시, 다른 네트워크 대역의 ip로 같은 스위치가 존재하는 경우, 센서 트리 스위치의 정보가 갱신되도록 개선	4.0.117, 5.0.14
102436	GN-23836		IP Mobility 중복노드 등록 발생 방지 방식의 변경	6.0.1
102436	GN-23835	Center	장비 수명주기 관리 추가필드(NI_CUSTOM) 관련 노드그룹 조건을 설정할 수 없는 문제	4.0.129, 5.0.26
102436	GN-23819	WebUI	tomcat webapps 폴더 링크 존재하지 않아 Custom Web Application을 설정 할 수 없는 오류	5.0.40
102436	GN-23760	Enforcer, Sensor	VXLAN 터널링시 발생하는 중복 포이즈닝 문제	6.0.1

16.2.22 Genian ZTNA 6.0.1 Release Notes (2021-12-08)

Last Updated: 2022-02-10

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
101693	GN-24305	GNOS	Apache 취약점 조치를 위한 2.4.52 버전 업그레이드		9.8
101614	GN-24253	WebUI	log4j 취약점 개선		9.8
100944	GN-23714	Center	인증처리가 미비한 에이전트관련 API 보완		4.6
100944	GN-23461	WebUI	[SaaS] Saas 보안인증 소스코드 점검결과 조치		9.1
100944	GN-23446	gnlogin, WebUI	비밀번호에 특정단어를 사용할 수 없도록 처리		8.7

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
99155	GN-23327	Center, Sensor	사이트관리 K8s에서 동작하도록 개선	
104132	GN-23367	Center, RADIUSD	RADIUS 2차 SMS 인증 및 속성(Axgate-Auth-Type) 추가	
102166	GN-24251	WebUI	OTP 인증키 분실 시 재발급 방법 변경	
102130	GN-24279	WebUI	[gndbcp] local.conf에 저장된 DB 패스워드 복호화시 쓰레기 값은 제거하고 복호화 될 수 있도록 수정	
101774	GN-24304	WebUI	IP 신청시스템 승인 신청이 느린 문제 개선	
101542	GN-24315	Documents	5.0.44 Global Release	
101503	GN-24265	macOS Agent	macOS Agent 네트워크 정보에 연결된 무선랜의 BSSID 정보 추가	5.0.0
101486	GN-24149	GnBrowser	GnBrowser에서 노드삭제등 일부 기능 동작 안되는 문제	
101418	GN-24190	Center, MySQL	MYSQL/CENTERD 메모리 사용량감소를 위한 conf 설정 변경 및 jemalloc 메모리 할당자 사용	
100944	GN-24132	macOS Agent	macOS Agent 무선랜제어 플러그인 정보에 프로토콜 정보 추가	
100944	GN-23982	Windows Agent	ZTNA 연결관리자에 OpenVPN 기반 2차인증 기능 추가 (SMS)	
100944	GN-23809	Windows Agent	ZTNA 연결관리자에 로고 이미지 변경 및 도움말 출력 기능 추가	
100944	GN-23791	WebUI	시스템 > 사이트에서 사용중인 Cloud Provider가 Cloud Provider 메뉴에서 삭제가능한 문제 개선	
100944	GN-23771		시스템 재기동 KeepAlive Down 시에도 가능 하도록	
100944	GN-23746	WebUI	[JSF/컴포넌트] 패턴 입력 컴포넌트 추가	

continues on next page

Table 21 – continued from previous page

Revision	Key	Components	Description	Affects Versions
100944	GN-23735		대시보드 위젯설정 팝업창 사이즈 변경	
100944	GN-23723	Sensor	SNMP Switch 정보수집시 Juniper Switch MAC 정보 수집	
100944	GN-23672	-Unknown/None-	[금오공대] 동기화를 위한 오라클 바이너리 개발	
100944	GN-23658	Sensor	MDNS를 통한 호스트명 탐지 개선	
100944	GN-23642		누락된 C30G_R1, C50G_R1 제품 설치 script 추가	
100944	GN-23635	WebUI	관리역할 편집기능 기본제공	
100944	GN-23626		비밀번호 암호화 방식 SHA256 에서 BASE64_DECODE(UNHEX(HASH)) 된 HASH 값 지원	
100944	GN-23622		부팅시 syslog 구동에 오랜시간이 소요되는 문제 해결을 위한 debug 로그 처리 방법 개선	
100944	GN-23618	WebUI	노드관리에서 하드웨어(hardwareinfo) 검색 컬럼에 대한 설명 보강	
100944	GN-23602	gnlogin	DB migration 진행상태를 좀더 알기쉽게 표시	
100944	GN-23583	WebUI	노드관리 목록에서 관리뷰에 사용자정보의 부서명을 추가할 시 부서명 단계가 표시되도록 개선	5.0.41
100944	GN-23570	WebUI	IP 매트릭스뷰에서 다중 선택/해제 가능하도록 기능 추가	
100944	GN-23568	WebUI	관리 > 노드 상세에서 오탐보고시 감사로그에 XSS 탐지 로그가 남는 문제	
100944	GN-23561		VXLAN over IPSEC 구조 동작 지원	
100944	GN-23537	WebUI	Flow log 컬럼 정렬 기능 추가	
100944	GN-23536	WebUI	Flow 로그 기반의 Top 10 traffic source 위젯 추가	
100944	GN-23524	WebUI	패턴 입력 컴포넌트 추가	
100944	GN-23516	Windows Agent	시스템종료 플러그인에서 종료시 응용프로그램 종료 옵션 추가	
100944	GN-23507	WebUI	코드내에 분산되어 있는 Http Header Security 관련 설정을 Tomcat에서 하도록 개선	
100944	GN-23495	WebUI	ZTNA Client 서버 password 생성을 센터에서 하도록 변경에 따른 WebUI 관련 수정	
100944	GN-23490	Center, DKNS	IPSecVPN Connection상태 수집 기능	
100944	GN-23487	Sensor	IPSEC관련 모듈 OnPrem 센서 탑재	
100944	GN-23482	Center, DKNS	ZTNA Client 서버 password 생성을 센터에서 하도록 변경	

continues on next page

Table 21 – continued from previous page

Revision	Key	Components	Description	Affects Versions
100944	GN-23474	Enforcer, ulogd	Flow log 생성시 http header/sni 등 부가정보를 남기도록 한다.	
100944	GN-23459	Enforcer	icmp echo, reply에 대해서 개별 세션이 생기는 문제	
100944	GN-23453	Center, Sensor	ZTNA Client 센서모드가 Bind Interface모드를 따르도록 개선	
100944	GN-23450	WebUI	사이트 관리 IPSEC 설정 개선	
100944	GN-23447	Center, Enforcer, Sensor	권한의 노드그룹 설정 전송 개선	
100944	GN-23424	WebUI	대시보드 UI 개선	
100944	GN-23423	WebUI	정책 > 객체 > 권한 > 네트워크 객체에 상태그룹 할당 기능 추가	
100944	GN-23406	WebUI	사이트 관리 Routing 설정 센서선택 옵션 추가	
100944	GN-23401	Center	Cloud 수집기에 의해 생성된 노드에 대한 플랫폼 탐지기능 (GDPI API)	
100944	GN-23391	GNOS	최신 드라이버 지원을 위한 Kernel 버전 업그레이드 (5.10)	
100944	GN-23366	WebUI	Agentless AD SSO 설정을 LDAP 인증연동에서 분리	
100944	GN-23360	Center	사이트관리 다중센서 동작하도록 개선	
100944	GN-23332	Center, DKNS	ZTNA IPSec 로그파일 정책서버로 전송	
100944	GN-23331	WebUI	신규 대시보드 PDF, DOC 리포트 Export 기능 추가	
100944	GN-23182	WebUI	IPsec Status UI 추가	
100944	GN-23113	WebUI	웹 관리콘솔에 개발자모드 추가	
100944	GN-23075	Center	syslog VPN감사기록 추가 및 필터 매크로 변환시 대/소문자 변환, 노드정보 로그필터 동작 하도록 개선	
100944	GN-22673	WebUI	관리콘솔에서 노드정책에 노드액션 추가시 OS별 탭 카테고리 기능 추가	
100944	GN-22626	Containerization	Cloud NAC 정책서버 이미지에 Terraform 추가	
100944	GN-22606	Sensor	목적지 기반 동적 접근 제어 기능 구현 (Host - Host : VXLAN)	
100944	GN-22594	WebUI	관리 > 노드 > 그룹 트리 및 노드그룹에 속한 노드 목록 쿼리 개선	
100944	GN-20083	WebUI	노드 목록에서 전체 노드를 선택하고 일괄작업 실행시 관련 프로세스 UI 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
102413	GN-24428	WebUI	노드관리 목록에서 관리뷰에 사용자정보의 부서명의 코드가 없을 시에 오류 발생	5.0.44
102311	GN-24400	Windows Agent	전자서명 인증서 변경으로 인한 폐쇠망 환경에서 에이전트 업데이트 문제	5.0.0, 6.0.0
102262	GN-24239	WebUI	노드관리 검색에서 태그명으로 검색 되지 않는 문제	4.0.144, 5.0.41
102104	GN-24365	WebUI	액션 수정시 동일한 멀티 플러그인의 액션이 정책에 할당되어 있을때 수정되지 않는 문제	5.0.43, 6.0.0
102091	GN-24341	Center	네트워크대역에 에이전트센서가 등록되어있는 상태에서 동일한 네트워크대역의 에이전트센서가 재등록 되는 문제	5.0.40
102039	GN-24176	WebUI	노드 상세화면에서 변경된 항목이 화면 갱신이 없으면 반영되지 않아 보이는 문제	5.0.22
102032	GN-24417	WebUI	노드그룹 조건 중 MAC 주소가 소문자이면 노드가 인식되지 않는 문제	5.0.31
101846	GN-24293	WebUI	노드관리 > 작업선택 > 노드그룹 지정/해제 명령 동작하지 않는 문제	5.0.44, 6.0.1
101778	GN-24264		네트워크제어 플러그인에서 '자동 규칙 설정'으로 제어시 이상 동작	5.0.28
101737	GN-23675	Genian Syncer	지니안싱커에서 라이선스 파일등록이 안되는 문제	4.0.144, 5.0.41
101702	GN-24167	Center, Sensor	센서관리대상 노드 정보에 센서인터페이스정보가 비어있어 센서에서 노드를 관리할 수 없는 문제	5.0.36
101528	GN-24310	macOS Agent, Windows Agent	5.0.43이상 버전의 에이전트 업데이트시 에이전트 무한반복 재실행 되는 문제	5.0.43, 6.0.0
101332	GN-24259	WebUI	소프트웨어 업데이트 UI에서 현재버전(revision이100000번 이상일때)보다 낮은 버전이 업그레이드 가능에 표시되는 문제	5.0.20
101278	GN-24260	Center	에이전트지정액션 이벤트 전송시 비정상적인 이벤트프레임이 생성되면서 센터데몬 비정상 종료되는 문제	3.3.1.1009
101263	GN-24202	Center	노드그룹조건이 노드그룹에 속하면(하지않으면) 인데 조건에 해당하는 노드그룹이 사용안함 또는 없는 경우 노드그룹매칭이 비정상 동작하는 문제	5.0.35
101141	GN-24015	procmond, RADIUSD	정책서버 이중화 구성에서 radius 데몬이 지속적으로 재시작 되는 문제	4.0.143, 5.0.40
101018	GN-24078	Center	스위치 동작상태가 DOWN으로 잘못설정되는 문제	5.0.35
101005	GN-24124	WebUI	노드그룹에서 그룹조건으로 OR연산으로 IP관련조건 추가시 정책적용시간이 느려지는 현상	5.0.11
100944	GN-24161	WebUI	라이선스 수량이 초과되지 않았지만 노드관리 화면에서 라이선스 수량이 초과되었다는 메시지가 출력되는 문제	5.0.3
100944	GN-24122	WebUI	노드 관리에서 관리뷰 추가 시 설정한 컬럼의 내용이 출력되지 않는 문제	5.0.42 (LTS)
100944	GN-24118	macOS Agent	macOS Agent 소프트웨어 정보수집 플러그인에서 일부 누락되는 문제	5.0.0

continues on next page

Table 22 – continued from previous page

Revision	Key	Components	Description	Affects Versions
100944	GN-24114	WebUI	사용자 목록에서 태그 출력에 대한 문제 수정	5.0.34, 5.0.39
100944	GN-24075		외부인증 연동시 사용자패스워드에 특수문자(, ', ")를 사용하는 경우 인증실패 발생하는 문제	4.0.145, 5.0.42 (LTS), 6.0.1
100944	GN-24074		에이전트(4.x) 정보 업데이트(updateinfo) 요청이 SQL Injection 구문으로 탐지되어 업데이트 실패하는 문제	4.0.145, 5.0.42 (LTS)
100944	GN-24072	WebUI	Tomcat Context.xml에서 local.conf에 등록된 db 패스워드를 사용하지 못하는 문제	4.0.146, 5.0.44, 6.0.1
100944	GN-24066	Authsync	정상 파일인 경우에도 읽기 실패로 CSV 정보 동기화 실패하는 문제	4.0.146, 5.0.44, 6.0.1
100944	GN-24025	WebUI	작업선택의 노드바구니에 담기 기능이 동작하지 않는 문제	5.0.44, 6.0.1
100944	GN-23948	Sensor	SNMP v3 스위치 SNMP 정보수집이 비정상적인 문제	5.0.41
100944	GN-23845	WebUI	감사로그 > 분석차트로 출력되는 위젯이 로그필터로 필터링 될때 오류 메시지 출력되는 문제	4.0.14
100944	GN-23807	Center	Proxy 환경(운영체제 업데이트 Proxy 서비스설정)에서 WSUS서버 IP 가 PAC 에 포함되지 않아서 업데이트 실패하는 문제	4.0.115, 5.0.12
100944	GN-23804	WebUI	스위치 포트 관리자 Down 시 에러메세지 출력 형식 수정	4.0.106
100944	GN-23788	WebUI	IP사용신청서 결과조회 화면에서 사용위치 정렬시 데이터 검색하지 못하는 문제	4.1.0, 4.0.23
100944	GN-23773	WebUI	디버그로그 화면에서 파일 및 폴더 목록 가져오기 개선	
100944	GN-23761	WebUI	노드정책 생성시 파일배포 액션 할당 불가	5.0.36
100944	GN-23755	WebUI	[4.0.1] 설정 > 환경설정 > 감사기록에서 Syslog 감사기록 필터 추가/삭제가 정상 동작하지 않는 문제	4.0.145
100944	GN-23751	CLOUD	Cloud site 소산백업용 secondary backup이 object storage에 계속 누적해서 백업파일이 생기는 문제	6.0.0
100944	GN-23703		사이트 관리 > IPSEC 네트워크 설정 변경시 센서의 vxlan 재설정이 되지 않는 문제	6.0.1
100944	GN-23691	Authsync	CLOUD 정책서버(NAC6) AUTHSYNC > gndbserver 설정이 dbserver로 설정되어서 정보동기화 실패 하는 문제	6.0.0
100944	GN-23689	WebUI	로그인 시점에 생성되는 대시보드 관련 데이터를 관리자 생성시점에 생성되도록 개선	6.0.0
100944	GN-23664	WebUI	log2migration이 정상동작하지 않는 문제	5.0.41
100944	GN-23656	WebUI	SNMP Switch 일괄설정시 v3 설정이 불가능한 문제	5.0.17
100944	GN-23648		VXLAN 인터페이스 사라짐 문제	6.0.1
100944	GN-23625	WebUI	관리콘솔 관리자 계정 AllowIP 설정에 X.X.X.X/0로 설정시 로그인페이지에서 오류 발생 문제	5.0.41
100944	GN-23621		4.0.112, 5.0.9 이전 버전에서 업그레이드시 SSL 인증서 생성 오류로 httpd 데몬이 구동되지 않는 문제	4.0.112, 5.0.9

continues on next page

Table 22 – continued from previous page

Revision	Key	Components	Description	Affects Versions
100944	GN-23612	WebUI	빠른검색에서 노드목록으로 이동 후 페이징 처리가 되지 않는 문제	5.0.38
100944	GN-23609	WebUI	노드 상태검사 최소 주기 옵션 최소값 수정	5.0.38
100944	GN-23601		grub.conf에 GNTARGET=S_i686 설정된 장비 업그레이드 시 부팅불가 현상	4.0.12
100944	GN-23599	WebUI	노드 상세화면에서 태그 할당 후 화면갱신 하지 않은 상태에서 삭제 시 삭제되지 않는 문제	5.0.22
100944	GN-23590		4.0 업그레이드시 관리콘솔이 구동되지 않는 문제	4.1.M5
100944	GN-23571	WebUI	사용자 정의 버튼 업로드 파일 삭제 후 수정버튼 클릭시 필수입력 값으로 오류출력나지만 파일이 삭제되는 문제	4.0.106
100944	GN-23553	CWP	CWP 사용자 등록 페이지에서 파일 업로드 에러 출력시 html 태그 출력되는 문제	4.0.106
100944	GN-23534	Center	에이전트로 인해 등록되는 노드의 DPI 링크가 표시되지 않는 증상	5.0.39
100944	GN-23528	WebUI	노드의 에이전트액션(파일 배포) 수행시 패스워드 확인에 실패하는 문제	4.0.4
100944	GN-23519	WebUI	소프트웨어 현황의 수량과 노드관리의 노드 수가 일치하지 않는 문제	5.0.38
100944	GN-23440	Windows Agent	백신정보수집 플러그인을 통하여 백신전체 검사시 네트워크드라이브가 포함되는 문제	4.1.0, 5.0.0
100944	GN-23275	WebUI	노드리포트 chart에서 UTC 시간으로 표시되는 문제	5.0.22
100944	GN-23217	Authsync	csv 사용자 정보동기화시 csv read 오류가 발생할 경우 전체 사용자가 삭제될수 있는 문제	4.0.1
100944	GN-23026	IPMGMT	IPMGMT 파일업로드 추가필드 기능 오류	5.0.36

16.2.23 Genian ZTNA 6.0.0 Release Notes (2021-10-06)

Last Updated: 2021-12-06

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
99988	GN-23981	macOS Agent, Windows Agent	에이전트에 UDP 이벤트의 패킷 조작을 통한 비정상 종료 문제		3.4
99968	GN-23966	WebUI	CWP 사용자 신청시 Excel 파일로 신청되는 경우 XSS 공격 가능 취약점		6.8
99964	GN-23965	WebUI	Agent Download 페이지에서 상대경로를 통한 내부 파일 다운로드 취약점	5.0.37	5.2
99926	GN-23967	WebUI	REST API Command Injection		6.7
99901	GN-23970	WebUI	모바일 앱을 이용한 관리자 로그인 우회 취약점		6.1
99890	GN-24014	Center	HTTP로 호출가능한 SOAP/REST 제한		2.5
99806	GN-23972	Center, Sensor	UDP event 패킷처리시 데몬 비정상 종료 가능한 문제	5.0.36	6.4
99620	GN-23700	Center	(KVE-2021-1061) 노드에 인증된 사용자가 아님에도 비밀번호를 변경할 수 있는 취약점		8.7
99365	GN-23794	WebUI	REST API 호출시 유효한 인증 토근이 존재하지 않아도 호출 가능한 문제		4.9
98877	GN-23743	Center	API를 통한 서비스 거부 공격(DoS, Denial of Service) 취약점 개선		6.4
98877	GN-23708	Center	인증처리가 미비한 센서관련 API 보완		4.6
98877	GN-23706	Center	내부적으로 사용되는 SOAP API가 RPC를 통해 외부로 노출된 취약점		
98877	GN-23705	WebUI	(KVE-2021-1062) Conf Engine 에서 파일 업로드 컴포넌트의 이름 유효성 체크 강화		6.7
98877	GN-23702	WebUI	(KVE-2021-1062) CWP Design Template 에서 SSTI 취약점		
98877	GN-23701	Windows Agent	(KVE-2021-1062) Agent 파일 생성시 상대경로를 사용할 수 있는 취약점		6.1
98877	GN-23699	Center, Sensor	(KVE-2021-1061) 센서정보 없이 모든 노드의 정보를 얻을 수 있는 취약점		
98877	GN-23663	macOS Agent, Windows Agent	에이전트 OpenSSL 1.1.1l 업데이트		9.8
98877	GN-23662	GNOS	openssl 버전 1.1.1l 로 업그레이드	4.0.146, 5.0.44, 6.0.1	9.8
98877	GN-23563	Center	Command injection 공격 방어를 위한 수정		8
98877	GN-23533	Center	사용불가 플러그인이 에이전트로 전달되지 않도록 개선		7.6
98877	GN-23500	Center	SQL Injection 방어 처리방법 개선		8.7
98877	GN-23499	GNOS	GNOS 내부 취약한 LD_LIBRARY_PATH 환경변수 제거		
98877	GN-23488	WebUI	[SaaS] SaaS 보안인증 WAS(Tomcat) 취약점 개선		7.5
98877	GN-23377	GNOS	openssh 버전 8.6p1 으로 업그레이드		
98877	GN-23358	WebUI	[CC] Web 취약성 점검결과 보안		6.5
98877	GN-	GenianOS	Apache httpd(2.4.48) / tomcat(8.5.63) 업그레이드		7.5

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
99345	GN-23866		Sophos Anti-Virus 정보 제공 확대	
98877	GN-26823		[2023] GPDB 업데이트 관리 (GitHub)	
98877	GN-23639		노드그룹 목록에서 사용 가능한 OS 이미지가 출력되지 않는 문제 (CLOUD)	
98877	GN-23564	Linux Agent	Linux Agent, 도메인을 통한 센터 접속 및 동작 기능 개발	
98877	GN-23509	WebUI	신규대시보드에서 출력되는 팝업의 버튼 동작될 수 있도록 수정	
98877	GN-23443	Linux Agent	Linux Agent 사용자 인증 기능 추가	
98877	GN-23435	Center, CLI/gnlogin	센서 상태 확인 CLI 명령어 (show sensor) 필터 개선	
98877	GN-23429	WebUI	사이트 생성시 AWS Region, vpcid 설정 drop-down 형식으로 개선	
98877	GN-23370	WebUI	유틸성 js 컴포넌트 추가를 위한 프로젝트 구조 설정	
98877	GN-23369	Windows Agent	에이전트 액션 검사조건의 해쉬값 옵션에 SHA2-256도 체크가능하도록 추가	
98877	GN-23350	Linux Agent	Linux Agent 트레이 메뉴 및 프로그램 정보 화면 표시 기능 개발	
98877	GN-23348	WebUI	정책 > 서비스 객체 생성 및 수정할때 ICMP 프로토콜에 포트 넘버 입력 가능한 문제 개선	
98877	GN-23323	WebUI	노드 > 현황 & 필터 > 위험노드 현황 목록 출력 개선	
98877	GN-23260	Windows Agent	에이전트 윈도우 11 지원	
98877	GN-23243	build	빌드서버 프록시 설정 스크립트 추가	
98877	GN-23227	-Unknown/None-	타 벤더용 DAS(Dynamic Authorization Server) 구현	
98877	GN-23211	Linux Agent	Linux Agent Tray Icon 표시 기능 추가	
98877	GN-23190	macOS Agent	macOS 에이전트의 macOS Monterey 지원	
98877	GN-23185	WebUI	사용자 기본정보에서 비밀번호변경 강제 시 감사로그 추가	
98877	GN-23179	WebUI	AdminPopup 기능을 Top 메뉴에서 동작되도록 기능 수정	
98877	GN-23177	WebUI	CONF 엔진 TYPE_PASSWORD_NO_CONFIRM 항목 show password 기능 추가	
98877	GN-23175	Center	SNMP를 통한 연결방식 감지시 무선이 우선하도록 개선	
98877	GN-23174	WebUI	라이센스 유지보수 만료일 적용 개선 - 최근(큰 값) 날짜 우선	

continues on next page

Table 23 – continued from previous page

Revision	Key	Components	Description	Affects Versions
98877	GN-23131	Windows Agent	인터페이스제어 플러그인에서 반복된 제어 관련한 불필요 로그 제거	
98877	GN-23117	- Unknown/None-	DAS(Dynamic Authorization Server) 구현	
98877	GN-23110	Sensor	에이전트 단말과 센서의 네트워크설정(netmask)이 다른 경우 에이전트에서 keepalive 를 받지 못하는 문제	
98877	GN-23086	WebUI	NAC6 에서 관리자 로그인 시에 기본 대시보드가 존재하지 않는 경우 추가	
98877	GN-23085	WebUI	NAC6 에서 신규 노드그룹이 기본 사용으로 설정 및 실험실에서 해당 항목 제거	
98877	GN-23084	Linux Agent	Linux Agent 액션 수행 조건 검사기능 추가	
98877	GN-23081	Center	Cloud 수집기에 의해 저장된 JSON Data에 대한 노드그룹 조건 추가	
98877	GN-23074	WebUI	노드 상세 > 노드정보 탭의 AWS/VM 정보 조회 UI 개선	
98877	GN-23068	WebUI	위젯 타입에 따라 UI 옵션 설정 출력되도록 개선	
98877	GN-23052	Center	Cloud collector에 의해 수집된 정보에 대한 Macro 치환 기능	
98877	GN-23049	CWP	CWP 신규 사용자 등록 화면에 본인인증 기능 추가	
98877	GN-23038	WebUI	감사로그 타임라인 차트에서 데이터가 없는 구간이 있을 경우 시작점에서 데이터가 있는 구간까지 선이 이어지는 문제 개선	
98877	GN-23023	Center	사이트 설정 저장 구조 변경	
98877	GN-23019	ulogd	ulogd negative filter 지원	
98877	GN-23017	Windows Agent	독립실행형 GPI 에이전트를 NAC 플러그인으로 변환	
98877	GN-23015	macOS Agent, Windows Agent	에이전트 삭제방식 옵션을 글로벌옵션에서 노드 정책으로 변경	
98877	GN-22997	WebUI	노드 관리범위 제한이 센서그룹인 경우 IP주소 관리에서 제한된 센서만 출력되도록 개선	
98877	GN-22978	Center, DKNS	ClientVPN 프로파일 다운로드 가능하도록 수정	
98877	GN-22968	WebUI	IP사용신청서 결과조회 화면에서 신청일자 기간 검색 기능 제공	
98877	GN-22961	Center	RADIUS Attribute를 이용한 장비/노드 정보 업데이트	
98877	GN-22930	WebUI	NAC 6.0 UI 작업을 위한 theme style 작업	
98877	GN-22918	Authsync	사용자가 소속된 멤버쉽이 10개를 초과하는 경우 AD 정보동기화 시 멤버쉽 동기화되지 않는 문제	

continues on next page

Table 23 – continued from previous page

Revision	Key	Components	Description	Affects Versions
98877	GN-22890	Linux Agent	Linux Agent 수행 조건만 검사 액션 추가	
98877	GN-22853	Center	사이트관리에 따른 확장네트워크 구현	
98877	GN-22847	Windows Agent	Nets 업체의 ESSO 시스템과 인증 연동되는 SSO 플러그인 개발	
98877	GN-22837	WebUI	Header 검색바 영역안 CONTROLS (select,input,button) UI 통일성 개선	
98877	GN-22809	WebUI	NAC 관리&설정 페이지에서 input field와 맞지 않는 버튼 수정	
98877	GN-22808	Center	확장 노드타입을 이용한 노드그룹조건 추가	
98877	GN-22798	Center	RADIUS 인증패킷을 이용한 노드등록시 인증이 실패하는 경우에도 노드 등록되는 문제	
98877	GN-22723	WebUI	Flow 로그 조회기능	
98877	GN-22692	WebUI	신규 대시보드 설정 UI 엔진 개발	
98877	GN-22622	WebUI	사이트 관리기능 추가	
98877	GN-22616	Sensor	VTEP센서 노드 처리를 위해 underlay interface를 이용하던 방식 변경	5.0.41
98877	GN-22614	GenianOS	제품에 AWS CLI 탑재 및 제어정책을 통한 명령수행 기능	
98877	GN-22607	WebUI	노드그룹 IP/MAC 주소 같은면 조건의 다중입력 사항을 CSV 파일을 통해 입력되도록 기능 추가	
98877	GN-22595	WebUI	사용자정의 리포트의 노드 리포트(추이리포트) 생성시 수행주기를 주기적 수행만 동작하도록 개선	
98877	GN-22591	WebUI	무선랜 일괄등록 기능 추가	
98877	GN-22550	WebUI	신규 대시보드 UI 엔진 개발	
98877	GN-22542	WebUI	위험노드 현황 기능 추가(내보내기, 검색)	
98877	GN-22536	Windows Agent	에이전트 확장 플러그인 패키지 추가	
98877	GN-22531	Center, Sensor	Cloud 센터와 On-Prem 센서간의 SSL 터널을 통한 정보동기화 및 인증연동	
98877	GN-22526	Sensor	VTEP센서 Group Based Policy 제어 정책 적용	
98877	GN-22384	WebUI	신규 Dashboard 관련 API 설계 및 개발	
98877	GN-22234	WebUI	Event연동 서비스	
98877	GN-22097	WebUI	NAC6 빌드시 lib내의 java를 사용하도록 구조 변경	

continues on next page

Table 23 – continued from previous page

Revision	Key	Components	Description	Affects Versions
98877	GN-21960	WebUI	flowdata UI 모듈 및 노드그룹, 노드 flowdata 출력 화면 추가	
98877	GN-21909	Center, ElasticSearch, WebUI	NAC6 Elasticsearch 7.9.1 upgrade	
98877	GN-21750	WebUI	노드 상세정보 및 flowdata 서비스 추가	
98877	GN-21665	Center	노드그룹간 트래픽정보 가시성제공	
98877	GN-21520	Center	VMware Collector 서비스 개발	
98877	GN-21203	Windows Agent	ESTsoft 알약4.0, 5.0 백신 제품 연동	
98216	GN-23396	WebUI	XSS Filter 적용 개선	
100381	GN-23603	WebUI	대시보드 위젯 페이징기능 추가	
100325	GN-22966	IPMGMT, WebUI	IP신청시스템에서 신규신청시 엑셀파일을 이용할 때 사용종료일이 반영되지 않는 문제	
100143	GN-23858	macOS Agent	에이전트와 정책서버에서 서로다른 표준시간대 사용에 대한 예외처리 (MacAgent)	5.0.0, 6.0.0
100105	GN-23856	Windows Agent	에이전트와 정책서버에서 서로다른 표준시간대 사용에 대한 예외처리	5.0.0, 6.0.0

Issues Fixed

Revision	Key	Components	Description	Affects Versions
99886	GN-23957		KeepAlive 전송시 센터 도메인에 대한IP를 캐쉬하는 문제	5.0.15
99877	GN-23991	Center	에이전트에 의한 노드 등록상태에서 수동스위치에 의한 노드등록시 중복노드 발생	4.0.117, 5.0.14
99578	GN-23890		macOS Agent AD 대체 인증설정 후 OS재부팅시 인증 해제되는 증상	4.0.124, 5.0.21, 6.0.0
99464	GN-23351	Center, Sensor	NODEPOISONSTATUS를 Agent 설치단말에 한하여 전송하도록 개선	3.4.M6
99436	GN-23935	syslog	로그필터 syslog TLS 연동시 SSL 연결에 대한 Timeout 이동작하도록 센터데몬 수정	4.0.137, 5.0.34
99426	GN-23946	Sensor	AD SSO 계정 정보에 특정 특수문자 포함 시 syntax 에러 발생하는 문제	5.0.25
99158	GN-23911	Center	SSDP Multicast 를 통해서 User-Agent정보가 수집된 단말에 대해서 오탐보고가 안되는 문제	5.0.31

continues on next page

Table 24 – continued from previous page

Revision	Key	Components	Description	Affects Versions
98922	GN-23877	WebUI	CWP 디자인템플릿 수정화면의 Components 탭에서 이미지 변경이 되지 않는 문제	CC40, CC50, 4.0.145, 5.0.42 (LTS), 6.0.0
98877	GN-23824	Center	감사기록 보존기한이 지나지 않은 감사기록이 삭제될 수 있는 문제	4.1.3
98877	GN-23816	Center	[NAC6] Elastic Prefix 정보가 센서로 전달안되어 Flow log 남지 않는 문제	6.0.0
98877	GN-23786	Center	가상센서에 다수의 스위치를 등록시 노드가 업다운 되는 오류 개선	5.0.35
98877	GN-23780	WebUI	사용자 관리화면에서 사용자 가져오기 시 USER_PASSCRYPTTYPE 컬럼값이 csv 에 입력한 값으로 저장되지 않는 문제	5.0.41
98877	GN-23739		Microsoft Store 로 설치된 일부 앱이 삭제 후 프로그램제거 플러그인 삭제 리스트에 설치상태로 표시되는 문제 수정	5.0.42 (LTS)
98877	GN-23729	WebUI	사용자 생성시 패스워드 암호화 방식이 HMAC-SHA256 으로만 설정되는 오류	5.0.42 (LTS)
98877	GN-23725	WebUI	사용자 정의 버튼에서 정보수집 버튼 사용시 장비 수명주기 항목 입력 안되는 오류	5.0.11
98877	GN-23707	Center	webhook 인증연동시 x-www-form-urlencoded 방식이 지원되지 않는 문제	5.0.35
98877	GN-23673	Authsync	정보동기화시 $문자를 이용한 치환식이 포함된 컬럼명이 있는경우 정보동기화 실패 문제	5.0.42 (LTS), 6.0.0
98877	GN-23669	Windows Agent	윈도우 64비트에서 NAC 4.X버전을 5.0버전으로 업데이트할 때 정책서버 IP 입력 대화상자 표시 오류	5.0.41, 6.0.0
98877	GN-23641	Sensor	SNMPv3 password가 변경될경우 switch discovery 동작오류 수정	5.0.17
98877	GN-23637		macOS BigSur 화면보호기 정보가 '사용 안함'으로 수집되는 증상	5.0.15, 6.0.0
98877	GN-23630	WebUI	RADIUS 정책 수정에서 연산이 변경되지 않는 문제	5.0.30
98877	GN-23617	Sensor	센서가 센터보다 먼저 업그레이드된 경우 노드 동작 상태가 계속해서 UP/DOWN 반복 변경되는 문제	5.0.38
98877	GN-23616		VPN사용환경하의 macOS Agent에서 TouchBar MacAddress 사용으로 인한 중복노드 발생	4.0.0, 5.0.0, 6.0.1
98877	GN-23606	WebUI	노드정책 노드액션 설정 중 패스워드 입력 후 진행이 되지 않는 문제	5.0.42 (LTS)
98877	GN-23595	Center	netsnmp lib 업그레이드로 인한 정책서버 snmptrap 전송 실패	4.0.145, 5.0.42 (LTS)
98877	GN-23586		사용자정의 버튼의 파일 업로드 시 Slave와 동기화되지 않는 문제	5.0.36
98877	GN-23581	Center	2차 인증 사용시 패스워드변경 강제 동작하지 않는 문제	4.0.145, 5.0.42 (LTS), 6.0.0
98877	GN-23575	WebUI	정책에서 액션할당할때 관리자 인증을 거쳐야 하는 플러그인임에도 인증 다이얼로그가 출력되지 않는 문제	5.0.41
98877	GN-23565	Windows Agent	인테퍼이스 제어 정책을 통해 기본 장치를 제외한 인터페이스 차단시 IP가 변경되면 오동작하는 문제	4.0.0, 5.0.0, 6.0.0

continues on next page

Table 24 – continued from previous page

Revision	Key	Components	Description	Affects Versions
98877	GN-23562	Database	제품 업그레이드 이후 백업시 오류메시지가 발생하는 문제	5.0.41
98877	GN-23560	WebUI	시스템관리 > 정책서버 플러그인 업로드 오류	6.0.0
98877	GN-23551		신규 대시보드 위젯 추가시 위젯의 설정이 추가되지 않는 문제	6.0.0
98877	GN-23529	Sensor	soap 통신 실패 후 recovery 동작시 누락된 정보를 가져오도록 개선	4.0.123, 5.0.20
98877	GN-23498		사용자정보 동기화 수행시 MySQL 오류 발생되면 무한루프에 빠지는 문제	3.3.3
98877	GN-23489	WebUI	플랫폼 명에 '(apostrophe)가 포함된 경우 링크 이동하지 않는 문제(노드 플랫폼 위젯)	5.0.20
98877	GN-23460	Windows Agent	인터페이스제어 플러그인을 통하여 인터넷 연결 공유가 해제되지 않는 문제	4.1.0, 5.0.0
98877	GN-23456	WebUI	디자인 템플릿 > 이미지 업로드에서 업로드/삭제 버튼 사라짐 문제	6.0.0
98877	GN-23455	Center	logrotate 미동작으로 로그들이 정리되지 않는 문제	5.0.41
98877	GN-23442	WebUI	IP 매트릭스뷰에서 센서가 출력되지 않는 문제	5.0.40
98877	GN-23438	Windows Agent	GnPlugin.exe 메모리 누수현상 발생	4.1.0, 5.0.0
98877	GN-23432	Center	윈도우에이전트설치단말의 PLID가 잘못 설정되는 문제	5.0.39
98877	GN-23426	WebUI	라이선스 정보의 장비수와 클릭시 보여지는 노드목록의 노드수가 일치하지 않는 문제	5.0.26
98877	GN-23419	Sensor	AXGATE 센서에서 네트워크 객체 변경시 갱신되지 않는 문제	5.0.40
98877	GN-23411	WebUI	노드리스트 엑셀 다운로드시 노드 관점으로만 출력되는 문제	5.0.38
98877	GN-23408	Center	사용자ID 에 ' 문자가 들어가 있는 경우 db 쿼리 에러 발생하는 문제	5.0.18
98877	GN-23405	GenianOS	장비 부팅에 오랜 시간이 소요되는 문제	4.0.144, 5.0.41
98877	GN-23404	Center	센서의 관리대상 IP에 속하지 않는 노드 삭제시 노드그룹에서 삭제되지 않는 문제	3.5.0
98877	GN-23397	WebUI	노드관리 화면에 IP 매트릭스 뷰 전환 버튼이 사라지는 문제	5.0.38
98877	GN-23395	Windows Agent	GnPlugin 미동작시 반복 재실행되도록 수정	4.0.0, 5.0.0
98877	GN-23340	Center	ldap 인증연동/정보동기화 실패하는 문제	5.0.42 (LTS)
98877	GN-23328	Sensor	ARP Bomb 위험감지 설정의 임계치를 초과하지 않아도 위험노드로 감지되는 문제	4.0.106
98877	GN-23310	WebUI	전체현황 위젯의 전체 에이전트 수와 노드 검색에서의 수와 일치하지 않는 문제	5.0.22
98877	GN-23306	Sensor	에이전트가 있음에도 센서가 수집한 domain 명으로 노드 정보가 업데이트 되는 문제	4.0.0

continues on next page

Table 24 – continued from previous page

Revision	Key	Components	Description	Affects Versions
98877	GN-23299	Windows Agent	에이전트 수행계정이 로컬시스템계정에서 PC로그인계정으로 변경되지 않는 문제	5.0.38
98877	GN-23298	Center	cloud 환경에서 시스콜렉트 동작 오류 문제	5.0.33
98877	GN-23294	Windows Agent	잘못된 보안센터 정보로 인하여 삭제된 백신정보가 보고되는 문제	5.0.0
98877	GN-23292	Center	무선랜 AP 가 삭제 되어도 노드의 접속 AP 정보는 계속 남아있는 문제	4.0.0
98877	GN-23287	macOS Agent	macOS Agent 도메인명 설치파일로 Agent설치시 센터의 Agent 동작상태 갱신되지 않는 문제	5.0.36, 6.0.0
98877	GN-23283	WebUI	노드정책에서 액션 라벨 할당할때 오류 발생하는 문제	5.0.30
98877	GN-23272	Database	SSDEV 를 사용하는 장비에서 mysql 심볼릭 링크 잘못 생성되는 문제	5.0.41
98877	GN-23266	WebUI	쿼리리포트 생성 및 수정이 되지 않는 문제	5.0.41
98877	GN-23220	Authsync	CSV 사용자, 부서, 직급 동기화를 하나의 설정으로 사용하는 경우 동기화가 실패하는 문제	4.0.0
98877	GN-23215	WebUI	누락된 리소스 번들 내용 추가	5.0.30, 5.0.41
98877	GN-23214	WebUI	노드목록 화면과 노드상세 화면에서의 [메모리 전체]가 상이하게 출력되는 문제	5.0.22
98877	GN-23192	CLI/gnlogin	센서 장비의 CLI 접속 시 라이센스 관련 불필요한 디버그 출력되는 문제	5.0.41
98877	GN-23187	Database	SNMP Version 2 (snmpv2) 스위치의 정보가 수집되지 않는 문제	5.0.17
98877	GN-23172	WebUI	IP신규신청 시 /24 Prefix 보다 작은 네트워크센서의 유동 IP 할당 문제	4.1.M3
98877	GN-23160	Center	프로파일 수신 후 6.x 에이전트가 동작하지 않는 문제(에이전트의 사용안함 정책)	6.0.0
98877	GN-23157	Windows Agent	플러그인으로 수집된 백신정보의 이름이 공백으로 출력되는 문제.	5.0.17
98877	GN-23152	WebUI	리포트 > 이메일발송의 default 제공 일일리포트 메일 폼 수정	5.0.32
98877	GN-23142	Enforcer	CWP Redirection이 아닌 패킷 차단에 대한 제한감사기록 동작하지 않는 문제	5.0.40
98877	GN-23141	macOS Agent	macOS 파일배포 시 지정경로에 파일이 저장되지 않는 문제	5.0.0
98877	GN-23128	Authsync	정보 동기화를 통한 노드 정보 갱신 시 감사로그의 노드 IP가 역순으로 표시되는 문제	5.0.1, 4.0.108
98877	GN-23127	WebUI	노드 조건검색에서 AgentActionName 검색시 할당되지 않은 노드가 검색되는 문제	5.0.26
98877	GN-23120	WebUI	노드 조건검색에서 [같지 않으면/일부가 같지 않으면] 검색 결과 문제	5.0.38
98877	GN-23119	Authsync	정보 동기화 오류 발생 시 WebUI의 최근 동기화 상태정보가 업데이트되지 않는 문제	5.0.17
98877	GN-23108	macOS Agent	macOS Agent에서 MacAddress가 없는 인터페이스 정보를 서버로 전송하는 문제	4.0.0, 5.0.0

continues on next page

Table 24 – continued from previous page

Revision	Key	Components	Description	Affects Versions
98877	GN-23100	WebUI	일일리포트 로그필터 항목들의 오늘 Count가 0으로 나오는 증상	5.0.36
98877	GN-23088	Authsync	mysql 정보동기화시 한글이 깨지는 문제	5.0.36
98877	GN-23083	WebUI	신규 노드그룹 설정 페이지 오류 수정 및 개선사항 반영	5.0.37
98877	GN-23007	Sensor	센서 DHCP 사용시 WINS 서버를 여러개 설정하면 DHCP 패킷이 정상적으로 만들어지지 않는 문제	4.0.0, 5.0.0
98877	GN-22996	WebUI	센서 트리에서 센서 그룹 대상 내보내기 시 전체 노드로 내보내기 되는 문제	5.0.38
98877	GN-22969	WebUI	IP신청서 추가필드명 변경사항이 IP사용신청서 결과조회 화면의 조건검색에 반영 안되는 문제	4.0.M9
98877	GN-22861	WebUI	노드관리 검색의 NIC Vendor가 정상적으로 검색되지 않는 문제	5.0.38
98877	GN-22855	WebUI	MAC 주소 형태의 검색 시 빠른검색과 노드검색시 결과가 상이한 문제	5.0.38
98877	GN-22821	WebUI	'노드 타입' 위젯에서 에이전트 센서, 가상센서 노드타입이 미표시되는 문제	5.0.40
98877	GN-22755	WebUI	시스템관리의 장비유형 검색시 페이지 오류 발생	5.0.36
98877	GN-22720	WebUI	노드상세 화면에서 정책 변경시 수정 버튼이 출력되지 않는 현상(특정 케이스 한 함)	4.1.3
98877	GN-22715	WebUI	감사 > 로그 > 디버그로그 화면에서의 기능오류	5.0.40
101199	GN-23938		Scheduler 타입이 한번 실행(ONCE_AFTER) 인 경우 Scheduler 비정상 동작문제	5.0.42 (LTS)
100868	GN-24133	Center	OR 조건으로 노드그룹 업데이트시 노드그룹이 변경되지 않는 문제	5.0.11
100855	GN-24166	WebUI	적용범위가 포함된 노드액션에서 적용범위를 전체로 수정시 오류 메세지 발생	5.0.43, 6.0.0
100824	GN-24162		잘못된 인터페이스의 MAC 주소를 가지고 서브넷스캔 수행하는 문제	3.4.M2
100468	GN-24129	Center	노드 관리범위 제한설정시 로그필터에의한 감사기록 전송 안되는 문제	5.0.36
100440	GN-24101	Sensor	네트워크객체 및 권한객체 생성시 커널에서 네트워크 객체 참조 오류	3.5.0, 4.0.0, 5.0.0, 6.0.0
100395	GN-24089	Windows Agent	Keep Alive 소캣 생성에 실패할 경우 에이전트 재시작 전까지 노드 DOWN으로 유지되는 문제	4.0.142, 5.0.39
100384	GN-24069	WebUI	위젯 타이틀 수정 후 새로고침 시 기본 타이틀이 표시되는 문제 외 1	6.0.0
100378	GN-24040	WebUI	대시보드 화면에서 정책적용 오류	6.0.0
100358	GN-24070	WebUI	에이전트 트레이 메뉴를 통한 사용자 인증 페이지 호출시 오류 메시지 출력되는 문제	5.0.14
100334	GN-23942	WebUI	센서관리 > IP설정에서 팝업창 mask 가려지는 현상 및 누락된 팝업창 ui 통일	6.0.0
100283	GN-23928	WebUI	소프트웨어 수동업로드 시 progressBar 미출력	6.0.0

continues on next page

Table 24 – continued from previous page

Revision	Key	Components	Description	Affects Versions
100273	GN-23914		사용자ID정규식 적용시 센터데몬 비정상 종료되는 문제	5.0.41

16.3 Security Advisories

16.3.1 Genian ZTNA Security Advisories

Last Updated: 2024-04-01

Security Vulnerability

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
6.0.9	GN-25753	WebUI	CWP 에서 PAGEFW 파라미터를 통한 불법 경로로 리다이렉트 하지 않도록 개선		4.2
6.0.9	GN-25746	Center, Sensor	시큐어코딩 점검결과 취약점 패치		
6.0.9	GN-25438	Center, Sensor	_filelist.html 파일을 센터마다 다르게 생성하도록 개선		3
6.0.8	GN-25561	WebUI	노드검색바 Blind SQL Injection 취약점		5.3
6.0.8	GN-25184	Sensor	DNS Cache Poisoning 공격방어를 위해서 Dnsmasq 에서 쿼리 결과를 캐쉬하지 않도록 수정		3.7
6.0.8	GN-23677	Center, Sensor	센서 정책서버 등록시 보안성 강화를 위한 관리자 승인 시스템		7.9
6.0.7	GN-25387	Database, WebUI	정책 > 클라우드 보안그룹 정책에 대한 관리역할 미적용 문제		3.5
6.0.7	GN-25309	Center, Sensor	CSAP(SaaS) 보안인증 심사 소스코드 취약점 조치 - C/C++		7.5
6.0.7	GN-25250	WebUI	HTML Tag 문자열 뒤에 /를 붙이는 경우 XSS가 가능한 문제		4.9
6.0.7	GN-25239	WebUI	Tomcat version upgrade (8.5.78 -> 9.0.65)		7.5
6.0.7	GN-25237	WebUI	CSAP(SaaS) 보안인증 심사 소스코드 취약점 조치		0
6.0.7	GN-25193	WebUI	[범용OS Ubuntu] 관리콘솔 > CWP Design Template 목록 페이지 'X-Frame-Options' Header 가 allowall로 표시되는 문제		6.5
6.0.7	GN-25119	macOS Agent	macOS Agent, OpenVPN(2.5.7) 및 OpenSSL(1.1.1q) 최신 버전으로 업그레이드		5.3
6.0.6	GN-25306	WebUI	사용하지 않는 HTTP-Method를 통해 사용가능 method 정보가 출력되는 문제		5.3

continues on next page

Table 25 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
6.0.6	GN-25110	Linux Agent	Linux Agent, OpenVPN(2.5.7) 및 OpenSSL(1.1.1q) 최신 버전으로 업그레이드		5.3
6.0.5	GN-25104	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1q)		5.3
6.0.5	GN-24782	WebUI	취약점 점검에 따른 라이브러리 업그레이드		9.8
6.0.4	GN-25064	WebUI	웹서비스 취약점 Apache WAS 정보를 노출하지 않도록 개선	4.0.119, 5.0.16	2.5
6.0.4	GN-24583	WebUI	WebUI에서 사용하는 java lib 중 취약점이 발견된 lib 업그레이드		9.8
6.0.4	GN-23947	Windows Agent	윈도우 에이전트 시큐어코딩 점검결과 취약점 패치	5.0.0, 6.0.0	
6.0.3	GN-24917	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1o)		9.8
6.0.3	GN-24908	WebUI	Tomcat version upgrade (8.5.78)		8.6
6.0.3	GN-24851	Center	Apache HTTP Server 2.4.53 업그레이드		9.8
6.0.22	GN-26723	WebUI	관리자의 권한 변경시 즉시 반영 안되는 취약점 수정		3.3
6.0.21, 6.0.16 (LTS)	GN-28063	WebUI	노드관리 검색바에 Blind Injection 가능한 문제		2.2
6.0.20, 6.0.16 (LTS)	GN-27107	WebUI	권한 없는 관리자로 인한 Tomcat 재구동 명령 수행으로 서비스 무력화	5.0.41	2.7
6.0.2	GN-24689	WebUI	감사 > 로그 > 로그검색에서 XSS가 가능한 문제		4.3
6.0.2	GN-24687	WebUI	디버그로그 화면에서 상대경로로 파일 접근 가능한 문제		3.83
6.0.2	GN-24651	Center, macOS Agent, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1n)	4.0.0, 5.0.0, 6.0.0	7.5
6.0.2	GN-24535	WebUI	logstash 제거		5.9
6.0.18, 6.0.16 (LTS)	GN-26393	WebUI	접근 권한 없는 페이지에 직접 URL을 입력하여 정보 수정이 가능한 취약점		3.1

continues on next page

Table 25 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
6.0.18, 6.0.16 (LTS)	GN-26390	WebUI	감사로그 REST API를 통한 권한 없는 관리자의 파일 내보내기 권한 우회 취약점		3.1
6.0.17, 6.0.16 (LTS)	GN-27492	WebUI	Tomcat Version Upgrade (8.5.94 -> 8.5.96 / 9.0.81 -> 9.0.83)		7.5
6.0.17, 6.0.16 (LTS)	GN-27278	WebUI	Tomcat Version Upgrade (8.5.94 / 9.0.81)		7.5
6.0.17, 6.0.16 (LTS)	GN-26315	WebUI	2단계 인증에서 인증코드 입력값 횟수제한, 시간제한하도록 개선		4.3
6.0.17	GN-26600	WebUI	비정상 api 호출 후 로그인 되지 않는 문제	5.0.42, 5.0.49, 6.0.7, 4.0.156, 5.0.56 (50 LTS)	5.3
6.0.16 (LTS)	GN-27014	WebUI	권한이 없는 상태에서 Passkey 재등록 기능을 이용해서 Passkey를 등록할 수 있는 문제		3.9
6.0.16 (LTS)	GN-26935	WebUI	부서명으로 출력된 html tag가 tree에서 실행되는 취약점	5.0.0	1.2
6.0.16 (LTS)	GN-26835	Center	데이터 업데이트에 사용되는 SQL을 통한 Command Injection 취약점		6.6
6.0.16 (LTS)	GN-26833	Sensor	센서의 NMDB 업데이트 과정에서 nmap 스크립트 변조 취약점		4.1
6.0.16 (LTS)	GN-26696	Sensor	센서의 수신 이벤트에 대한 검증 미흡		6.3
6.0.16 (LTS)	GN-26694	Center	다운로드 URL 검증 미흡으로 인한 Parameter Injection 취약점		6.6
6.0.16 (LTS)	GN-26383	WebUI	html/script 코드 주입 가능한 취약점		5.3
6.0.15	GN-26814	Center	Bufferoverflow 에 대한 코드 개선		2
6.0.15	GN-26725	Linux Agent, macOS Agent, Windows Agent	[Agent] 센터 및 센서에서 전송된 이벤트에 대한 유효성 검사 추가		6.3
6.0.15	GN-26392	WebUI	권한 없는 관리자가 디버그 로그 다운로드 가능한 취약점		2.9
6.0.15	GN-26368	WebUI	관리자의 API 키가 다른 관리자에게 노출되는 취약점		5.3
6.0.15	GN-26222	WebUI	관리콘솔 내 페이지 이동시 사용하는 returnUrl 파라미터를 변조하여 리다이렉트 할 수 있는 문제		1.9
6.0.14	GN-26460	Windows Agent	에이전트를 통해 일반 사용자가 PC 관리자 권한을 획득할 수 있는 취약점	5.0.0, 6.0.0	4.6

continues on next page

Table 25 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
6.0.14	GN-26391	WebUI	권한 없는 관리자가 디버그로그 실시간 보기 가능한 취약점	5.0.0, 6.0.0	2.9
6.0.13	GN-26286	WebUI	Google OTP 2단계 인증에서 보안키를 신규로 발급받아 2단계 인증을 통과할 수 있는 문제		6.5
6.0.12	GN-26205	Database	mysql 버전 업그레이드 5.7.40 -> 5.7.41		
6.0.12	GN-26150	WebUI	Tomcat version upgrade (9.0.68 -> 9.0.72, 8.5.78 -> 8.5.86)		
6.0.12	GN-26062	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 1.1.1t 업그레이드 - 임의 포인터를 memcmp 호출에 전달하여 메모리 내용을 읽거나 서비스 거부를 유발할 수 있음		7.4
6.0.12	GN-26000	MySQL	mysql 버전 업그레이드 5.7.33 -> 5.7.40		
6.0.12	GN-25869	CWP	IP관리 메시지 우선 On 일때 에이전트 사용자 인증 메뉴로 CWP 인증 시 계정(ID)으로만 인증되는 문제	6.0.3, 5.0.46	3.4
6.0.11	GN-25982	WebUI	WebUI Response Header에 CSP, HSTS Header 추가		
6.0.11	GN-25875	Windows Agent	에이전트가 웹브라우저 실행할 때 High권한 가지는 문제	4.0.0, 5.0.0, 6.0.0	3.3
6.0.11	GN-25849	WebUI	WebUI lib 취약점 항목 점검		
6.0.11	GN-25811	IPMGMT	IP 신청시스템에서 frontpage를 통해 사용자ID만으로 로그인 가능한 문제		4.9
6.0.10	GN-25925	IPMGMT, WebUI	IP 신청시스템 > IP신청 화면 XSS 가능한 문제		5.4
6.0.10	GN-25847	WebUI	CWP 화면에서 사용자 정보 수정 페이지 접근시 재인증 절차 추가		4.2
6.0.10	GN-25740	WebUI	감사 > 로그 > 로그검색바에서 XSS가 가능한 문제		5.6
6.0.1	GN-24305	GNOS	Apache 취약점 조치를 위한 2.4.52 버전 업그레이드		9.8
6.0.1	GN-24253	WebUI	log4j 취약점 개선		9.8
6.0.1	GN-23714	Center	인증처리가 미비한 에이전트관련 API 보완		4.6
6.0.1	GN-23461	WebUI	[SaaS] Saas 보안인증 소스코드 점검결과 조치		9.1
6.0.1	GN-23446	gnlogin, WebUI	비밀번호에 특정단어를 사용할 수 없도록 처리		8.7
6.0.0	GN-24030	GNOS	제품에 포함된 netcat(nc) 명령에서 reverse shell 기능 제거		
6.0.0	GN-24014	Center	HTTP로 호출가능한 SOAP/REST 제한		2.5

continues on next page

Table 25 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
6.0.0	GN-23981	macOS Agent, Windows Agent	에이전트에 UDP 이벤트의 패킷 조작을 통한 비정상 종료 문제		3.4
6.0.0	GN-23977	macOS Agent, Windows Agent	에이전트에서 인스턴트 메시지 표시할 때 존재하는 XSS 취약점 수정		6.8
6.0.0	GN-23972	Center, Sensor	UDP event 패킷처리시 데몬 비정상 종료 가능한 문제	5.0.36	6.4
6.0.0	GN-23970	WebUI	모바일 앱을 이용한 관리자 로그인 우회 취약점		6.1
6.0.0	GN-23967	WebUI	REST API Command Injection		6.7
6.0.0	GN-23966	WebUI	CWP 사용자 신청시 Excel 파일로 신청되는 경우 XSS 공격 가능 취약점		6.8
6.0.0	GN-23965	WebUI	Agent Download 페이지에서 상대경로를 통한 내부 파일 다운로드 취약점	5.0.37	5.2
6.0.0	GN-23794	WebUI	REST API 호출시 유효한 인증 토근이 존재하지 않아도 호출 가능한 문제		4.9
6.0.0	GN-23743	Center	API를 통한 서비스 거부 공격(DoS, Denial of Service) 취약점 개선		6.4
6.0.0	GN-23708	Center	인증처리가 미비한 센서관련 API 보완		4.6
6.0.0	GN-23706	Center	내부적으로 사용되는 SOAP API가 RPC를 통해 외부로 노출된 취약점		
6.0.0	GN-23705	WebUI	(KVE-2021-1062) Conf Engine 에서 파일 업로드 컴포넌트의 이름 유효성 체크 강화		6.7
6.0.0	GN-23702	WebUI	(KVE-2021-1062) CWP Design Template 에서 SSTI 취약점		
6.0.0	GN-23701	Windows Agent	(KVE-2021-1062) Agent 파일 생성시 상대경로를 사용할 수 있는 취약점		6.1
6.0.0	GN-23700	Center	(KVE-2021-1061) 노드에 인증된 사용자가 아님에도 비밀번호를 변경할 수 있는 취약점		8.7
6.0.0	GN-23699	Center, Sensor	(KVE-2021-1061) 센서정보 없이 모든 노드의 정보를 얻을 수 있는 취약점		
6.0.0	GN-23663	macOS Agent, Windows Agent	에이전트 OpenSSL 1.1.1l 업데이트		9.8
6.0.0	GN-23662	GNOS	openssl 버전 1.1.1l 로 업그레이드	4.0.146, 5.0.44, 6.0.1	9.8
6.0.0	GN-23563	Center	Command injection 공격 방어를 위한 수정		8
6.0.0	GN-23533	Center	사용불가 플러그인이 에이전트로 전달되지 않도록 개선		7.6
6.0.0	GN-23500	Center	SQL Injection 방어 처리방법 개선		8.7

continues on next page

Table 25 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
6.0.0	GN-23499	GNOS	GNOS 내부 취약한 LD_LIBRARY_PATH 환경변수 제거		
6.0.0	GN-23488	WebUI	[SaaS] SaaS 보안인증 WAS(Tomcat) 취약점 개선		7.5
6.0.0	GN-23377	GNOS	openssh 버전 8.6p1 으로 업그레이드		
6.0.0	GN-23358	WebUI	[CC] Web 취약성 점검결과 보안		6.5
6.0.0	GN-23237	GenianOS	Apache httpd(2.4.48) / tomcat(8.5.63) 업그레이드		7.5
6.0.0	GN-23233	Elastic-Search	[CC] elasticsearch 5.6.16 버전으로 업그레이드		8.8

CHAPTER

SEVENTEEN

SECURITY ADVISORIES

17.1 GZ-SA-2024-001: Genian ZTNA - Blind SQL Injection Vulnerability

17.1.1 날짜

- 2024년 04월 26일

17.1.2 CVSS score

- 2.2

17.1.3 영향도

- 낮음

17.1.4 내용

지니안ZTNA 관리콘솔의 노드 검색시 검색조건에 대한 입력값 검증 미흡으로 인한 Blind SQL Injection 공격이 가능한 문제가 발견되어 조치와 함께 제품 보안성 강화를 위한 보안 업데이트를 발표했습니다.

해당 버전을 사용하는 이용자들은 최신 버전으로 업데이트를 권고합니다.

- Genian ZTNA SQL 인젝션

17.1.5 영향 버전

- Genian ZTNA 6.0.20 이하
- Genian ZTNA 6.0.16 LTS(Revision 125554 이하)

17.1.6 해결 방법

이 권고 사항에 포함된 취약점은 아래 버전으로 업데이트하여 해결할 수 있습니다.

- Genian ZTNA 6.0.21 이상
- Genian ZTNA 6.0.16 LTS(Revision 12555 이상)

17.1.7 임시 조치 방법

- 없음

17.2 GZ-SA-2023-001: Genian ZTNA - Multiple Vulnerabilities

17.2.1 날짜

- 2023년 08월 01일

17.2.2 영향도

- 높음

17.2.3 내용

지니언스 업데이트 서버에서 아래 취약점을 발견하여 조치를 진행했으며 추가적으로 제품 보안성 강화를 위한 보안 업데이트를 발표했습니다. 해당 버전을 사용하는 이용자들은 최신 버전으로 업데이트를 권고합니다.

- 평문 노출 취약점(CVE-2023-40251)
- 비인가 스크립트 실행 취약점(CVE-2023-40252)
- 부적절한 인증 취약점(CVE-2023-40253)
- 무결성 검증 미흡 취약점(CVE-2023-40254)

17.2.4 영향 버전

- Genian ZTNA 6.0.15 이하

17.2.5 해결 방법

이 권고 사항에 포함된 취약점은 아래 버전으로 업데이트하여 해결할 수 있습니다.

- Genian ZTNA 6.0.16 이상

17.2.6 임시 조치 방법

- 평문노출 취약점은 이벤트 포트 변경을 통해 임시조치 가능합니다.

Note: 취약점 관련 사항을 해결하기 위해서는 **정책서버, 네트워크센서, 에이전트** 를 업그레이드 해야 합니다.