
Genian NAC

Release 5.0.63

GENIANS, INC.

May 03, 2024

관리자 가이드

1 Network Access Control의 이해	3
2 Genian NAC 구축	9
3 Genian NAC 설치	29
4 네트워크 자산 모니터링	63
5 네트워크 접근제어	105
6 네트워크 연결 프로세스	189
7 사용자 인증	217
8 엔드포인트 제어	289
9 위험감지	385
10 로그 및 이벤트 관리	395
11 시스템관리	419
12 API 가이드	489
13 로그포맷	499
14 FAQ	501
15 Troubleshooting	505
16 Release Notes	541
17 Security Advisories	743



NETWORK ACCESS CONTROL의 이해

1.1 NAC란 무엇인가?

Note: Genian NAC 소개 영상입니다.



네트워크 접근제어(Network Access Control)는 네트워크에 접속하는 장치에 대해 접속 가능 여부를 확인하여 인가된 장치만이 접속할 수 있도록 제한하는 것에서 출발하였다. 이 같은 접속 제어는 통상 802.1X라 불리는 기술을 통하여 제공되었는데 이때 AAA(Authentication, Authorization, Accounting)라 불리는 3가지 중요한 기능이 제공된다.

Authentication

Authentication은 네트워크에 접속하는 사용자나 장치에 대해 검증하는 과정이다. 통상적으로 사용자명/비밀번호를 통해 제공되는데 경우에 따라서는 장치의 MAC 주소가 인증의 수단으로 사용되기도 한다.

Authorization

Authorization은 인증된 장치가 어떤 네트워크 자원에 대해서 접근할 수 있는지에 대해 결정하는 과정이다. 인증된 장치의 종류나 식별된 사용자의 그룹에 따라 접근할 수 있는 네트워크, 서비스 및 시간대를 제한할 수 있다.

Accounting

Accounting은 장치가 네트워크를 접근한 기록을 남겨 향후 과금이나 보안상의 목적으로 사용할 수 있도록 해주는 과정이다. 이를 통해 어떤 장치를 누가, 언제, 어디서, 어떻게 사용했는지 확인할 수 있다.

이 같은 AAA 기능이 네트워크 접근제어의 기본 기술로 오랜 기간 사용되었는데 최근 네트워크 단말들의 다양한 보안 문제로 인해 단말의 보안 규제 준수상태에 따라 네트워크 접속 가능 여부를 결정하길 원하게 되었다. 이에 단말의 사용자에 대한 식별을 뛰어넘어 장치의 종류가 무엇인지 장치의 현재 보안설정이나 상태를 확인하여 관리자가 정한 조건에 부합하는 단말만이 네트워크에 접속할 수 있도록 해주는 제품군을 NAC라는 명칭으로 부르게 되었다.

NAC를 네트워크 연결 시점을 기준으로 보면 연결이 이루어지기 이전 단계에서 수행되는 작업과 연결 이후 수행되는 작업으로 구분하여 설명할 수 있다.

Pre-Connect

Pre-Connect는 단말이 네트워크에 연결되어 정상적인 통신이 이루어지기 이전에 수행되는 작업들을 말한다. 어떤 단말에 네트워크에 연결하고자 할 경우 단말에서 제공되는 사용자명/비밀번호/인증서/MAC 주소와 같은 신원정보를 이용하여 단말을 식별하고 인증하게 된다. 이 과정을 통해 네트워크에 접속 가능한 단말로 인가되지 못하면 네트워크 연결이 거부된다. 이 과정은 스위치나 무선랜 액세스포인트와 같은 장치를 통해 802.1X를 통해 제공되거나 ARP통제를 통해 제공될 수 있다.

Post-Connect

단말이 Pre-Connect 단계에서 요구하는 요구사항을 충족하면 주어진 권한에 따라 네트워크를 사용할 수 있게 된다. 이때 NAC는 지속적으로 단말의 상태 및 정보를 수집하여 관리자가 요구하는 조건을 충족하는지 여부를 모니터링하게 되고 만일 단말이 보안정책을 위배하는 상태가 되면 단말을 네트워크로부터 즉시 격리하게 된다. 지속적인 단말의 상태를 모니터링하기 위해 선택적으로 Agent를 사용할 수 있다. Agent는 단말에 설치되어 시스템의 상태 변경을 모니터링하면서 변경이 감지되면 즉시 NAC 정책서버로 알려 새로운 정책을 적용받도록 해준다.

1.2 NAC의 발전

초창기 1세대의 NAC는 과거부터 사용되던 네트워크 접속 사용자 인증 프로토콜인 802.1X를 기반으로 한 제품들이 주를 이루었다. 이는 스위치 및 무선 접속장치에서 제공되는 802.1X 표준을 통하여 인터페이스에 연결이 감지되면 정해진 인증서버(RADIUS)를 통하여 사용자명/비밀번호 또는 인증서를 통해 접속자를 식별한 뒤 인증서버에서 접속이 허가되면 연결 인터페이스를 활성화시켜주는 방식이다. 이 방식은 스위치의 포트 수준에서 작동되기 때문에 가장 완벽한 접근제어를 제공할 수 있다. 하지만 802.1X를 지원하지 못하는 장치들에 대한 인증 문제 및 모든 접속장치가 802.1X를 지원해야 하는지 확인해야 하는 등 기존 네트워크를 일순간에 접근제어를 적용하기에는 어려운 점이 많아 구축실패 사례가 많이 발생되었다.

이에 2세대로 나온 NAC는 802.1X에서 벗어나 네트워크 접속장치들과 SNMP를 통해 정보를 수집하거나 각 네트워크마다 센서 또는 Probe라 불리는 장치를 통해 독립적으로 정보를 수집할 수 있게 되었고 접근제어 또한 대체적인 수단으로 제공하기 시작했다. 802.1X 이외에 네트워크에서 적용 가능한 접근제어는 스위치의 VLAN을 조정하여 단말은 제한된 VLAN으로 위치시키거나 ACL을 설정하는 것부터 네트워크센서를 통해 ARP를 이용한 제어, SPAN(미러링) 포트를 통한 연결 끊기 방식까지 사용자의 환경이나 요구사항에 맞게 다양한 방식으로 진화되었다. 네트워크 접속방법이 유선랜 방식에서 무선랜으로 변화됨에 따라 네트워크센서, 무선컨트롤러, 에이전트를 통해 무선 네트워크에 대한 가시성을 확보하는 기능들도 추가되고 그를 바탕으로 Rogue AP와 같은 무선 보안에 대응할 수 있게 되었다.

3세대의 NAC는 수집과 제어를 넘어서 다양한 자동화를 위한 기술들이 추가되었다. 에이전트를 통해 단말의 보안수준을 기업이 원하는 상태로 자동적으로 설정되도록 해주며 네트워크에 존재하는 다양한 시스템들과의 연동을 통해 상호 협력적인 보안 모델을 구축할 수 있도록 해주었다. 예를 들어 인터넷 게이트웨이 구간에서 동작하는 보안시스템은 중단 네트워크의 장치가 주변 장치와 동일한 서브넷 내에서 통신하는 것을 제어할 수 없기 때문에 NAC와 연계하여 NAC를 통해 제어를 할 수 있게 된다. 또한 차세대 방화벽과 같이 단말의 사용자 정보를 통해서 접근제어 정책을 수립할 수 있게 된 보안시스템들이 필요한 IP에 대한 사용자 정보를 제공하여 보다 향상된 보안시스템 구축을 쉽게 만들어 준다. 이 같은 연동은 REST, Webhook, Syslog와 같은 표준화된 프로토콜을 통하여 제공되게 된다.

4세대의 NAC는 최근의 BYOD와 IoT 트렌드로 기하급수적으로 늘어난 접속 단말들로 인해 IT관리자의 가시성이 저하되고 네트워크 관리가 어려워지는 것을 해결하는 것에 중점을 두고 있다. 단말을 보다 정확히 식별하고 더 나아가서 단말의 다양한 비즈니스 상태 (End-of-Life, End-of-Support 등)를 손쉽게 관리하거나 단말에 알려진 취약점등을 자동적으로 관리할 수 있도록 해주는 방향으로 진화하고 있다. 그와 더불어 클라우드와 같이 변화하는 IT 환경에 맞게 클라우드 기반 관리형 서비스도 새롭게 선보이고 있다.

1.3 NAC가 해결해주는 문제점들

허가되지 않은 기기의 무단 반입

NAC가 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. NAC는 이 문제를 해결하기 위해 모든 연결되는 기기에 대해 인증하고 일정 수준 이상의 보안 요구사항을 충족하는 경우에만 네트워크를 사용할 수 있게 해준다.

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. NAC는 지속적인 네트워크 감시를 통해 연결되는 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. 이로 인해 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 시간등의 정보가 정확히 수집되어야 한다. NAC는 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. NAC는 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. NAC는 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. NAC는 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. NAC는 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 NAC와 Firewall의 차이점

NAC 기술에 익숙하지 않은 사용자는 종종 Firewall과 그 역할을 혼동하기도 한다. 이는 네트워크 접근제어(Network Access Control)라는 용어가 가지는 일반성 때문에 Firewall도 같은 기능의 제품으로 생각하기 쉽다. 하지만 두 제품은 다음과 같은 큰 차이점을 가지고 있다.

네트워크 중심 vs 단말 중심

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

가시성 확보

NAC를 구축하는 궁극적인 목적은 관리자가 정한 보안규정을 준수하지 않는 단말이 네트워크에 접속해서 사용하는 것을 통제하고 관리하는 것이다. 하지만 이 목적을 위해 단말에 대한 통제기능을 네트워크에 즉시 적용하기는 매우 어렵다. 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 인증을 위해 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 플랫폼 종류/이름/제조사, 호스트명, 연결 스위치/포트, 연결 SSID, 서비스포트, 동작상태와 같은 정보들이 제공되어야 한다. 추가적으로 단말에 대한 보다 상세한 가시성을 위해 Agent를 제공될 수 있다.

단말의 분류

가시성이 확보되면 그 데이터를 기반으로 보안정책을 수립해야 한다. 보안정책 수립의 첫 단계는 수집된 데이터를 바탕으로 단말을 분류하는 것이다. NAC에서 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 식별하는 것이 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 사용자에게 대해 네트워크 접근제어 정책을 수행하는 것보다는 에이전트를 통하여 자동으로 정책을 따르도록 처리된다면 보다 손쉽게 NAC를 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 사항을 참고하기 바란다.

1.6 Genian NAC의 특징

4세대 NAC

Genian NAC는 4세대 NAC의 대표적인 제품으로 네트워크센서를 통해 기존 IT 환경의 변화 없이 가장 진보된 가시성을 제공한다. 이를 통해 500여 개 이상의 다양한 그룹 조건을 제공하여 단말의 상태에 따른 동적인 그룹을 상세히 관리할 수 있다. 다양한 구성방식을 지원하여 빠르고 쉽게 성공적인 NAC 구축을 할 수 있다.

네트워크센서 기반의 진보된 가시성

Genian NAC는 각 네트워크의 브로드캐스트 도메인에 직접 연결되는 네트워크센서를 사용해 기존 IT 인프라와의 연동을 최소화하여 도입이 간편하고 허브와 같은 레거시 네트워크 환경에서도 문제 없이 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 NAC 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 관리업무를 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 NAC 제품 대비 가장 폭넓은 제어 방식을 지원하여 관리자의 요구사항에 맞게 단계적인 보안정책을 수립하기 쉽게 해 준다. (참고 제어 방법)

다양한 IT보안 자동화

Genian NAC에서 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 AP 차단 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 NAC은 위에서 설명한 구축 단계에 맞게 3가지의 *Edition* 으로 구분되어 있다. Basic Edition은 NAC구축 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, ARP통제, 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.

GENIAN NAC 구축

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

2.1 구성 요소 이해

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

Note: 유튜브를 통해 Genian NAC 구성 요소 교육 영상을 확인할 수 있습니다: [Online EDU 2 Chapter](#), 관리자 교육-제품 소개 및 기본 구성 요소와 이해

2.1.1 정책 서버

정책서버는 NAC의 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 포트에 구성해야 합니다.

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 되어야 합니다. 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 관련된 보안을 모니터링 할 수 있습니다. 무선 센서는 네트워크 센서 시스템에 무선 LAN 인터페이스를 추가하여 작동시킬 수 있습니다. 그러나, 센서의 위치는 무선 네트워크의 특성으로 인해 검출 될 수 있는 영역에 크게 영향을 미치기 때문에, 네트워크 센서와 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 네트워크 센서에서 제어기능을 활성화 하면 ARP Layer 2 기반 제어가 제공 됩니다. 추가 하드웨어 없이 네트워크 센서로 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 수 있는 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 설치하는 선택적 요소이므로 에이전트 없이 NAC 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 Update Server는 보다 강력한 수준의 보안체계가 도입된 실시간 업데이트 서비스 서버입니다.

또한 제품 이미지와 제품에서 사용되는 주요 업데이트 데이터를 제공하고 있습니다.

Genian Data

Genian Data는 소프트웨어 공급망 보안을 강화하여 **SLSA3** (Supply-chain Levels for Software Artifacts, 소프트웨어 공급망 무결성 보호를 위한 프레임워크) 수준의 요구사항을 만족시켜 주요 데이터를 제공하고 있습니다.

SLSA3 요구 수준은 NIST에서 권고하는 **SSDF** (Secure Software Development Framework, 안전한 소프트웨어 개발 프레임워크) 요구사항을 더 세분화하여 만족하고있으며,

Geni Update Server에서는 제품에 등록된 노드들의 **CVE** 위협 정보, **NODE** 분류정보, **OS** 업데이트 정보, 플랫폼 분류 및 플랫폼 정보 등의 업데이트를 제공 하고 있습니다.

Genian Data는 기본적으로 2시간 간격으로 업데이트를 체크하며 환경에 따라 수동 및 자동으로 업데이트 기능을 사용할 수 있습니다.

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 NAC를 통한 성공적인 NAC 구축

NAC를 구축하는 것은 네트워크 환경의 다양한 변화로 이어질 수 있습니다. 사용자의 가용성을 확보하기 위해 단계별 구축과정이 중요합니다. Genian NAC는 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 확보해야 합니다. 따라서 802.1x 기술 만을 통해 점진적인 네트워크 액세스 제어 환경을 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 고려하여야 합니다.

이러한 복잡성과 호환성 문제를 해결하기 위해 Genian은 별도의 독립적 네트워크센서를 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.

Link	Anomaly	Connectivity	MAC	IP	Trg	Enforcement Policy	Platform	Hostname (Name)	Network Access Device	Access Port	SSID	Time Detected	Location
00:18:0A:09:C2:58			20:16:01:25:00:75	172.23.48.61		Antivirus Not Compliant	Microsoft Windows 10 Professional x64	LAPTOP-DEVLBT	BostonManoSG300	g1/4		2019-03-26 20:35:31	C-172.17.6.5
00:02:86:3A:07:00			00:16:85:02	192.168.50.2		Default Policy	ASUS RT-AC68P Wireless Router	RT-AC68P-0700	GNTTEST1-C3750v2	Fa1/0/5		2017-12-28 14:54:44	Boston
00:01:2E:83:CA:D7			00:16:85:02	192.168.50.2		SPAM Denied	Linux		192.168.50.250	g1		2019-01-23 21:05:23	Boston
F4:4D:30:66:0F:64			192.168.50.11	192.168.50.11		Default Policy	SS84	USA-eh0(Boston)	Boston_C3750	G1/0/6		2017-12-28 14:54:38	C-172.17.6.5
C4:8E:1F:07:07:F2			192.168.50.15	192.168.50.15		Default Policy	TP-LINK TECHNOLOGIES CO.,LTD.,AP		Cisco3750	Fa1/0/1		2019-03-26 16:36:04	Boston
38:C9:86:20:0E:C4			192.168.50.20	192.168.50.20		Default Policy	Apple macOS High Sierra	IMAC200E64	Boston_C3750	G1/0/5		2019-02-11 09:54:31	Boston
40:8D:40:1A:00:64			192.168.50.24	192.168.50.24		SPAM Denied	Ubuntu Linux	kyryeon	Boston_C3750	G1/0/11		2017-12-28 14:54:47	Boston
10:41:7F:29:62:4A			192.168.50.30	192.168.50.30		Default Policy	Apple Device	Doseok	GNTTEST1-C3750v2	Fa1/0/5		2019-03-12 16:50:00	Boston
00:80:ED:0C:68:F9			192.168.50.31	192.168.50.31		Default Policy	Apple iPhone	iPhone	Boston_C3750	G1/0/12		2019-04-01 11:08:28	Boston
10:92:66:08:D5:C3			192.168.50.32	192.168.50.32		Default Policy	Samsung Android Device	android-6e1b2fa1a5592e9	Boston_Cisco2954	Boston	GeniansSG	2019-03-05 08:48:03	Boston
88:D7:AF:A4:5A:E7			192.168.50.33	192.168.50.33		Default Policy	Android OS	Android	Boston_Cisco2954	Boston	GeniansSG	2019-03-12 13:09:50	Boston
F8:83:5F:08:F9:CD			192.168.50.34	192.168.50.34		Default Policy	Microsoft Windows 10 Pro	WIN10-DJKM	Boston_C3750	G1/0/12		2019-03-12 16:29:21	Boston
0C:29:95:0F:2C:F1			192.168.50.35	192.168.50.35		Default Policy	Microsoft Windows 10 Home	YOUNGAEISO	Boston_C3750	G1/0/12		2019-03-12 13:19:03	Boston
00:08:DC:4E:D3:26			192.168.50.36	192.168.50.36		Default Policy	D-Link DL-524 wireless broadband router	WiFi DHCP Client	Boston_C3750	G1/0/12		2019-03-07 10:13:22	Boston
00:28:F8:6B:47:70			192.168.50.38	192.168.50.38		Default Policy	Microsoft Windows	www	Boston_C3750	G1/0/12		2019-03-12 13:09:50	Boston
84:CA:91:18:D6:A6			192.168.50.42	192.168.50.42		Default Policy	Genians Genian NAC	GNTTEST1-C3750v2	Fa1/0/3		2019-02-28 14:54:54	Boston	
00:90:0B:0C:2B:9E			192.168.50.45	192.168.50.45		Default Policy	Linux	Linux	Boston_C3750	G1/0/8		2019-02-28 14:54:54	Boston
00:F5:DA:4A:C0:E0			192.168.50.101	192.168.50.101		Default Policy	Microsoft Windows	DESKTOP-6UHF774	Boston_C3750	G1/0/12		2019-03-05 11:21:59	Boston
00:A1:FC:BA:CA:7E			192.168.50.109	192.168.50.109		Antivirus Not Compliant	Microsoft Windows 10 Professional x64	WIN10-DJKM	Cisco3770	Fa1/0/2		2019-03-05 16:28:27	Boston
A0:56:F3:C0:79:39			192.168.50.115	192.168.50.115		Default Policy	Apple iPhone	Scotts-iPhone	Boston_C3750	G1/0/12		2019-03-12 09:03:11	Boston
38:F9:D3:77:58:93			192.168.50.115	192.168.50.115		Default Policy	Apple MacBook Pro	MACBOOKPRO-6803	Boston_C3750	G1/0/12		2019-04-01 08:46:43	Boston
80:E0:1D:92:08:74			192.168.50.118	192.168.50.118		Default Policy	Cisco Networking Device	APB60-1692-0874	BostonManoSG300	g1/1		2019-01-21 03:12:34	Boston
08:00:27:F8:21:3C			192.168.50.125	192.168.50.125		Default Policy	CentOS Linux	centos	Boston_C3750	G1/0/11		2019-02-28 13:09:50	Boston
9C:32:CE:58:F4:58			192.168.50.129	192.168.50.129		Default Policy	Canon Printer	Canon	Boston_C3750	G1/0/12		2019-02-14 14:01:02	Boston
D8:6C:63:31:D6:8B			192.168.50.135	192.168.50.135		Default Policy	Google Home Smart Speaker	Google-Home	Boston_C3750	G1/0/12		2019-03-29 10:58:04	Boston
FC:EC:DA:37:CD:85			192.168.50.153	192.168.50.153		Default Policy	Linux	Linux	GNTTEST1-C3750v2	Fa1/0/4		2019-01-21 18:36:09	Boston
88:1F:C2:07:07:09			192.168.50.157	192.168.50.157		Default Policy	Apple Mobile Device	GEMANS-TV	Boston_C3750	G1/0/12		2019-01-21 18:36:09	Boston
3A:57:A5:0E:0F:14			192.168.50.188	192.168.50.188		Default Policy	HP HP DesignJet Pro X5700a MFP	HPDFCBA	Boston_C3750	G1/0/12		2017-12-28 14:54:44	Boston
00:17:88:22:35:1F			192.168.50.160	192.168.50.160		Default Policy	Linux	Phillip-hue	BostonManoSG200	g9		2019-01-21 03:12:34	Boston
70:14:A0:47:0E:D8			192.168.50.161	192.168.50.161		Default Policy	Apple iPhone	iPhone	Boston_C3750	G1/0/12		2019-04-01 08:02:40	Boston
80:6E:BF:74:8A:34			192.168.50.164	192.168.50.164		Default Policy	ASUSTek COMPUTER INC. AP	ASUSTek	GNTTEST2	Boston_C3750	G1/0/9	2019-01-21 03:12:34	Boston
C4:83:01:D7:98:F7			192.168.50.176	192.168.50.176		Antivirus Not Compliant	Apple macOS Mojave	jean-macbook-pro.local	GNTTEST1-C3750v2	Fa1/0/5		2019-03-28 08:12:03	Boston
AC:E5:9E:C4:E7:0F			192.168.50.176	192.168.50.176		Default Policy	Samsung GearS2	GearS2-ETNE	Boston_C3750	G1/0/12		2019-03-28 15:58:20	Boston
68:05:CA:37:5B:8D			192.168.50.177	192.168.50.177		Default Policy	Ubuntu Linux	andrew	Boston_C3750	G1/0/3		2018-12-12 15:42:07	Boston
80:6E:BF:74:8A:70			192.168.50.178	192.168.50.178		Default Policy	ASUSTek COMPUTER INC. AP	GNTTEST1	Boston_C3750	G1/0/12		2018-10-17 08:02:50	Boston

Genian NAC는 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 정렬해야 합니다.

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

Device Platform Intelligence / Cisco SG300-20 Switch



Cisco SG300-20 Switch

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

[Suggest Update](#)

Platform's Common Vulnerabilities and Exposures (CVE)

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

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 NAC는 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 제어해야 합니다. 그러나 식별된 모든 위반 단말를 한 번에 제어하는 것은 쉽지 않습니다. 이를 위해서는 단계별 자동 접근이 필요합니다.

IT 보안 정책이 수립되면 이를 위반하는 단말를 제어해야 합니다. 그러나 식별된 모든 위반 단말를 한 번에 제어하는 것은 생각보다 어려운 일이며 단계별 대응이 필요합니다. 이를 위해 Genian NAC는 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 NAC는 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 unreachable.	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 (<i>Poor wired device support</i>)	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 네트워크센서는 아래와 같이 구성하여 구축 할 수 있습니다.

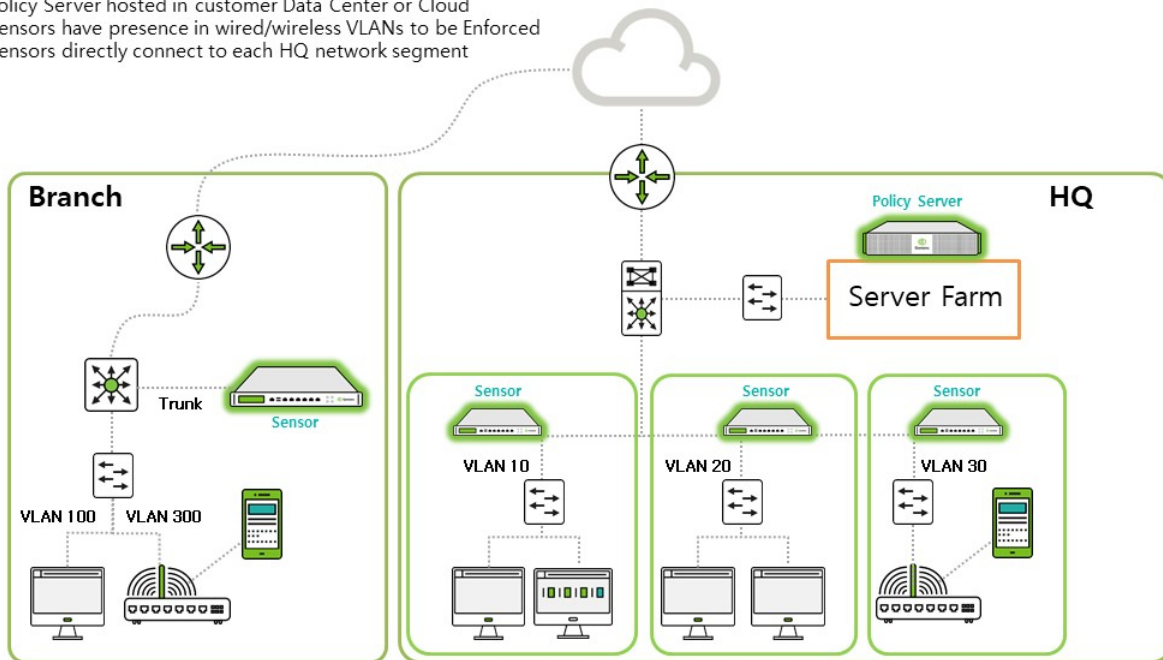
스위치 포트는 표준 액세스 포트이거나 최대 128 개(권장 64개)의 VLAN에 대한 트렁킹 포트가 될 수 있습니다. 하나의 네트워크센서에 128 개 이상의 VLAN이있는 경우 두 번째 네트워크센서가 필요합니다. (동일한 네트워크에 두 개의 네트워크센서가 있거나 802.1q 환경에서 중복되는 네트워크가있는 경우에 중복된 노드를 갖는 것은 문제가 되지 않으며, 단지 주의해야 할 사항일 뿐입니다.)

다른 구축 유형

On-Premise

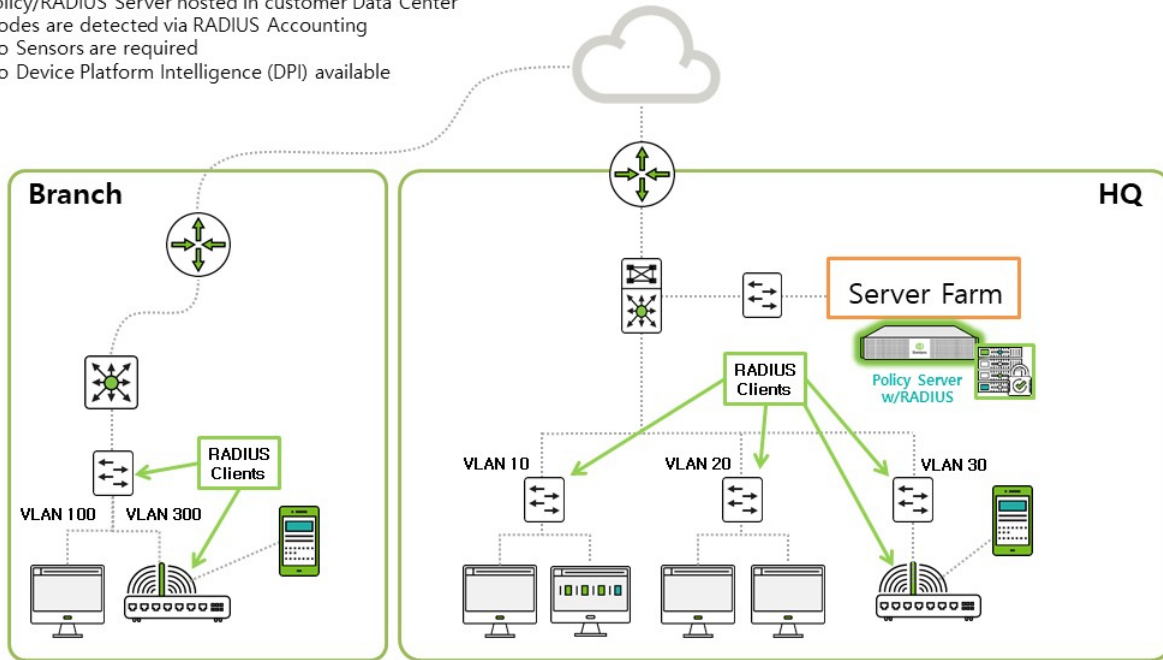
Distributed HQ Sensor Deployment

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



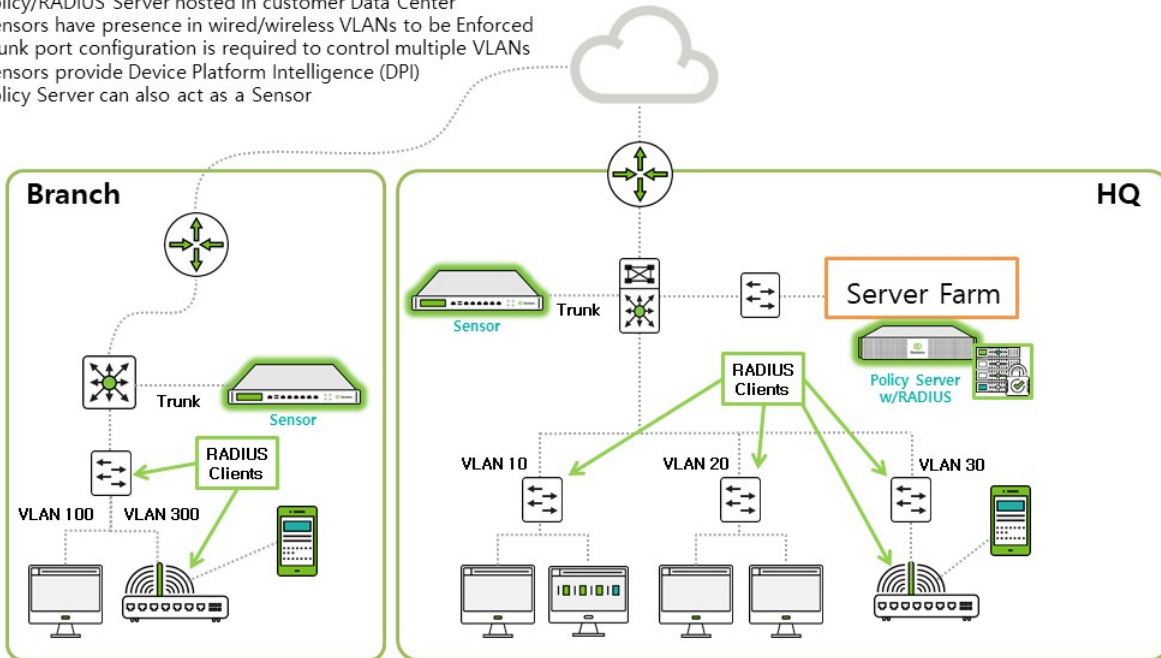
Typical On-Prem RADIUS Deployment

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



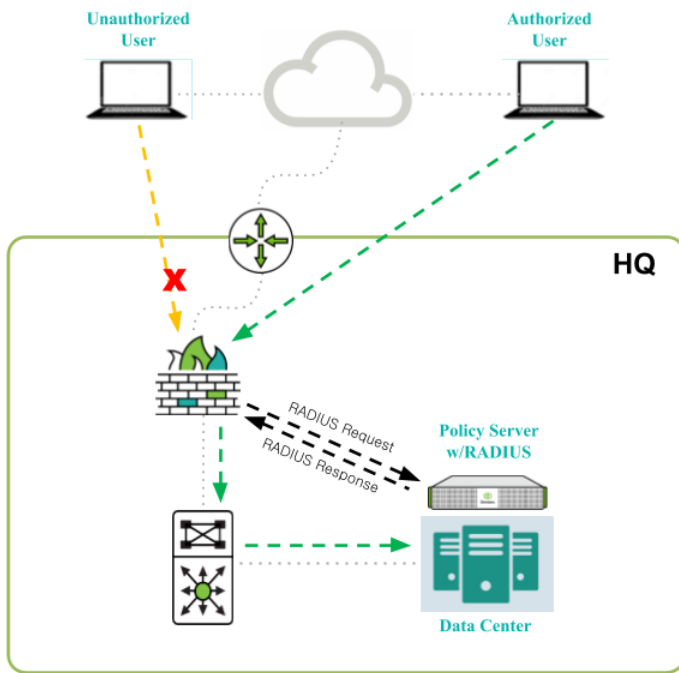
Typical On-Prem RADIUS Deployment with DPI

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



Genians

Genians VPN Enforcement – Unauthorized User



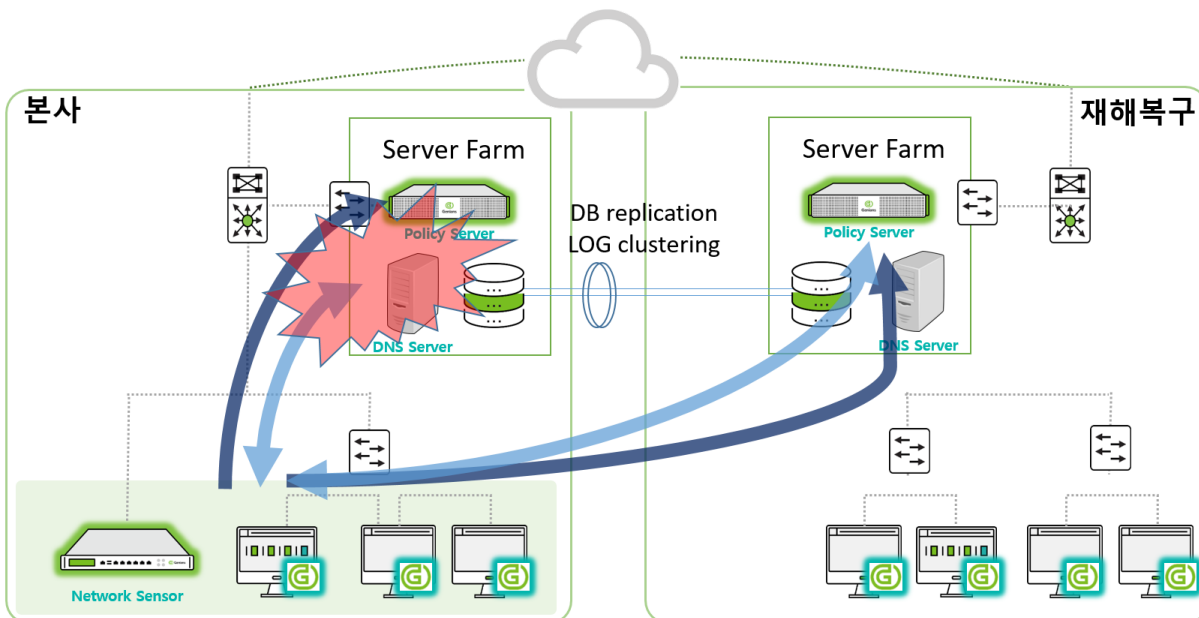
Highlights:
No Agent Required
AD/Local User Accounts
No RADIUS CoA Required

RADIUS Enforcement

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



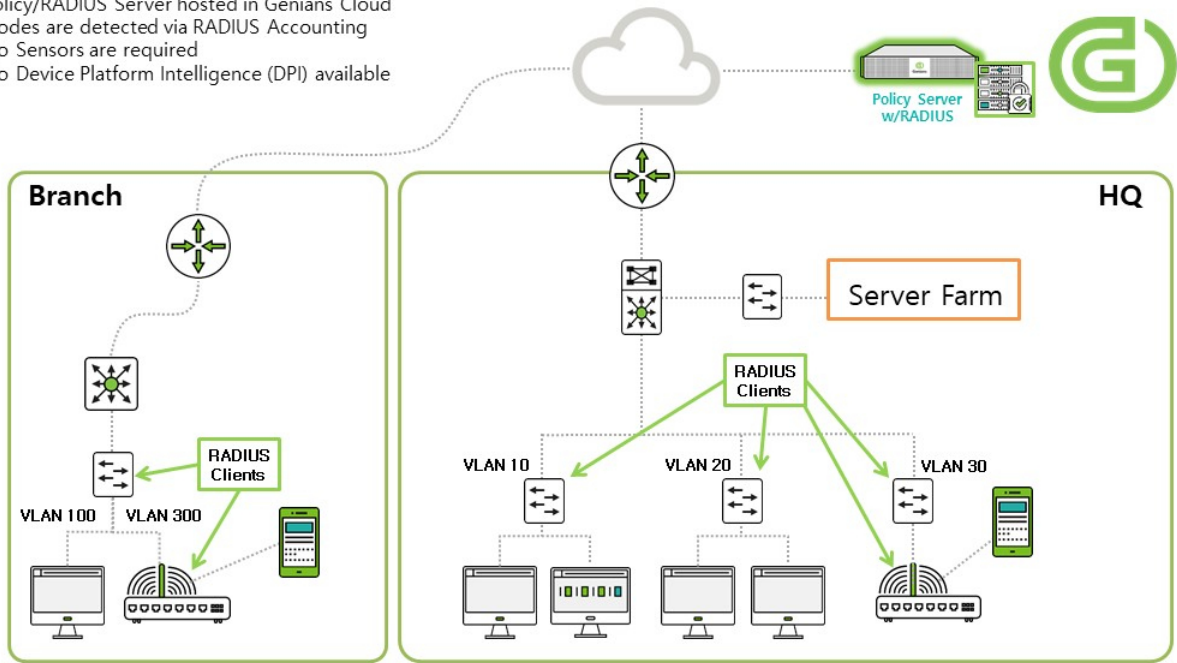
일반적인 NAC 재해복구 구축



Cloud

Typical Cloud RADIUS Deployment

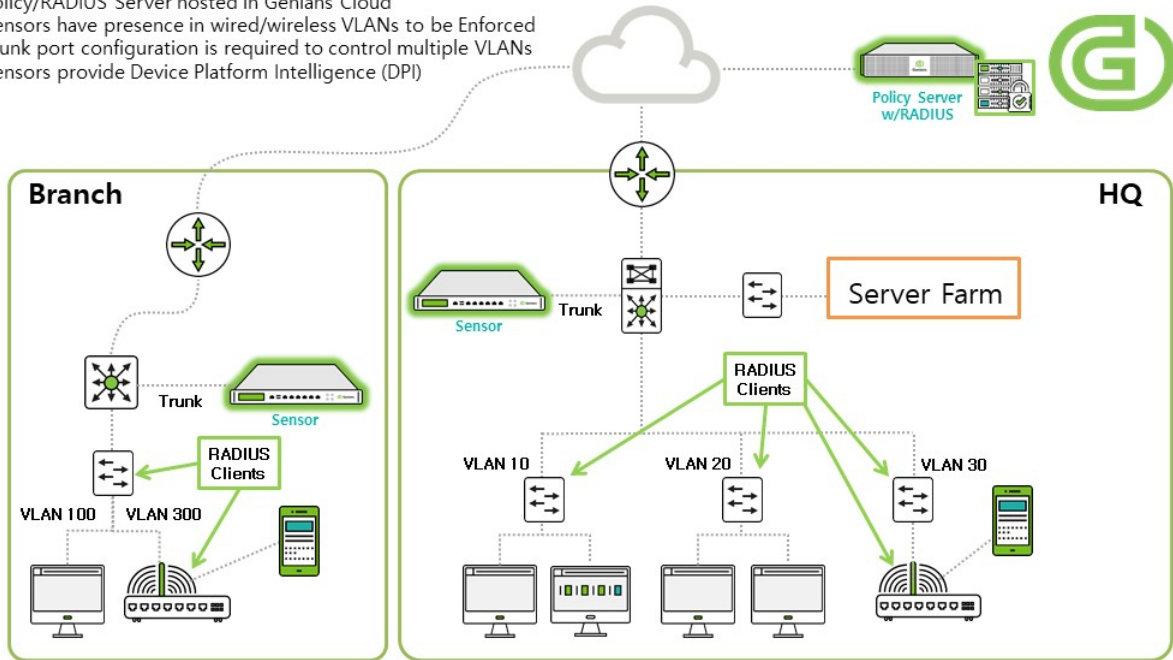
- Policy/RADIUS Server hosted in Genians Cloud
- Nodes are detected via RADIUS Accounting
- No Sensors are required
- No Device Platform Intelligence (DPI) available



Genians

Typical Cloud RADIUS Deployment with DPI

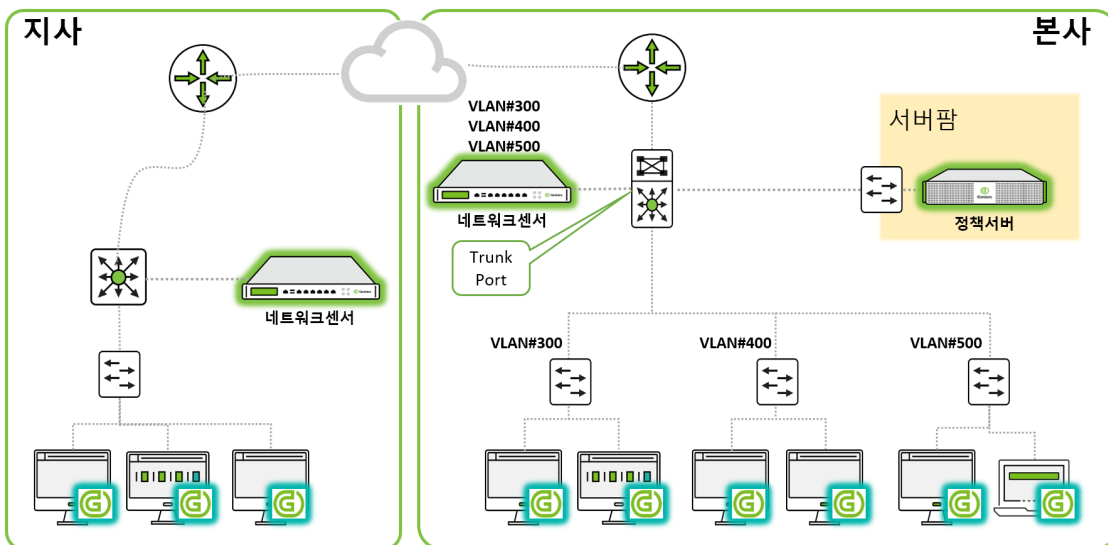
- Policy/RADIUS Server hosted in Genians Cloud
- Sensors have presence in wired/wireless VLANs to be Enforced
- Trunk port configuration is required to control multiple VLANs
- Sensors provide Device Platform Intelligence (DPI)



Genians

일반적인 On-Premise 구축

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

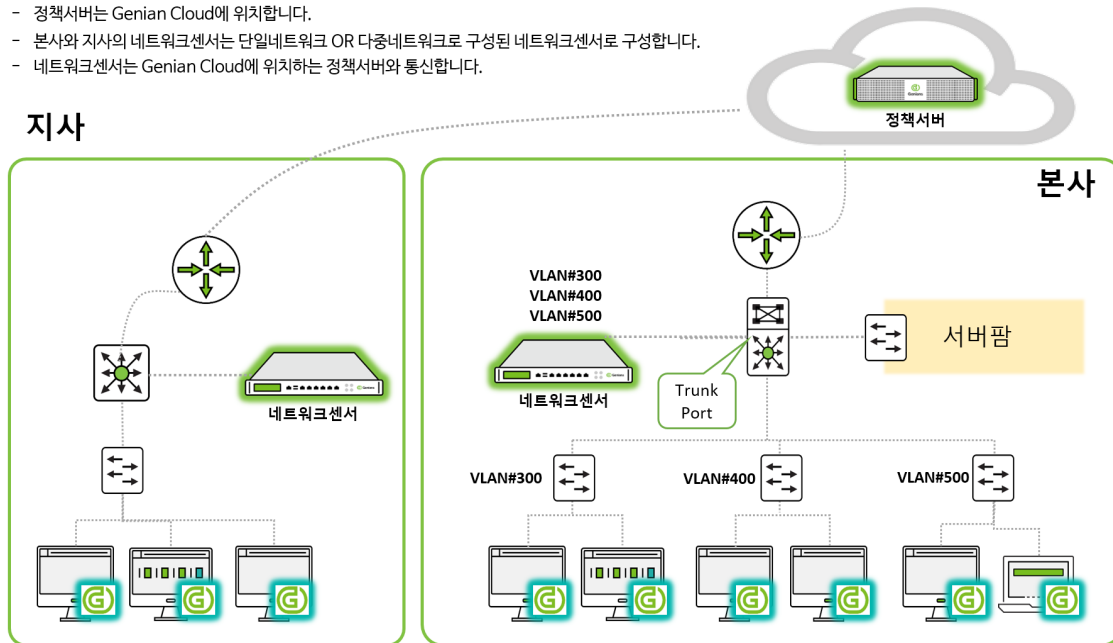


CLOUD

정책서버는 클라우드에 설치되며 네트워크센서는 원격 사이트 위치의 Edge Switch에 연결하여 설치할 수 있습니다. Edge Switch 포트는 액세스 포트이거나 최대 128개(권장 64개)의 VLAN을 위한 트렁킹 포트일 수 있습니다. 네트워크센서에 128개 이상의 VLAN이 있는 경우 두 번째 네트워크센서가 필요합니다.

일반적인 Cloud 구축

- 정책서버는 Genian Cloud에 위치합니다.
- 본사와 지사의 네트워크센서는 단일네트워크 OR 다중네트워크로 구성된 네트워크센서로 구성합니다.
- 네트워크센서는 Genian Cloud에 위치하는 정책서버와 통신합니다.



2.3 에디션 비교

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

각 에디션의 기능 범위는 다음과 같습니다.

Basic

네트워크 및 IT 자산에 대한 모니터링을 제공합니다.

Professional

IT 보안 정책에 따라 네트워크 접근 제어를 제공합니다.

Enterprise

Active Directory 연동, Desktop management, API 연동 등 다양한 IT 자동화 플랫폼을 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	Professional	Enterprise
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 엔드포인트 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
	사용자, WLAN 및 장치/노드에 대한 태그 기반 제어 (예: 게스트 장치, 임시 권한, 정책 면제)		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
데스크탑 관리	보안규제준수 검사 (안티 바이러스, OS 업데이트, 펌 수 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
	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	CWP를 통한 요청 / 승인 (IP, 장치, 사용자, 게스트 사용자, 외부 장치)			Yes
	역할 기반 관리자			Yes
	사용자 정의 필드 (노드, 장치, 사용자)			Yes
	목적에 위한 포털 포털 페이지			Yes
	다국어 지원			Yes
확장성 및 가용성	고 가용성 (정책 서버 / 네트워크 센서)			Yes
	인터페이스 채널 분당			Yes

continues on next page

Table 1 – continued from previous page

카테고리	특징	Basic	Profes- sional	Enter- prise
	장애 복구 (DB 동기화, 정책 서버 이중화)			Yes

2.4 네트워크 준비

네트워크에 NAC 구축을 계획할 때 몇 가지 고려 사항이 있습니다.

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

2.4.1 유선 연결

정책서버는 Core Switch 포트에 액세스 포트로서 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
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 섀다운 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 관리해야 할 또 다른 네트워크가 있는 경우 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 탐지할 수 있습니다.

2.4.3 방화벽 요구 사항

Genian NAC가 제대로 동작하려면 아래의 포트들이 방화벽으로부터 개방되어야 합니다.

[On-Premises]

SRC IP	DST IP	Service	Note
정책서버	로그 서버 DB 서버 네트워크 센서 IP, PC IP(에이전트) https://alarm.geninetworks.com https://alarm2.geninetworks.com https://geniupdate.geninetworks.com https://techlab.geninetworks.com https://pi-api.genians.com https://api.genians.com https://geniupdate2.genians.com https://dzxsljwm8reh.cloudfront.note	TCP/9200~9300, TCP/9300~9400 TCP/3306 UDP/3871 TCP/443 TCP/443 TCP/443 TCP/80, TCP/443 TCP/443 TCP/443 TCP/8844 TCP/443	로그 서버 데이터베이스 Kepp Alive, 이벤트 송신 Alarm 서비스 Alarm 서비스 GenianData 업데이트 플랫폼 미탐지, 오탐 보고 Genian DPI Zero Config Sensor Lookup GenianData Update Syscollect
네트워크센서 IP	정책서버 IP/FQDN https://dzxsljwm8reh.cloudfront.note	UDP/3870 TCP/80, TCP/443 UDP/514, TCP/6514 TCP/443	Keep Alive 정책, 액션 정보 업데이트 Syslog Syscollect
PC IP (에이전트)	정책서버 IP/FQDN	UDP/3870 TCP/80, TCP/443 TCP/8000	Keep Alive 정책, 액션 정보 업데이트 Windows 업데이트
관리자 PC	정책서버 IP, 네트워크센서 IP 정책서버 IP	TCP/3910 TCP/8443	SSH 웹 콘솔

[Cloud managed]

SRC IP	DST IP	Service	Note
정책서버 IP	3.34.24.101 네트워크 센서 IP, PC IP(에이전트)	TCP/80, TCP/443 UDP/Random	플랫폼 미탐지, 오탐 보고 Kepp Alive, 이벤트 송신
네트워크센서 IP	정책서버 IP/FQDN	UDP/Random TCP/80, TCP/443 UDP/Random, TCP/Random	Keep Alive 정책, 액션 정보 업데이트 Syslog
PC IP (에이전트)	정책서버 IP/FQDN	UDP/Random TCP/80, TCP/443, TCP/8000	Keep Alive 정책, 액션 정보 업데이트 Windows 업데이트
관리자 PC	정책서버 IP/FQDN	TCP/22	SSH

Note: Keep Alive 트래픽은 VLAN 인터페이스(ethX 및 ethX.X)를 포함한 모든 센서 인터페이스에서 전송됩니다.

Note: 운영정보 데이터 다운로드 및 플랫폼 오탐보고를 전송하기 위해서는 정책서버가 외부 통신이 가능해야 합니다.

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

Note: 파일배포v2 keyless 방식을 사용하는 경우 다음 파일배포v2 정보도 방화벽에서 허용해야 합니다.

GENIAN NAC 설치

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

3.1 정책서버 설치

3.1.1 구축 형태

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

On-premises

내부 네트워크에 직접 물리적인 정책서버를 설치하여 고객의 정책 및 네트워크를 관리하는 시스템입니다.

Cloud managed

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

3.1.2 하드웨어 준비

물리적 시스템 또는 가상 시스템에 정책서버를 설치할 수 있습니다.

물리적 장비

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

최소 하드웨어 요구 사항

- 프로세서 : Intel 또는 AMD 듀얼 코어
- 메모리 : 4GB (8GB 권장)
- 저장 용량 : 120GB
- NIC : 유선 네트워크 인터페이스, 무선 인터페이스 (옵션)

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

가상 머신

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

Cloud managed

Genians은 사용자가 정책서버를 수동으로 설치 및 관리할 필요가 없는 클라우드 관리 서비스를 제공합니다.

3.1.3 네트워크 연결 준비

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

Genian NAC는 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 선택해야 합니다.

VMWare ESXi 를 802.1Q trunk 포트와 함께 사용하려고 하면 VGT 모드를 활성화해야 합니다.

VMWARE KB 문서 또는 가상환경에서 Trunk 설정 을 참조 하십시오.

3.1.4 소프트웨어 다운로드

기술지원센터 를 통하여 정책서버 ISO 파일을 다운로드하고 물리적 장비 설치용 부팅 USB를 생성합니다.

부팅 가능한 USB 드라이브 만들기

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

UNETbootin 얻기

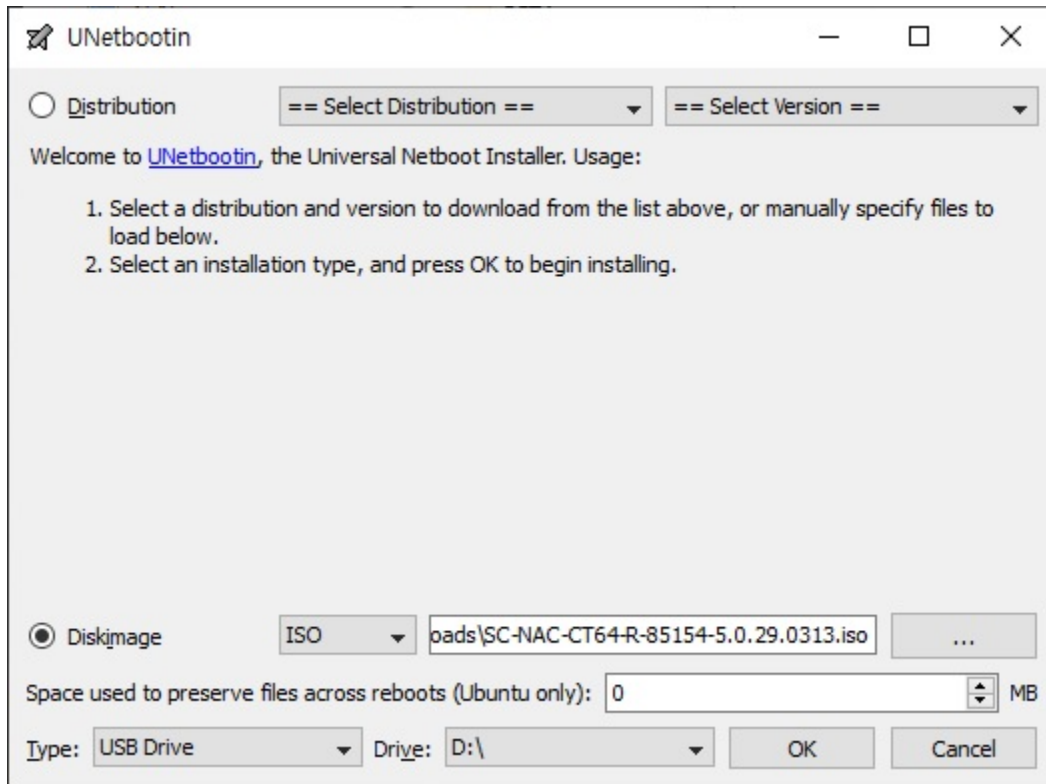
Genians 는 CD를 굽지 않고 Genian NAC 설치용 USB 플래시 드라이브를 만들 수 있는 UNETbootin 을 권장합니다. UNETbootin을 다운로드하려면 운영 체제를 선택하십시오.

USB 드라이브 만들기

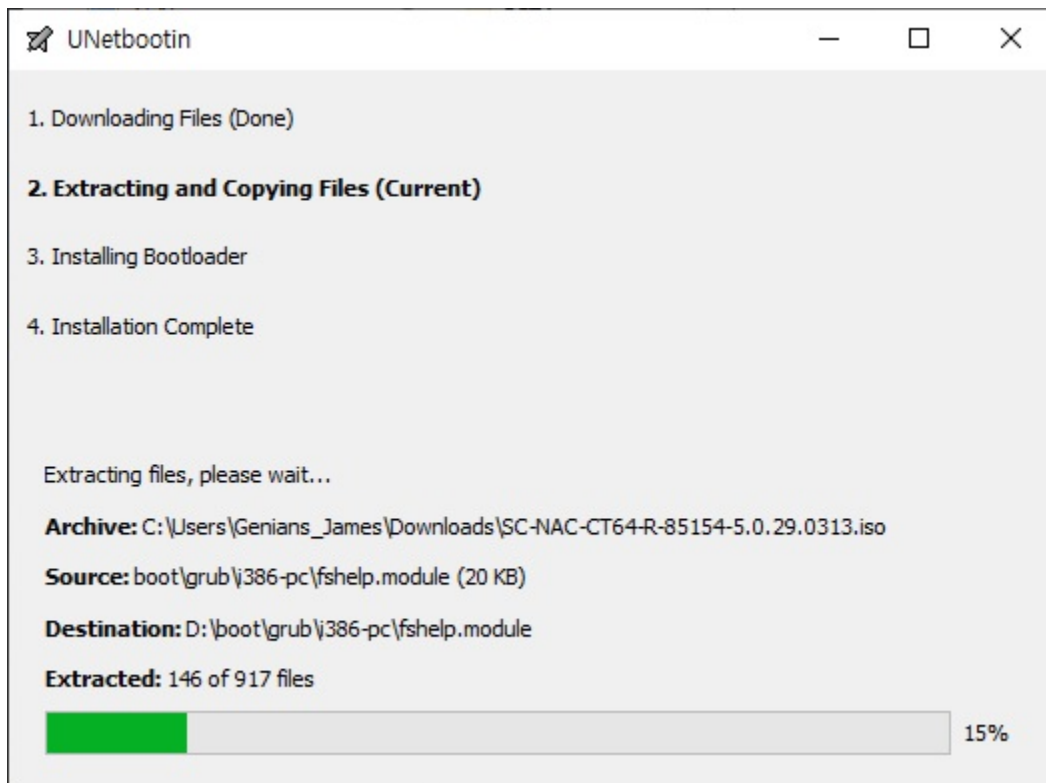
USB 드라이브가 포맷 된 FAT32인지 확인하십시오. 다른 파일 시스템은 지원되지 않을 수 있습니다.

UNETbootin 이 설치되면 다음 단계를 수행 하십시오.

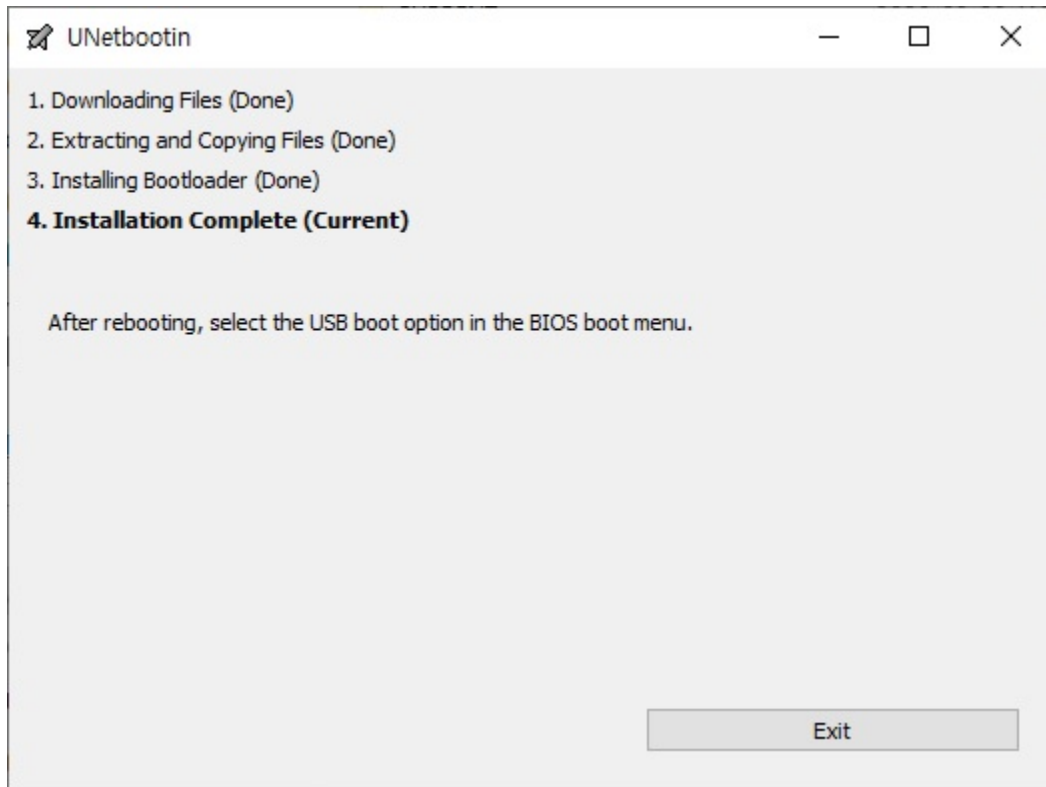
1. Diskimage 불러오기



2. 확인을 클릭하고 계속합니다.



3. 나가기를 클릭하십시오.



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

문제 해결 하기

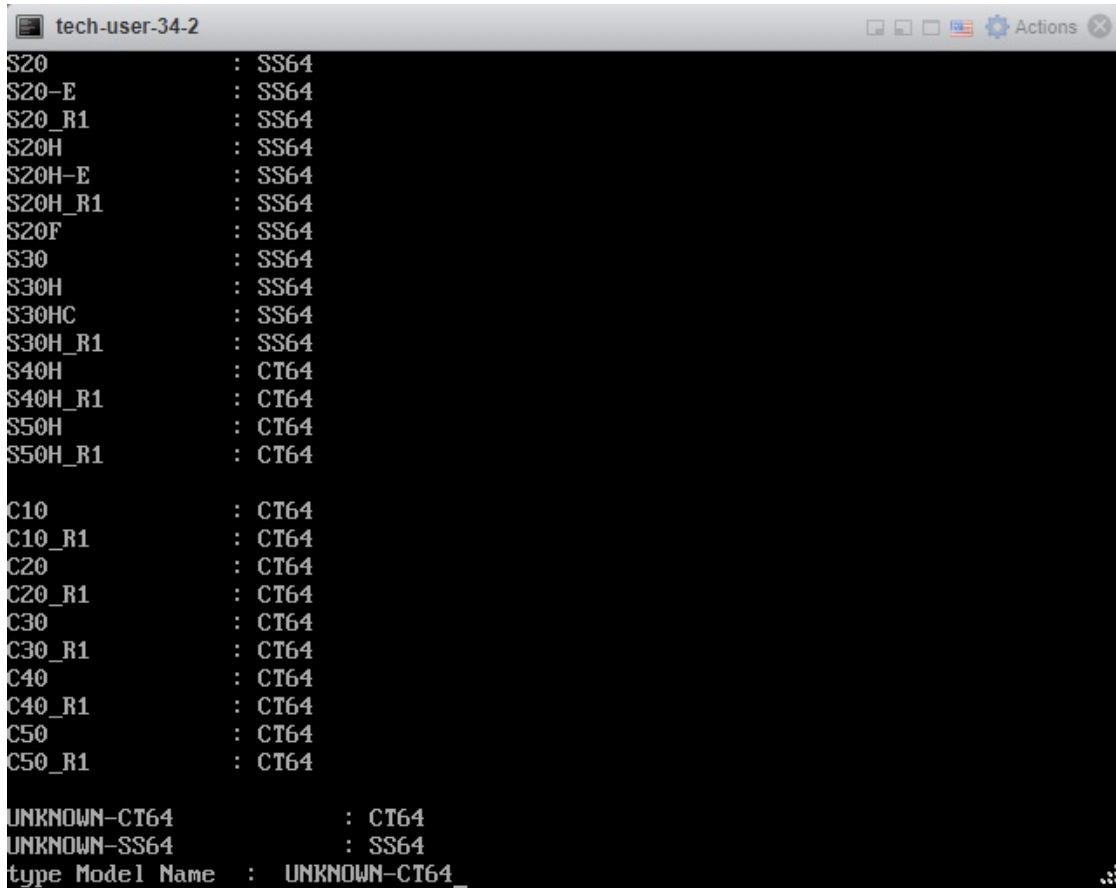
- 오류 메시지: "BOOTMGR is missing" indicative of improperly formatted USB drive.(잘못 포맷 된 USB 드라이브를 나타내는 "BOOTMGR 이 없습니다".)

Note:

NAC는 별도의 OS를 설치할 필요 없이 자체 OS로 설치됩니다.

3.1.5 정책서버 설치

1. 장비 부팅
 - 부팅 USB를 컴퓨터에 연결하십시오.
 - BIOS 설정에서 USB가 먼저 부팅되도록 부팅 순서를 변경합니다.
 - 가상 컴퓨터에서 설치 미디어의 ISO 파일을 선택하십시오. (가상 머신인 경우)
2. Genians에서 제공하는 Appliance가 아닌 자체 하드웨어 또는 가상머신에 제품을 설치하는 경우 **type Model Name** 에 "UNKNOWN-CT64" 을 입력합니다.



```
tech-user-34-2
S20 : SS64
S20-E : SS64
S20_R1 : SS64
S20H : SS64
S20H-E : SS64
S20H_R1 : SS64
S20F : SS64
S30 : SS64
S30H : SS64
S30HC : SS64
S30H_R1 : SS64
S40H : CT64
S40H_R1 : CT64
S50H : CT64
S50H_R1 : CT64

C10 : CT64
C10_R1 : CT64
C20 : CT64
C20_R1 : CT64
C30 : CT64
C30_R1 : CT64
C40 : CT64
C40_R1 : CT64
C50 : CT64
C50_R1 : CT64

UNKNOWN-CT64 : CT64
UNKNOWN-SS64 : SS64
type Model Name : UNKNOWN-CT64
```

3. “i” 를 입력하고, 기존 시스템이 있는 경우 y를 입력하여 삭제하고 진행하십시오.
4. 설치가 완료되면 미디어를 제거하십시오. (USB 또는 ISO파일)

```

tech-user-34-2
All rights reserved.
=====
Target Platform      : UNKNOWN-CT64
working target      : CT64
Install target       : CT64
Installation from    : /tmp/image

Target system information
version             : NAC-CT64-R-82402-5.0.25.1121
system disk         : /dev/sda1
log/data disk       : /dev/sda2
DB disk             : /dev/sda2
SSD disk            :
PATCH disk         :
SWAP disk           : /dev/sda3
=====

[il]install         : format all disk and install new software
[el]xit             : exit

Install or Exit ? (i/e) i
Delete old Data/Log DISK ? (y/N) y
Make filesystem: /dev/sda ... done
Install Product: /dev/sda1 ... done
Install BootLoader: /dev/sda ... done

Installation complete ....
Please remove installation media and reboot

Genians$ reboot

```

3.1.6 초기 구성

시스템이 재부팅 된 후 초기 설정을 수행해야 합니다.

1. 초기설정 방법 선택하기 ("1" 입력)
 - Interactive Wizard : 위자드를 이용하여 설정하는 방법입니다.
 - Manual Configuration : 수동 CLI 명령으로 설정하는 방법입니다.
2. 정책서버 동작형태 선택하기 ("1" 입력)
 - Single Server - Stand Alone : 단일서버로 동작하는 형태입니다.
 - Multi Server - Backend (Log/Database Server) : Log, DB(Backend)가 분리된 형태입니다.
 - Multi Server - Frontend (Node/Mgmt Server) : Node, Management(Frontend)가 분리된 형태입니다.
3. 언어 선택하기 ("2" 입력)
4. 웹 UI 및 SSH 연결을위한 관리자 계정 만들기
 - 관리자 계정 이름을 입력하십시오.
 - 관리자 계정 비밀번호를 입력하십시오.

```

tech-user-34-2
cat: can't open '/var/geni/etc/COMMUNITY': No such file or directory

Genian NAC Initial Configuration Tool

Press Ctrl+C if you want to restart the configuration process

1. Interactive Wizard
2. Manual Configuration

Select installation type: 1

1. Single Server - Stand Alone
2. Multi Server - Backend (Log/Database Server)
3. Multi Server - Frontend (Node/Mgmt Server)

Select Server Type: 1

1. English
2. Korean

Select System Language: 2

Enter administrator username (4-31 characters)

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

```

5. NTP 서버 설정

- NTP 서버 IP 또는 FQDN을 입력하십시오 (기본값은 *pool.ntp.org* 입니다).

6. 연결 유형 선택

Note:

네트워크 연결이 시스템의 첫 번째 인터페이스 (eth0)에 연결되어 있는지 확인하십시오.

- 인터페이스 eth0가 연결된 경우 액세스 포트 (일반 포트)
 - "n" 입력
- 인터페이스 eth0가 802.1Q 트렁크 포트에 연결되어있는 경우
 - "y" 입력
 - NAC 서비스 활성화를 위한 VLAN ID를 입력하십시오. (범위에 대해 쉼표 또는 AB로 연결됨, 예: 10,20-30)
 - 인터페이스 관리용 VLAN ID 입력
 - VLAN 센서 인터페이스는 기본적으로 DHCP 클라이언트로 설정됩니다.
 - 초기 설치 후 VLAN 인터페이스에 대한 정적 IP를 정의하려면 인터페이스 IP 주소 변경하십시오. 참고: 인터페이스 IP 주소 변경
 - 센서 인터페이스는 초기 설치 후 각 VLAN에 대해 구성되어야 합니다. : 네트워크센서 추가 및 삭제 를 참고하십시오.

```

tech-user-28-4
Select System Language: 2

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

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

Enter NTP server [pool.ntp.org]:

0. eth0
1. eth1

Select management interface: 0

Select the network connection method with the switch.

- ACCESS PORT: A typical network connection to only one subnet
- TRUNK PORT: Connect to multiple VLANs tagged by the 802.1Q standard.
                Switch configuration required

Is 'eth0' connected to 802.1Q trunk port (y/n) ? y

Enter the VLAN IDs you want to monitor (e.g. 20,30-35): 20

Enter VLAN ID for management interface: 20

# Network configuration for [eth0.20]

Enter IP Address: 1.1.1.1

```

7. 네트워크 구성

이 단계는 관리를 위해 인터페이스 IP 주소를 설정하는 것입니다.

- IP 주소 입력
- 넷마스크 입력
- 기본 게이트웨이 입력
- DNS IP 주소 입력 (선택으로 연결)

8. 모든 정보 확인

- 모든것이 올바른 경우. "y" 입력 및 시작
- 올바르지 않을 경우. "n" 입력 후 재설정


```

tech-user-34-2
# Network configuration for [eth0]
Enter IP Address: 172.29.48.210
Enter Netmask [255.255.255.0]:
Enter Default Gateway: 172.29.48.254
Enter DNS Server IP Address(es) (seperated by comma): 8.8.8.8
Do you want to enable 'eth0' as a wired network sensor (y/n) ? y

Configuration Summary
-----
Installation type:          Single Server - Stand Alone
System Language:           Korean
Administrator username:    admin
Timezone:                  Asia/Seoul
Monitored VLAN IDs:
Management interface:     eth0
  IP address:              172.29.48.210
  Netmask:                 255.255.255.0
  Default gateway:         172.29.48.254
DNS server IP address:     8.8.8.8
-----

Verify all information above.
If all is correct, type 'y' to start Genian NAC.
If not, type 'n' to start from the beginning. (y/n) ? y

```

7. Genian NAC 관리 UI에 로그인하십시오. 참고: 관리자 콘솔

3.1.7 지원되지 않는 하드웨어

자체 하드웨어에 설치가 정상적으로 진행이 되지 않는 경우 담당 파트너 엔지니어 또는 기술지원센터에 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 NAC 설치 중에 저장 장치, 이더넷 어댑터 또는 무선 LAN 어댑터와 같이 지원되지 않는 하드웨어가 있는 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

```

(continues on next page)

(continued from previous page)

```
$ lspci >> report.txt
$ lshw >> report.txt
```

4. report.txt 파일을 보내주세요.

3.2 소프트웨어 버전 정책서버 설치

Linux 배포판 중 Ubuntu 기반(18.04.05 LTS) 운영체제에서 동작할 수 있는 Genian NAC를 설치할 수 있습니다.

3.2.1 하드웨어 준비

물리적 시스템 또는 가상 시스템에 정책서버를 설치할 수 있습니다.

시스템 할당 자원(최소 요구사항)

최소 하드웨어 요구사항

- CPU : 2 core 이상
- 메모리 : 8192MB 이상
- 디스크 : 500GB 이상 권장

가상머신

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

3.2.2 사전준비

1. ISO 파일 준비

- 파트너 엔지니어 혹은 기술지원센터 를 통하여 ISO파일을 다운로드 받으시기 바랍니다.

2. H/W에 설치하는 경우, 부팅USB를 제작해주시기 바랍니다.

3.2.3 1. Ubuntu 서버 설치하기

Genian Appliance, H/W장비와 가상머신에 제공된 ISO파일을 이용하여 Ubuntu서버 설치를 진행할 수 있습니다.

Step 1: 장비 부팅

- **Genian Appliance**에 설치하기
 - Genian Appliance는 기본적으로 Ubuntu 서버와 NAC S/W가 설치되어있습니다.
 - **2. Genian NAC 정책서버 설정하기** 로 이동하여 NAC 정책서버 설정을 진행해주시기 바랍니다.
- **H/W** 혹은 가상머신에 설치하기
 - 다운로드한 ISO파일을 가상머신에 업로드합니다.

Step 2: 최초 Ubuntu 설치

Note: 유튜브를 통해 범용 OS 설치 가이드 영상을 확인할 수 있습니다.



1. Ubuntu 설치 언어, GENIANS Server, 언어, 설치국가, 키보드를 기본값으로 설정합니다.
2. 네트워크를 설정합니다.
 - 최우선 순위로 DHCP 서버를 통해 IP를 할당받는 과정이 진행됩니다. 자동 IP 할당 실패 시 수동 설정 혹은 네트워크 설정하지 않기를 선택할 수 있습니다.
 - 네트워크를 설치하지 않아도 정상적으로 설치가 가능합니다.
3. 호스트명과 사용자계정 및 암호를 생성합니다.
4. 타임존을 설정합니다.
5. 디스크 선택과 파티션 설정을 진행합니다.
6. Proxy 설정을 공란으로 입력하여 사용하지 않음으로 설정합니다.
7. 자동 업데이트 설정 화면에서 **No automatic updates** 를 선택합니다.
8. 추가 패키지 설치화면에서 **continue** 를 선택하여, 해당 과정을 통과합니다.
 - Installation step failed가 나오더라도, **continue** 를 선택하여 다음 과정으로 이동합니다.
9. 하드디스크에 GRUB 부트로더를 설치합니다.
 - 설치메뉴 화면에서 **Install the GRUB boot loader on a hard disk** 를 선택합니다.
 - 선택 후, GRUB 부트로더 설치화면에서 **YES** 를 선택하여 설치를 진행합니다.

위의 9단계가 완료되면 재부팅이 된 후, 아래의 화면과 같이 설치가 완료됩니다.

```

Ubuntu 18.04.5 LTS admin tty1
Hint: Num Lock on
admin login: genians
Password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0 )

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

genians@admin:~$
  
```

3.2.4 2. Genian NAC 정책서버 설정하기

단일구성 설정 방법을 기준으로 안내합니다.

Step 1: Ubuntu 및 Gnlogin 접속

설치가 완료된 후, 장비 초기설정을 위해 Ubuntu 및 Gnlogin 접속이 필요합니다.

```
genians login:
Password :
user@genians:~# sudo su
#root 권한을 획득합니다.
root@genians:~# gnlogin
#Genian Shell 진입
```

Note:

root 권한을 획득해야만 인터페이스 설정을 정상적으로 적용할 수 있습니다.

Step 2: 인터페이스 설정

장비의 기본 인터페이스를 설정합니다.

1. enable 명령어를 통해 글로벌 구성모드로 진입합니다.
2. configure terminal 명령어를 통해 설정모드로 진입합니다.
3. 인터페이스의 IP와 서브넷 마스크를 설정합니다.
4. 인터페이스의 기본 게이트웨이를 설정합니다.
5. 장비의 기본 게이트웨이를 설정합니다.
6. 장비의 DNS서버를 설정합니다.
7. 장비의 NTP서버를 설정합니다.

```
genian> enable
Password :
genian# configure terminal
genian(config)# interface [인터페이스명] address [IP] [Subnetmask]
genian(config)# interface [인터페이스명] gateway [IP]
genian(config)# ip default-gateway [IP]
genian(config)# ip name-server [IP]
genian(config)#ntp server [IP]
```

Step 3: Database 서버 설정

Database 서버 설정을 진행합니다.

1. DB 계정을 설정합니다.
2. DB 서버를 구동합니다.
3. DB 서버 접속 계정 패스워드를 설정합니다.
4. DB 접근 권한 설정합니다.

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

Step 4: LogServer 설정

Log 서버를 구동합니다.

```
genian(config) # log-server enable
```

시스템에 다중 인터페이스가 활성화되어 있는 경우, 로그서버 통신 인터페이스 설정이 필요합니다. 단일 인터페이스인 경우, 해당 설정을 하지 않아도 됩니다.

```
genian(config) # log-server publish-port [인터페이스명]
```

Step 5: WebUI, SopaServer 설정

1. WebUI를 구동합니다.
2. Soap 서버를 구동합니다.

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

Step 6: 관리자 계정생성

Genian NAC WebUI의 관리자 계정을 생성합니다. 최초 1회만 설정 가능합니다.

1. WebUI 계정을 생성합니다.

```
genian(config) # superadmin [관리자 계정] [관리자 패스워드] [관리자 이메일]
```

Note:

관리자 계정의 PASSWORD는 알파벳, 숫자, 특수문자를 포함하여 최소 9자 이상으로 설정해야 합니다.

Step 7: Debug 설정

1. 정책서버 디버그를 설정합니다.

```
genian(config) # debug centerd all
```

Note:

네트워크 센서 디버그 설정은 설치 완료 후, 정책서버 Web 콘솔을 통한 네트워크 센서 디버그 설정하기를 참고하여 WebUI에서 설정해주시기 바랍니다.

Step 8: WebUI 접속

위의 과정이 모두 완료되었다면, Genian NAC WebUI에 로그인하여 설치가 정상적으로 되었는지 확인해주시기 바랍니다.

Note:

WebUI 관련 정보는 관리자 콘솔 을 참고해주시기 바랍니다.

3.3 네트워크센서 설치

네트워크센서는 사용자의 내부 네트워크에 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.

Note: 클라우드 버전을 사용하는 경우에도 네트워크센서를 내부 네트워크에 설치해야 합니다.

3.3.2 네트워크 연결 준비

Genian NAC는 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 있어야 합니다.

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 가능해야 합니다.

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

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

무선 어댑터 호환성

Genian NAC와 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

continues on next page

Table 1 – continued from previous page

Vendor	Model Name	Chipset	Band	Type
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
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 액세스 포트를 통해 여러 세그먼트를 모니터링 할 수 있습니다.

Trunk Port

단일 인터페이스에서 여러개의 VLAN을 모니터링하려면 802.1Q 프로토콜을 사용하여 스위치 포트를 Trunk Port로 설정해야 합니다. 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
```

3.3.3 네트워크센서 설치

설치 프로세스는 정책 서버 설치와 동일합니다. 그러나 설치 2 단계에서 네트워크센서 2를 선택해야 합니다.

참고 정책서버 설치

3.3.4 초기 설정하기

시스템초기설정은 시스템이 구성된 이후 등록되는 모든 GENIAN 장비에 기본설정이 됩니다. 이를 통하여 추가로 등록되는 네트워크센서의 환경설정 및 네트워크센서설정을 별도로 변경하지 않아도 초기설정이 자동 반영됩니다.

장비 환경설정 자동으로 세팅하기

Genian NAC 장비가 최초 등록되면 관리자가 등록된 장비에 환경설정을 변경해야 합니다. 다수의 네트워크센서가 등록되는 환경이라면 초기 설정값을 지정하여 신규장비 등록 시 자동으로 환경설정이 적용되도록 할 수 있습니다.

1. 상단 패널에 시스템 으로 이동합니다.
2. 왼쪽 시스템 항목에서 시스템 초기설정 > 환경설정 을 선택합니다.
3. 환경설정 설정값 을 입력합니다.
4. 수정 버튼을 클릭합니다.

Note: 개별장비의 설정을 변경하기 위해서는 시스템 > 장비IP 선택 > 환경설정탭 에서 진행합니다.

보안설정

SSH를 통한 원격 액세스 허용

SSH 접속을 통한 CLI 콘솔 접속을 허용하는 IP를 2개 설정합니다. 일반적으로 관리자의 단말 IP를 지정합니다.

1. 보안설정에서 **CLI 콘솔 접속 IP** (예: 192.168.1.10)에 대해 **IP** 주소를 입력하십시오.
2. 수정을 클릭하십시오.

Windows 업데이트 프록시 설정

네트워크 센서에서 운영체제 업데이트 파일을 다운로드하도록 설정합니다. 네트워크 센서에 데이터 디스크가 존재할 경우에만 동작하도록 되어 있어, 데이터 디스크가 없는 경우에는 설정과 상관없이 동작하지 않습니다.

1. 운영체제 업데이트 **Proxy** 서비스설정을 찾아 **사용여부**를 찾아 드롭다운에서 **On**을 선택하십시오.
2. 프록시 서비스를 사용할 **대상 네트워크그룹** 선택하십시오.
3. 수정을 클릭하십시오.

SNMP 에이전트 설정

네트워크 센서의 시스템 정보를 외부에서 수집할지 여부를 설정합니다. 제공되는 정보로는 시스템 기본정보(이름, 설명, 업타임등), 인터페이스 정보, 시스템 상세정보(CPU, Memory, disk)가 있습니다.

1. **SNMP Agent** 설정을 찾아 드롭다운에서 **On**을 선택하십시오.
2. 다음을 입력하십시오.:
 - **Username**
 - **Auth Password** (SHA, 최소 길이 - 8자)
 - **Priv Password** 데이터 암호화 (AES, 최소 길이 - 8자)
3. 수정을 클릭하십시오.

자원경고

네트워크 센서의 자원(데이터 디스크, 메모리, CPU, 노드수)에 임계치 모니터링을 설정합니다. 임계치 이상으로 자원이 사용될 경우 감사기록을 통해 관리자에게 알람을 줄 수 있습니다.

1. **자원경고** 설정화면을 찾으십시오.
2. 다음을 입력하십시오.:
 - **데이터 디스크** 데이터 디스크가 이 설정값을 초과하면 로그 생성 (Default is 90)
 - **메모리** 메모리가 이 설정값을 초과하면 로그 생성 (Default is 90)
 - **CPU** CPU가 이 설정값을 초과하면 로그 생성 (Default is 95)
3. 수정을 클릭하십시오.

날짜 및 시간

네트워크 센서가 운영될 타임존을 설정합니다. (기본으로 Asia, Seoul로 설정되어 있습니다.)

1. 날짜 및 시간 설정화면을 찾으십시오.
2. 타임존 드롭다운에서 국가를 선택하고 가장 가까운 도시를 선택하십시오.
3. 수정을 클릭하십시오.

기타설정

네트워크 센서의 디버그 로그 설정과 노드의 UP/DOWN 상태 검사방식을 설정합니다. 데이터 디스크가 없는 네트워크 센서일 경우에는 디버그 로그 설정 시 무조건 정책서버에 저장됩니다.

1. 기타설정 설정화면을 찾으십시오.
2. 드롭다운에서 기본문자셋을 선택하십시오.
3. 수정을 클릭하십시오.

장비 센서설정 자동으로 세팅하기

정책서버에 추가되는 모든 네트워크센서에 대한 초기설정을 구성할 수 있습니다. 초기설정은 선택 사항이며 이후에 개별 네트워크센서에 대해 고유 설정은 각 센서에서 변경할 수 있습니다

Note: 개별장비의 설정을 변경하기 위해서는 시스템 > 장비IP 선택 > 환경설정탭 에서 진행합니다.

네트워크센서 초기설정

신규 등록될 네트워크센서의 초기 센서설정이 됩니다.

1. 상단 패널에서 시스템으로 이동
2. 좌측 패널에서 시스템 초기설정 > 센서설정 으로 이동하십시오.

센서동작

네트워크 센서가 동작하는 모드를 지정합니다. 네트워크 환경에 따라서 동작모드와 운영모드의 조합으로 다음과 같이 설정할 수 있습니다.

- 센서 모드를 Inactive, Mirror, Inline, 또는 Host(권장)로 설정 합니다.
- VLAN이 여러개인 경우 VLAN Interface 별로 센서가 구동되며, 각 VLAN Interface 별 센서에 대하여 모두 Host모드로 설정해야 합니다.

네트워크 센서 동작모드	네트워크 센서 운영모드	설명
Inactive	Monitoring / Enforcement	네트워크 센서 동작모드가 Inactive 설정일 경우에는 운영모드와 관계없이 네트워크 센서가 동작하지 않음
Host	Monitoring	네트워크 센서 관리범위 네트워크에 대해서 스캔만 수행, 네트워크 제어는 수행하지 않음(권장)
Host	Enforcement	네트워크 센서 관리범위 네트워크에 대해서 스캔과 네트워크 제어 수행(권장)
Mirror(local)	Monitoring	네트워크 센서 관리범위 네트워크에 대해서 트래픽 모니터링만 수행, 네트워크 제어는 수행하지 않음
Mirror(local)	Enforcement	네트워크 센서 관리범위 네트워크에 대해서 트래픽 모니터링과 네트워크 제어 수행
Mirror(Global)	Monitoring	네트워크 센서 동작하지 않음
Mirror(Global)	Enforcement	네트워크 센서의 관리범위가 아닌 IP 통신에 대해서 네트워크 제어 수행

Warning: 네트워크센서가 Enforcement 모드로 동작하면 네트워크가 즉시 차단될 수 있으므로 설정시에 주의하시기 바랍니다.

트래픽 모니터링

네트워크 센서가 Mirror(local) 동작모드로 운영될 경우 관리범위 네트워크에 트래픽 현황을 확인하도록 설정합니다.

노드등록

하나의 MAC당 최대 등록 가능한 노드수, 일정 비율 이상의 IP가 사용중이면 경고 설정이 가능합니다.

노드정보 검사

플랫폼 감지를 위한 포트스캔 및 서비스스캔 여부를 결정할 수 있습니다. NetBIOS 검사를 하거나 검사 주기를 변경할 수 있습니다.

네트워크 스캔

노드정보 검사 이외 추가적으로 정의된 스캔 항목에 수집 여부를 설정합니다.

노드상태 검사

위험감지 MAC+IP Clone 탐지를 수행하기 위한 상태검사를 설정합니다.

서브넷 노드스캔

노드스캔 주기, 초당 스캔 개수 등을 설정할 수 있습니다.

DHCP

DHCP 서비스 활성화 여부를 설정할 수 있습니다.

가상IP

사용하지 않는 IP를 위험 트래픽 유도용(허니팟) 가상 IP로 사용할 수 있습니다.

IP 관리

신규로 연결되는 노드에 대하여 차단여부를 설정하거나, 센서에 설정된 IP에 대해서 충돌보호 기능을 On / Off 할 수 있습니다.

기타설정

NAC의 관리대상에서 예외처리할 MAC을 지정할 수 있습니다.

센서 로그 설정 구성

1. 상단 패널에서 시스템으로 이동
2. 출력되는 화면에서 네트워크 센서 IP를 선택
3. 환경설정 클릭

기타 설정 참고

- 기본문자셋
- 센서 디버그로그 생성
-로그 저장 위치 - (로컬, 정책 서버, 로컬&정책 서버)

Note: 로그 위치가 정책서버에 저장되도록 설정된 경우 발생된 로그는 포트 6514를 사용하여 TLS를 통해 syslog에 의해 전송 됩니다.

TLS를 통한 syslog 전송이 실패하면, 표준 syslog 포트인 514 포트를 사용하여 전송 됩니다.

CLOUD NAC의 경우 랜덤 포트 가 사용됩니다. 시스템 > 서비스 관리 > 접속포트 에서 할당된 포트를 확인할 수 있습니다.

Genian Air-Sentry 환경설정 자동으로 설정하기

정책서버에 추가되는 모든 Genian Air-Sentry에 대한 초기설정을 구성할 수 있습니다. 초기설정은 선택 사항이며 이후에 개별 고유 설정은 개별 Genian Air-Sentry에서 변경할 수 있습니다.

Genian Air-Sentry 초기설정

신규 등록될 Genian Air-Sentry의 초기 센서설정이 됩니다.

1. 상단 패널에서 시스템 으로 이동
2. 좌측 패널에서 시스템 초기설정 > 무선센서 환경설정 을 선택합니다.

Genian Air-Sentry 동작

Genian Air-Sentry가 동작하는 모드를 지정합니다.

Genian Air-Sentry 운영 모드	설명
None	Genian Air-Sentry가 동작하지 않습니다.
Active	Genian Air-Sentry가 설정된 환경(AP모드, 정보수집, 무선제어)에 따라 동작을 수행합니다.

보안설정

Genian Air-Sentry Console 접속을 설정합니다.

항목	설명
CLI 콘솔 비밀번호	SSH / Serial 접속을 사용하여 연결되는 CLI(Command Line Interface)에 접속 비밀번호를 설정합니다.
SSH 접속 허용	SSH 프로토콜을 이용한 CLI(Command Line Interface) 접속 세션을 사용할 수 있게 설정합니다.

신호감도

Genian Air-Sentry가 수집하는 신호 세기 범위를 설정합니다.

Note: dBm 이란 mW(1/1000W) 단위의 전력을 dB 스케일로 나타낸 절대값 단위

항목	설명	예시
최소값	무선 네트워크 센서에서 수신하는 RSSI 값을 기준으로 신호를 수신할 범위를 설정합니다.(설정값은 음수처리 됩니다.)	1. 입력값 : 70, 설정값 : -70 2. 입력값 : 70 > 100
신호 변화 감지 범위	Genian Air-Sentry에서 업데이트 하는 RSSI 값 변동폭을 설정합니다.	1. 최소값 : 70, 신호 변화 감지 범위 : 10, 실제 신호변경 : 70 -> 80 (신호감도 최소값보다 작은 값으로 업데이트 안함) 2. 최소값 : 70, 신호 변화 감지 범위 : 10, 실제 신호변경 : 70 -> 60 (신호감도 최소값보다 높은 값으로 업데이트 처리)

유효시간

Genian Air-Sentry가 AP를 등록하는 최소 시간을 설정합니다.

정보갱신 주기

Genian Air-Sentry에서 정보를 최신으로 유지할 주기를 설정합니다.

항목	설명
AP 정보 갱신 주기	무선 네트워크 센서가 수집하는 AP 정보를 최신으로 유지할 주기를 설정합니다.
접속 단말정보 갱신 주기	무선 네트워크 센서가 수집하는 접속 단말정보를 최신으로 유지할 주기를 설정합니다.

무선제어

무선 네트워크 접속 시 Deauthentication 패킷을 사용하여 접속을 차단할 무선 네트워크 대상을 설정합니다.

무선랜카드 설정

Genian Air-Sentry가 AP로 동작할 무선 네트워크를 설정합니다.

항목	설명
주파수 대역	Genian Air-Sentry가 AP로 동작할 경우 사용할 수 있는 주파수 대역을 설정합니다.(2.4GHz만 제공)
무선모드	무선 전송방식 표준 형태를 설정합니다. #. 802.11b : 2.4GHz 대역 전파를 사용, 최고 전송속도 11Mbps를 제공 #. 802.11n : 2.4GHz / 5GHz 대역 전파를 사용, 최고 전송속도는 600Mbps 제공 #. 802.11ng : 2.4GHz 대역 전파를 사용, 최고 전송속도는 54Mbps 제공
채널	주파수 대역폭을 20MHz 기준으로 나눈 채널을(1~13, Auto) 설정합니다.

자원 경고

Genian Air-Sentry의 자원(메모리, CPU)에 임계치 모니터링을 설정합니다. 임계치 이상으로 자원이 사용될 경우 감사기록을 통해 관리자에게 알람을 줄 수 있습니다.

3.4 관리자 콘솔

Genian NAC는 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 NAC

1. 웹 브라우저를 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 브라우저를 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://nac.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 추가해야 합니다.

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 정책서버의 설치 방식에 따라 다릅니다. 각각의 설치 방식별 포트 정보는 아래와 같습니다.

- On-Premises 포트 정보 : 3910
- 소프트웨어 NAC 포트 정보 : 22
- Cloud managed : 클라우드 정책서버는 SSH CLI 콘솔을 제공하지 않습니다.


```
#On-premises CLI 콘솔 접속
ssh "정책 서버 관리 IP" -p 3910 (e.g. : ssh 192.168.50.10 -p 3910)

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

Note:

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

2. Web 콘솔에서 SSH 접속을 통한 CLI 콘솔 접속

1. 상단 패널에 시스템 으로 이동합니다.
2. 왼쪽 시스템 항목에서 시스템관리 를 선택합니다.
3. SSH 접속 대상 IP주소 오른쪽  아이콘을 클릭합니다.
4. 팝업창에 Username, Password를 입력하여 SSH 접속을 수행합니다.

3.5 라이선스 설치

Genian NAC가 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 설치해야 합니다. 평가판 라이선스 페이지로 이동하여 30 일 동안 Professional / Enterprise Edition을 체험 할 수 있는 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 시스템을 클릭하십시오.
2. 왼쪽 시스템 패널에서 시스템 > 라이선스로 이동하십시오.
3. 서버 ID 확인

3.5.2 평가판 라이선스 받기

1. 평가판 라이선스 페이지
2. 서버 ID 섹션을 찾아 정책 서버에 있는 서버 ID를 추가하십시오.
3. 전체 이름, 회사 이름, 이메일을 입력하십시오.
4. 시범 사용권 얻기를 클릭하십시오.
5. —BEGIN CERTIFICATE— 부터 —END CERTIFICATE— 까지 라이선스를 복사하십시오.

3.5.3 라이선스 설치

1. 상단 패널의 시스템을 클릭하십시오.
2. 왼쪽 시스템 패널에서 라이선스로 이동하십시오.
3. 라이선스 등록 클릭하여 라이선스 파일을 업로드 하거나 복사 & 붙여넣기합니다.
4. 적용을 클릭 하십시오.

3.6 에이전트 설치

Genian NAC는 엔드포인트의 시스템 정보수집, 액세스 제어, 사용자 인증 뿐만 아니라 엔드포인트의 보안상태를 점검하는 역할을 수행합니다. 이를 위해 Windows 및 macOS에 에이전트를 수동 설치하거나 에이전트 미설치 차단정책을 통해 에이전트를 자동 설치하기도 합니다. 설치 이후 엔드포인트의 보안정책 점검, 준수를 위해 정책서버와 통신합니다.

3.6.1 Windows Agent 설치

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

Windows 에이전트 설치

- 에이전트 다운로드 페이지를 통해 다운로드 및 설치
- CWP를 통한 에이전트 설치
- Active Directory GPO를 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 실행해야 합니다.

CWP를 통한 에이전트 설치

에이전트를 설치하지 않으면 제어 정책에 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 NAC Agent for Windows** 항목 우측의 MSI 버튼을 클릭하면 MSI 설치패키지가 다운로드 됩니다.

Note: Genian NAC 5.0.38 이상 버전은 *Active Directory GPO*정책을 이용한 에이전트 배포 과정을 바로 진행합니다

Genian NAC 5.0.37 이하 버전은 아래 MSI 파일 설정문서 에서 MSI파일 수정 과정을 진행한다음 배포를 진행합니다.

MSI 파일 설정

Genian NAC 5.0.37 이하버전의 정책서버에서 다운로드 받은 MSI 설치파일은 Microsoft Orca를 사용하여 정책 서버IP 설정을 해야합니다.

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 Installers 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.

MSI 파일에 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 IP나 Domain Name 입력"
 5. 저장 & 종료
-

Active Directory GPO 정책을 이용한 에이전트 배포

Note: 로그인한 계정의 권한이 사용자권한일 경우 에이전트가 제대로 작동하지 않을 수 있으며 로컬 시스템 계정으로 에이전트 수행 계정을 변경해야 합니다.

아래 순서에 따라 노드정책 에이전트의 수행계정을 수정합니다.:

1. 상단 패널의 정책으로 이동합니다.
2. 노드 정책으로 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(Group 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 패키지를 클릭합니다
- (예: [도메인]공유폴더)와 같은 공유 폴더 경로로 이동합니다. 폴더 권한을 인증됨 = 읽기, 도메인 컴퓨터 = 읽기, 시스템 = 모든 권한 으로 설정 합니다.
- 에이전트 MSI 파일 선택 > 소프트웨어 배포 팝업 에서 고급 선택
- 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 메시지 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 수행 해야합니다)
 - **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)	v5.0.x
Microsoft Windows XP Sp3 (32bit Only)	N/S
Microsoft Windows Vista	N/S
Microsoft Windows 7	5.0.3~
Microsoft Windows 8	5.0.3~
Microsoft Windows 8.1	5.0.3~
Microsoft Windows 10	5.0.3
Microsoft Windows 11	5.0.43~
Microsoft Windows Server 2003	N/S
Microsoft Windows Server 2008	5.0.3~
Microsoft Windows Server 2012 (64bit Only)	5.0.3~
Microsoft Windows Server 2016	5.0.3~
Microsoft Windows Server 2019	5.0.3~

3.6.2 macOS 에이전트 설치

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

macOS 에이전트 설치

1. 에이전트 다운로드
 - [https://\(IP 또는 도메인 \)/agent](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	v5.0.x
OS X Lion	10.7	N/S
OS X Mountain Lion	10.8	N/S
OS X Mavericks	10.9	5.0.0~
OS X Yosemite	10.10	5.0.0~
OS X El Capitan	10.11	5.0.0~
macOS Sierra	10.12	5.0.1~
macOS High Sierra	10.13	5.0.12~
macOS Mojave	10.14	5.0.16~
macOS Catalina	10.15	5.0.26~
macOS Big Sur	11.0(M1 포함)	5.0.38~
macOS Monterey	12.0(M1 포함)	5.0.42~
macOS Ventura	13.0(M1 포함)	5.0.42, 5.0.47~
macOS Sonoma	14.0(M1 포함)	5.0.55~

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 NAC에서 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://정책서버IP/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 실행해야 합니다. 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.
 - 설치 경로: /usr/share/genians
 - 로그 경로: /var/log/genians
 - 설정 파일 경로: /usr/share/genias/GenianDB
 - PID 파일 경로: /var/run/genians

Linux 에이전트 지원 OS 목록

Linux OS	버전	v5.0.41 이상
Ubuntu	18 ~ 22	5.0.41~
Gooroom	2 ~ 3	5.0.41~
HamoniKR	3.0 ~ 4.0	5.0.41~
Tmax Gooroom	2, 21	5.0.47~
Hancom Gooroom	2 ~ 3	5.0.47~

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 그룹을 생성하여 에이전트를 삭제할 노드를 추가 하십시오.
2. 노드 정책을 생성하여 선택한 노드에서 에이전트를 삭제 하십시오.
 - 아래: 노드정책에서 에이전트 정책 항목 메뉴의 Delete 옵션을 설정합니다.
3. 노드 정책을 작성한 후 오른쪽 상단의 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 NAC 관리자에게 제공하여 **인증 코드** 를 요청하십시오.
4. 제공받은 **인증 코드** 를 입력하고 **삭제** 버튼을 클릭하십시오.

관리자 인증코드 발급 :

1. 정책서버 관리 WebUI에 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 NAC 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.

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 NAC는 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 설정하기 위한 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 NAC에서 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

네트워크노드 및 장비

노드는 IP주소와 MAC주소의 조합으로 구성된 NAC의 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 NAC는 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 NAC는 네트워크센서 또는 에이전트를 통해 네트워크의 노드를 감지합니다. 네트워크센서는 네트워크 상에 발생하는 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 연결되었는지 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 발생하는 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

네트워크 센서는 WMI 쿼리를 Windows로 보낼 수도 있습니다. 노드는 하드웨어, 소프트웨어 및 네트워크 속성에 대한 정보를 수집합니다.

WMI 노드 정보 스캔

수집 능력

하드웨어

- 마더보드
 - Chassis 타입
 - 제조사
 - CPU 제품명
 - CPU 제조사
 - 리비전
 - 배터리
- 메모리 정보
 - 총 메모리 크기
 - 메모리 사용량
 - 메모리 사용량(%)
- 저장 장치
 - 장비 이름
 - 장비 타입

- Unique #
- 파일 시스템
- 용량
- 사용량
- 사용량(%)
- **USB 장치**
 - 클래스 이름
 - 장치 이름
 - 제조사
 - 상태
- **운영체제**
 - 운영체제 이름
 - 버전
 - 빌드 버전
 - 서비스 팩
 - 최근 업데이트 시간
 - 언어
 - 사용자
 - 조직
 - 컴퓨터 이름
 - 도메인
 - 설치 시간
 - 가동 시간
- **사용자**
 - 사용자 이름
 - 계정 유형
 - 비밀번호 설정
 - 로그인 상태
- **화면 보호기**
 - 활성화/비활성화
 - 비밀번호 설정
 - 대기 시간
 - 이름

네트워크

- 상호 작용
- 이름
- 연결 방법
- MAC
- 장치 이름
- 링크
- 속도
- 난잡
- **IPV4 설정**
- 이름
- IPV4
- IP/넷마스크
- 게이트웨이
- 1차/2차 DNS
- **IPV6**
- 이름
- IPV6
- IPV6 주소
- IPV6 링크 로컬

공유 폴더

- 공유 폴더 이름
- 타입
- 경로
- 감지 시간
- 세부사항

프린터

- 이름
- 장치 이름
- 포트 정보

소프트웨어

- 소프트웨어 정보
 - 프로그램 이름
 - 버전
 - 경로
 - 설치 일자
 - 탐지 시간

WMI 노드 정보 수집 구성

전체 조건 설정 구성

1. 대상 노드가 도메인에 가입되어 있는지 확인하십시오.
2. 엔드포인트/도메인 계정이 WMI 쿼리에 응답하도록 허용합니다.
3. 권한이 있는 도메인 계정에 대한 Bind DN 및 Bind 비밀번호를 입력하십시오. 설정->사용자인증->인증연동->LDAP 인증연동

WMI 스캔 활성화

1. 시스템 탭으로 이동하여 원하는 센서를 선택합니다.
2. 센서관리 탭을 선택한 후 설정을 진행할 인터페이스를 선택합니다.
3. 노드정보 검사 아래에서 포트/서비스 스캔을 활성화 한 다음 WMI 정보검사를 활성화 시킵니다.

Note: WMI 스캔은 에이전트가 설치되지 않은 노드에서만 동작 합니다. 에이전트를 통해 정보를 수집하려면 Windows 시스템 WMI정보 수집을 참고 하십시오.

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 NAC는 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 비즈니스 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 식별해야 합니다. Genian NAC는 네트워크에서 IT 장치를 식별하고 CVE를 표시하여 네트워크 관리를 보다 쉽게 할 수 있습니다.

장비 플랫폼을 찾는 방법

Genian NAC는 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 NAC는 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 NAC는 장비 플랫폼을 탐지하기 위해 자체 플랫폼 데이터베이스(GPDB)를 사용하고 있습니다. GPDB는 장비 정보와 일치하는 다양한 패턴을 통해 플랫폼이 정확하게 감지 되도록 합니다. 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 노드의 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 추가해야 합니다.

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

아래에서 기본정보 탭

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

알 수 없는 / 잘못된 플랫폼 감지 보고

어떤 이유로 Genian NAC가 장비의 플랫폼을 감지 할 수 없는 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 NAC는 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 클릭 합니다.

- **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 탭**으로 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 상단에 있는 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 수 없는 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 드롭**으로 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
 - **IP** 관리뷰
 - 위험뷰
 - 운영체제 업데이트뷰
 - 자산관리뷰
 - 에이전트액션뷰
 - 인증사용자뷰
 - 장치사용 관리뷰
 - 장비수명주기 관리뷰

세부 정보 찾기

1. 상단 항목에서 **관리 > 노드** 로 이동합니다.
2. 노드의 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
 - **IP**관리
 - 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
 - 노드 이름
 - 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, 사용자에게 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. 노드의 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 **드롭다운**항목의 **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 **노드리스트**에서 확인합니다.

Note: 설정된 태그 모두 삭제를 선택하여 노드에서 모든 태그를 제거합니다.

MAC에 대한 태그 해제

1. 상단 패널의 **관리 > 노드** 로 이동합니다.
2. 노드의 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 NAC는 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 파일을 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.

<p>Warning: 네트워크에 연결되고 동작 중인 노드를 실수로 삭제하면 해당 노드가 즉시 새롭게 등록 됩니다.</p>
--

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 30일)
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 3일입니다.)
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 틀입니다. 정책에는 사용할 수 없습니다.

노드바구니에 추가

1. 상단 관리 > 노드 이동
2. 원하는 노드를 찾아 좌측 체크박스에 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 변경되거나 확인된 노드타입은 지정된 형태로 유지됩니다.

4.2.6 노드 그룹 관리

노드 그룹 만들기

노드 그룹은 노드들의 그룹으로 특정 조건 기반의 유사함이 있습니다. 노드 그룹을 사용하면 여러 노드에 대해 동일한 작업을 동시에 수행할 수 있습니다. Genian NAC는 노드정책 및 제어정책에 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 정책을 클릭 하십시오.
2. 왼쪽 정책 항목에서 그룹 > 노드 로 이동합니다.
3. 작업선택 > 정책그룹 생성 또는 작업선택 > 상태그룹 생성 을 클릭합니다.

아래 기본정보를 설정합니다.

1. **Category** 의 경우 기본값 또는 새로 만들어 사용합니다.(Node Groups를 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: 추가를 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 NAC는 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 NAC에서 수집하는 정보 중 노드와 관련된 세부정보와 정책현황을 표시할 수 있습니다. 노드 상세 정보는 네트워크 센서에 의해 수집되는 정보와 에이전트에 의해 수집되는 정보, 노드가 적용받는 정책으로 나뉘지며 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), TCP 세션 (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 NAC에서 생성할 수 있는 노드그룹은 타입은 노드정책 전용 노드그룹(정책그룹)과 일반 노드그룹(상태그룹)으로 나뉩습니다.

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	NAC에서 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	NAC에서 분류한 노드타입을 기반으로 그룹을 생성합니다.
등록여부	정책서버에 등록된 노드를 기반으로 그룹을 생성합니다.
등록일자	NAC에 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	NAC 에이전트의 설치/동작 기반에 그룹을 생성합니다.
인증사용자	NAC의 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	NAC에서 정의한 정책을 기반으로 그룹을 생성합니다.	IP관리, 노드그룹, 노드정책, 인증사용자, 태그, 호스트명 제한
센서 정보	네트워크 센서에서 수집한 정보를 기반으로 그룹을 생성합니다.	노드타입, 서비스, 센서, 업/다운상태, 열린포트, 운영체제유형 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
장비 정보	장비에 설정한 정보를 기반으로 그룹을 생성합니다.	장비명, 장비설명, 제조일, 구입처, 내용연수 시작일, 내용연수 만료일 일련번호, 구입가격, 책임자, 책임부서, 메모
추가 설정 정보	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 이름/설명, 장비내 무선랜, 장비소유자, 접속AP, 접속장치/접속포트, 플랫폼 보안취약점

4.3 IP 주소 모니터링

네트워크센서는 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 항목에서 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 뷰를 통하여 IP 사용량과 현재 상태를 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 마우스를 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, 사용자 등 얼마나 많은 장치가 연결되어 있는지 확인 할 수 있습니다.

4.4.1 스위치 찾아보기

스위치를 식별하기 위해 Genian NAC는 SNMP 요청을 전송합니다. 요청에 대한 응답이 OID(dot1dBaseBridgeAddress(1.3.6.1.2.1.17.1.1.1))로 반환되는 경우 Genian NAC는 MAC 주소를 스위치의 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. 수행주기의 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. 검색주기의 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 NAC 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-SNMP로 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 필드**에 입력 하십시오.
5. 수정 버튼을 클릭 하십시오.

4.4.2 스위치 포트

스위치 포트 찾아보기

스위치 포트 목록은 네트워크에서 감지된 모든 스위치 포트에 대한 자세한 정보를 제공합니다. 스위치 포트 목록은 왼쪽 상단에 있는 **스위치 관리** 항목으로 이동한 후 스위치 포트를 클릭하면 볼 수 있습니다.

스위치 관련 정보

1. **관리 > 스위치** 로 이동 하십시오.
2. 원하는 스위치 이름을 찾아 클릭합니다.
3. 다음과 같은 정보를 찾습니다.
 - **스위치** - 스위치 호스트명
 - **이름** - 스위치 포트 번호
 - **설명** - 스위치 포트 설명
 - **접속사용자** - 연결된 스위치 포트를 통해 인증된 사용자의 전체 이름
 - **접속호스트** - 연결된 스위치 포트를 통해 확인된 단말의 호스트명
 - **IP/MAC** - 스위치 포트를 통해 연결된 IP/MAC 정보
 - **노드** - 스위치 포트를 통해 연결된 노드의 수
 - **MACs** - 스위치 포트를 통해 연결된 MAC 의 수
 - **연결방식** - 스위치 포트를 통해 연결된 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 트래픽 (byte/s)
 - **Utilization** - 스위치 포트 이용률 %
 - **VLAN ID** - 포트에 할당된 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 > 노드뷰**에 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 ID**를 입력합니다.
2. **수정** 을 클릭합니다.

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

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 전체스위치포트를 선택합니다.
3. 확인하고 싶은 포트의 이름을 클릭합니다.

항목	설명
스위치명	스위치를 구분하는 이름이 표시됩니다.
이름	스위치 포트의 이름이 표시됩니다.
포트#	포트 번호를 표시합니다.
설명	NAC에서 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 과부하가 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 포트에 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 네트워크 센서는 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 SSID를 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 네트워크 센서에 무선NIC가 있거나 엔드포인트에 무선랜 제어 플러그인이 활성화된 에이전트가 설치되어 있어야 합니다.

네트워크에서 탐지된 모든 SSID 보기

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)** 열에서 숫자를 클릭합니다.
 - 이제 MAC 주소에 대한 모든 접속정보를 보고 **외부/내부** 보기를 변경할 수 있습니다.
 - 검색창을 사용하여 특정 접속정보를 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** 주소를 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.

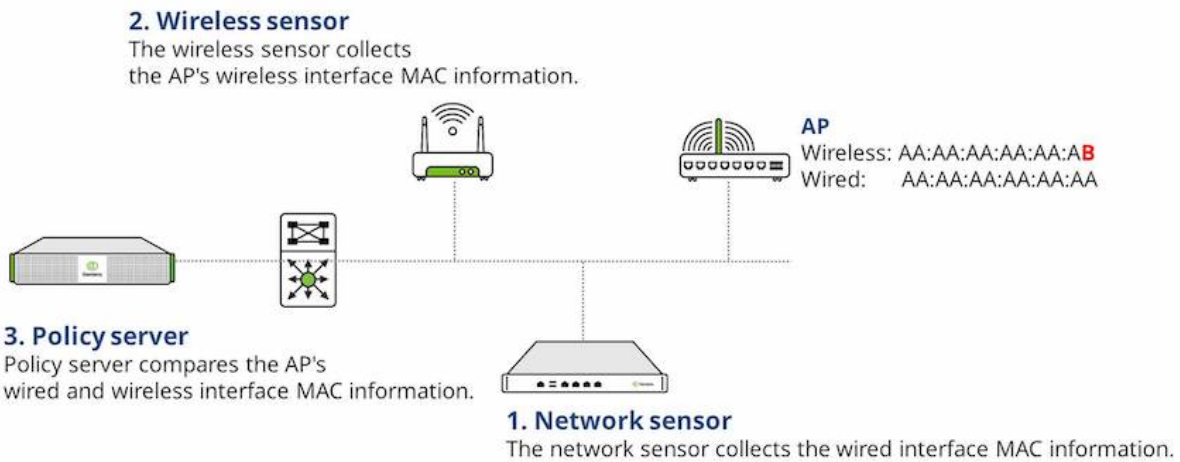
내부 SSID 표시

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

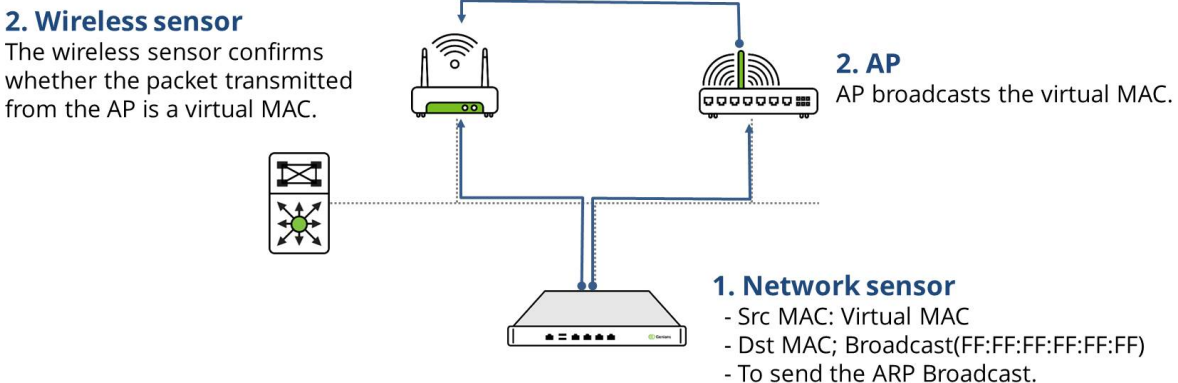
Agent와 무선센서에 의해 탐지된 AP는 내부적으로 연결된 AP에 의해 여러 기준에 의해 구별될 수 있습니다. 내부 AP 감지 방법은 다음과 같습니다.

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 그룹은 식별자로 설정된 조건 또는 속성으로 인해 함께 그룹화된 **SSID**의 감지된 수량입니다. 이는 네트워크 관리자가 대량의 **SSID**를 처리할 때 특정 **SSID** 또는 **카테고리**로 신속하게 이동할 수 있도록 하기 위한 것입니다.

무선랜 그룹 생성

무선랜 그룹을 생성하여 **SSID**를 더 효율적으로 분류할 수 있습니다.

1. 상단 항목에서 정책로 이동하십시오.
2. 그룹 > 무선랜으로 이동하십시오.
3. 작업선택 > 생성을 클릭하십시오.

아래 기본정보에서:

1. 그룹ID를 생성하기 위한 고유의 이름을 입력합니다.
2. 설명의 경우 이 그룹을 구성하는 내용에 대해 입력합니다.
3. 적용모드의 경우 드롭다운에서 **사용함**을 선택합니다.
4. 감사로그의 경우, **SSID**가 그룹에 추가될 때 로그를 생성하려면 **On**을 설정합니다.

그룹조건에서 다음을 수행합니다.

1. 조건연산의 경우 모든 조건을 일치하기 위해 **AND**를 선택하고, 특정 조건에 일치하기 위해서는 **OR**를 선택하십시오.
2. 조건설정에서 추가를 클릭하여 조건을 추가합니다.

조건설정에서 다음을 수행:

다음은 **SSID**를 식별할 수 있도록 해주는 조건부 설정입니다.

1. 항목의 경우 **MAC**, **프로토콜**, **SSID**, **보안 설정**, **태그** 등을 선택할 수 있습니다.
2. 조건의 경우 다음과 같거나, 같거나, 포함하지 않거나, 포함하지 않는 등의 항목을 선택할 수 있습니다.
3. 설정의 경우 검색한 값과 일치하는 값을 입력합니다.
4. 설정메모의 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, 밴드, 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 그룹을 만들고 해당 국가에 있는 무선랜 센서를 추가할 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	인증 방법	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 암호화 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 NAC에서 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.
신 호 강 도 (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 벤더	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	NAC 사용자 인증 시 인증된 사용자 이름이 표시됩니다.
부서명	NAC 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 NAC는 123개의 위젯을 제공합니다.

4.6.1 대시보드 추가

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

1. 메인화면 상단 우측 항목의 **대시보드 설정** 으로 이동합니다.
2. **설정 > 대시보드 탭** 추가 를 클릭 하십시오.
3. 대시보드 탭 추가 창에서 **탭 이름** 을 찾고 **고유의 이름** 을 입력합니다.
4. 대시보드 탭 추가 창에서 **탭 종류** 및 **대시보드 레이아웃** 을 선택 하십시오.
5. **확인버튼** 을 클릭 하십시오.

4.6.2 대시보드 삭제

1. 메인화면 상단 우측 항목의 **대시보드 설정** 으로 이동합니다.
2. 원하는 대시보드 탭을 클릭합니다.
3. **설정 > 대시보드 탭** 삭제 로 이동 하십시오.
4. **확인버튼** 을 클릭 하십시오.

4.6.3 대시보드 위젯을 추가

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

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. 톱니 바퀴 아이콘을 클릭하면 해당 위젯의 설정이 표시됩니다. 완료되면 **저장**을 클릭하여 설정 변경 사항을 위젯에 적용 할 수 있습니다.

4.6.6 위젯 삭제

1. 메인화면 상단 우측 항목의 **대시보드 탭** 로 이동 하십시오.
2. 위젯 을 찾아 제목 표시 줄 위로 마우스를 가져갑니다.
3. **X** 버튼을 클릭 하십시오.
4. **확인** 버튼을 클릭 하십시오.

4.6.7 센서 맵 만들기

Google Maps를 사용하여 전세계에 센서 배치를 모니터링하고 사용자 정의합니다.

1. 메인화면 상단 우측 항목의 **대시보드 설정** 으로 이동 하십시오.
2. **설정 > 대시보드 탭** 추가 를 클릭 하십시오.
3. 대시보드 탭 추가 창에서 **탭 이름** 을 찾고 고유의 이름을 입력합니다.
4. 대시보드 탭 생성창에서 **탭 종류** 를 찾고, **센서 맵** 을 선택 하십시오.
5. 생성 된 **센서 맵** 탭을 클릭 하십시오.
6. 화면 오른쪽 위치에서 **설정** 아이콘 을 찾으십시오. **관심노드그룹 지정**을 클릭 하십시오.
7. 관심노드그룹 창에서 **노드 그룹** 을 찾습니다. 추가할 노드 그룹을 더블 클릭 하십시오.
8. **저장** 버튼을 클릭 하십시오.

4.6.8 센서 맵에 센서 배치

1. 메인화면 상단 우측 항목의 **대시보드 설정** 으로 이동 하십시오.
2. Sensor Map (센서 맵) 탭으로 이동합니다.
3. 화면 오른쪽 위 모서리에 있는 메뉴 찾기 아이콘을 클릭 하십시오.
4. 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 이동 하십시오.
2. 내보 낼 **대시보드 탭** 을 선택합니다.
3. **내보내기** 를 클릭하고 출력 형식(*PDF / DOCX / PPTX*)을 선택합니다.

4.6.10 사용자 정의 위젯 생성하기

기존 정의된 위젯이 아닌 사용자가 정의한 위젯을 추가할 수 있습니다. 사용자 정의로 생성할 수 있는 항목은 위젯 코드 기반과 URL 기반에 위젯이 존재합니다.

HTML 페이지와 URL을 기반으로 Genian NAC에서 제공하지 않는 형태의 위젯을 생성하거나, 외부 Web 페이지를 모니터링 할 수 있습니다.

위젯코드 기반 사용자 정의 위젯 생성하기

위젯코드 기반으로 생성되는 위젯은 HTML Code 값을 기반으로 설정합니다. HTML로 작성된 페이지 소스를 입력하여 해당 페이지가 위젯으로 동작하도록 합니다.

1. 메인화면 상단 우측 항목의 **대시보드 설정** 으로 이동합니다.
2. **설정 > 위젯 추가** 를 클릭 하십시오.
3. 위젯 추가 창에서 위젯 카테고리 항목을 찾습니다. **사용자 정의** 항목을 선택합니다.
4. 위젯 추가 창에서 **사용자정의 위젯 추가** 버튼을 클릭합니다.
5. 위젯 추가 창에서 위젯구분 항목을 **위젯코드기반** 으로 선택합니다.
6. 위젯을 구분할 **위젯명** 을 입력합니다.
7. 위젯을 설명할 **설명** 을 입력합니다.
8. 위젯을 이미지로 구분할 **이미지 URL** 에 이미지 파일을 업로드 합니다.(선택사항)
9. 위젯을 출력할 **위젯 옵션** 을 입력합니다.(선택사항)
10. 위젯에 표시할 내용을 **위젯코드** 에 입력합니다.

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

11. **생성** 버튼을 클릭합니다.

URL 기반 사용자 정의 위젯 생성하기

URL(Uniform Resource Locator) 값을 기반으로 위젯을 설정합니다. 위젯으로 표현할 URL을 입력하여 해당 페이지가 위젯으로 동작하도록 합니다.

1. 메인화면 상단 우측 항목의 **대시보드 설정** 으로 이동합니다.
2. **설정 > 위젯 추가** 를 클릭 하십시오.
3. 위젯 추가 창에서 **위젯 카테고리** 항목을 찾습니다. **사용자 정의** 항목을 선택합니다.
4. 위젯 추가 창에서 **사용자정의 위젯 추가** 버튼을 클릭합니다.
5. 위젯 추가 창에서 **위젯구분** 항목을 **위젯코드기반** 으로 선택합니다.
6. 위젯을 구분할 **위젯명** 을 입력합니다.
7. 위젯을 설명할 **설명** 을 입력합니다.
8. 위젯을 이미지로 구분할 **이미지 URL** 에 이미지 파일을 업로드 합니다.(선택사항)
9. 위젯을 출력할 **위젯 옵션** 을 입력합니다.(선택사항)
10. 위젯에 표시할 페이지를 **URL** 에 입력합니다.
11. 위젯에 표시할 URL에 파라미터가 존재할 경우 **기본 파라미터** 를 입력합니다.

`https://www.genians.com`

12. **생성** 버튼을 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. **관점**, **카운트사이즈**, **이름사이즈**, **추이차트**, **타이틀**, **화면갱신주기**, **높이**를 설정합니다.
8. **저장** 버튼을 클릭합니다.

Note: 유튜브를 통해 WEB UI를 통한 네트워크 자산 모니터링에 대한 교육 영상을 확인할 수 있습니다.



네트워크 접근제어

Note: 이 기능을 사용하려면 Professional 또는 Enterprise Edition이 필요합니다.

네트워크센서 및 에이전트를 통해 수집된 정보를 기반으로 정책을 설정하여 미준수 단말의 네트워크 사용을 제한할 수 있습니다. 제어 정책은 다양한 방식으로 적용될 수 있습니다. Genian NAC는 다음과 같은 방법을 제공합니다.

5.1 접근제어 정책의 이해

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

Note: 유튜브를 통해 정책생성 교육 영상을 확인할 수 있습니다



5.1.1 IP/MAC 정책

IP/MAC 정책은 관리자가 수동 또는 자동으로 장치의 IP사용을 제어할 수 있습니다. 또한 IP와 MAC을 기반으로 네트워크 액세스를 제어합니다.

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

IP관리를 사용하여 네트워크접근 제어 준비

IP관리에 의해 거부된 IP관리 정책을 변경하여 적용이 가능하도록 설정하고 개별 네트워크센서 IP관리 정책을 변경할 수 있습니다.

IP 관리 차단정책 활성화

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

1. 상단 항목의 정책 으로 이동합니다.
2. 왼쪽 정책 항목의 제어정책 으로 이동합니다.
3. 제어정책 창에서 IP 관리 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 NAC는 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

(IP관리 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 주소를 클릭 하십시오.
4. 설정 탭 그리고 센서설정을 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 > 노드로 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 추가MAC주소를 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 NAC관리범위 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.(노드상 세화면 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 사용 가능합니다.)
 - **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 **MAC 허용 - 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 **MAC 허용 - 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 액세스 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 **IP 허용 - 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 **IP 허용 - 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. **IP**정책 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. **MAC**정책 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
IP 사용신청서	IP 사용신청	CWP 페이지에서 IP 사용신청 버튼에 대한 표시부분을 설정합니다.
	IP 신청서 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.
	IP 신청서 등록권한	신청서 등록 권한을 할당할 대상을 설정합니다.
	IP 다중신청서 양식	다수의 신청서를 신청할 경우 사용할 수 있는 신청서 양식을 업로드 합니다.
IP 신청시스템 화면설정	IP 신청서 처리결과 자동알림	신청자에게 처리결과를 전송하는 방법을 선택합니다.
	신청시스템 메뉴	신청시스템에서 사용할 수 있는 메뉴를 설정합니다.

2. IP 관리기능 사전 설정하기

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

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

항목	설명	참고
IP/MAC 사용 만료 처리방법	사용시간이 만료된 IP/MAC에 대한 노드 삭제여부를 설정합니다.	시간 기준의 IP/MAC 허용
특수정책 우선	특수정책(시간제한, 충돌보호, 변경금지)에 대한 우선순위를 설정합니다.	<ol style="list-style-type: none"> 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 생성해야 합니다.

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 액세스하는 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 밀그림이 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 액세스를 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 이해해야 합니다.)

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 80의 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 순위 는 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 알림 메시지	사용자에게 알림 메시지를 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 알림 메시지	사용자에게 알림 메시지를 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 체크박스를 클릭합니다.
4. 작업선택 > 삭제 를 클릭합니다.
5. 우측 상단의 변경정책적용 을 클릭합니다.

5.1.4 무선랜 정책

무선랜 정책은 프로파일(AP, Client)을 배포하는 역할과 **Genian Air-Sentry** 로 접속하는 대상이 네트워크에 액세스하는 것에 대해 허용/차단하는데 사용됩니다.

무선랜 정책에서 접근제어 기능을 사용하기 위해서는 **Genian Air-Sentry** 가 필요합니다.

무선랜 정책 설정하기

무선랜 정책을 통해 다수의 **Genian Air-Sentry** 에 적용할 프로파일을 관리할 수 있으며, 무선 네트워크 사용 대상에 대한 접근제어를 적용할 수 있습니다.

기본정보 설정하기

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

항목	세 부 항 목	설 명	비 고
기본 정보	SSID	무선연결을 위한 SSID(Service Set Identifier)를 설정합니다.	AP, 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

AP 정책 설정하기

Genian Air-Sentry 를 대상으로 동작하는 정책을 설정합니다.

항목	세부항목	설명	비고
AP 정책	AP 프로파일	Genian Air-Sentry 를 대상으로 적용할 AP 프로파일을 지정합니다.	무선 네트워크 센서 AP 프로파일 적용하기
	적용대상	프로파일과 접근제어를 적용할 Genian Air-Sentry 를 지정합니다.	
	동작시간	AP로 동작할 시간객체를 지정합니다.	
	접근제어	Genian Air-Sentry에서 적용할 접근제어 권한을 지정합니다.	권한 생성하기

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 생성해야 합니다.

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

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

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-Station-Id	접속한 장비 (AP)의 MAC
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 사용자에게 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 AAA 프로파일의 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

continues on next page

Table 2 – continued from previous page

속성 항목	설명	예시
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 ACL 명	
Cisco-AVPair(url-redirect)	Redirect 주소	http(s)://IP or DOMAIN
Cisco(AVPair)	Cisco AVPair 속성	문자열
Filter-ID	접속장비에 설정된 ACL 명	
NAS-Filter-Rule	ACL 리스트 설정	permit in tcp from any to any
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 NAC는 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.

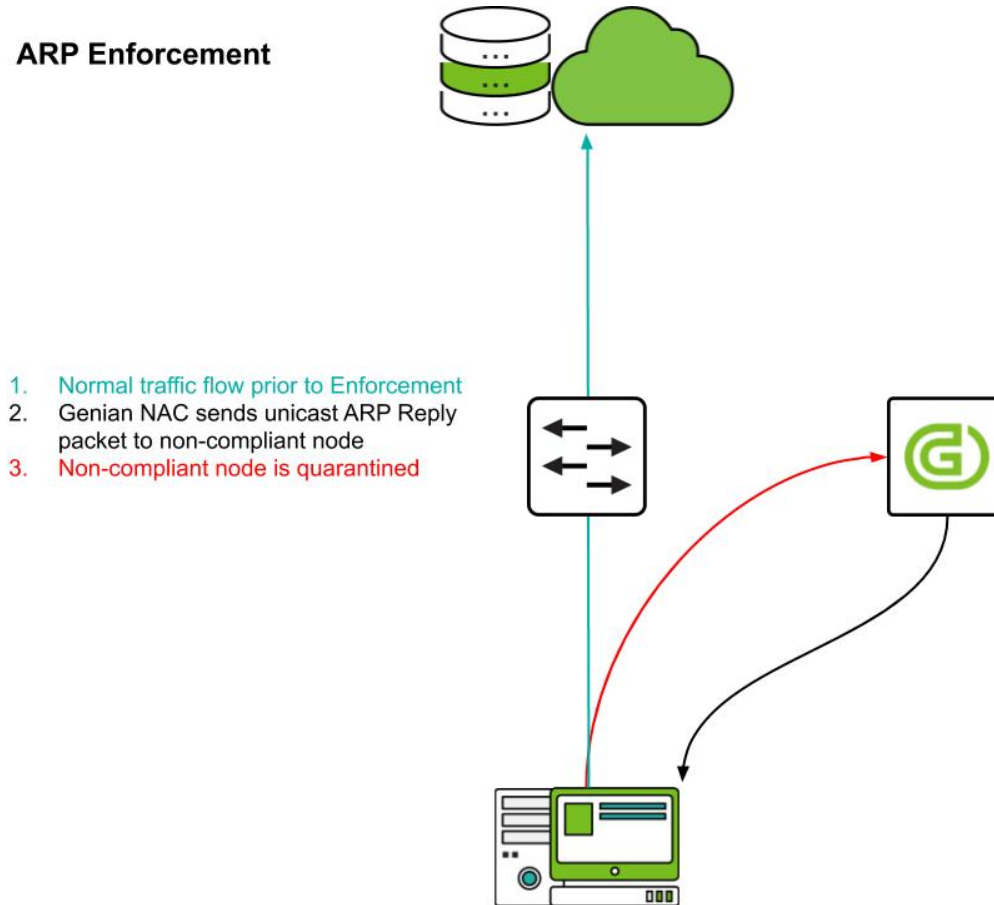
또한 모든 네트워크 장비가 802.1x를 지원하지 않기 때문에 연결된 각 스위치 포트에 수동 구성이 자주 필요합니다. 거대한 엔터프라이즈 네트워크에서 각 스위치 포트에 대한 802.1x에 대한 예외 또는 MAC 주소를 설정하면 매우 큰 관리 문제가 야기되어 배포 및 관리에 매우 오랜 시간이 걸릴 수 있습니다.

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 적용할 수 있도록 ARP 프로토콜의 특성을 사용합니다.

Genian NAC는 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.

ARP Enforcement



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 NAC에서는 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

- RADIUS 서버 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)

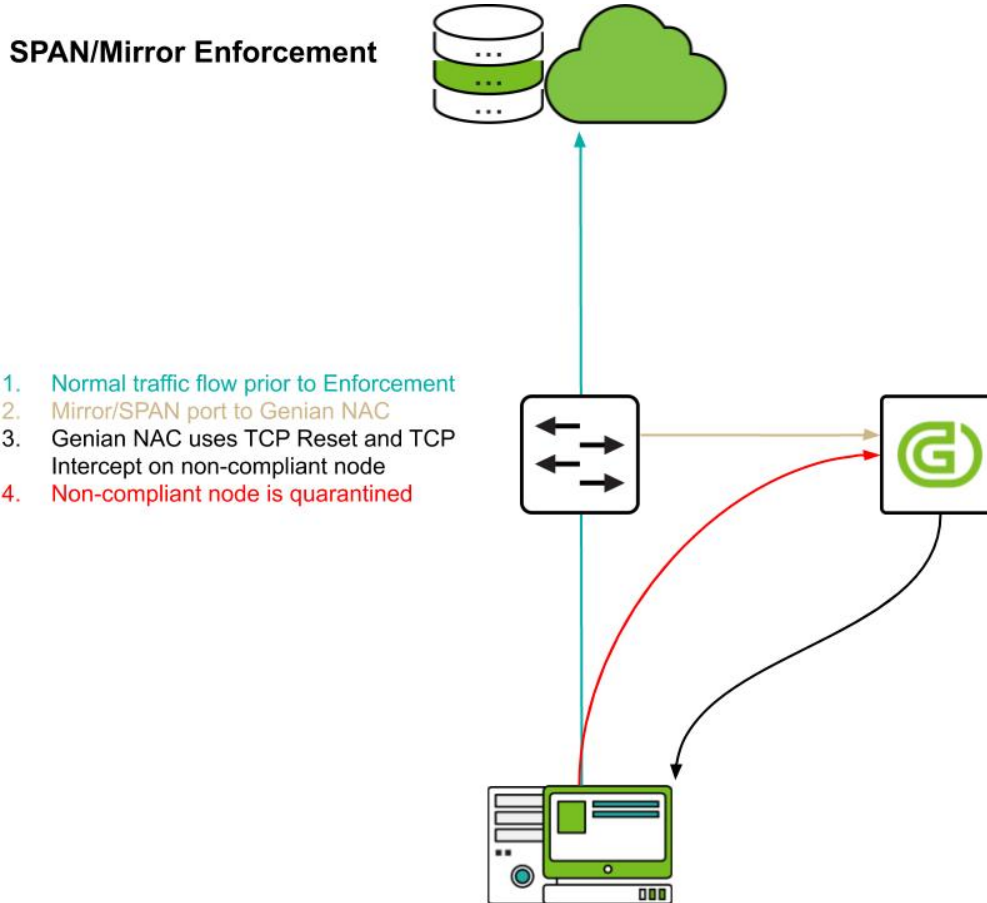
Genian NAC에는 RADIUS 서버가 내장되어 있어 802.1x 및 ARP 변조를 통해 패킷을 센서로 경유시키고, 사용하는 네트워크 환경에 따라 이를 선택 할 수 있습니다.

5.2.2 포트 미러링 (SPAN)

Genian NAC는 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 NAC에 트래픽을 전송해야 합니다.

Genian NAC는 두 가지 유형의 포트 미러링 모드를 제공합니다.



글로벌 미러 센서

글로벌 미러 센서는 Genian NAC에 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 제어할 수 있습니다. 이 문제를 해결하기 위해 각 최종 네트워크에 설치된 네트워크 센서에 미러링 포트를 추가할 수 있습니다. 이를 통해 로컬 네트워크 내에서 발생하는 연결을 제어할 수 있습니다.

로컬 미러 센서는 네트워크 센서 장비에서만 감지되고 기존 노드에 대한 제어만을 수행하기 때문에 글로벌 미러 센서와 비교할 때 상대적으로 낮은 사양의 하드웨어에서 작동할 수 있습니다.

5.2.3 802.1x (RADIUS)

802.1x 포트 기반 접근 제어는 엔터프라이즈 무선랜 환경에 적용할 수 있는 가장 이상적인 접근 제어 방법입니다. 사용자 기반 인증을 사용하면 권한이 부여된 사용자만 네트워크에 액세스할 수 있습니다. 또한 단말의 보안준수 상태에 따라 특정 VLAN에 연결하거나 연결된 상태를 강제로 해제할 수 있습니다.

802.1x를 지원하는 사용자 단말, 802.1x 지원 액세스 포인트(AP) 또는 스위치와 같은 네트워크 액세스 장비 및 RADIUS 서버가 필요합니다. Genian NAC는 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 참조하십시오.

격리 VLAN

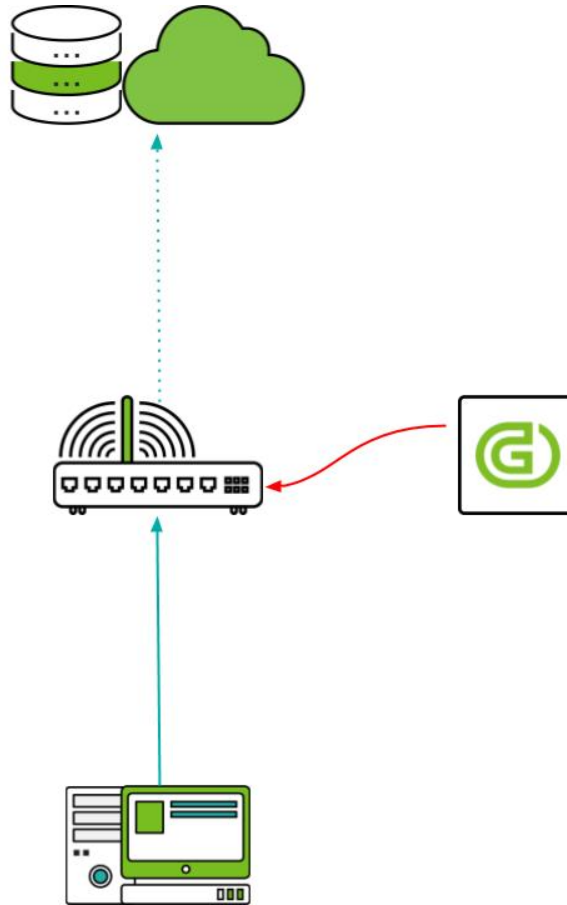
802.1x가 가능한 액세스 포인트(AP) 또는 스위치가 RADIUS *Tunnel-Private-Group-ID* 속성을 지원하면 장치의 상태에 따라 특정 VLAN에 대한 액세스를 제어할 수 있습니다. RADIUS 서버가 사용자 인증 성공 결과를 전송하면 이 속성이 추가되어 전송되고 액세스 포인트 또는 스위치는 VLAN ID를 수신하고 해당 VLAN ID를 액세스 포트에 할당합니다.

Change of Authorization(CoA)

단말 상태 변경으로 인해 네트워크 접근을 제한해야 하는 경우 RADIUS CoA (권한 변경)를 사용하여 단말의 접속상태를 종료시킬 수 있습니다. 연결이 끊긴 단말은 새 연결을 시도하고 이 때 분리된 VLAN에 연결하여 단말을 네트워크에서 안전하게 분리합니다. 이렇게 하려면 액세스 지점 또는 스위치가 RADIUS에 대한 표준 (*RFC 5176 - Dynamic Authorization Extensions*)을 지원해야 합니다.

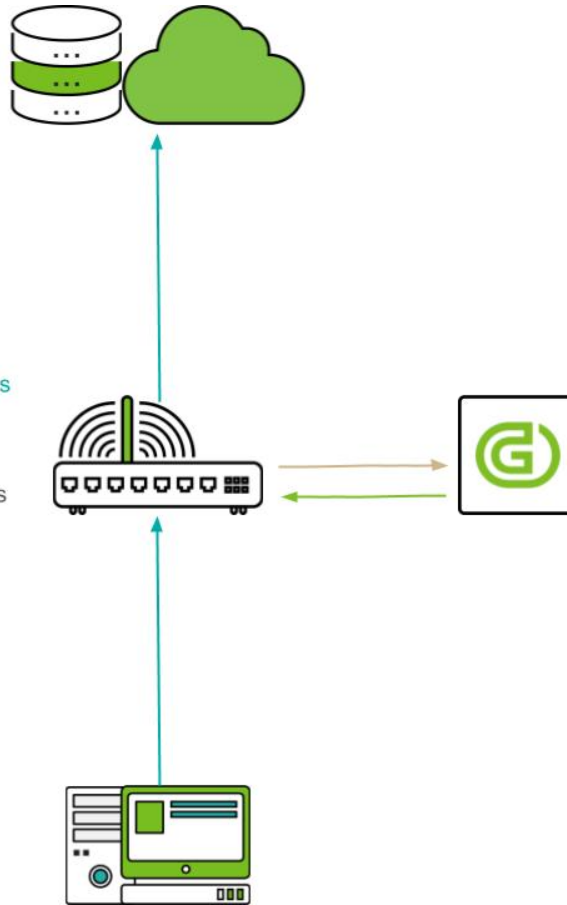
RADIUS Enforcement CoA

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



RADIUS Enforcement VLAN Assignment

1. Node connects to wired or wireless 802.1X / WPA2E network
2. Authentication Request is sent to Genian Radius Server
3. Authentication and Authorization is performed
4. Genian NAC Radius returns appropriate VLAN



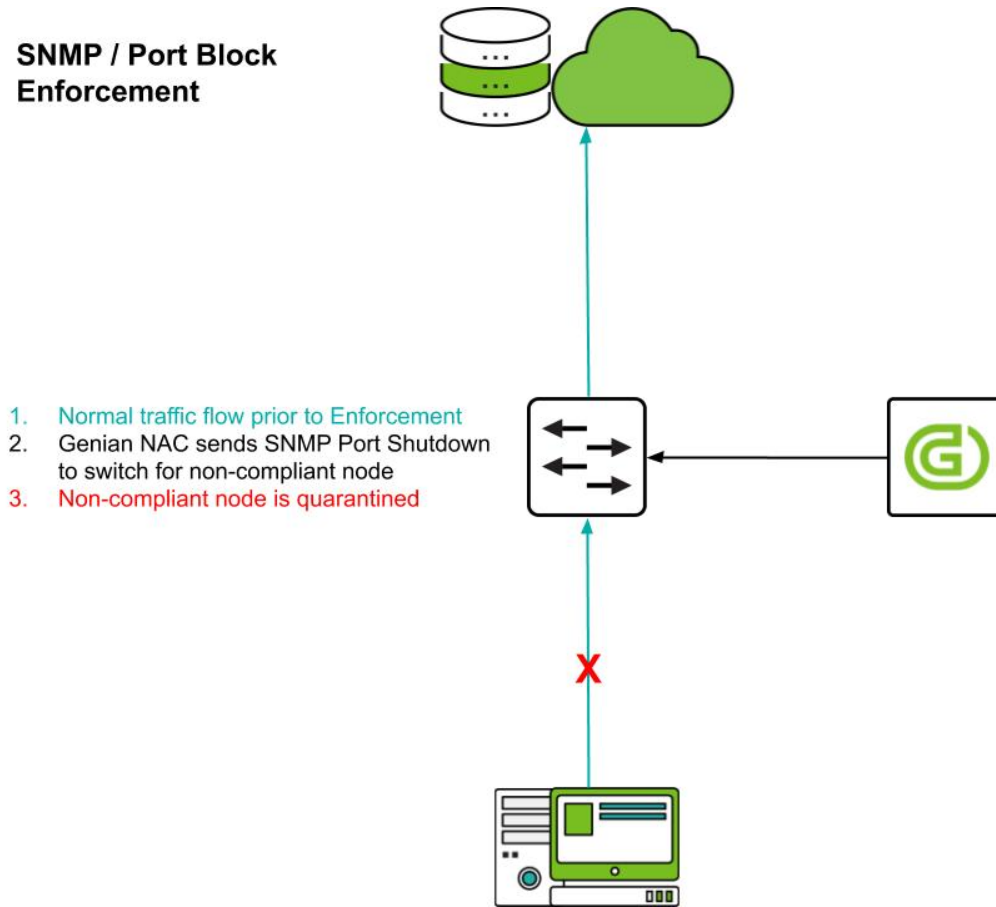
5.2.4 DHCP

Genian NAC는 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 NAC는 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 제공해야 합니다.

SNMP / Port Block Enforcement



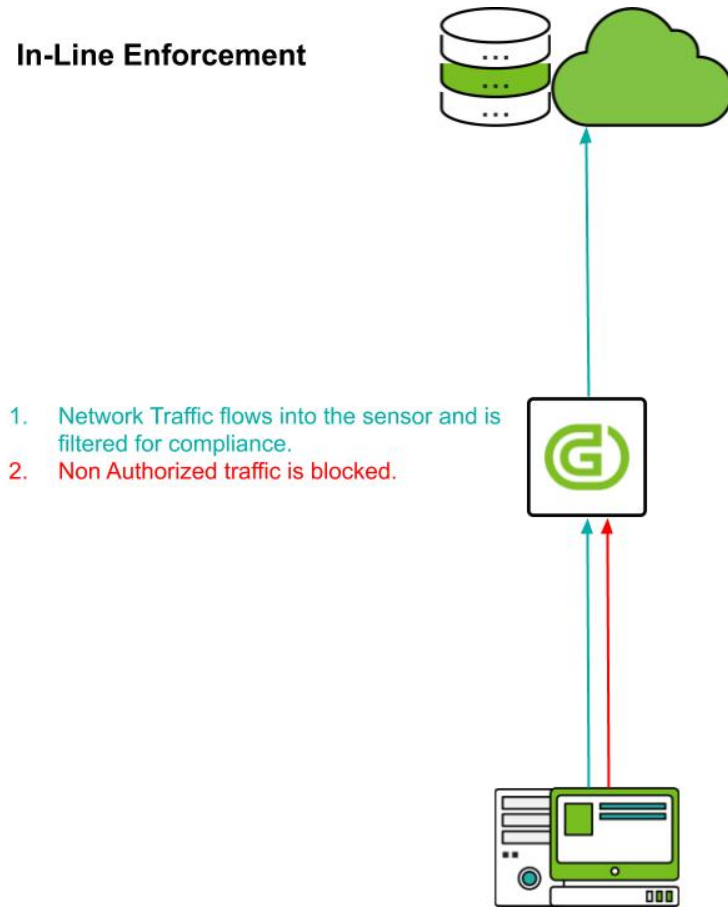
5.2.6 인라인 패킷 필터링

적용 정책에 따라 지정된 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 허용된 패킷만 전송하기 때문에 보안이 강화됩니다. 그러나 인라인 장비는 통과하는 모든 패킷에 대해 보안 정책 검사를 받아 패킷 전송 지연을 유발할 수 있습니다. 또한 인라인 장비를 통과하지 않는 패킷에는 접근 제어 정책을 적용할 수 없습니다. 따라서 배포하기 전에 설치 위치를 주의해야 합니다.

인라인 패킷 필터링의 경우 네트워크 센서 소프트웨어는 두 개 이상의 네트워크 인터페이스가 있는 하드웨어에 설치해야 합니다. 설정을 통해 센서 작동 모드가 'Inline'으로 설정되면 보안 정책이 수신된 패킷에 적용된 다음 라우팅 테이블에 따라 시스템의 다른 인터페이스로 전달됩니다.

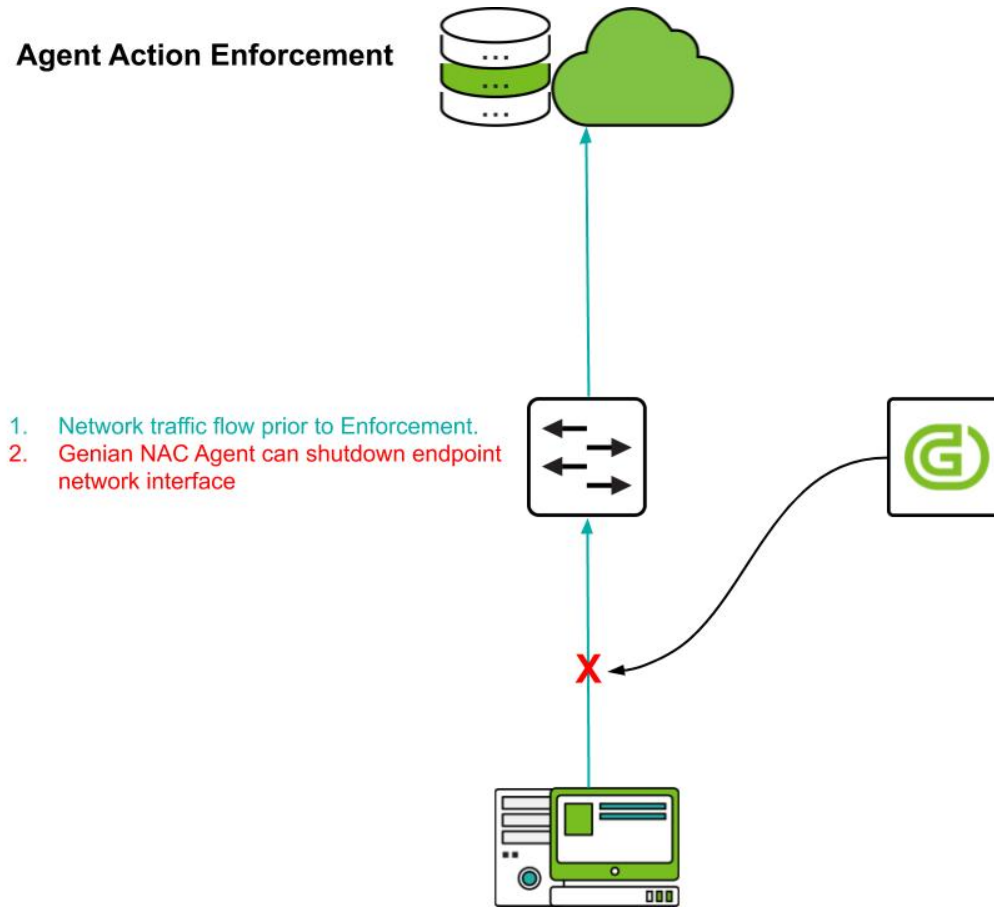
In-Line Enforcement



5.2.7 에이전트 액션

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

Agent Action Enforcement



5.3 ARP 제어 설정


네트워크센서는 기본적으로 네트워크의 트래픽을 수신하도록 구성되어 있으며 정책 서버로 전달되는 정보를 수동으로 수집합니다. 수집된 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.

Note: ARP 제어는 IDS 또는 EDR 제품에서 보안 경고를 발생시킬 수 있고, NAC의 APR 제어를 차단할 수 있습니다. 참조 : *arp-enfoce* 실패

5.3.1 ARP 제어 설정 방법

네트워크센서를 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 설치해야 합니다.

5.4.2 로컬 미러(Local Mirror)

Monitoring 모드 센서와 함께 사용하면 더 많은 정보를 수집할 수 있습니다. **Monitoring** 모드 센서와 동일한 장비에서 사용할 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** 주소를 선택합니다.
4. **설정 탭 > 센서 설정** 를 클릭합니다.
5. 미러 모드에서 사용할 인터페이스를 클릭합니다. **eth1** 이 인터페이스에 할당된 IP가 없습니다.
6. 센서 동작 모드에서 **Mirror** 를 선택합니다.
7. 미러 동작범위에서 **Local** 을 선택합니다.
8. 센서 운영모드의 경우 **Enforcement** 로 변경합니다.
9. 수정 버튼을 클릭합니다.

Note: 로컬 미러는 트래픽 모니터링 기능을 추가로 사용할 수 있습니다.

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

5.5 RADIUS 제어 설정

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

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

또한 RADIUS 서버는 장비정보를 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, 액세스포인트 등)를 인증하기 위해 미리 공유된 비밀번호를 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 NAC 사용자에게 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 RADIUS 서버의 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. 이것은 IEEE 802.1 네트워크 프로토콜 그룹의 일부입니다. LAN 또는 Wireless LAN 에 연결하려는 단말에 인증 메커니즘을 제공합니다.

802.1X 인증에 필요한 3가지 구성요소: 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 바뀌어도 사용 됩니다.

인증자는 이더넷 스위치 또는 무선 AP 와 같은 네트워크 장비입니다. 인증자는 보호된 네트워크에 대한 보안 감시 역할을합니다. 요청자는 신원이 확인되고 승인 될 때까지 인증자로 인해 보호 된 네트워크에 접근 할 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. 인증서 서버가 자격 증명 유효하다고 판단하면 요청자(사용자 단말)는 네트워크의 보호 된쪽에있는 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 > RADIUS 서버 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 > RADIUS 서버 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 OS 기본 제공사항이 아니기 때문에 Genian NAC 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 > RADIUS 서버 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 nac.genians.com, FQDN(정규화된 도메인 이름) 또는 IP와 같은 일반 이름을 입력 합니다. (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 인증서의 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 등록된 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 제공되어야 합니다.

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 NAC는 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 이 세가지를 말한다. 엔드포인트가 네트워크에 인증(authenticate)되면 수행하는 권한 부여(Authorization)은 선택적 사항이다.

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

Genian NAC RADIUS 서버는 인증 후 VLAN을 할당하는 인가를 지원합니다. RADIUS 서버 외부의 Genian NAC에서도 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 NAC는 네트워크에 연결할 때 장치의 속성을 지정할 수 있는 기능이 제공됩니다. 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. 조건설정을 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-Info, NAS-Port-ID, Aruba-User-Role, Aruba-Essid-Name* 등의 RADIUS 속성을 사용할 수 있습니다.

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

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 제한하거나 거부할 수 있습니다. 이것은 CoA(Change of Authorization, RFC 5176 - RADIUS 표준에 대한 동적 인증 확장)라는 표준을 통해 제공 됩니다.

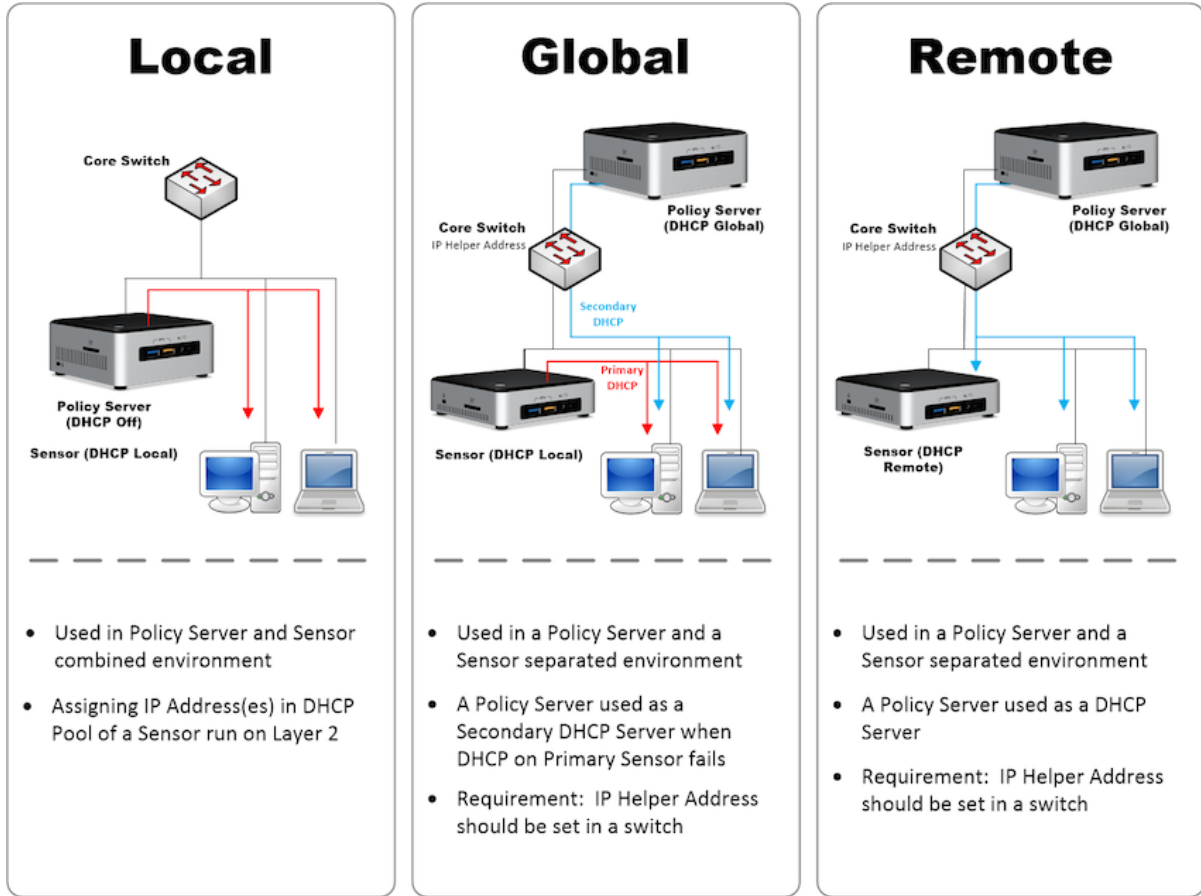
CoA는 제어 정책이 변경된 단말에 대한 현재 연결을 끊습니다. 연결이 끊어진 단말은 다시 연결을 시도한 다음 VLAN 할당을 통해 격리 된 VLAN으로 이동합니다.

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 NAC는 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

```
genian# 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 VLAN 설정에 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 설정해야 합니다.

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 개수의 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 포트를 종료할 수 있습니다.

1. 상위 항목의 **관리 > 스위치**로 이동합니다.
2. 전체 스위치포트 관리 뷰에서 이름을 클릭합니다.
3. 관리자 **Down** 옆의 체크박스를 클릭합니다.
4. 수정 버튼을 클릭합니다.

5.7.3 제어정책의 스위치 VLAN 설정

스위치포트 VLAN 설정 대상은 제어정책에 따라 결정 됩니다. 특정 노드의 스위치 포트에 대한 VLAN을 설정하려면 해당 노드를 대상으로 하는 제어정책을 생성한 다음 스위치 VLAN 설정 옵션을 설정해야 합니다.

노드의 스위치 포트 이동에 따른 VLAN 설정을 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 적용할 제어정책의 원하는 **ID**를 클릭합니다.

제어옵션 > 스위치포트 제어 에서 아래와 같이 설정합니다.

1. 스위치포트 제어 옵션을 **VLAN 설정**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.

Genian NAC는 다양한 보안 벤더와 통합되어 보안 인텔리전스를 구축할 수 있습니다.

5.8.1 Cisco VPN 연동 가이드

이 가이드는 CISCO VPN 제품과 네트워크 접근제어 시스템인 Genian NAC의 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 NAC는 내부보안 관리를 위해 내부네트워크에 존재하는 단말에 대하여 가시성 확보, 사용자 권한별 네트워크 접근제어, 단말의 보안정합성 제어방안을 제공합니다.

각각의 솔루션이 제공하는 기능을 연동하여, VPN 접속자에게 Genian NAC의 기능으로 구현된 보안정책에 만족하는지 체크 후 VPN 접속을 허용하기 위하여 본 연동을 진행하였습니다.

연동의 목적

Genian NAC와 CISCO VPN의 연동은 다음을 목적으로 합니다.

VPN 접속단말의 보안정합성 체크

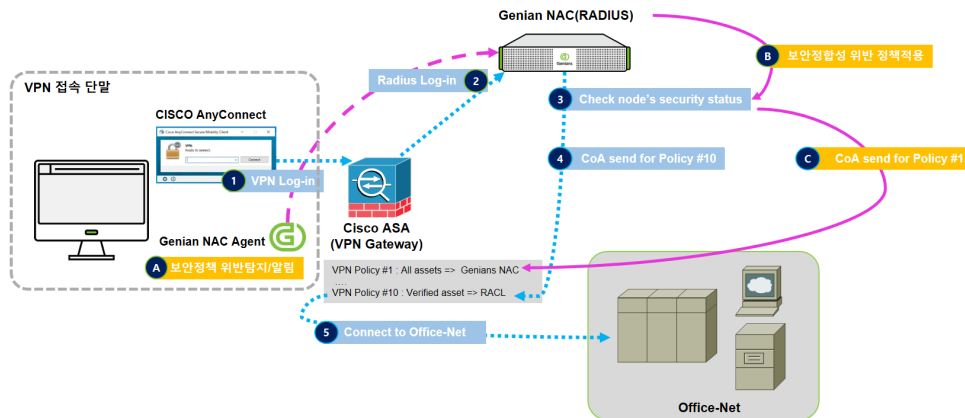
- VPN 접속단말은 VPN-Gateway가 제공하는 부분에만 한정하여 정보가 수집됩니다. 그러나 Genian NAC와 연동시, Genian NAC가 접속단말의 정합성 정보를 제공합니다.

VPN 접속단말의 보안정합성 결과에 따른 제어

- CISCO VPN과 Genian NAC의 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]

- 사용자가 CISCO AnyConnect 를 이용하여 CISCO VPN Gateway 로 접속 시도
- CISCO VPN Gateway 는 사용자 인증서버로 Genian NAC 의 RADIUS 로 지정 및 차단 정책 적용(접속단말은 CWP 만 접속가능)
- Genian NAC 는 접속단말에 NAC Agent 설치시도 및 단말의 보안정합성 만족여부 체크
- 보안정합성 만족 시, AllowAll 정책을 부여할 것을 CISCO VPN Gateway 로 전송(CoA)
=> VPN 접속단말의 네트워크 진입

[접속중인 단말이 보안정합성 위반시]

- (A) Genian NAC 의 Agent 가 접속단말의 보안정합성 체크 및 Genian NAC Policy-Center 로 위반정보 전송
 - (B) Genian NAC 는 정합성위반에 따른 차단정책적용
 - (C) 차단정책을 적용할 것을 CISCO VPN Gateway 로 전송(CoA)
- => 세션이 종료되며, 최초 접속시의 (3) 단계로 이동하여 이후 과정을 거치게 됨

사전준비 사항

Genian NAC RADIUS 와 CISCO VPN Gateway 간 Secret Key 정하기

본 가이드에서 제시하는 연동의 구성은 CISCO VPN Gateway 의 인증서버가 Genian NAC(RADIUS)가 되어 접속을 시도하는 모든 VPN User 는 Genian NAC 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 NAC 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 NAC 인증을 거친 단말	업무용 네트워크, 인프라	업무용 서비스 포트
Redirect	모든 VPN 접속자	Genian NAC의 안내 페이지지만 접속가능	http, https

AllowAll 정책: VPN 접속단말이 Genian NAC에 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 NAC의 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	GNAC	

Advanced 메뉴에서 Accounting에서 Server Group은 GNAC으로 설정합니다.

Step 3: CoA (Change of Authorization) 설정

Configuration > Remote access VPN > AAA/LocalUsers > AAA Server Groups로 이동하여, GNAC서버 그룹을 만들어 줍니다. 다음과 같이 설정 해 줍니다.

설정 항목	설정 값	참고
Server Group	GNAC	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 NAC 설정

Step 1: VPN 접속단말 관리를 위한 노드그룹 만들기

정책 > 그룹 > 노드 로 이동하여, 생성 을 클릭하여, 다음 3개의 노드그룹을 만들어 줍니다.

VPN을 통해서 접속하는 단말을 상태별로 관리하기 위한 노드그룹을 만듭니다.(Genian NAC에서 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 IP' 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 NAC의 에이전트 동작상태와 백신정보 존재 여부를 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	'속 하면', '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	'속 하면', '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 NAC는 접속단말의 네트워크 사용권한을 할당하기 위해서 제어정책을 활용합니다. VPN 보안정합성에 따라 다른 권한을 부여하기 위해서 각각의 제어정책을 생성해 줍니다. (Genian NAC의 정책은 순서대로 적용받습니다)

(1) 보안정합성 미검증 제어정책 만들기

VPN으로 접속한 최초접속자와 접속중이던 사용자가 보안정합성에 위배되는 행위를 하였을 때, 적용받는 정책으로 Genian NAC의 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 2개의 조건을 모두 만족 해야함.(1.VPN access policy 노드그룹에 속함 2.VPN Compliance 그룹에 속하지 않음)
권한설정	PERM-DNS	Genian NAC CWP 만 접속 허용 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 3개의 조건을 모두 만족 해야함.(1.VPN access policy 노드그룹에 속함 2.NAC 에이전트가 동작중이어야 함 3.백신 정보 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:CiscoSecureDefend:DenyAll ACL=AllowAll	참고. 앞서 CISCO ASA 에 설정한 DenyAll 을 적용하도록 함

참고: 보안정합성이 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 RADIUS 서버를 설정하는 과정입니다.

연동기능을 활용하기 위해서는 기본제공되는 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	속성 값 이 같으면	Virtual	
Calling-Station-id	노드 그룹에 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 접속 단말의 기본접속 URL 은 Genian NAC의 CWP로 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	속성 값 이 같으면	Virtual	
Calling-Station-id	노드 그룹에 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 RADIUS 서비스를 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 NAC의 연동설정 완료

CISCO VPN과 Genian NAC의 연동을 위한 설정이 완료되었습니다.

정상 동작여부의 테스트를 위해서,

VPN 접속단말이 최초 접속시의 노드그룹과 보안정합성 검증여부 확인 시의 노드그룹이 변경된 것을 확인하도록 합니다. 노드그룹이 변경된다면 연동설정이 정상적으로 적용되어 있는 상태입니다.

확인 방법은

- 1) 정책 > 제어정책 에서 VPN 접속단말이 적용받는 제어정책을 확인하셔도 되고,
- 2) 관리 > 노드 에서 VPN 접속단말의 그룹, 적용받는 정책이 변경된 것을 확인할 수 있습니다.

작업이 완료되었습니다.

5.8.2 IGLOO Corporation Spider TM 연동

이 가이드는 Genian NAC와 IGLOO Coporation Spider TM 간의 연동에 대한 정보를 제공합니다.

가이드 개요

본 가이드는 통합 관제 솔루션인 IGLOO Coporation사의 Spider TM 제품과 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정방법 및 연동테스트에 대한 가이드입니다.

Genian NAC의 위험관리 정책을 통한 네트워크제어 기능을 활용하며, 차단 단말에 대한 정보를 SpiderTM에서 실시간으로 전달되도록 연동합니다.

SpiderTM은 Genian NAC와 연동을 통해 위험 IP / MAC 을 실시간으로 차단 / 해제하여 안전하고 자동화된 단말제어를 수행 할 수 있습니다.

권장 버전

제품명	버전	비고
Genian NAC	4.0 이상	

연동의 목적

Genian NAC와 Spider TM 연동은 다음의 효과를 제공합니다.

위협 IP / MAC에 대한 실시간 차단

- Genian NAC는 Spider TM에서 전달된 SNMP Trap을 통해 전달된 IP/MAC을 즉시 위험감지 정책으로 관리하며 제어정책을 활용하여 차단합니다.

위협 IP / MAC에 대한 실시간 차단 해제

- Genian NAC는 Spider TM에서 전달된 SNMP Trap을 통해 전달된 IP/MAC을 즉시 위험감지 해제하여 네트워크차단 상태에서 해제합니다.

사전준비 사항

Networking 사전 준비

- Spider TM과 Genian NAC와 SNMP trap 에 사용되는 기본 포트는 UDP/162 입니다. 방화벽을 통해 해당 포트를 통한 통신을 허용해야 합니다.

연동을 위한 Genian NAC 설정

본 항목에서 다루는 Genian NAC의 설정 부분은 Spider TM과 연동을 위해 설정하는 최소한의 부분만을 소개합니다. 본 과정은 최초 1회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step1. 위험 감지 정책 설정

정책 > 노드 정책 > 위험 감지 로 이동하여 아래 신규 위험 감지 정책을 생성합니다.

- SNMP Trap을 통한 위험탐지를 위한 위험 감지 정책 생성

설정 항목	설정 값	참고
기본설정 > ID	SNMP Trap 위험 감지	위험감지정책 이름 입력
기본설정 > 설명	Spider TM SNMP 연동을 위한 위험감지 정책	위험감지정책 설명 입력
기본설정 > CWP 메시지		
이벤트정의 설정 > 이벤트	SNMP 차단요청	

SNMP OID 정보

항목명	OID 값	참고
SNMP Trap OID	.1.3.6.1.4.1.29503.1.1.0.100	트랩 송신을 위한 OID
차단대상 IP	.1.3.6.1.4.1.29503.10.0.1	차단할 IP 지정
차단대상 MAC	.1.3.6.1.4.1.29503.10.0.2	차단할 MAC 지정
차단대상 DEVID	.1.3.6.1.4.1.29503.10.0.8	차단할 장비ID 지정
차단사유	.1.3.6.1.4.1.29503.10.0.3	차단사유 기록
해제대상 IP	.1.3.6.1.4.1.29503.10.0.4	차단해제할 IP 지정
해제대상 MAC	.1.3.6.1.4.1.29503.10.0.5	차단해제할 MAC 지정
해제대상 DEVID	.1.3.6.1.4.1.29503.10.0.9	차단해제할 장비ID 지정
해제사유	.1.3.6.1.4.1.29503.10.0.6	해제사유 기록

- 위험감지 정책을 노드정책에 할당

1. 정책 > 노드정책 메뉴로 이동

2. 위험감지 정책을 적용할 대상 노드정책을 선택
 3. 최하단 위험감지 섹션에서 할당 클릭
 4. 생성한 SNMP Trap 위험감지 정책을 선택
 5. 노드정책 수정
- 3) 위험탐지된 노드 그룹핑을 위한 노드그룹 추가
1. 정책 > 그룹 > 노드 이동
 2. 신규 노드그룹 생성

설정 항목	설정 값	참고
기본정보 > ID	SNMP Trap 위험탐지 대상	노드그룹 이름 입력
기본정보 > 설명	Spider TM SNMP 연동으로 위험탐지된 노드 그룹	노드그룹 설명 입력
기본정보 > CWP 메시지	Spider TM 연동으로 위험에 탐지된 노드로 차단됨	원하는 형태의 차단 안내 메시지 작성
그룹조건 > OR		
그룹조건 > 조건추가	노드정보 > 위험감지 > 특정위험이 감지되면 > SNMP Trap 위험 감지 선택	앞에서 생성한 위험감지정책 선택

1. 생성
 - 4) 위험 탐지된 노드 차단을 위한 제어정책 설정
 1. 정책 > 제어정책 > IP관리 정책 클릭
 2. 노드그룹 섹션 할당 클릭
 3. SNMP Trap 위험탐지 대상 선택 할당
 4. 하단 수정 버튼 클릭
 5. 변경 정책 적용 클릭

연동 확인을 위한 테스트

SNMP Trap을 수신하면 Genian NAC Web콘솔 감사로그 메뉴에서 아래와 같은 형태의 감사로그를 확인 할 수 있습니다.

```
Block IP SNMP Trap 감사로그
SNMP Trap 수신..1.3.6.1.2.1.1.3.0=0:0:00:00.00, .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.4.1.29503.1.1.0.100, .1.3.6.1.4.1.29503.10.0.1=172.29.132.117
```

SNMP Trap 수신 후 설정한 위험감지 정책으로 탐지되는지 확인합니다.

```
위험감지 탐지 감사로그
새로운 위험노드 발견됨.ANOMALY_DEF='TEST-SNMP trasp block'
```

위험에 탐지된 노드 상세정보의 정책현황 탭에서 노드에 할당되어있는 정책들을 확인하여 정상적으로 차단 및 해제가 되었는지 확인합니다.

5.8.3 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 IT 관리자와 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 NAC는 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=	IP 정보를 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.

설 정 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.

설 정 항목	설정 값	참고
태 그 (Tag)	할당	Tag의 상태를 설정합니다.
검 색 대상	노드	검색의 대상을 지정합니다.
할 당 대상	노드	태그(Tag)의 할당 대상을 노드로 합니다.
태 그 (Tag) 추가	Infoblox-DDI-Isolation	연동을 위한 Genian NAC 설정에서 정해 둔 태그(Tag)명을 설정합니다.

연동을 위한 설정이 완료되었습니다.

5.8.4 FireEye의 연동 가이드

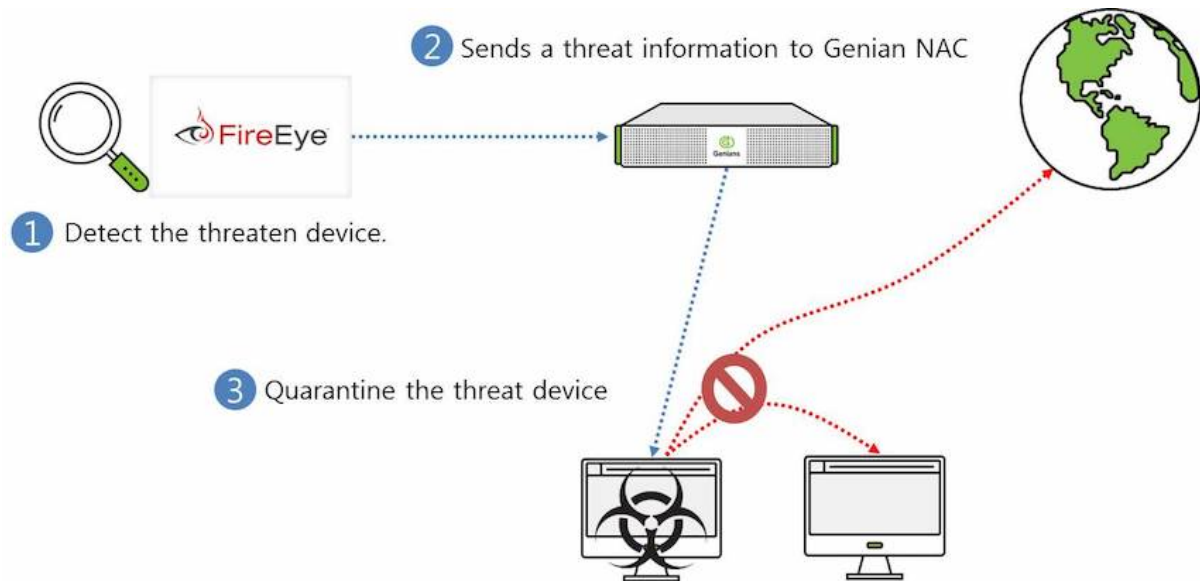
본 가이드에서는 Genian NAC와 FireEye와 연동하는 방법을 안내합니다.

가이드 개요

FireEye에 의해 특정 이상 징후가 감지되면 FireEye는 SYSLOG를 통해 Genian NAC에 이상 징후 정보를 전송합니다.

Genian NAC는 이상 징후 대상을 격리하여 이상 징후가 확산되는 것을 방지 할 수 있도록합니다.

FireEye를 이용한 Genian NAC 구축 구성



1. FireEye가 위협 단말을 감지합니다.
2. FireEye는 이상 정보를 SYSLOG를 통해 Genian NAC로 전송합니다.
3. Genian NAC는 위협 단말을 격리하여 위협 단말이 다른 네트워크에 연결 할 수 없습니다.

SYSLOG를 통한 FireEye 연동 구성

Genian NAC의 설정

Genian NAC는 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 완료해야 합니다.

1. 관리자 계정으로 Genian NAC에 로그인
2. 상단 항목의 설정 탭으로 이동
3. 왼쪽 항목의 환경설정 > 감사기록 이동
4. **Syslog** 감사기록 저장 옵션에 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 NAC에 데이터를 보내려면 다음 단계를 수행해야 합니다.

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 NAC Name 입력 > **Add Rsyslog Server** 버튼을 클릭합니다.
8. IP 주소 필드에 Genian NAC의 IP 주소를 입력합니다.
9. 아래의 **Update** 버튼을 클릭합니다.

검증

위의 단계를 완료하게 되면 Genain NAC는 FireEye로부터 SYSLOG 메시지를 수신 할 수 있습니다.

1. 상단 항목의 **감사** 로 이동합니다.
2. 로그 메시지가 표시되면 **LogID** 는 FireEye입니다.

FireEye 데이터를 기반으로 Genian NAC 정책 적용

Genian NAC가 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.

5.8.5 Genian GPI 연동 가이드

이 가이드는 Genian NAC와 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 NAC의 연동 기능을 수행하기 위한 설정방법 및 연동 기능의 테스트 방법을 안내하는 문서입니다.

Genian GPI는 보안성이 확보된 PC에 한하여 네트워크 사용을 허가하도록 Genian NAC와의 연동 설정을 Web콘솔에서 제공합니다. (별도의 기능 추가/설정 불필요)

연동 기능이 설정되면, Genian GPI는 수치화한 PC의 정보보안 수준 정보를 Genian NAC로 전송하고, Genian NAC는 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 NAC	V5.0 이상	정책서버 버전 (2020.10 이후 버전)

연동의 목적

Genian NAC와 Genian GPI의 연동은 다음의 효과를 제공합니다.

1. 취약 PC의 강제조치, 자동제어 수행

- Genian GPI가 진단한 점수를 기준으로 Genian NAC에서 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 NAC가 조치한 PC의 초기 접속페이지를 차등 적용하여 차단된 사유 안내 및 차단된 사유를 해소하여 정상적으로 네트워크 사용을 위한 조치 방법에 대한 안내페이지를 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 NAC의 접속 포트정보는 Web콘솔에서 시스템 > 서비스 관리 > 접속포트에 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	x 일 후 xx시 xx분 부터	점검 일시 입력 (정책 설정 시간 이후부터 적용)

- 4) 우측 상단 저장 버튼 클릭하여 저장

Genian NAC와 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 NAC 정책서버의 IP주소 입력

연동을 위한 Genian NAC 설정

본 가이드에서 다루는 Genian NAC의 설정 부분은 Genian GPI와 연동을 위해 최소한의 부분만을 소개합니다. 본 과정은 최초 1회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: GPI 점검 미수행 그룹 제어를 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_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 이동한 후 작업선택 > 생성 셀렉트박스를 클릭 하면 제어정책 마법사가 실행됩니다. 제어정책 마법사에서 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 > 적용 모드	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 메시지는 Step 1의 사용자 메시지와 중복되므로 공백 처리
- 본 가이드에서는 격리 과정만 수행하므로 제어액션은 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,GPI 정책) / 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 이동한 후 작업선택 > 생성 셀렉트박스를 클릭 하면 제어정책 마법사가 실행됩니다. 제어정책 마법사에서 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 메시지는 Step 3의 사용자 메시지와 중복되므로 공백 처리
- 본 가이드에서는 격리 과정만 수행하므로 제어액션은 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 NAC와 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 NAC Web콘솔 "감사 > 로그" 에서 이벤트 발생 확인

- 192.168.100.40 IP에 GPI 점수 추가 감지됨 이벤트 확인

Step 4: Genian NAC 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 PC는 보안점수가 70점 미만이므로 네트워크가 차단되었습니다. 네트워크 접속을 원하시면 PC 조치 후 상태 재검사를 수행하시기 바랍니다.

5.8.6 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 위해 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 syslog 방식의 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 Profile 창이 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

웹 브라우저를 이용하여, `[https://PAN-OS IP/api/?type=keygen&user=[username]&password=[password]]` 를 입력하여 API-Key를 생성합니다.

웹 브라우저에 위와 같이 입력하면, 다음의 결과를 얻을 수 있습니다.

```
#Script
<response status='success'>
<result>
<key>
↪LUFRPT1KbW80SU1hRXJuNk5XNHBUdUhCNGMydE0rSUK9RFIzdEJ5RGcwWkRCVlhYMX10Q1FPdz09
</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	선택박스에서 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 Filter 선택

Step 3: Syslog Listener 서비스 활성화

Network > *Network Profiles* > *Interface Mgmt* 로 이동한 후, *ADD* 를 클릭하면, *syslog Listener New profile* 이 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	선택박스에서 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 정보 전송	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 IP 입력	
전송방법	UDP	UDP, TLS 중 선택
전송포트	514	UDP(514), TLS(6514)
포맷	Default	Default, CEF 중 택1
Syslog 메시지	USERAUTH, ID={ID}, IP={_IP}	
CHARACTER 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.

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

5.8.7 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.

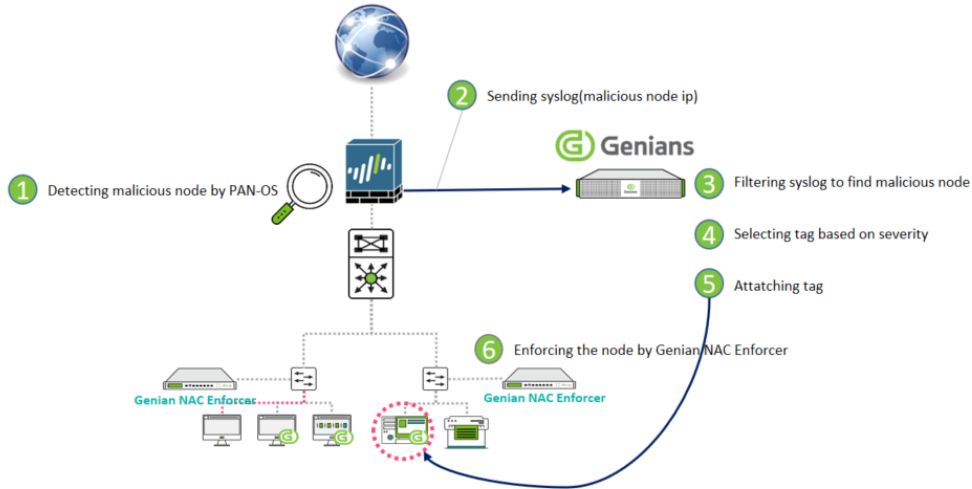
위협을 범위를 최소화하여 노드의 네트워크 차단 수행

- 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 위협 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 위협의 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. IP 정보 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 창에 다음과 같이 입력합니다.

1. Profile의 이름을 정해줍니다.
2. 각 로그 별로 type을 지정하고 위협도를 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 추가를 클릭한 후, 다음의 설정 값을 입력합니다.

설정 항목	설정 값	참고
필터 이름	PANOS_critical	
필터 타입	host	Program, Host, Match, netmask 중 택 1
필터 값	xxx.xxx.xxx.xxx	PAN-OS 장비의 IP
IP키 값	src=	노드의 IP
MAC 키 값	입력하지 않음	
User 키 값	입력하지 않음	
문자셋	유니코드(UTF-8)	

작성 후, 추가를 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 > 생성을 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 > 로그로 이동합니다.
2. 로그검색창에서 Add Filters를 클릭하면 필터 설정화면이 열립니다.
3. 설정화면 중, 설명란에 '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 > 할당으로 변경하고 다음과 같이 입력합니다.

설 정 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, 위협도, 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.

설 정 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.

5.8.8 Paloalto Networks Firewall의 연동 가이드

이 가이드에서는 Palo Alto 방화벽을 통한 연동에 대한 내용을 제공합니다.

가이드 개요

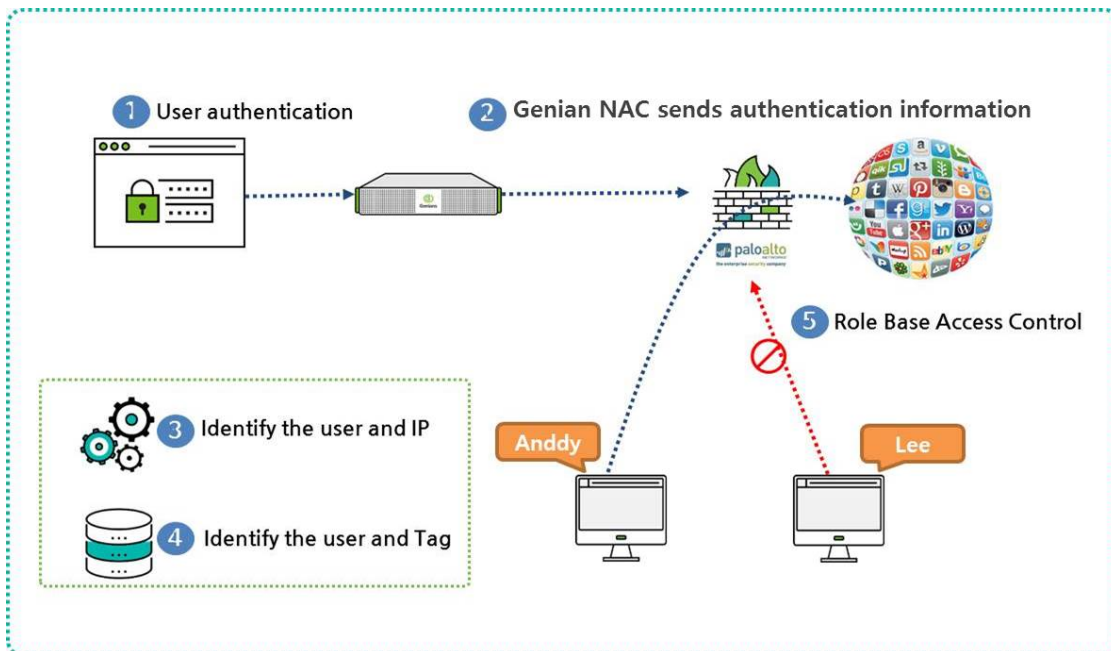
이 가이드는 Genian NAC 엔지니어 및 기업 운영자가 Genian NAC 및 PAN 방화벽과 협력하여 PAN 인증 방화벽에 사용자 인증 정보를 보내는 방법에 대해 설명합니다.

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 가능하게 합니다.



인증 프로세스는 다음과 같습니다.

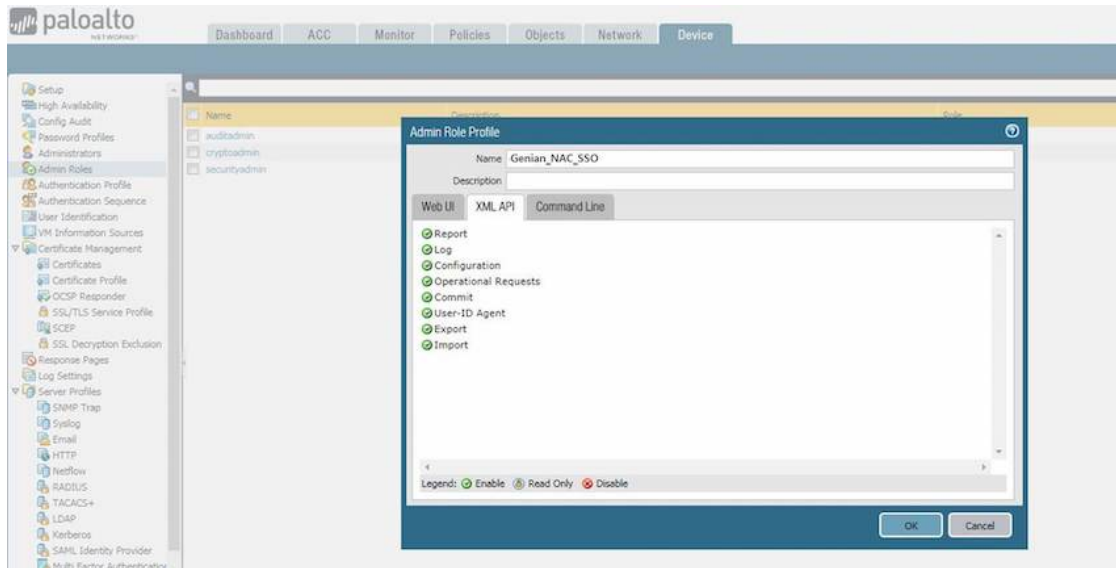
1. Genian NAC의 사용자 인증
2. Genian NAC는 인증 사용자 및 IP 정보를 PAN 방화벽에 보냅니다.
3. PAN 방화벽은 인증 사용자와 Genian NAC에서 받은 IP 정보를 자체 사용자 ID 테이블과 비교합니다.
4. PAN은 User-ID에 할당 된 태그를 확인합니다.
5. 각 사용자에게 할당 된 태그를 기반으로 역할 별 액세스 제어 정책이 수립됩니다.

XML API를 통해 연동을 위한 PAN Firewall 구성

1. PAN 방화벽에서 관리자 역할 생성

먼저 웹에서 관리자 역할을 생성

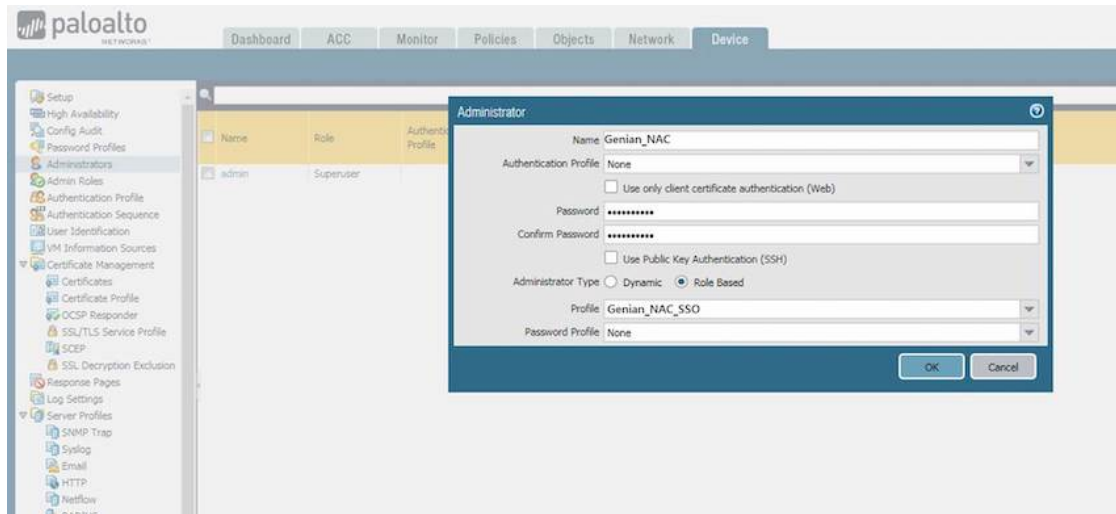
- **Device > Admin Roles > Add** 으로 이동합니다.
- Genian_NAC_SSO 의 role **Name** 을 만들고 **XML API** 탭 아래를 설정합니다.
- 모든 것을 활성화하고 **OK** 를 사용하여 확인합니다.



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=\[password\]](https://[IP of PAN firewall]/api/?type=keygen&user=[username]&password=[password])
아래에서 생성된 키를 볼 수 있습니다.

```
Script
<response status = 'success'>
<result>
<key>
↪LUFRT1KbW80SU1hRXJuNk5XNHBUhCNGMydE0rSUK9RFIzdEJ5RGcwWkRCV1hYMX10Q1FPdz09
</key>
</result>
</response>
```

4. Genian NAC에서 SYSLOG 전송을 위한 설정

Genian NAC는 감사 로그의 필터를 사용하여 XML과 연동합니다.

- 상위 항목의 감사로 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=LUFRT1KbW80SU1hRXJuNk5XNHBUhCNGMydE0rSUK9RFIzdEJ5RGcwWkRCV1hYMX10Q1FPdz09
```

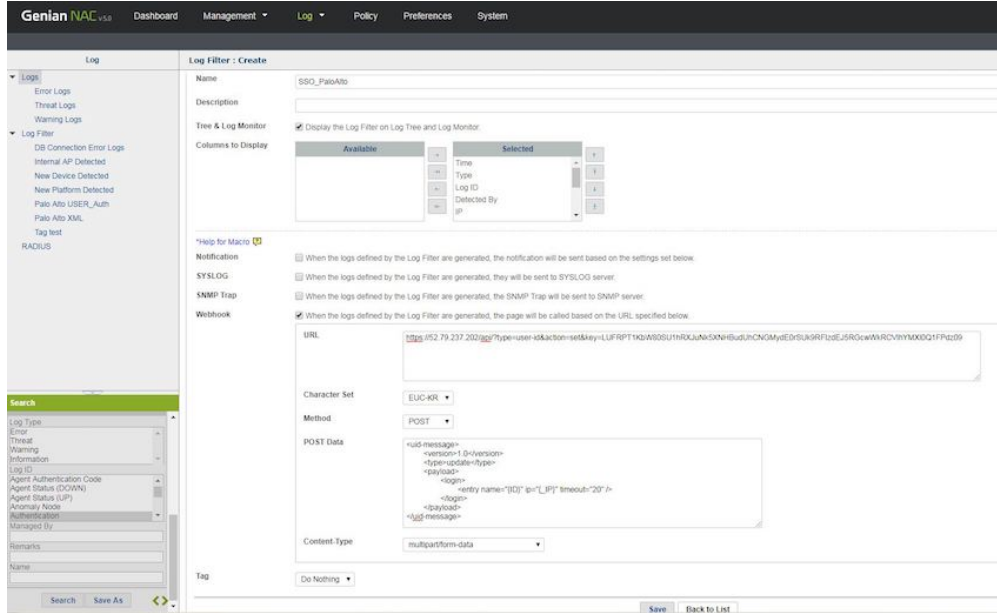
(나) 로그필터 문자셋 및 전송내용 설정

- **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

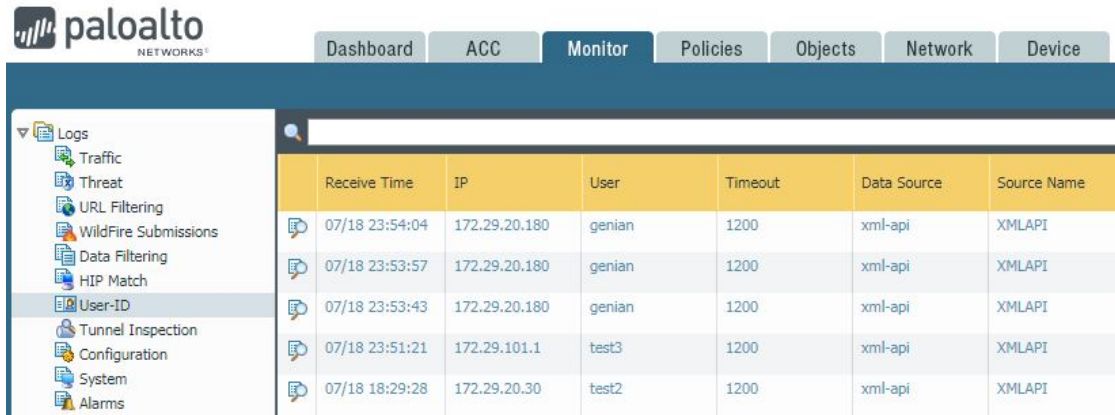
- **Network > Zone** 로 이동
- **Enable User Identification** 선택 및 **OK** 클릭.

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.



	Receive Time	IP	User	Timeout	Data Source	Source Name
	07/18 23:54:04	172.29.20.180	genian	1200	xml-api	XMLAPI
	07/18 23:53:57	172.29.20.180	genian	1200	xml-api	XMLAPI
	07/18 23:53:43	172.29.20.180	genian	1200	xml-api	XMLAPI
	07/18 23:51:21	172.29.101.1	test3	1200	xml-api	XMLAPI
	07/18 18:29:28	172.29.20.30	test2	1200	xml-api	XMLAPI

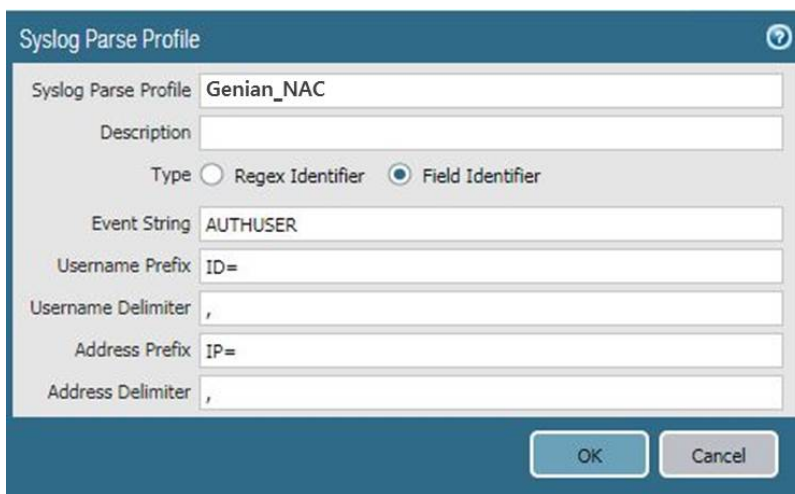
SYSLOG를 통해 연동을 위한 PAN Firewall 구성

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: ,
```



Syslog Parse Profile

Syslog Parse Profile: Genian_NAC

Description:

Type: Regex Identifier Field Identifier

Event String: AUTHUSER

Username Prefix: ID=

Username Delimiter: ,

Address Prefix: IP=

Address Delimiter: ,

OK Cancel

2. PAN 방화벽이 모니터링하는 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.

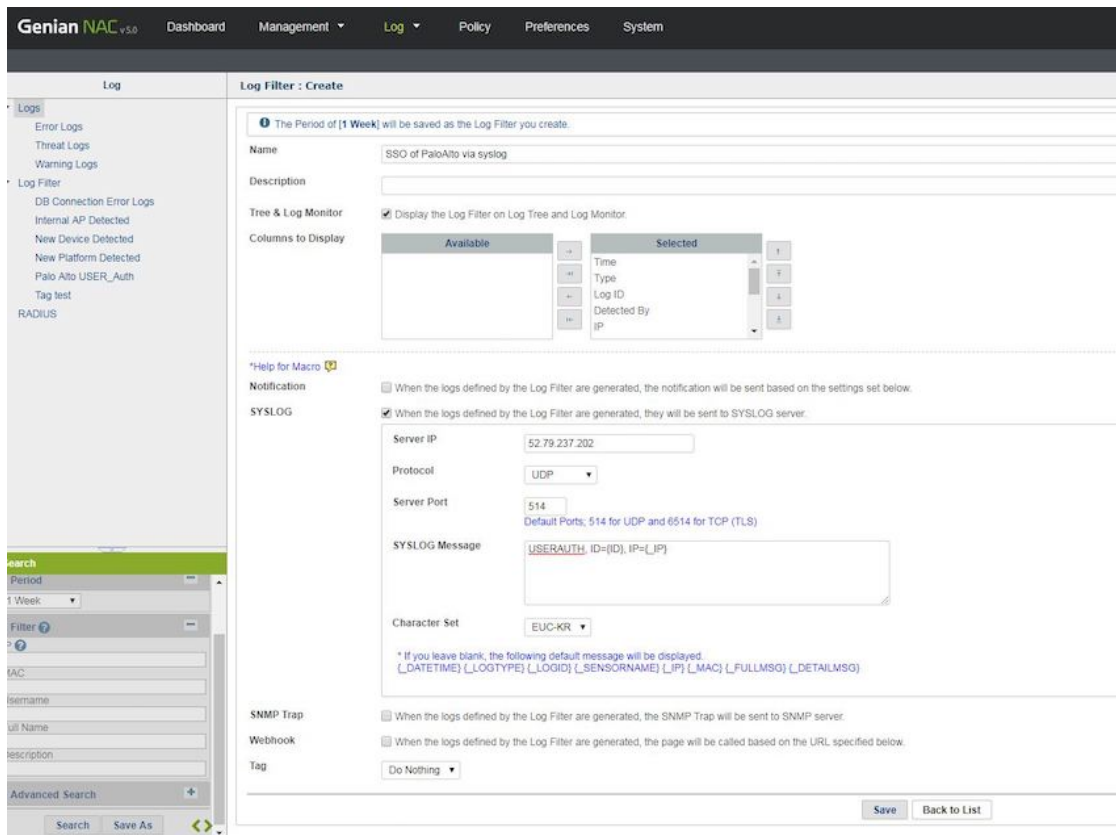
• Commit

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

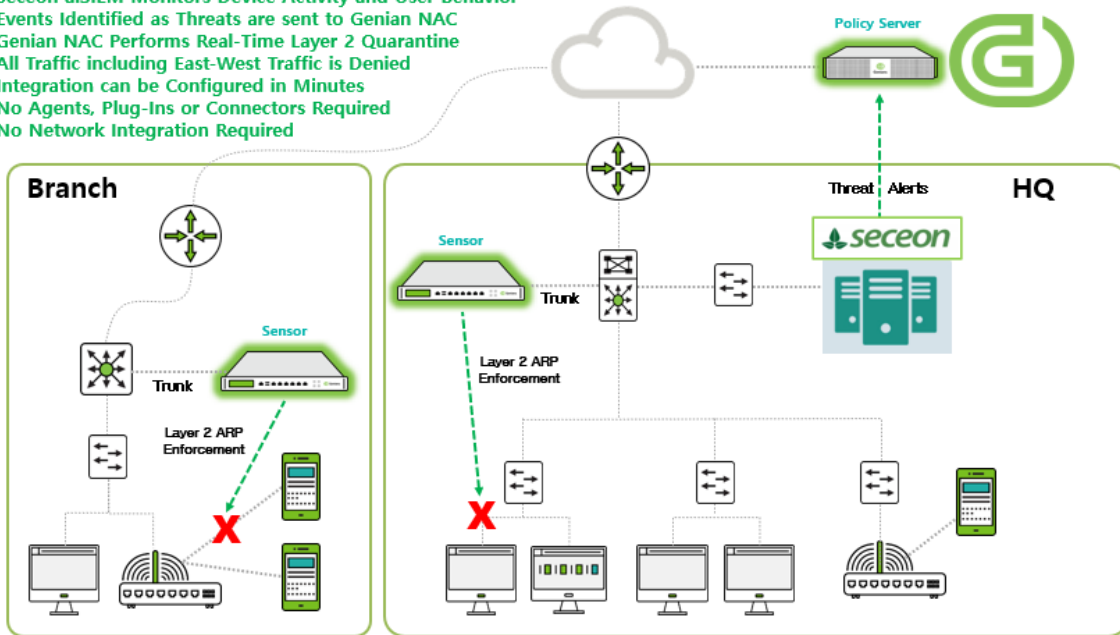
```
CLI command
admin@PA-VM> show user ip-user-mapping all type SYSLOG
IP                Vsys      From      User      IdleTimeout (s)
↔MaxTimeout (s)
-----
↔
172.29.101.1     vsys1    SYSLOGI   genian    2220
↔2220
Total: 1 users
```

5.8.9 Seceon aiSIEM 연동

이 가이드는 Syslog를 이용하여 Genian NAC와 Seceon aiSIEM과 연동방법에 대한 정보를 제공합니다. Seceon aiSIEM의 위협 탐지 기능을 Genian NAC의 강력한 제어 기능으로의 확장을 제공합니다. 데모영상을 통하여 연동하는 방법을 비디오 웨비나로 함께할 수 있습니다. Seceon

Genians and Seceon aiSIEM Security Automation

- Seceon aiSIEM Monitors Device Activity and User Behavior
- Events Identified as Threats are sent to Genian NAC
- Genian NAC Performs Real-Time Layer 2 Quarantine
- All Traffic including East-West Traffic is Denied
- Integration can be Configured in Minutes
- No Agents, Plug-Ins or Connectors Required
- No Network Integration Required



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 추가해야 합니다. 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 정책 서버 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 감사를 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 할당을 선택합니다.
검색대상, 할당대상을 노드나 MAC, IP, 무선랜, 사용자를 선택할 수 있지만 노드를 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, CWP 메시지 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 권한을 선택하고 제어된 사용자에게 표시될 CWP 메시지를 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 할당되어야 합니다.
5. 태그가 할당된 노드는 위협 제어정책이 할당되고 네트워크격리가됩니다. 단말에서는 Gateway로 Ping이 실패하고 단말이 격리되었음을 나타내는 CWP가 표시됩니다.

5.8.10 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 사용자에게 대한 안내페이지 제공

- 모니터랩 AISWG는 Genian NAC와 연동을 통해 인증서 설치 현황에 대한 정보를 실시간으로 전달 받아 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. (AISWG 와 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 설정 합니다.

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 구성 됩니다.

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 현황을 체크하기 위한 txt 파일 경로와 파일명(확장자 포함) 입력
액션 수행설정 > 플러그인 선택	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 현황을 체크하기 위한 txt 파일 경로와 파일명(확장자 포함) 입력
액션 수행설정 > 플러그인 선택	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 사용자명에 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 NO로 변경

Note: 인증서가 사용자의 PC에 존재하지 않을 시 AISWG의 정책에 의해 정상적인 웹서비스를 이용할 수 없게 되고, 인증서 설치 안내페이지가 제공됩니다.

5.8.11 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 연동테스트를 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 Web-hook(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 불가능한 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 고객에서는 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 SWG의 서버정보 확인

- Genian NAC에서 IP변경을 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](https://[eWalker SWG 서버 IP]:8501)
- API 경로 예) [https://\[eWalker SWG 서버 IP\]:8501/ewalker/orgdb/dhcp/macid](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 입력 하고 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 중인 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](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.)

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 정책을 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 메시지를 정의하여 사용자의 네트워크가 차단되었을 때 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 메시지를 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 있도록 하는 게시판 스타일의 메시지입니다. 공지 사항은 일반적으로 하나 이상의 항목을 설명하는 긴 문장이지만, 메시지는 사용자가 차단 된 이유 또는 네트워크에 액세스하기 위해 수행해야 하는 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 체크박스를 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 체크박스를 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 기능을 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 NAC는 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 CWP 페이지에서 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 NAC는 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.

Note: 유튜브를 통해 임시 사용자 방문 프로세스 교육 및 설정 방법을 확인할 수 있습니다.



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 사용자 등록페이지가 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 승인을 **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 승인을 **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 승인을 **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 CWP 페이지 신청결과조회와 이메일 확인이 있습니다.

Case 1 : CWP 페이지에서 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 나뉩니다.

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 NAC에서 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 NAC에서 제공하는 CWP 페이지 Redirection 기능을 사용할 수 없으므로 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 접속인증페이지의 디자인 템플릿으로 이동합니다.
3. 디자인 템플릿 목록에서 현재 사용중인 템플릿을 클릭합니다.
4. 컴포넌트 설정에서 확인버튼을 클릭합니다.
5. 이미지 파일이 있는 경우 아이콘이미지를 업로드합니다.
6. 확인버튼 옵션에서 항상사용 또는 모든조건 만족시 사용을 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 정책으로 이동합니다.
2. 왼쪽 정책 항목에 무선랜정책 > Client 프로파일을 선택합니다.
3. 작업선택 항목에서 생성을 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 AP 정책과 Client 정책으로 나뉘지며 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 정책에 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 무선 네트워크 센서 AP 프로파일 적용하기

Genian NAC 무선 네트워크 센서에서 제공하는 AP(Access Point) 기능의 프로파일을 관리하고 적용할 수 있습니다.

AP의 프로파일을 설정하여 배포하는 기능을 사용함으로써 전체/개별 무선 네트워크 센서에 대한 프로파일 관리 기능을 사용할 수 있습니다.

Note:

- Genian NAC 무선 네트워크 센서의 AP 프로파일만 관리할 수 있습니다.
 - AP 프로파일에 상세 설정 부분은 다음에 ap-profile-detail 참고하시기 바랍니다.
-

6.7.1 1. AP 프로파일 설정하기

프로파일에서 설정할 수 있는 보안방식으로는 **Open, WEP, WPA2-Personal, WPA2-Enterprise** 가 있습니다.

1. 상단 패널에 정책 으로 이동합니다.
2. 왼쪽 정책 항목에 무선랜정책 > AP 프로파일 을 선택합니다.
3. 작업선택 항목에서 생성 을 선택합니다.
4. AP 프로파일 설정값을 입력합니다.
5. 생성 버튼을 클릭합니다.

6.7.2 2. 무선 네트워크 센서에 적용할 무선랜 정책 설정하기

무선랜 정책은 AP 정책과 Client 정책을 설정할 수 있습니다. AP 정책은 무선 네트워크 센서에서 배포하는 프로파일을 지정하는 기능으로 단말의 무선접속에 대한 Client 정책 설정이 없어도 동작을 수행합니다.

1. 상단 패널에 정책 으로 이동합니다.
2. 왼쪽 정책 항목에 무선랜정책 을 선택합니다.
3. 작업선택 항목에서 생성 을 선택합니다.
4. AP 정책에 생성된 AP 프로파일 을 할당합니다.
5. 생성 버튼을 클릭합니다.

6.8 사용자 IP 신청 연동(With Google Form)

본 가이드는 Google Form(app script)을 활용하여 Genian NAC에 서비스중 하나인 IP신청시스템을 사용하는 방법을 안내합니다.

6.8.1 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 사용자에게 대한 감사 증적을 남길 수 있습니다.

권장 버전

제품명 (구성요소)	버전	비고
Genian NAC (정책서버)	V5.0.55 이상	

6.8.2 연동의 목적

Goole Form과 Genian NAC IP 신청 연동은 다음의 효과를 제공합니다.

사용자 친화적 IP 신청 프로세스

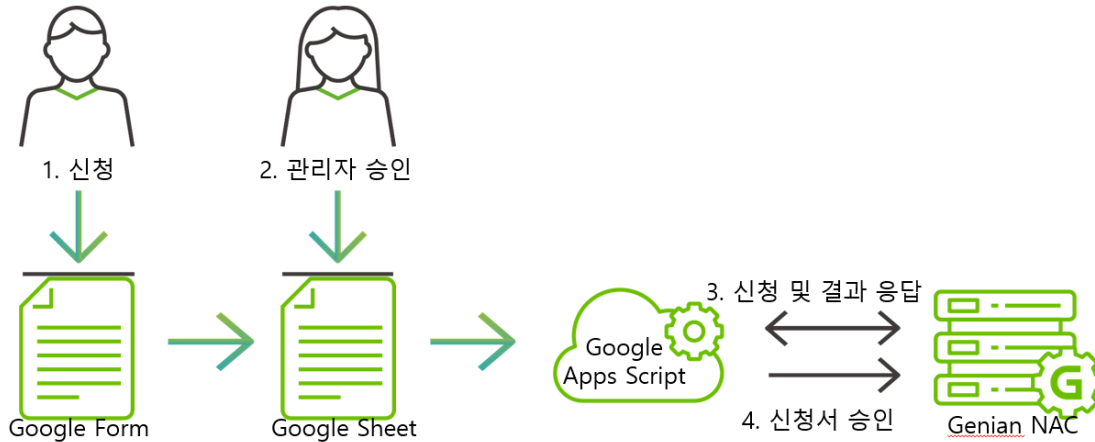
- 일정한 틀이 만들어져있는 기본 제공 IP 신청화면이 아닌 사용자측에서 개발한 UI를 사용하여 IP 신청 시스템을 구축할 수 있습니다.

관리자 친화적 IP 신청 프로세스

- 관리자가 원하는 IP 신청/승인 프로세스를 만들 수 있으며 언제든지 프로세스를 변경 할 수 있습니다.

6.8.3 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



6.8.4 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
- geniains(<https://www.genians.com/>) 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 설치를 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 선택할 때 센서를 선택하게됩니다. 센서의 Key가 Node ID 입니다.
- 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.

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.

IP 신청 (테스트 설문)

설문지 설명

사용위치 *

1 172.29.50.52

2 172.29.50.100

사용자 ID *

사용중인 ID를 입력하세요.

답답형 텍스트

용도 *

IP용도를 선택하세요.

1 유동IP사용

2 고정IP사용

IP 주소

고정IP사용일 때만 입력하세요.

답답형 텍스트

MAC 주소

고정IP사용일 때만 입력하세요.

답답형 텍스트

이메일

신청 완료 후 결과를 통보받을 이메일을 입력합니다.

답답형 텍스트

- 응답결과에 대한 Sheets를 생성합니다.
- 응답 > Sheets에서 보기 클릭
- Sheets 에서 컬럼 두개를 추가 합니다.
- 승인여부: 관리자가 승인 여부를 선택할 수 있도록 컬럼을 추가합니다.(드롭다운)
- idx: 신청서 추가 후 발급받은 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/{idx} (신청서 상태 수정) API를 확인합니다.

applications API for Request	
GET	/applications/ips List IP Requests
POST	/applications/ips Add a new IP Request
GET	/applications/ips/count Retrieve the number of IP Requests
GET	/applications/ips/purposes Retrieve purpose list for IP Application
GET	/applications/ips/sensors/{purpose} Retrieve sensor list for purpose
GET	/applications/ips/{idx} Retrieve a specific IP Request's information
PUT	/applications/ips/{idx} Update an existing IP Request
GET	/applications/medias List External Device Requests
GET	/applications/medias/count Retrieve the number of the External Device Requests
GET	/applications/medias/{idx} Retrieve a specific External Device Request's information
PUT	/applications/medias/{idx} Update an existing External Device Request
GET	/applications/users List User Account Requests
GET	/applications/users/count Retrieve the number of User Account Requests
GET	/applications/users/{idx} Retrieve a specific User Account Request's information
PUT	/applications/users/{idx} Update an existing User Account Request

- 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 = "[apiKey]"
// 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, 9).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
const options = {
```

(continues on next page)

(continued from previous page)

```

    "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 = {'172.29.50.52': '0d300156-7c51-103e-8002-
↪080027a65e65-cc2d2503',
                       '172.29.50.53': '0d300156-7c51-103e-8002-
↪080027a65e65-cc2d2504'};
  // 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["applicantId"] = itemResponses["사용자 ID"][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 form 이 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',
                    '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 = 8; // idx 컬럼
  const editedRow = e.range.getRow();
  const val = e.range.getValue();
  // 수정된 셀이 타겟 컬럼에 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);
    }
  }
}
/**
 * IP 신청서 승인
 */
function approveIpApplication(idx) {
  // 관리자의 API Key를 생성한 뒤 api 호출 시 사용할 수 있도록 선언한다.
  const API_KEY = "[apiKey]"
  const apiUrl = "https://[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);
  }
}
```

- 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.

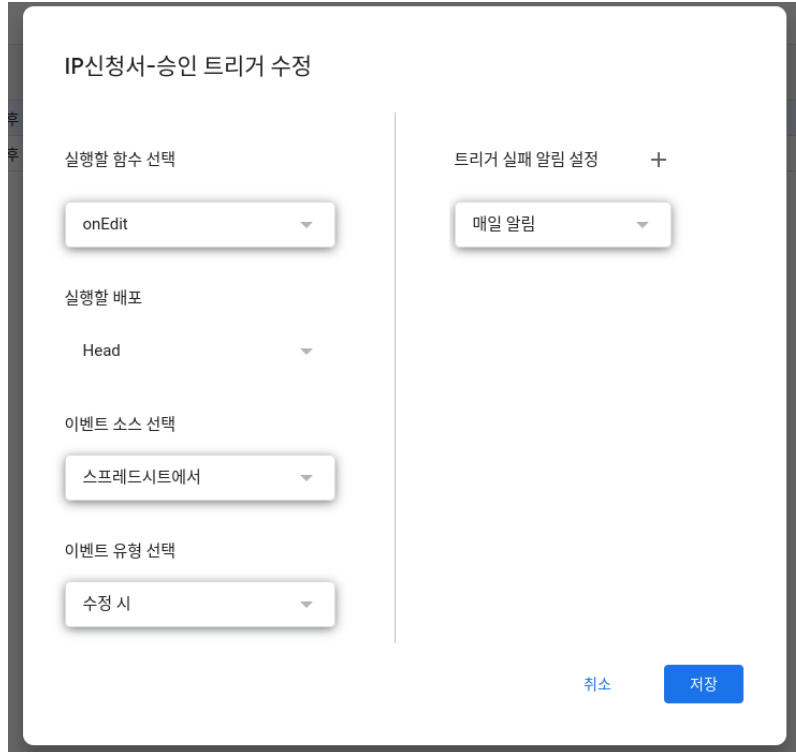
- 트리거로 등록
- 트리거 메뉴로 이동합니다.
- 트리거 추가

- 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

번호	처리일자	최종승인자	구분	용도	신청부서	신청자명	사용자명	부서명	처리결과	승인번호	정책	할당IP
15	2024-03-25 04:1...	Super Administr...	IP신청	지정IP사용	test	test			처리완료		모두허용	172.29.50.53
14	2024-03-25 02:3...	Super Administr...	IP신청	지정IP사용	test	test			처리완료		모두허용	172.29.50.5
13	2024-03-25 02:3...	Super Administr...	IP신청	유동IP사용	admin	admin			처리완료		모두허용	172.29.50.3
12	2024-03-25 02:1...	admin	IP신청	유동IP사용	admin	admin			처리완료		모두허용	172.29.50.1
1	2024-03-25 01:4...	admin	IP신청	유동IP사용	admin	test			처리완료		모두허용	172.29.50.1

6.9 문제해결

6.9.1 차단단말이 CWP 페이지 Redirection이 되지 않는 문제

Genian NAC는 회사의 보안 정책을 준수하지 않은 사용자가 브라우저로 네트워크 접속을 시도할 때 CWP를 통해 준수해야 하는 보안 정책을 보여 줍니다. 사용자에게 접속인증페이지를 표시하기 위해 Genian NAC은 사용자 PC가 네트워크 통신 프로세스를 모니터링하고 사용자가 액세스하려는 페이지 대신 Genian NAC의 CWP 페이지를 볼 수 있도록합니다.

Genian NAC가 제어하는 PC에서 CWP 페이지에 연결되어 있지 않습니다. 또는 웹브라우저에 "연결이 비공개입니다." 라는 문구만 표시되는 경우가 있습니다

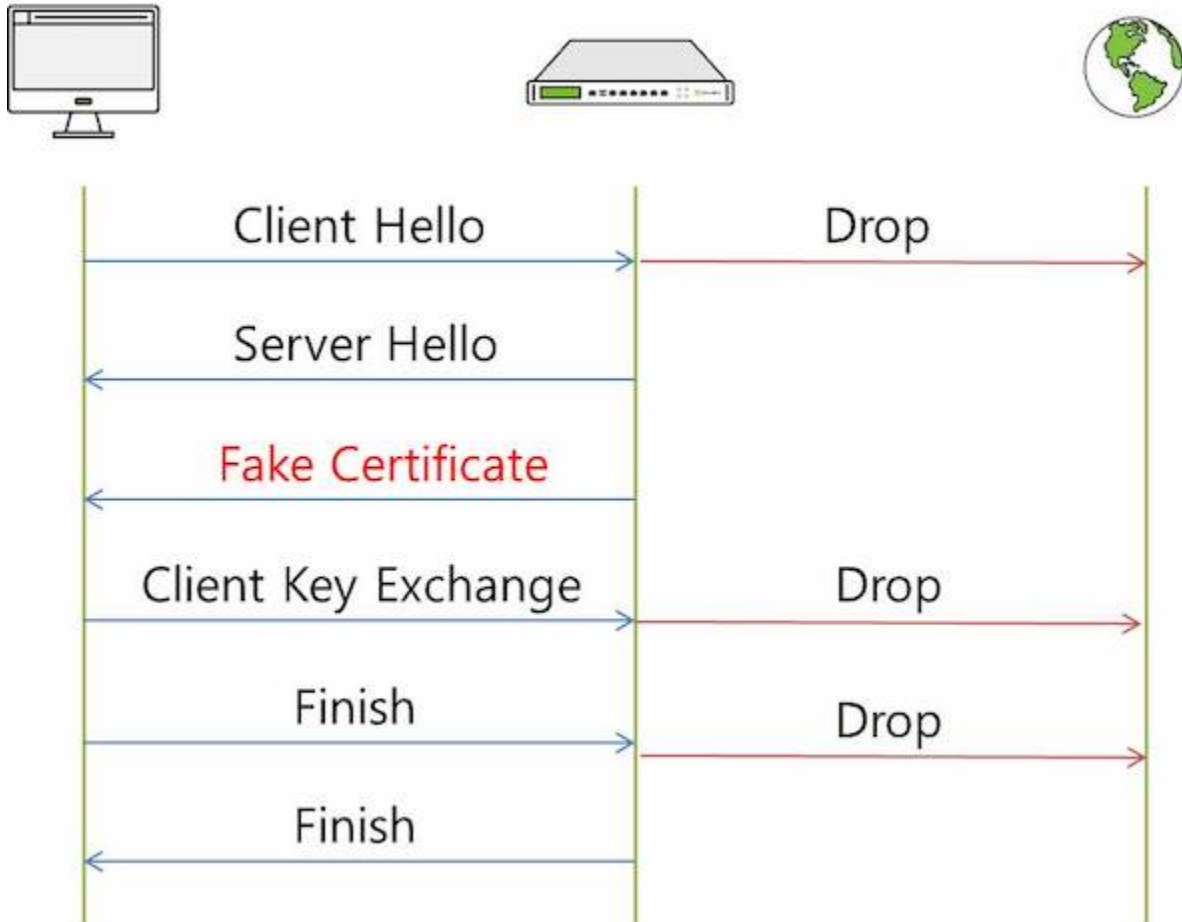
이 문제는 보안 정책을 준수하지 않은 사용자가 HTTPS 서비스를 사용하여 특정 사이트에 연결할 때 발생합니다. Genian NAC는 기본적으로 단말에서 발생하는 패킷을 우회시켜 사용자에게 CWP 화면을 표시하지만 HSTS 및 HPKP(브라우저의 인증서 확인)라는 브라우저의 기능으로 CWP 페이지 리다이렉션이 되지 않을 수 있습니다. 아래 내용들을 확인하여 NAC의 차단 페이지 동작방식을 이해할 수 있습니다.

HTTP 통신을 시도하는 PC에 CWP 페이지를 표시하는 방식

Genian NAC가 HTTPS 통신을 하려는 PC에 CWP 페이지를 표시하는 방법입니다. 차단된 단말이 WEB 브라우저로 통신을 시도할때 GENIAN NAC 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 NAC에서 생성한 CA 인증서(FAKE 인증서)로 전송되어 암호화된 통신이 웹 서버에 연결되지 않고 Genian NAC로 세션이 설정되므로 네트워크센서에서 통신 내용을 확인할 수 있습니다.

따라서 Genian NAC는 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 NAC가 CWP 페이지를 표시하지 못하는 경우와 보안 정책을 준수하지 않는 사용자를 제어하는 방법에 대해 설명하겠습니다.

제어 대상 PC가 HTTPS 사이트에 액세스 할 때 Genian NAC는 자체 인증서를 특정 사이트 인증서 대신 제어 대상 PC에 전달합니다.

여기서 브라우저는 **Genian NAC**에서 받은 인증서의 PIN 값을 사전 등록된 특정 사이트의 PIN 값과 비교합니다. PIN 값이 서로 다른 것으로 판단되면 Genian NAC는 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

Note: 5.0.53(LTS) 버전부터 Proxy를 통한 연결시에도 CWP Redirect가 동작하도록 개선되었습니다.(#25704)

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";
};
```


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.

NAC는 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 NAC 정책서버 내에 생성된 로컬 데이터베이스에 인증을 시도합니다. 자격 증명이 일치하면 사용자가 네트워크를 이용할 수 있습니다.

외부 (Active Directory, RADIUS, IMAP, POP3, SMTP, CSV)

NAC는 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 접속 인증페이지(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

에이전트는 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 에이전트는 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 메뉴를 찾습니다. 추가 를 클릭합니다.
6. 다음을 입력합니다:
 - 항목: 에이전트
 - 조건: 설치상태
 - 설정: 설치됨
7. 수정 버튼을 클릭합니다.

- 우측 상단의 변경정책적용 버튼을 클릭합니다.

2단계. 에이전트 플러그인을 통한 사용자 인증 설정

- 상단 항목에서 정책 으로 이동합니다.
- 왼쪽 정책 항목에서 정책 > 노드정책 > 노드액션 으로 이동합니다.
- 에이전트 인증창 을 찾아 클릭합니다.
- 원하는 조건 및 에이전트 옵션 설정 를 추가합니다.
- 수정 을 클릭합니다.
- 우측 상단의 변경정책적용 버튼을 클릭합니다. 단기를 클릭합니다.

3단계. 에이전트 인증을 위한 노드 정책을 생성

- 상단 항목에서 정책 으로 이동합니다.
- 왼쪽 정책 항목에서 정책 > 노드정책 으로 이동합니다.
- 작업선택 > 생성 을 클릭합니다. 노드정책 마법사 의 단계를 완료합니다.
- 정책 기본설정 탭에서 ID 를 에이전트 인증 으로 입력합니다.
- 노드그룹 설정 탭에서 에이전트 인증 노드 그룹을 선택하고 선택 위치로 이동합니다.
- 정책 세부설정 탭에서 원하는 옵션 을 입력합니다.
- 노드액션 설정 탭에서 에이전트 인증창 을 선택하고 선택 위치로 이동합니다.
- 위험감지 설정 탭 (이 탭에는 아무것도 필요하지 않습니다)
- 완료 를 클릭합니다.
- 우측 상단의 변경정책적용 버튼을 클릭합니다. 단기를 클릭합니다.

노드 정책에 에이전트 액션 할당

- 상단 항목에서 정책 으로 이동합니다.
- 왼쪽 정책 항목에서 정책 > 노드정책 으로 이동합니다.
- 원하는 노드정책 명을 찾아 클릭합니다.
- 노드액션 설정 에서 할당 을 클릭합니다.
- 에이전트 인증창 액션을 선택 위치로 이동 시킵니다.
- 추가 를 클릭합니다.
- 수정 를 클릭합니다.
- 우측 상단의 변경정책적용 버튼을 클릭합니다. 단기를 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 NAC에는 802.1x 포트 기반 액세스 제어를 지원하는 자체 RADIUS 서버가 있습니다. 일반적으로 802.1x는 무선 네트워크에 접속하는 단말에 대해 향상된 사용자 인증을 제공하는데 널리 사용됩니다. 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 > RADIUS 서버 로 이동합니다.
3. RADIUS 서버 > 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 > RADIUS 서버 로 이동합니다.
3. RADIUS 서버 > 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 > **RADIUS 서버** 로 이동합니다.
3. **RADIUS 서버 > 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 > **RADIUS 서버** 로 이동합니다.
 3. RADIUS 서버 화면에서 **RADIUS Authentication Server > MAC 인증** 옵션을 찾습니다.
 - **MAC 인증 옵션 On** 설정
 - **노드그룹 옵션**에서 MAC 인증을 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 NAC가 타사의 인증을 활용한 SSO 구현가이드

AD Dommain Login

Genian NAC는 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 설정해야 합니다. 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 등과의 통신이 원활한 상태여야 합니다.

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 설정시 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 NAC에 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 NAC는 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. wmicgmt.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 액세스 권한을 부여하면 계정 시작(Acct-Status-Type 속성의 값이 "start"인 RADIUS Account Request 패킷)이 NAS에서 RADIUS 서버로 전송되어 사용자의 네트워크 액세스 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 액세스가 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 NAC가 아닌 다른 인증서버에서 인증한 결과를 가지고 NAC에 인증한 것으로 대체하는 인증방법입니다.

RADIUS 대체인증 설정

1. 상단 항목의 설정 으로 이동합니다.
2. 왼쪽 설정 항목에서 서비스 > RADIUS 서버 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 **PowerPack**의 사용자인증 수행 시 **Genian NAC**에는 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 사용자 인증을 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 항목**에서 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 1회만 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) 액션수행설정 에서 다음과 같이 설정 값 입력

설정 항목	설정 값	참고
라이브러리 경로	선택 박스 : %SystemDrive% 선택 / 입력 값 : \Program-Data\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 인증 여부를 확인하여, PowerPack에서 인증 정보가 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-SSO**의 사용자인증 수행 시 **Genian NAC**에는 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 (세부 버전은 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 플러그인입니다.
 - 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 접근 제어 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 **SafePC**의 사용자인증 수행 시 **Genian NAC**에는 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 (세부 버전은 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 설정 되어 있지만, 고객사에서 예외적으로 변경된 경우 경로와 파일명을 확인 후 연동을 위한 *Genian NAC 설정 > Step 2: 에이전트 플러그인 설정 > 3번 항목*에서 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	선택박스: %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 인증 여부를 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 선택박스에서 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 (세부 버전은 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 선택트박스에서 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

유비엔티스랩 PassNI SSO

본 가이드는 통합인증 보안플랫폼(SSO)인 유비엔티스랩 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-Ni로그인만으로 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 유비엔티스랩의 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. (새울시스템등과 추가 연동시, 안내페이지의 형태가 다를 수 있습니다)

사전준비 사항

연동을 위한 Genian NAC 에이전트 플러그인 준비

Genian NAC는 Pass-Ni와 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 (세부 버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상 (2020.08 Release 이후 버전)

Pass-Ni SSO의 사용자용 API 호출도구 및 사용을 위한 License Key 발급

- Pass-Ni 용 사용자 단말용 사용자 정보의 API 호출도구 (**SSO-CS-API-getUserInfo.zip** 와 같은 형태로 배포)
- Pass-Ni SSO 연동 Library 사용을 위한 License Key (각 기관마다 Pass-Ni가 별도로 제공하는 라이선스 키로 **3130312XXXXE352XXXX3** 와 같은 형식입니다.)

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 Pass-Ni와 연동을 위해 최소한의 부분만을 소개합니다. 최초 1회만 작업해주시면 이후엔 자동으로 적용됩니다.

Step 1: 연동을 위한 에이전트 플러그인 업로드

- Genian NAC Web콘솔에서 시스템 > 업데이트 관리 > 소프트웨어 > 에이전트 플러그인 메뉴로 이동
- 작업선택 > 플러그인 업로드 > 파일선택 버튼을 클릭하여 업로드할 **NAC-C_PassNiSSO-R-89967-1.1.8.gpf** 플러그인 선택
- 업로드 버튼 클릭

Step 2: 에이전트 플러그인 설정

- Genian NAC Web콘솔에서 정책 > 노드정책 > 노드액션 메뉴로 이동
- PassNi** 대체 인증 플러그인 클릭
- 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?initparameter	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 NAC과 KSignAccess 제품 간 연동 전, 사용자는 제품별로 각각 사용자인증을 수행하는 불편함이 있지만, 연동 후 두 제품간의 SSO가 구현되어 사용자는 **KSignAccess**의 사용자인증 수행 시 **Genian NAC**에는 사용자 인증이 자동으로 처리됩니다.

Genian NAC 에이전트 플러그인은 사용자의 인증을 위해 사용자PC에 암호화된 인증 정보가 담긴 토큰 값을 케이사인에서 제공하는 별도의 프로그램으로 복호화하여 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 NAC 가 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 선택트박스에서 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

파수 Fasoo DRM SSO 연동

본 가이드는 문서보안 솔루션인 파수사의 Fasoo Enterprise DRM(이하 Fasoo DRM)과 네트워크 접근제어 시스템인 Genian NAC의 인증 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

Genian NAC와 Fasoo DRM 제품 간 연동 전, 사용자는 제품별로 각각 사용자인증을 수행하는 불편함이 있지만, 연동 후 두 제품간의 SSO가 구현되어 사용자는 **Fasoo DRM**의 사용자인증 수행 시 **Genian NAC**에는 사용자인증이 자동으로 처리됩니다.

Genian NAC 에이전트 플러그인은 사용자의 인증을 위해 사용자PC에 구동중인 Fasoo DRM에서 제공하는 API를 이용하여 인증정보를 얻어와 Genian NAC에 대체인증 처리를 하고 네트워크를 사용할 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	
Genian NAC (에이전트)	V5.0 이상	
Fasoo DRM		

연동의 목적

Genian NAC와 파수사의 Fasoo DRM 연동은 다음의 효과를 제공합니다.

SSO 환경 제공

- 사용자는 Fasoo DRM에 먼저 사용자인증을 진행하고, Genian NAC 에이전트 플러그인 연동을 통해 Genian NAC 사용자인증이 자동으로 진행됩니다. Genian NAC는 Fasoo DRM의 사용자인증 여부를 통해 Genian NAC에 사용자인증이 대체되어 SSO 환경이 구성됩니다.

Fasoo DRM 미인증 사용자에게 네트워크 차단 사유 및 안내페이지 자동 연결

- Genian NAC는 Fasoo DRM 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 Fasoo DRM과 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_FasooSSO-R-118210-1.1.11.gpf (세부버전은 상이할 수 있음)	Genian NAC 에이전트 V5.0 이상

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 Fasoo DRM과 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_FasooSSO-R-118210-1.1.11.gpf 플러그인 선택
- 3) 업로드 버튼 클릭

Step 2: 에이전트 플러그인 설정

- 1) Genian NAC Web콘솔에서 정책 > 노드정책 > 노드액션 메뉴로 이동
- 2) Fasoo DRM 대체 인증 플러그인 클릭
- 3) 액션 수행설정 에서 다음과 같이 설정 값 입력
- 4) 고객사 식별 ID 를 Fasoo에서 발급한 해당 고객사별 SSO DomainID를 입력
- 5) 하단부 수정 버튼 클릭

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 선택트박스에서 연동API 선택
- 4) 하단 노드액션 설정 항목으로 이동 후 할당 버튼 클릭
- 5) Fasoo DRM 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 NAC는 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 (세부 버전은 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 PC의 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 ID가 존재함 (예. PSI_nac_CS_Prod / Genian NAC의 ISign+ 연동 ID)

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 ISign+와 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_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	ISign의 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 NAC의 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 NAC의 에이전트 플러그인을 이용하여, 사용자 PC와 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 노드그룹이 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 부수정 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 레지스트리 값과 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	입 력 값 : HKEY_LOCAL_MACHINE\SOFTWARE\NetMan\SNPC_SSOState	암호화된 사용자 정보가 저장된 레지스
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 Web 콘솔에서 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 선택박스에서 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 NAC 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 SK인포섹 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 (EagleEye) 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.

SK 인포섹 이글아이 (EagleEye) 인증 연동파일, 파일의 실행경로, 실행옵션 확인

SK 인포섹 이글아이 (EagleEye) 인증실행용 파일은 SK 인포섹에서 제공받아서 설치하여야 하며, 연동시 사용되는 경로와 실행옵션은 다음과 같습니다.

참고) 각 설정 값은 SK 인포섹 이글아이 (EagleEye) 의 연동인증 실행용 파일에 따라 달라질 수 있습니다.

- 1) SK 인포섹 이글아이 (EagleEye) 인증실행용 파일 (예. EYNAC.EXE)
- 2) 실행경로: C:\EY\NAC.EXE
- 3) 실행옵션: cmd=-nac "-authid:{AUTH_ID}"

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 SK 인포섹 이글아이 (EagleEye) 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
경로 입력 창	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 항상수행하도록 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 업로드하는 하지 않으셔도 됩니다.

파수 Enterprise DRM 인증연동파일, 파일의 실행경로, 실행옵션, 암호화 방식의 확인(파수 제공)

파수Enterprise DRM 인증실행용 파일은 (주)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, SEED 중 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\fssoex_cast.exe 2) C:\WINDOWS\System32\fssoex_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	상호협의를 한 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.

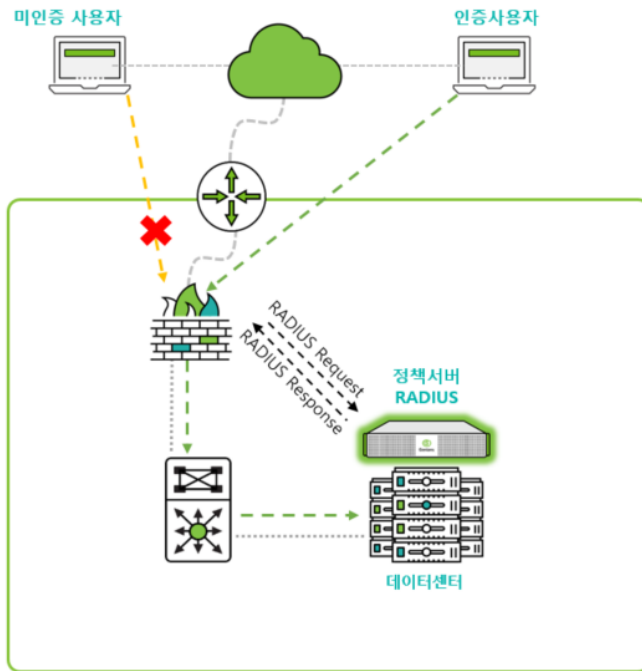
- 1) Genian NAC Web 콘솔에서 정책 > 노드정책 메뉴로 이동

- 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 RADIUS 서버는 VPN 환경에서 인증서버로 사용할 수 있으며 인증 사용자에 대한 제한이 가능합니다.

Genians VPN 제어 - 미인증 사용자



주요사항
 에이전트 필요 없음
 AD/Local 사용자 인증
 RADIUS CoA 필요없음

- RADIUS 제어**
- VPN서버에서 지니언스로 인증 요청
 - 지니언스 거부응답 메시지 전송
 - 사용자 VPN 연결 불가

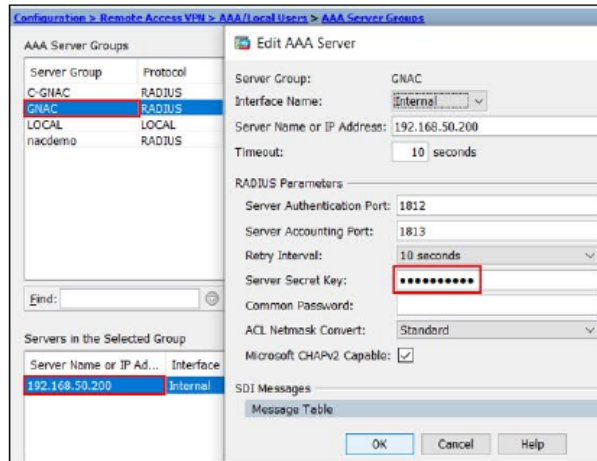


Radius 서버 연동

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** 정책을 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 않는 경우 인증 요청이 정의된 조건에 충족하면 접근이 거부 됩니다.

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: 사용자ID, 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 합니다.
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) 사용 여부를 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 체크박스를 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 NAC에서 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 생성을 참고하십시오.

7.2.6 사용자 신청서를 통한 사용자 관리하기

Genian NAC 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. 왼쪽 사용자 신청서 항목에서 신규등록 을 선택합니다.
3. 오른쪽 신청서 리스트에서 번호를 클릭하여 신청서 세부정보를 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. 왼쪽 사용자 신청서 항목에서 결과조회 을 선택합니다.

Note: 처리결과 리스트에서 번호를 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 NAC에서 사용되는 사용자 계정에 기본정보를 표시합니다.

항목	세부항목	설명	수정 가능 여부
기본 설정	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
	계정 사용 만료	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 NAC에 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 대상으로 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.	
마지막인증시각	사용자 계정에 마지막 인증시각을 정보로 그룹을 생성합니다.	
만료시각	사용자 계정에 사용 제한 시간 정보로 그룹을 생성합니다.	
멤버쉽	AD/LDAP 맴버쉽(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 NAC에 등록된 사용자 계정정보를 부서와 직급에 형태에 맞추어 현황을 확인할 수 있습니다.

1. 사용자 전체 현황 확인하기

관리>사용자>전체사용자 항목에서 NAC 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
사용자그룹 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 비밀번호가 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 인증을 **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 SSL연결을 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.

이메일은 대부분의 조직에서 제공하는 서비스이므로 사용자 디렉토리를 제공하는 것이 가장 쉽습니다. 이메일에서 사용되는 **SMTP**, **POP3** 및 **IMAP** 을 사용하여 사용자의 아이디와 비밀번호를 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 NAC는 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 NAC 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 NAC가 SAML을 통해 Google과 통합되면 Genian NAC는 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 NAC 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 NAC의 인증연동 기능을 수행하기 위한 설정 방법을 안내합니다.

Genian NAC와 Okta 솔루션의 APP 연동을 통하여 Genian NAC 자체 사용자DB를 관리할 필요가 없이 Okta를 통해 사용자 인증을 수행할 수 있습니다.

사용자 인증을 위해 Genian NAC CWP 페이지에서 SAML2.0 프로토콜을 이용하여 Okta 인증을 호출하고 Okta에서 사용자인증여부를 확인하여 정상적인 SSO가 이루어집니다.

권장버전

제품명(구성요소)	버전	비고
Genian NAC(정책서버)	V5.0 이상	2020.05 이후 Release 버전
Okta APP	SAML2.0	2021.05 현재 연동기능

연동의 목적

Genian NAC와 Okta 연동은 다음의 효과를 제공합니다.

- NAC, Okta 개별 인증을 위한 사용자DB 관리 불필요
- Okta 계정을 이용하여 NAC 인증가능

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 NAC와 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 Account' 버튼을 클릭하여 계정을 활성화 하십시오.
 - 인증을 위한 초기패스워드 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

General tab(Okta APP에 Genian NAC의 SP정보를 입력)

1. 메뉴에서 **Applications > Applications** 로 이동합니다.
2. **Browse App Catalog** 메뉴에서 Genians NAC application을 검색하세요.
3. 검색된 NAC 앱을 선택한 후 **Add Integration** 버튼을 클릭하여 추가합니다.
4. Sign On 탭을 선택하세요.
5. 화면 중간에 **Sign on methods > SAML 2.0 > More details** 버튼을 클릭하여 IdP 정보를 확인합니다.
6. Genian NAC ****Web 콘솔 > 설정 > 사용자인증 > 인증연동 > SAML2 인증연동****에 다음 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.
 - JIT provisioning 기능을 사용하려면 **JIT provisioning** 을 'On' 으로 변경하십시오.
 - 추가정보 추가를 통해 사용자 계정의 이름, 이메일 등을 설정하십시오.
 - Single Logout(SLO)를 사용하려면 **Single Logout(SLO)** 설정을 'On' 하십시오.
 - SP X.509 certificate 를 다운로드해서 okta의 **Signature Certificate** 에 업로드 하십시오. SLO 기능을 사용하기 위해서는 SP의 인증서가 필요합니다.
 - **IdP SLO URL** - Okta의 **Single Logout URL**.
 - Signed Requests를 사용하려면 **Signed Requests** 설정을 'On' 하십시오.
 - 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.
7. Genian NAC CWP 인증 화면에서 표시할 Okta 인증버튼에 표시할 문구를 **로그인 버튼** 문구에 입력합니다.
8. Genian NAC Web 콘솔 설정 화면 하단 수정 버튼을 클릭합니다.

Note: General tab의 subDomain 필드에 올바른 값을 입력했는지 확인하세요. 잘못된 값을 사용하면 SAML을 통해 NAC로 인증할 수 없습니다.

- JIT provisioning 기능을 사용하기 위해서 SAML Attributes를 설정해야 합니다.
- 지원되는 SAML Attributes 입니다.

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

Step 3: Okta 인증연동에 사용할 계정 추가 및 할당

이미 사용자가 등록되어 있다면 5번으로 이동

1. Okta 콘솔화면 메뉴 **Directory > Groups** 으로 이동합니다.
2. 화면 중간 **Add Group** 버튼을 클릭하여 그룹을 생성합니다.
3. Okta 콘솔화면 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 콘솔화면 메뉴 **Application > Application** 으로 이동합니다.
6. 위에서 등록한 APP 우측 삼각형아이콘을 클릭하여 **Assign to Users** 를 클릭합니다.
7. 팝업화면에서 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 NAC SAML App을 클릭한다.

Genian NAC Web 콘솔에서 테스트하는 방법 (SP-initiated SSO)

1. Web 콘솔에 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 NAC CWP 페이지에서 테스트하는 방법 (SP-initiated SSO)

1. Genian NAC 노드정책 비밀번호 정책을 할당 받은 단말(노드)를 준비합니다.
2. Genian NAC CWP 페이지에 접속합니다.

3. CWP 페이지에 인증 버튼을 클릭합니다.
4. 인증화면에 위 Step2 5번 항목에서 설정한 인증버튼을 클릭합니다.
5. 새로운 팝업창에 Okta 인증페이지가 표시되며 사용자명, 암호를 입력하여 인증합니다.
6. '인증에 성공하였습니다.' 메시지가 표시되면 정상적으로 인증연동이 되었습니다.

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 NAC의 인증연동 기능을 수행하기 위한 설정 방법을 안내합니다.

관리자 인증을 위해 Genian NAC Web 콘솔 페이지에서 SAML2.0 프로토콜을 이용하여 Okta 인증을 호출하고 Okta에서 사용자인증여부를 확인하여 정상적인 SSO가 이루어집니다.

권장버전

제품명(구성요소)	버전	비고
Genian NAC(정책서버)	V5.0 이상	2022.05 이후 Release 버전
Okta APP	SAML2.0	2021.05 현재 연동가능

연동 전 필요한 사항

연동의 목적

Genian NAC와 Okta 연동은 다음의 효과를 제공합니다.

- NAC, Okta 개별 인증을 위한 사용자DB 관리 불필요
- Okta 계정을 이용하여 NAC 인증가능

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 NAC와 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 Account' 버튼을 클릭하여 계정을 활성화 하십시오.
 - 인증을 위한 초기패스워드 변경과 2차 인증에 대한 설정을 합니다.
 - Okta 콘솔접속시 OTP 2factor 인증을 요구하며 아이폰, 안드로이드 OTP 앱 설치 및 OTP등록이 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 NAC application을 검색하세요.
3. 검색된 NAC 앱 선택한 후 **Add Integration** 버튼을 클릭하여 추가합니다.
4. Sign On 탭을 선택하세요.
5. 화면 중간에 **Sign on methods > SAML 2.0 > More details** 버튼을 클릭하여 IdP 정보를 확인합니다.
6. Genian NAC Web 콘솔 > 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.
 - JIT provisioning 기능을 사용하려면 **JIT provisioning** 을 'On' 으로 변경하십시오.
 - 추가정보 추가를 통해 사용자 계정의 이름, 이메일을 설정하십시오.
 - 관리자 관리역할 추가를 통해 관리역할이 설정될 수 있도록 하십시오.
 - * SP X.509 certificate 를 다운로드해서 okta의 Signature Certificate 에 업로드 하십시오. SLO 기능을 사용하기 위해서는 SP의 인증서가 필요합니다.
 - * IdP Attribute에 Group Attribute에서 설정한 이름 (예) _ADMINROLE_superAdmin) 을 입력하시기 바랍니다.
 - Single Logout(SLO)를 사용하려면 **Single Logout(SLO)** 설정을 'On' 하십시오.
 - **IdP SLO URL** - Okta의 **Single Logout URL**.
 - Signed Requests를 사용하려면 **Signed Requests** 설정을 'On' 하십시오.
 - 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.
7. Genian NAC Web 콘솔 인증 화면에서 표시할 Okta 인증버튼에 표시할 문구를 **로그인 버튼** 문구에 입력합니다.
8. Genian NAC Web 콘솔 설정 화면 하단 수정 버튼을 클릭합니다.

Note: General tab의 subDomain 필드에 올바른 값을 입력했는지 확인하세요. 잘못된 값을 사용하면 SAML을 통해 NAC로 인증할 수 없습니다.

- 지원되는 SAML Attributes :

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

- JIT provisioning 기능을 사용하기 위해서 Group Attributes를 설정해야 합니다.

- 아래의 예와 같이 Name에 `_ADMINROLE_` prefix를 붙여서 지정해야 합니다.

Name	Filter
<code>_ADMINROLE_superAdmin</code>	<code>Equals superAdmin</code>

Step 3: Okta 인증연동에 사용할 계정 추가 및 할당

이미 사용자가 등록되어 있다면 5번으로 이동

1. Okta 콘솔화면 메뉴 **Directory > Groups** 으로 이동합니다.
2. 화면 중간 **Add Group** 버튼을 클릭하여 그룹을 생성합니다.
 - JIT provisioning 기능을 위해서는 관리자 Role Group을 생성해야한다. (e.g. superAdmin)
3. Okta 콘솔화면 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. 팝업화면에서 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 NAC SAML App을 클릭한다.

Genian NAC Web 콘솔 페이지에서 테스트하는 방법 (SP-initiated SSO)

1. Genian NAC Web 콘솔 페이지에 접속합니다.
2. **SAML 로그인** 버튼을 클릭합니다.
3. 인증화면에 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. geniains.okta.com)
6. 생성 클릭
7. 권한 메뉴로 이동
8. 생성한 네트워크객체를 이용하여 권한 생성
9. 단말 네트워크를 제어하는 제어정책에 생성한 권한 할당

Google G Suite(SAML2.0)

본 가이드는 G-suit와 Genian NAC의 인증연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

Genian NAC와 Google G Suite를 연동하여 Genian NAC 자체 사용자 DB를 관리할 필요 없이 Google G Suite를 통해 사용자 인증을 수행할 수 있습니다. 사용자 인증을 위해 Genian NAC CWP 페이지에서 SAML2.0 프로토콜을 이용하여 G-suite 인증을 호출하고 사용자 인증여부를 확인하여 정상적인 SSO가 이루어집니다.

연동 설정 방법

Step 1: Google G suite 연동을 위한 설정 방법

1. <https://admin.google.com> 에 로그인 합니다. (**Workspace 관리자 계정으로 로그인 합니다.**)
2. 좌측 콘솔 메뉴바에서 **앱 -> 웹 및 모바일 앱** 을 클릭합니다.
3. **앱 추가 -> 맞춤 SAML 앱 추가** 를 클릭합니다.
4. **앱 이름과 설명** 그리고 **앱 아이콘** 을 설정 합니다.
5. Genian NAC 웹 콘솔 접속 후, **설정 -> 사용자 인증 -> 인증 연동 -> SAML2 인증연동 -> 추가** 를 클릭합니다.
6. Google 관리 콘솔에 작성된 (**SSO URL, 엔티티ID, x.509 Certificate**) 값을 Genina NAC SAML2 인증연동 창에 (**IdP SSO URL, IdP Entity ID, x509 Certificate**) 입력합니다.
7. 반대로 Genian NAC SAML2 인증연동 화면에 작성된 값 (**SP Entity ID, SP ACS URL**) 을 Google 관리콘솔 창 (**ACS URL, Entity ID**) 에 입력합니다.
8. 정책 - 노드 정책 - 인증방법 - 인증방식 할당을 클릭하여 SAML2 인증을 추가 합니다.

step 2: Google G suite 연동을 위한 사용자 추가

1. Google 관리 콘솔 메인화면에 있는 사용자를 클릭합니다.
2. 새 사용자 추가 를 클릭합니다.
3. 사용자의 이름과 메일을 설정후, 새 사용자 추가 를 클릭합니다.
4. 메인화면 - 사용자 - 비밀번호 재설정 클릭 후, 사용자의 비밀번호를 재설정 합니다.

Note: Password 항목은 관리자가 패스워드를 지정하여 생성할지 사용자 최초로그인시 변경하도록 할지 선택 합니다.

Step 3: Google G suite 연동 테스트 진행

1. 설정 - 사용자 인증 - 인증연동 - 인증 테스트 클릭
2. 인증정보 저장소를 SAML2 로 수정
3. 출력되는 화면에서 설정한 SAML 인증 로그인 버튼을 클릭 - 로그인 진행
4. 정상적으로 설정되었을 경우 Google 로그인창이 출력되고, 인증에 성공하게 됩니다.
5. 감사로그에서 로그인한 계정의 ID와 로그인한 인증방식(SAML)을 확인할 수 있습니다.

Note: 인증연동 설정 후, 정책적용시 제어정책 권한에 IdP 도메인을 추가해주어야 차단상태에서도 인증연동 창이 표시됩니다.

- | |
|---|
| <ol style="list-style-type: none">1. 권한 추가 방법2. 정책 > 객체 > 네트워크3. 작업선택 > 생성4. 기본정보 입력5. 네트워크주소 > FQDN 선택 > IdP 도메인 입력 (e.g. accounts.google.com)6. 생성 클릭7. 권한 메뉴로 이동8. 생성한 네트워크객체를 이용하여 권한 생성9. 단말 네트워크를 제어하는 제어정책에 생성한 권한 할당 |
|---|

7.3.7 Webhook 인증연동

Webhook 인증연동은 사용자가 로그인 시도 시, Webhook 이벤트가 발생하고 Genian NAC는 Webhook URL을 호출하게 됩니다.

호출된 URL로부터 리턴 성공값이 Genian NAC로 반환되면 사용자 로그인이 되는 인증방식 입니다.

다음은 Webhook 인증연동을 사용하기 위한 설정 방법입니다.

1. 정책 - 노드정책 클릭 후, Webhook 인증을 사용할 노드정책을 선택합니다.
2. 노드정책 세부 설정에 있는 인증방식에 할당 버튼을 클릭후 Webhook을 추가합니다.(인증방식 목록 상단에 위치한 인증방식부터 인증에 사용됩니다.)
3. 설정 - 인증연동 - Webhook 인증연동 으로 이동합니다.
4. 이벤트 발생시 호출할 URL 과 호출 방식을 설정 합니다.(GET,POST 중 호출방식을 선택합니다.)

```

예시) 데이터 형식 - json
GET 방식: http://호출할 URL/?id={_USERID}&pwd={_USERPASSWORD}
POST 방식: http://호출할 URL/

```

5. POST 방식일 경우 **데이터전송타입** 을 선택 후, 데이터 형식에 맞는 POST 데이터를 입력합니다.

```

예시) 데이터 형식 - application/json
POST 데이터 : id={_USERID}&pwd={_USERPASSWORD}

```

6. 결과검증 정규식을 입력합니다. (리턴 성공값을 작성합니다.)
7. 결과메세지 정규식을 입력합니다.
8. 결과메세지 문자셋을 설정합니다.

Note: SSL 기반 암호화 통신 사용을 위해서는, Webhook URL을 https로 수정합니다.

7.3.8 인증 연동 테스트

RADIUS, LDAP, IMAP, POP3, SMTP 또는 **Webhook** 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. NAC는 RDBMS, LDAP, CSV, Google G Suite, REST API Server 등 다양한 외부시스템을 지원합니다.

7.4.1 동기화 테스트

1. 상단 탭에서 **설정** 을 클릭합니다.
2. 왼쪽 설정 탭에 **사용자 인증 -> 정보 동기화** 를 클릭합니다.
3. 생성한 작업을 선택하고 **작업선택 -> 즉시수행** 을 클릭합니다.
4. **웹 콘솔 -> 감사로그** 에서 동기화 성공 여부를 확인할 수 있습니다.

Note: 동기화를 여러 소스로부터 수행하는 경우, 소스별로 작업을 구분하기 위해 데이터소스 구분 값을 설정합니다. 데이터소스 구분 값이 서로 다른 각각의 동기화는 다른 DB에서 동기화한 내용이 삭제되지 않도록 합니다. 하지만 데이터소스 구분 값을 설정하지 않을 경우, 모두 삭제하고 동기화합니다.

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: 정책서버와 동기화 서버 간 정상적인 통신 여부를 우선적으로 확인하여 접속 테스트를 사전에 수행하시기 바랍니다.

동기화 설정하기

1. 상단 항목의 설정으로 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.(CSV를 사용할 경우 비워 둡니다).
8. 생성 버튼을 클릭합니다.
9. 정보 동기화 목록에서 동기화하고자 하는 항목을 선택합니다.
10. 작업선택 > 즉시수행 을 클릭합니다.

LDAP (Active Directory)

Genian NAC는 LDAP 디렉토리를 사용자 및 조직 정보의 소스로 사용할 수 있습니다. LDAP 동기화를 통해 사용자 계정을 로컬에서 생성하여 관리 또는 정책에 사용할 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 정책서버와 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 적용함을 선택합니다. 동기화 설정이 여러 개인 경우 적용안함으로 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 설정해야 합니다. *LDAP (Active Directory) 서버 연동* 을 참조합니다.

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, 부서, 직급, 노드, 및 장비수명주기) 항목들을 찾아 필요한 정보를 추가 합니다. (CSV를 사용할 경우 비워 둡니다)
8. 정보 동기화 리스트에서 원하는 동기화 목록의 체크박스 를 클릭합니다.

9. **작업선택 > 즉시수행** 을 클릭합니다.

Google G Suite

Genian NAC는 G Suite 디렉토리를 사용자 및 조직 정보의 소스로 사용할 수 있습니다. G Suite 동기화를 통해 사용자 계정을 로컬에서 생성하여 관리 또는 정책에 사용할 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 정책서버와 동기화 서버 간 정상적인 통신 여부를 우선적으로 확인하시기 바랍니다.

Note: 유튜브를 통해 Google G suit 가이드 영상을 확인 할 수 있습니다 

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 선택합니다. 일반적으로 admin 권한의 계정인 경우 admin_view 를, 그렇지 않은 경우 domain_public 을 선택합니다.

사용자정보 옵션

1. 사용자테이블명: users 을 입력합니다.
2. 사용자ID 컬럼명: primaryEmail 을 입력합니다.
3. 사용자이름컬럼명: name/fullName 을 입력합니다.
4. 부서ID 컬럼명: orgUnitPath 을 입력합니다.

부서정보 옵션

1. **Table Name:** orgunits 을 입력합니다.
2. 출력정렬순서: 부서명을 기준으로 출력하기 위해 @NAMEPATH 을 입력합니다.
3. 부서ID 컬럼명: 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 설정해야 합니다. 외부 인증서버 설정의 SAML 2.0 을 참조합니다.

REST API Server

Genian NAC는 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.

NAC 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 정책서버와 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>, NAC의 경우 [https://\(정책서버IP\):8443](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 방법을 참고하시기 바랍니다.
 - 컬럼명은 JSON Object에서 값을 추출하기 위한 경로를 입력합니다. 경로는 . 으로 구분합니다.
 - 예) JSON Response [{ "id": "..", "name": ".." }, { "id": "..", "name": ".." }] 인 경우에 ID 컬럼명은 id, 이름컬럼명은 name 을 입력합니다.
 - 예) JSON Response { "users": { "members": [{ "id": "..", "name": ".." }, { "id": "..", "name": ".." }] } } 인 경우에 ID 컬럼명은 users.members.id, 이름컬럼명은 users.members.name 을 입력합니다.
1. 사용자정보출처 : 사용자정보동기화를 위한 URI 정보를 입력합니다. 입력된 URI 설정은 서버주소 뒤에 경로명으로 추가됩니다.(예. /api/users.list 를 입력한 경우에 <https://slack.com/api/users.list> 를 호출합니다.)
 2. 사용자조건문 : 사용안함.
 3. 사용자ID 컬럼명 : JSON Object에서 사용자 ID 값의 경로를 입력합니다.(예. users.id)
 4. 사용자이름컬럼명 : JSON Object에서 이름 값의 경로를 입력합니다.(예. users.name)
 5. 부서ID 컬럼명 : 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, 로그인 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 로그인 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 NAC인증정보로 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 있는 경우 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 NAC에서는 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 나뉘집니다.

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 NAC에서 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 NAC 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 NAC에서 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 NAC에서 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 3일로 설정할 경우 사용자는 최소 1일부터 최대3일까지 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 90일 에서 3일 로 수정합니다.
6. 필수입력 설정 항목에 설정값을 ON 으로 변경합니다.
7. 수정 버튼을 클릭합니다.

엔드포인트 제어

엔드포인트 장치는 TCP/IP 네트워크에서 인터넷이 가능한 컴퓨터 하드웨어 장치입니다. 데스크톱 컴퓨터, 랩톱, 스마트폰, 태블릿, thin client, 프린터 또는 기타 특수 하드웨어에 이르기까지 다양합니다.

Genian NAC Agent를 사용하여 Windows 및 macOS 엔드포인트 단말을 제어 할 수 있습니다. 엔드포인트에 설치 되면 백그라운드에서 실행되고 엔드포인트에 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.

Note: Windows 기반 Agent 동작방식과 Plugin 교육 영상을 Online EDU Chapter 5 에서 확인 하실수 있습니다.



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 경로직접 입력**)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 SSL인증서 설치

- 옵션 선택: 에이전트가 정책서버의 SSL인증서를 사용자PC에 설치할지 여부를 선택합니다. (Windows and macOS 전용)

8.1.14 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

Genian NAC가 각 OS의 정보를 수집, 제어하기 위한 플러그인 목록은 다음과 같습니다.

PluginName	Description	Win-dows	macOS	Linux
ARP 관리	사용자 PC의 ARP 테이블에 대한 관리 작업을 수행합니다.	5.0.0~	5.0.31~	5.0.49~
DNS 제어	DNS 관련 로컬설정을 제어합니다.	5.0.0~		
IE보안옵션 제어	IE의 보안옵션을 강제화 하는 기능을 제공합니다.	5.0.0~		
Linux 업데이트	Linux의 업데이트 상태를 검사하고 보고합니다.			5.0.45~
macOS 업데이트	macOS의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.		5.0.11~	
Malware Detector	Insights ECO 시스템과 연동하여 단말에서 발생하는 악성코드를 감지합니다.	5.0.19~		

continues on next page

Table 1 - continued from previous page

PluginName	Description	Win-dows	macOS	Linux
TCP세션검사	주기적으로 TCP 세션수를 수집하며 임계치이상되는 세션수가 발견되면 네트워크 인터페이스를 차단합니다.	5.0.0~		
Windows 방화벽 제어	Windows 방화벽을 사용하여 사용자 네트워크를 제어합니다.	5.0.28~		
Windows 보안설정	시스템에 설정된 Windows 방화벽, 원격데스크탑, 자동실행의 동작을 제어합니다.	5.0.0~		
Windows 업데이트	Windows의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.	5.0.0~		
WMI정보수집	WMI를 통하여 시스템 정보를 수집합니다.	5.0.0~		
네트워크 공유폴더	네트워크에 공유된 폴더정보를 수집하며 일정시간 이상 공유되는 폴더를 제어합니다.	5.0.0~	5.0.47~	5.0.42~
네트워크 트래픽 제어	주기적으로 네트워크 사용량을 수집하여 설정된 수치 이상일 경우 네트워크 인터페이스를 차단합니다.	5.0.13~		
네트워크정보 수집	네트워크 인터페이스 정보와 탐지된 포트정보를 수집하여 노드정보에 표시합니다.	5.0.0~	5.0.11~	
모니터정보 수집	로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다.	5.0.0~	5.0.17~	
모양 및 개인설정	바탕화면, 화면보호기에 대한 설정 정보를 수집 및 제어합니다.	5.0.0~	5.0.15~	
무선랜제어	무선 네트워크 인터페이스에서 탐지되는 무선 AP에 대한 정보를 제공하며 허용되지 않은 AP 연결을 제한합니다.	5.0.0~	5.0.30~	
무선연결관리자	Wireless Connection Manager 프로그램에 대한 옵션및 동작을 제어합니다.	5.0.0~		
백신정보 수집	PC에 설치되어있는 백신프로그램 정보 및 백신으로 검출된 바이러스치료로그를 실시간으로 수집합니다.	5.0.0~	5.0.11~	5.0.46~
비밀번호유효성검사	계정의 비밀번호에 대한 유효성을 검사하고 검증되지 않은 비밀번호를 안전한 비밀번호로 변경시킵니다.	5.0.0~	5.0.61~	
사용자알림메시지	사용자에게 알림메시지를 표시합니다.	5.0.0~	5.0.27~	
소프트웨어정보 수집	설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.	5.0.0~	5.0.11~	5.0.42~
수행조건만 검사	액션에 설정된 수행 조건을 체크하는데 사용하는 플러그인 입니다.	5.0.0~	5.0.14~	5.0.42~
시스템 종료	지정된 시각에 Windows 시스템의 절전, 재시작, 종료를 수행합니다.	5.0.0~	5.0.17~	
에이전트 인증창	사용자인증 수행시 WEB페이지가 아닌 에이전트 자체 인증창을 사용합니다.	5.0.0~	5.0.15~	
운영체제정보 수집	Windows 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.	5.0.0~	5.0.11~	5.0.42~
유선인증관리자	유선인터페이스의 인증 설정 및 유선인증창에 대한 옵션을 정의합니다.	5.0.17~		
인터페이스 제어	위험이벤트 발생시 인터페이스를 사용안함으로 바꾸는 기능을 제공합니다.	5.0.0~		5.0.45~
장치제어	사용자 PC에서 사용금지된 장치들을 사용중지로 변경합니다.	5.0.0~	5.0.46~	
파일 배포v2	파일을 실행하거나 특정 위치에 다운로드합니다.	5.0.55~		

continues on next page

Table 1 – continued from previous page

PluginName	Description	Win-dows	macOS	Linux
프로그램 제거	제어판의 프로그램 제거에 등록된 프로그램중 제거 가능한 특정 프로그램을 제거합니다.	5.0.0~		
프로세스 강제종료	액션 검사조건에 설정된 프로세스에 대해서 강제종료 기능을 수행합니다.	5.0.0~	5.0.28~	5.0.48~
프린터정보 수집	컴퓨터시스템에 등록되어있는 프린터에 대한 정보를 제공합니다.	5.0.0~	5.0.16~	
필수 소프트웨어 검사	사용자 PC에 필수 소프트웨어가 설치되어있는지 검사합니다.	5.0.21~	5.0.21~	
하드웨어정보 수집	마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다.	5.0.0~	5.0.11~	5.0.42~
호스트명 변경	컴퓨터 이름을 변경하는 기능을 제공합니다.	5.0.0~	5.0.34~	
에이전트정보 외부 전송	에이전트가 가지고 있는 정보를 외부 프로그램에 전송합니다.		5.0.62~	

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 로그인 할 때 실행되며, 시스템 정보를 수집하고 수집이 완료되면 프로세스가 종료됩니다. (로그온 시 I회성 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 설정된 에이전트 작업을 수행하거나 설치할 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. Active Directory를 통해 에이전트를 배포하려는 경우 GPO, SCCM 또는 기타 소프트웨어 배포 메커니즘을 사용하십시오.
- **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 업데이트된 정책을 확인할 수 있도록 **시간**의 기간을 지정합니다.
- 1-4 시간 중에서 선택합니다.

8.3.7 에이전트정보삭제

- 정책 서버에 연결되지 않은 경우 에이전트정보를 삭제할 **시간, 일, 주 또는 개월**의 기간을 정의합니다. 이 기능을 사용하지 않으려면 **0**을 입력합니다.

8.4 운영체제별 플러그인 설정방법

Genian NAC Agent에서 단말에 정보를 수집하거나 단말의 설정을 제어하기 위한 플러그인을 운영체제별로 생성할 수 있습니다.

8.4.1 플러그인 타입별 구분사항

Genian NAC Agent에서 동작하는 플러그인은 다음과 같은 타입으로 분류할 수 있습니다.

분류	설명
단독 플러그인	노드정책에 하나만 할당할 수 있는 플러그인
멀티 플러그인	노드정책에 다수를 할당할 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. NAC는 이러한 시도들을 방지하기 위해 다음과 같은 기능을 제공합니다.

- 악의적인 사용자가 패킷을 가로채는 ARP Spoofing 공격 대응
 - 수동으로 ARP 항목을 Static 설정하지 못하도록 강제화하여 네트워크 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. **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 > IP 관리 탭 > IP 정책으로 이동하여 충돌 방지 설정을 구성합니다.

DNS 제어

DNS 관련 로컬 설정을 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 활성화/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 브라우저의 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 브라우저의 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 브라우저가 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 브라우저에 전화 번호, 전자 메일 주소 및 배달 주소 정보가 저장되는 기능을 사용하지 않도록 설정합니다.
- **결제 정보 저장 및 채우기** 에서는 크롬과 엣지 브라우저에 카드및 결제 세부 정보를 저장하고, 자동으로 채우는 기능을 사용하지 않도록 설정합니다.
- **결제수단 확인 허용** 에서는 엣지 브라우저에 사이트에서 저장된 결제수단이 있는지 확인하도록 허용하는 기능을 사용하지 않도록 설정합니다.
- **폼 자동완성** 에서는 IE 브라우저에서 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 수 있는 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
- NAC의 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** 메시지의 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 수행설정이 있습니다.

1. 정보수집동의의 경우 플러그인을 사용하기 위해서는 정보수집에 대한 사용자의 동의가 필요합니다.
2. 수집제외경로의 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 수집을 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 되었을 때 NAC는 이를 감지하고 네트워크 차단이 가능합니다.

- 다량의 TCP 연결을 시도하는 악성 코드 또는 사이트에 감염되었을 때 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 **TCP 세션검사**을 찾아 **선택** 항목으로 드래그하여 이동합니다.
6. 추가 버튼을 클릭합니다.
7. 수정 버튼을 클릭합니다.

TCP 세션검사 설정

1. 상단 항목의 **정책**으로 이동합니다.
2. 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션**으로 이동합니다.
3. 노드액션 관리창에서 **TCP 세션검사**을 찾아 클릭합니다.
4. 옵션 설정에서 **조건설정**을 입력합니다.

아래에서 세션정보 전송주기를 설정합니다.

1. 세션정보 전송주기에서 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.(*LISTENING* 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.

- 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

- 상단 항목의 **정책** 으로 이동합니다.
- 왼쪽 정책 항목에서 **정책 > 노드정책 > 노드액션** 으로 이동합니다.
- 노드액션 관리창에서 **Windows 보안설정** 을 찾아 클릭합니다.

아래 기본설정 이 있습니다.

- CWP 메시지** 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
- 라벨** 의 경우 **라벨** 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.

아래의 액션 수행설정 을 구성합니다.

- 게스트계정 잠그기** 에서 **On** 설정을 하여 게스트계정을 비활성화 시킵니다.
- Windows 방화벽** 에서 **강제사용** 선택하여 Windows 방화벽 설정을 활성화 시킵니다.
- 원격 데스크톱** 에서 **사용안함** 을 선택하여 원격 데스크톱 사용을 비활성화 시킵니다.(예: 미디어, 외부 장치, 기타)
- 복구 콘솔 자동 로그인** 에서 **사용안함** 을 선택하여 복구 콘솔에 대한 자동 관리 로그인 허용 값을 비활성화 시킵니다.
- 자동실행** 에서 **사용안함** 을 선택하여 외부 장치의 자동실행을 비활성화합니다.
- 시간 동기화서버** 에서 **강제사용** 을 선택하여 NTP(Network Time Protocol) 서버와의 시간 동기화를 적용합니다. 시간 동기화서버 주소 및 동기화 주기를 입력합니다.
- 절전모드 해제시 암호 보호** 에서 **강제사용** 을 선택하여 절전모드 해제시 암호 보호 설정을 적용합니다.(절전모드 해제 시 로그Off 상태에서 비밀번호 입력창이 나타나도록합니다)
- 빠른 시작 켜기** 에서 전원 단추 동작에 대한 빠른 시작 옵션을 설정합니다. (Windows 8 이상)
- Windows XP 예약작업** 에서 **사용안함** 을 설정하여 Windows XP의 스케줄링 된 작업만 제어합니다.
- 수정 버튼을 클릭합니다.
- 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
- 노드정책창에서 **기본정책** 을 클릭합니다.
- 노드액션 설정 을 찾아 **할당** 버튼을 클릭합니다.
- 사용가능** 항목에서 **Windows 보안설정** 을 찾아 **선택** 항목으로 드래그하여 이동합니다.
- 추가 버튼을 클릭합니다.
- 수정 버튼을 클릭합니다.

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 Microsoft에서 제공하는 업데이트 서버와의 연결방법 설정으로 나뉩습니다. 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. **Microsoft Windows Update** : 외부망(인터넷)에 연결된 Microsoft 제공하는 업데이트 서버와 통신하는 방식
2. **WSUS** : 내부망에 연결된 WSUS 서버와 통신하는 방식
3. **Offline Scan File** : 내부망에 연결된 Genian NAC 정책서버와 통신하는 방식

검색방법	연결방법	환경사항
Microsoft Windows Update	Microsoft 직접연결	전체 내부망 네트워크에 대한 방화벽 허용권한 필요
	NAC를 통한 연결 (다운로드)	전체 내부망 네트워크에 대한 방화벽 허용권한 필요
	NAC를 통한 연결 (다운로드+검색)	NAC 장비(NAC Proxy 서비스 설정된 대상)에 대한 방화벽 허용권한 필요
WSUS	WSUS 직접연결	WSUS 위치(서버팜)에 따라서 서버팜 방화벽 허용권한 필요
	NAC를 통한 연결 (다운로드)	WSUS 위치(서버팜)에 따라서 서버팜 방화벽 허용권한 필요
	NAC를 통한 연결 (다운로드+검색)	NAC 장비(NAC 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 **NAC를 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 NAC에 의해 네트워크가 차단된 대상에 대해서 운영체제 업데이트를 수행할 수 있도록 접속허용 도메인을 설정할 수 있습니다.

플러그인 설정

- 사용자가 시스템 지연등의 이유로 자동 업데이트를 꺼놓은 경우

1. 상단 항목의 정책으로 이동합니다.
2. 왼쪽 정책 항목에서 정책 > 노드정책 > 노드액션으로 이동합니다.
3. 노드액션 관리 창에서 **Windows 업데이트**를 찾아 클릭합니다.

아래 기본설정 이 있습니다.

1. **CWP** 메시지의 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**: 예약된 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 > 삭제 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 업로드했다면 정책 서버 Windows Update 정책 설정을 통해 주기적으로 인터넷에 액세스할 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. 다시 한번 센터에서 다운로드 를 클릭합니다.
8. 정책 서버 주소와 관리자 계정정보를 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 계정정보를 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 노드정책 > Windows 업데이트 정책 으로 이동합니다.
3. Windows 업데이트 창에서 원하는 업데이트 이름을 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 지시하는 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.

Windows 시스템 WMI 정보 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

도메인에 가입한 노드들의 시스템 정보는 에이전트가 없는 환경에서 WMI 쿼리를 통해 수집할 수 있습니다.
참조: [WMI 스캔](#)

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. 수행주기의 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 정의된 일정에 따라 실행될 때까지 기다리거나 지금 바로 실행하여 결과를 즉시 볼 수 있습니다.

1. 상단 항목의 정책으로 이동합니다.
2. 왼쪽 정책 항목에서 노드정책으로 이동합니다.
3. 기본정책의 체크박스를 클릭합니다.
4. 작업선택 > 즉시수행 을 클릭합니다. (이 작업을 실행하려면 몇 분 정도 기다립니다)
5. 관리 > 노드로 이동하여 에이전트가 설치된 Windows 노드의 IP 를 찾아 클릭합니다.
6. WMI 정보수집결과 항목을 찾아 WMI 결과를 확인합니다.

WMI 결과에 대한 상태 그룹 만들기

위에 생성된 노드액션의 WMI 결과를 바탕으로 상태 그룹을 만듭니다. 그런 다음 이 상태 그룹을 통해 네트워크 요구 사항에 따라 정책을 식별하고 적용할 수 있습니다.

1. 상단 항목의 정책으로 이동합니다.
2. 왼쪽 정책 항목에서 그룹 > 노드로 이동합니다.
3. 작업선택 > 상태그룹 생성 을 클릭합니다.

아래 기본정보를 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 그룹조건을 설정합니다.

1. "AND" 또는 "OR" 조건연산을 선택합니다. ("AND" 는 모든 조건이 만족되어야 합니다. "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	Names-pace	WMI Query
Battery Info	rootCIMV2	SELECT Caption FROM Win32_Battery
HDD Vendor	rootCIMV2	SELECT Caption FROM Win32_DiskDrive
HDD Size	rootCIMV2	SELECT Size FROM Win32_DiskDrive
HDD Model	rootCIMV2	SELECT Model FROM Win32_DiskDrive
HDD Serial	rootCIMV2	SELECT SerialNumber FROM Win32_DiskDrive
Volume Serial	rootCIMV2	SELECT VolumeSerialNumber FROM Win32_LogicalDisk
Graphics Card Info	rootCIMV2	SELECT Caption, DriverVersion FROM win32_VideoController
Graphics Card Res-olution	rootCIMV2	SELECT CurrentHorizontalResolution, CurrentVerticalResolution FROM Win32_VideoController
HP Driver Version	rootCIMV2	SELECT * FROM Win32_PnPSignedDriver WHERE Devicename LIKE 'HP%'
NDIS Driver Ver-sion	rootCIMV2	SELECT * FROM Win32_PnPSignedDriver WHERE Devicename LIKE 'NDIS%'
Printer Info	rootCIMV2	SELECT Drivename 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

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** 메시지의 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 허용에 대해 **On**으로 설정하여 읽기권한만 있는 폴더는 허용하고 쓰기권한이 있는 폴더는 공유를 해제합니다.
 - **Everyone** 권한 외 허용에 대해 **On**으로 설정하여 Everyone 권한이 존재하는 폴더만 공유를 해제합니다.
 - 관리폴더 허용을 **Off**로 설정하여 관리 공유에 대한 액세스를 비활성화합니다.(예: *admin\$, c\$, d\$, e\$*)
3. 공유해제알림 방법은 사용자메시지 또는 에이전트팝업을 선택하여 공유 해제를 사용자에게 알려줍니다.
 4. 수정 버튼을 클릭합니다.
 5. 왼쪽 정책 항목에서 노드정책으로 이동합니다.
 6. 노드정책 창에서 원하는 정책ID를 클릭합니다.
 7. 노드액션 설정을 찾아 할당을 클릭합니다.
 8. 사용가능 항목에서 네트워크 공유폴더를 찾아 선택 항목으로 드래그하여 이동합니다.
 9. 추가 버튼을 클릭합니다.
 10. 수정 버튼을 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 정책으로 이동합니다.
2. 왼쪽 정책 항목에서 정책 > 노드정책으로 이동합니다.
3. 노드정책창에서 원하는 노드정책ID를 클릭합니다.
4. 노드액션 설정을 찾아 할당 버튼을 클릭합니다.
5. 사용가능 항목에서 네트워크 트래픽 제어를 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.

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. 조건연산의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. 조건설정의 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. 전송주기에 대해 주기적 간격(초 - 시간)을 조정합니다.
3. 이동평균 시간의 경우, 전송주기보다 이동평균 시간을 더 크게 조정합니다.
4. 열린포트 정보 수집에 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** 메시지의 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 보호기정보수집** 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 로그인 화면 표시** 을 **On** 으로 설정하여 화면보호기 해제 시 Windows 로그인 화면 표시 기능을 활성화합니다.

3. **NAC 재인증**: 화면 보호기 해제 시 NAC 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 검사주기**: 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 잠금 화면에서 윈도우 로그인을 하고 화면 잠금 해제를 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.

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 감지 시간)	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** 메시지의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. 라벨의 경우 라벨을 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 제어 까지 가능)
 - 차단알림: **On** 을 설정하여 사용자에게 무선 AP 모드가 비활성화되었음을 알립니다.
5. 네트워크 요구 사항을 기반으로 **CWP** 메시지, 조건설정 및 플러그인설정을 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.

무선 연결관리자 구성

Wireless Connection Manager 프로그램에 대한 옵션 및 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 수행설정을 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 연결 하도록합니다.
 - **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 포맷만 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.

백신정보 수집

PC에 설치되어있는 백신프로그램 정보 및 백신으로 검출된 바이러스치료로그를 실시간으로 수집합니다. 다양한 벤더들의 백신 정보를 NAC에서 수집합니다.

바이러스 백신은 에이전트가 없는 환경에서 WMI 쿼리를 통해 탐지할 수 있습니다. 참조 : wmi 스캔

- 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 NAC에서 지원되는 모든 안티바이러스를 버전별로 확인합니다.

벤더	제품명	제품 버전	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, 최근검사시간	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~

continues on next page

Table 2 – continued from previous page

벤더	제품명	제품 버전	정보제공 항목	v4.0.1x	v5.0.x
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~
Hauri	ViRobot Security 1.0	1.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.59~
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~
Avira	Internet Security Suite	15.x	백신명, 현재패턴 버전명, 현재패턴 날짜	N/S	5.0.3~
Avira	Antivirus 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~
Bitdefender	Antivirus Plus	23.x	백신명, 제품버전, 실시간감시	N/S	5.0.14~
Bitdefender	Internet Security	23.x	백신명, 제품버전, 실시간감시	N/S	5.0.14~
Bitdefender	Total Security	23.x	백신명, 제품버전, 실시간감시	N/S	5.0.14~
Cylance	PROTECT	2.0.1420.13	백신명, 제품버전, 실시간감시	4.0.106~	5.0.24~
CrowdStrike	CrowdStrike FALCON Sensor		백신명, 제품버전, 실시간감시	N/S	5.0.29~
ESET	NOD32 Antivirus	9.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.3~
ESET	NOD32 Antivirus	12.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	N/S	5.0.3~

continues on next page

Table 2 – continued from previous page

벤더	제품명	제품 버전	정보제공 항목	v4.0.1x	v5.0.x
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~
Kaspersky	Antivirus		백신명, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
Kaspersky	End-point Security	11.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
McAfee	Desktop Protection		백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.3~
McAfee	Total Protection (VirusScan)	22.3	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시, 최근검사시간	4.0.106~	5.0.24~
McAfee	End-point 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 End-point 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	End-point	2.1.x	백신명, 제품버전, 현재패턴 버전명, 현재패턴 날짜, 실시간감시	N/S	5.0.17~

continues on next page

Table 2 - continued from previous page

벤더	제품명	제품버전	정보제공 항목	v4.0.1x	v5.0.x
Symantec	End-point 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	End-point 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** 메시지의 경우 정책에 따라 표시 할 메시지를 추가합니다.
2. 라벨의 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. 실시간감시**OFF** 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.
 - 강제검사는 마지막 바이러스 검사시각이 설정주기이상일때 강제로 검사를 수행합니다.(시간 - 개월 /0이면 수행하지 않음)
 - 검사 방식 은 전체검사 선택합니다.
 - 검사창 UI 숨기기를 **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 수행설정을 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 로그인 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 적용된 시점부터 적용 됩니다.)
 - **검사예외ID** : 검사 예외대상의 사용자 ID의 전체문자열을 입력합니다. (여러개 입력시 콤마로 구분, 대소문자를 구분하지 않습니다.)
4. 수행주기의 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 설치된 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 **CWP접속** 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 소프트웨어 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. (Windows에 하나, MacOS에 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. 수행주기의 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.

시스템 종료

지정된 시각에 Windows 시스템의 절전, 재시작, 종료를 수행합니다. 사용자의 시스템 전원을 제어하여 단말 보안을 강화합니다.

- NAC의 여러 제어 기능 중 시스템 전원 제어 제공
- 직원 퇴근시간에 맞춰 시스템 자동 종료

시스템 종료 옵션 구성

1. 동작방식의 경우 PC의 전원을 제어하는 방식(절전, 다시시작, 시스템 종료)을 선택합니다.
2. 강제화모드를 **On** 으로 설정하여 사용자가 취소할 수 없도록합니다.
3. 종료전 알림 시간에 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 마법사를 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.

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 발생하는 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.
 - 서브넷스캐너: 6시간 주기로 관리 네트워크(C Class)에 대한 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 노드정책명을 클릭합니다.
 - 노드액션 설정 항목에서 할당을 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.

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

Note: 유튜브를 통해 Slack 을 활용한 2차인증 가이드 영상을 확인할 수 있습니다.



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 HTML 을 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.

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. (Windows에 하나, MacOS에 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 인증을 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)

4 단계. 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. NAC의 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 이름을 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 이름을 입력합니다. (예: "USB 스토리지 정책")
 5. 노드그룹 설정 에서 할당 버튼을 클릭하고 노드그룹 을 선택합니다.
 6. 차단장치 설정 에서 할당 버튼을 클릭하고 USB 저장 장치를 선택합니다.

7. 1단계에서 설정한 장치그룹이 아니더라도 아래의 기본장치그룹으로 정의되어있는 항목을 선택할 수 있습니다.

Bluetooth	<ul style="list-style-type: none"> • 블루투스 클래스에 속한 장치
CD/DVD/Floppy	<ul style="list-style-type: none"> • CD롬, 플로피 디스크 드라이브 클래스에 속한 장치
Local Printer	<ul style="list-style-type: none"> • 로컬PC에 직접 연결된 프린터 (프린터 클래스에 속하는 장치를 제거) • 로컬 프린터가 장치목록에서 "사용안함" 상태여도 프린트출력이 가능하므로 장치를 제거한다.
USB Disk	<ul style="list-style-type: none"> • USB 타입의 저장장치 (장치속성의 인스턴스 경로가 'USBSTOR'로 시작하는 디스크 드라이브)
USB Network Adapter	<ul style="list-style-type: none"> • USB 포트로 연결된 네트워크 어댑터 (장치속성의 인스턴스경로가 'USB'로 시작하는 네트워크 어댑터)
USB Tethering	<ul style="list-style-type: none"> • 모바일기기에 USB 케이블로 연결된 네트워크 어댑터 (장치속성의 서비스가 usbrndis나 Netaapl인 네트워크 어댑터) • 안드로이드로 연결된 경우 네트워크 어댑터는 usbrndis 서비스를 사용하며, 아이폰의 경우 Netaapl 서비스를 사용한다.
Wireless Network Adapter	<ul style="list-style-type: none"> • 무선 네트워크 카드 장치

8. 만약 USB저장장치 중에서 제어를 허용할 별도의 장치가 존재한다면 **1단계**. 장치그룹생성과 동일하게 예외그룹을 생성하여 차단예외장치 설정에 할당할 수 있습니다.

9. 생성 버튼을 클릭합니다.

3 단계. 장치 제어 플러그인 설정

1. 상단 항목의 정책으로 이동합니다.
2. 왼쪽 정책 항목에서 정책 > 노드정책 > 노드액션으로 이동합니다.
3. 노드액션 관리창에서 장치제어를 찾아 클릭합니다.
4. 액션수행설정 > 장치제어 방식에서 제거 또는 중지를 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 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 플러그인 v2에서는 **Sigstore**에서 제공하는 소프트웨어 무결성 보장을 위한 도구를 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 추가되어 있습니다.

검증 방식	Sigstore Keyless Signing (Keyless)	Public Key Signing (self-managed-key)
검증 내용	<ul style="list-style-type: none"> • Google/Github/MS 에 서 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 	<ul style="list-style-type: none"> • 자체적으로 보유한 비밀키/공개키를 사용하여 배포 파일에 전자서명 수행 • 검증을 위한 인증서(공개키)는 노드액션 수신 시 배포
환경 구성	<ul style="list-style-type: none"> • 인터넷이 가능한 환경에서만 사용 가능 	<ul style="list-style-type: none"> • 인터넷망/폐쇄망 환경에서 모두 사용 가능
키 관리	<ul style="list-style-type: none"> • 별도의 키 사용하지 않는 방식으로 관리자 계정에 대한 보안만 요구 	<ul style="list-style-type: none"> • 별도의 비밀키를 안전하게 보관 필요
준비사항	<ul style="list-style-type: none"> • 배포파일 전자서명을 위한 cosign 바이너리 파일 필요 (Sigstore Git hub Release v2.1.1 하단 Assets 에서 cosign-windows-amd64.exe 다운로드) • 배포파일 전자서명/서명 검증에 사용되는 외부 인터넷 통신 허용 필요 (전자서명 PC, 정책서버, 사용자단말), 도메인 정보 • 배포파일 전자서명에 사용되는 OIDC(Google, Git, MS) 계정이 필요 	<ul style="list-style-type: none"> • 배포파일 전자서명을 위해 cosign 바이너리 파일이 필요 • 배포파일 전자서명에 사용될 키가 필요하며 cosign을 사용해 생성하거나 별도의 키 준비 필요
제약사항	<ul style="list-style-type: none"> • 최초 등록된 배포자에서 다른 배포자로 변경 불가 	<ul style="list-style-type: none"> • 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 인증서를 생성합니다.

이 인증서는 소프트웨어를 서명하는 데 사용되며, 서명된 소프트웨어는 **cosign**을 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. **cosign**을 다운로드 받아 배포파일 전자서명에 사용할 디렉토리에 저장합니다.
2. 파일명을 **cosign.exe**로 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. cmd창에 표시된 URL 정보를 복사하여 브라우저를 사용하여 Web페이지에 접속합니다.
7. cmd창에 표시된 8자리 문자 값과 cmd창에 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. 설명은 용도에 따라 다르게 사용하는 경우 어떤 목적으로 사용하는 노드액션인지 구분할 수 있습니다.
6. 라벨을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래의 액션 수행설정을 구성합니다.

7. OS 종류는 macOS, Linux, Windows 대상에 맞는 OS를 선택합니다.
8. 조건 설정은 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. 플러그인선택에서는 파일 배포 V2 를 선택합니다.
10. 배포 파일에는 업로드 버튼을 클릭하여 파일을 선택합니다.
11. 배포파일 검증방법은 Sigstore Keyless Signing을 선택합니다.
12. 신뢰하는 OIDC 발행자에는 전자서명 시 인증에 사용한 OIDC(Github, Google, Microsoft)를 선택합니다.
13. 신뢰하는 ID에는 전자서명 시 인증에 사용한 ID(email주소 형태)를 입력합니다.
14. Certificate는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 cert 파일을 추가합니다.
15. Signature는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 sig 파일을 추가합니다.
16. 배포 옵션의 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 노드정책으로 이동한 후 기본정책을 클릭합니다.
19. 노드액션 설정을 찾아 할당 버튼을 클릭합니다.
20. 사용가능 항목에서 파일 배포를 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. CMD창에서 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 공개키는 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 개인키를 관리하면서, 관리되고있는 PC 의 포맷 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 검증하기 위해서는 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(Signature 생성)

- **Public Key Signing 방식 - Step1.** 배포파일 전자서명 에서의 cosign.exe sign-blob 명령 과 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. 수행주기는 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. 수행주기는 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. 수행주기의 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 액션수행설정 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. (Windows에 하나, MacOS에 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 15자를 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. NAC는 이러한 시도들을 방지하기 위해 다음과 같은 기능을 제공합니다.

- 악의적인 사용자가 패킷을 가로채는 ARP Spoofing 공격 대응
- 수동으로 ARP 항목을 Static 설정하지 못하도록 강제화하여 네트워크 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 > IP 관리 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. 수행주기를 설정하여 일정에 따라 작업을 실행하는 시간 간격을 지정합니다. (시간 - 개월)
2. 지정시각점사의 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 플러그인설정이 있습니다.

1. 공유 폴더 정보 수집에 대해 **Off** 를 선택하여 네트워크를 통해 공유 폴더에 대한 정보를 수집하지 않습니다.
2. 공유폴더 해제에 대해 **On** 을 설정하여 폴더 공유 상태를 해제합니다.
 - 공유 허용 시간: 공유폴더의 임시 사용 가능 시간을 설정합니다. (초 - 개월)
 - 읽기권한만 허용에 대해 **On** 으로 설정하여 읽기권한만 있는 폴더는 허용하고 쓰기권한이 있는 폴더는 공유를 해제합니다. (smb_read_only 값 체크)
 - **Everyone** 권한 외 허용에 대해 **On** 으로 설정하여 Everyone 권한이 존재하는 폴더만 공유를 해제합니다. (smb_guest_access 값 체크)
3. 공유해제알림 방법은 사용자메시지 또는 에이전트팝업을 선택하여 공유 해제를 사용자에게 알려줍니다.
4. 수정 버튼을 클릭합니다.
5. 왼쪽 정책 항목에서 **노드정책** 으로 이동합니다.
6. 노드정책 창에서 원하는 정책ID 를 클릭합니다.
7. 노드액션 설정을 찾아 할당을 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 기본설정이 있습니다.

1. **CWP** 메시지의 경우 정책에 따라 표시할 메시지를 추가합니다.
2. **라벨**의 경우 **라벨**을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래 플러그인설정이 있습니다.

1. 전송주기에 대해 주기적 간격(초 - 시간)을 조정합니다.
2. 열린포트 정보 수집에 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 NAC에서 수집합니다.

- 글로벌 벤더의 백신명, 버전, 패턴정보, 실시간 감시 정보 등을 수집하여 단말보안을 강화합니다.

백신 지원 목록

Genian NAC에서 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~
ESET	Endpoint Security	백신명, 제품버전, 현재패턴 버전명, 패턴 생성 날짜, 실시간 감시 여부, 최근검사시간	5.0.46~

백신정보 수집

1. 상단 항목의 정책으로 이동합니다.
2. 왼쪽 정책 항목에서 정책 > 노드정책 > 노드액션으로 이동합니다.
3. 노드액션 관리창에서 백신정보 수집을 찾아 클릭합니다.

아래 기본설정 이 있습니다.

1. **CWP** 메시지의 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 CWP접속 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 CWP접속 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 마법사를 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 소프트웨어 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. 수행주기의 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.

- NAC의 여러 제어 기능 중 시스템 전원 제어 제공
- 직원 퇴근시간에 맞춰 시스템 자동 종료

시스템 종료 옵션 구성

1. 동작방식의 경우 PC의 전원을 제어하는 방식(잠자기, 재시동, 시스템 종료)을 선택합니다.
2. 강제화모드를 **On** 으로 설정하여 사용자가 취소할 수 없도록합니다.
3. 종료전 알림 시간에 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 인증 보다 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.

- 수정 버튼을 클릭합니다.

에이전트를 통한 사용자 인증 설정

- 상단 항목의 정책 으로 이동합니다.
- 왼쪽 정책 항목에서 정책 > 노드정책 > 노드액션 으로 이동합니다.
- 노드액션 관리 창에서 에이전트 인증창 을 찾아 클릭합니다.
- 이미지 사용 의 경우 에이전트 인증창의 이미지를 지정합니다.
- 타이틀바 표시 의 경우 에이전트 인증창의 타이틀 문구를 표시할지를 지정합니다. (OS X Yosemite 이상)
- 배경색 은 인증 창의 색상을 지정합니다.
- 글자색 은 대화상자의 글자색상을 나타냅니다.
- HTML 사용 은 HTML을 사용하여 도움말을 표시합니다.
- 수정 버튼을 클릭합니다.

운영체제 정보 수집

Windows 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.

- 관리자가 운영체제 정보를 수집하여 운영체제별 별도 정책 적용
- 상단 항목의 정책 으로 이동합니다.
 - 왼쪽 정책 항목에서 정책 > 노드정책 > 노드액션 으로 이동합니다.
 - 노드액션 관리창 작업선택 오른쪽의 드롭다운 버튼을 클릭하여 macOS 운영체제를 선택합니다.
 - 노드액션 리스트에서 운영체제정보 수집 를 찾아 클릭합니다.

아래 기본설정 이 있습니다.

- CWP 메시지 의 경우 정책에 따라 표시 할 메시지를 추가합니다.
- 라벨 의 경우 라벨 을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류 할 수 있습니다.
- 수정 버튼을 클릭합니다.
- 왼쪽 정책 항목에서 노드정책 으로 이동합니다.
- 적용하고자 하는 노드정책 을 클릭합니다.
- 노드액션 설정 을 찾아 할당 을 클릭합니다.
- 사용가능 항목에서 운영체제정보 수집 을 찾아 선택 항목으로 드래그하여 이동합니다.
- 추가 버튼을 클릭합니다.
- 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 이름을 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 이름을 입력합니다. (예 : "USB 스토리지 정책")
 5. 노드그룹 설정 에서 할당 버튼을 클릭하고 노드그룹 을 선택합니다.
 6. 차단장치 설정 에서 할당 버튼을 클릭하고 USB 저장 장치를 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 중지를 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 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.

검증 방식	Sigstore Keyless Signing (Keyless)	Public Key Signing (self-managed-key)
검증 내용	<ul style="list-style-type: none"> • Google/Github/MS 에 서 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 	<ul style="list-style-type: none"> • 자체적으로 보유한 비밀키/공개키를 사용하여 배포 파일에 전자서명 수행 • 검증을 위한 인증서(공개키)는 노드액션 수신 시 배포
환경 구성	<ul style="list-style-type: none"> • 인터넷이 가능한 환경에서만 사용 가능 	<ul style="list-style-type: none"> • 인터넷망/폐쇄망 환경에서 모두 사용 가능
키 관리	<ul style="list-style-type: none"> • 별도의 키 사용하지 않는 방식으로 관리자 계정에 대한 보안만 요구 	<ul style="list-style-type: none"> • 별도의 비밀키를 안전하게 보관 필요
준비사항	<ul style="list-style-type: none"> • 배포파일 전자서명을 위한 cosign 바이너리 파일 필요 (Sigstore Git hub Release v2.1.1 하단 Assets 에서 cosign-linux-arm64 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 	<ul style="list-style-type: none"> • 배포파일 전자서명을 위해 cosign 바이너리 파일이 필요 • 배포파일 전자서명에 사용될 키가 필요하며 cosign을 사용해 생성하거나 별도의 키 준비 필요
제약사항	<ul style="list-style-type: none"> • 최초 등록된 배포자에서 다른 배포자로 변경 불가 	<ul style="list-style-type: none"> • 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 인증서를 생성합니다.

이 인증서는 소프트웨어를 서명하는 데 사용되며, 서명된 소프트웨어는 **cosign**을 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. **cosign**을 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. 터미널에 표시된 URL 정보를 복사하여 브라우저를 사용하여 Web페이지에 접속합니다.
7. 터미널에 표시된 8자리 문자 값과 cmd창에 표시된 8자리 문자값이 동일한지 확인하고 Submit 버튼을 클릭합니다.
8. Git, Google, Microsoft 세가지 OIDC중 하나를 선택하고 인증을 수행합니다.
9. 잠시 후 터미널에 서비스 약관 동의에 y 를 입력합니다.
10. 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. 설명은 용도에 따라 다르게 사용하는 경우 어떤 목적으로 사용하는 노드액션인지 구분할 수 있습니다.
6. 라벨을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래의 액션 수행설정을 구성합니다.

7. OS 종류는 macOS, Linux, Windows 대상에 맞는 OS를 선택합니다.
8. 조건 설정은 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. 플러그인선택에서는 파일 배포 V2 를 선택합니다.
10. 배포 파일에는 업로드 버튼을 클릭하여 파일을 선택합니다.
11. 배포파일 검증방법은 Sigstore Keyless Signing을 선택합니다.
12. 신뢰하는 OIDC 발행자에는 전자서명 시 인증에 사용한 OIDC(Github, Google, Microsoft)를 선택합니다.
13. 신뢰하는 ID에는 전자서명 시 인증에 사용한 ID(email주소 형태)를 입력합니다.
14. Certificate는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 cert 파일을 추가합니다.
15. Signature는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 sig 파일을 추가합니다.
16. 배포 옵션의 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 노드정책으로 이동한 후 기본정책을 클릭합니다.
19. 노드액션 설정을 찾아 할당 버튼을 클릭합니다.
20. 사용가능 항목에서 파일 배포를 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. CMD창에서 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 공개키는 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. 수행주기는 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. 수행주기의 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, 메모리 정보, 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 63자를 초과할 수 없고 하이픈(-)만 설정 가능)
2. 수행주기는 설정된 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. 로그인 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 적용된 시점부터 적용 됩니다.)
 - 검사예외ID: 검사예외대상의 사용자 ID의 전체문자열을 입력합니다. (여러개 입력시 콤마로 구분, 대소문자를 구분하지 않습니다.)
4. 수행주기의 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 설치된 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** 메시지의 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. 조건연산의 경우 **AND** 또는 **OR** 를 선택하여 선택 조건을 추가합니다.
2. 조건설정의 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 네트워크 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 강제화 합니다.
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.

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 수행설정을 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.

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** 메시지의 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.

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 ZTNA 에서 지원되는 모든 안티바이러스를 버전별로 확인합니다.

벤더	제품명	정보제공 항목
Cisco Sys-tems	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 "설정" 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.

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 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.

검증 방식	Sigstore Keyless Signing (Keyless)	Public Key Signing (self-managed-key)
검증 내용	<ul style="list-style-type: none"> • 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 Sigstore에서 명된 파일이 맞는지 검증 	<ul style="list-style-type: none"> • 자체적으로 보유한 비밀키/공개키를 사용하여 배포 파일에 전자서명 수행 • 검증을 위한 인증서(공개키)는 노드액션 수신 시 배포
환경 구성	<ul style="list-style-type: none"> • 인터넷이 가능한 환경에서만 사용 가능 	<ul style="list-style-type: none"> • 인터넷망/폐쇄망 환경에서 모두 사용 가능
키 관리	<ul style="list-style-type: none"> • 별도의 키 사용하지 않는 방식으로 관리자 계정에 대한 보안만 요구 	<ul style="list-style-type: none"> • 별도의 비밀키를 안전하게 보관 필요
준비사항	<ul style="list-style-type: none"> • 배포파일 전자서명을 위한 cosign 바이너리 파일 필요 (Sigstore Git hub Release v2.1.1 하단 Assets 에서 cosign-linux-arm64 다운로드) • 배포파일 전자서명/서명 검증에 사용되는 외부 인터넷 통신 허용 필요 (전자서명 PC, 정책서버, 사용자단말), 도메인 정보 • 배포파일 전자서명에 사용되는 OIDC(Google, Git, MS) 계정이 필요 	<ul style="list-style-type: none"> • 배포파일 전자서명을 위해 cosign 바이너리 파일이 필요 • 배포파일 전자서명에 사용될 키가 필요하며 cosign을 사용해 생성하거나 별도의 키 준비 필요
제약사항	<ul style="list-style-type: none"> • 최초 등록된 배포자에서 다른 배포자로 변경 불가 	<ul style="list-style-type: none"> • 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 인증서를 생성합니다.

이 인증서는 소프트웨어를 서명하는 데 사용되며, 서명된 소프트웨어는 **cosign**을 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. **cosign**을 다운로드 받아 배포파일 전자서명에 사용할 디렉토리에 저장합니다.
2. 파일명을 **cosign** 으로 변경합니다.
3. 전자서명할 파일을 디렉토리에 복사합니다.
4. 터미널을 열어서 **cosign** 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. 터미널에 표시된 URL 정보를 복사하고 브라우저를 사용하여 Web페이지에 접속합니다.
7. 터미널에 표시된 8자리 문자 값과 cmd창에 표시된 8자리 문자값이 동일한지 확인하고 Submit 버튼을 클릭합니다.
8. Git, Google, Microsoft 세가지 OIDC중 하나를 선택하고 인증을 수행합니다.
9. 잠시 후 터미널에 서비스 약관 동의에 y 를 입력합니다.
10. 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. 설명은 용도에 따라 다르게 사용하는 경우 어떤 목적으로 사용하는 노드액션인지 구분할 수 있습니다.
6. 라벨을 추가하면 "설명" 입력란에 표시되는 맞춤 라벨로 플러그인을 분류할 수 있습니다.

아래의 액션 수행설정을 구성합니다.

7. OS 종류는 macOS, Linux, Windows 대상에 맞는 OS를 선택합니다.
8. 조건 설정은 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. 플러그인선택에서는 파일 배포 V2 를 선택합니다.
10. 배포 파일에는 업로드 버튼을 클릭하여 파일을 선택합니다.
11. 배포파일 검증방법은 Sigstore Keyless Signing을 선택합니다.
12. 신뢰하는 OIDC 발행자에는 전자서명 시 인증에 사용한 OIDC(Github, Google, Microsoft)를 선택합니다.
13. 신뢰하는 ID에는 전자서명 시 인증에 사용한 ID(email주소 형태)를 입력합니다.
14. Certificate는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 cert 파일을 추가합니다.
15. Signature는 우측 파일읽기 버튼을 클릭하여 전자서명 시 생성되었던 sig 파일을 추가합니다.
16. 배포 옵션의 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 노드정책으로 이동한 후 기본정책을 클릭합니다.
19. 노드액션 설정을 찾아 할당 버튼을 클릭합니다.
20. 사용가능 항목에서 파일 배포를 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. 터미널에서 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 공개키는 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

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 수행설정을 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 업데이트최소비율** 의 경우 마지막으로 전송한 CPU 사용량이 현재 사용량과 설정비율 이상 차이가 나면 정보를 전송합니다.

8. 메모리 업데이트 최소비율의 경우 마지막으로 전송한 메모리 사용량이 현재 사용량과 설정비율 이상 차이가 나면 정보를 전송합니다.
9. 저장장치 업데이트 최소비율의 경우 마지막으로 전송한 저장장치 사용량이 현재 사용량과 설정비율 이상 차이가 나면 정보를 전송합니다.
10. 수행주기는 항상수행으로 10분 주기로 변경된 데이터가 존재하는 경우 업데이트됩니다.

Note: 정보업데이트 설정비율은 전체 용량 기준으로 계산됩니다.

Step2: 노드정책에 노드액션 적용하기

1. 왼쪽 정책 항목에서 노드정책으로 이동합니다.
2. 적용하고자 하는 노드정책을 클릭합니다.
3. 노드액션 설정을 찾아 할당을 클릭합니다.
4. 사용가능 항목에서 하드웨어정보 수집을 찾아 선택 항목으로 드래그하여 이동합니다.
5. 추가 버튼을 클릭합니다.
6. 수정 버튼을 클릭합니다.

8.5 확장 플러그인 설정방법

Genian NAC 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_FasooSSO	Fasoo Enterprise DRM 대체 인증	파수 <i>Fasoo DRM SSO</i> 연동
C_Suser	SafePC Enterprise 대체 인증	바이오닉스진 <i>SafePC</i>
C_PassNiSSO	Pass-Ni SSO 대체 인증	유비앤티스랩 <i>PassNI SSO</i>
C_NC_IBK	INISAFE Nexess 대체 인증	이니텍 <i>INISAFE Nexess</i>
C_PentaSSO	Penta Security SSO V2.0 대체 인증	
C_RathonSSO	Rathon SSO 대체 인증	라톤테크 <i>Rathon-SSO</i>
C_KsignSSO	Ksign SSO 대체 인증	케이사인 <i>KSignAccess</i>
C_Penta2SSO	Penta Security SSO V3.0 대체 인증	펜타시큐리티 <i>ISign+</i>
C_SIClient2SSO	SafeIdentity SSO 대체 인증	
C_SecuRegAuth	Smart NAC 대체 인증	
C_NetsESSO	Nets EnterpriseSSO 대체 인증	
C_PowerPackSSO	ESCARE PowerPack	<i>ESCARE PowerPack</i>
RegAuth	외부인증연동 (레지스트리)	
ExeAuth	외부인증대체 (실행파일)	
GnManager	Genian 통합에이전트	

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 NAC는 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 위협에 노출되어 있는 단말을 감지할 수 있습니다.

Note: 유튜브를 통해 위험감지 정책과 활용 교육 영상을 확인할 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 캐시를 가득 채웁니다. 곧 대상 노드는 캐시를 유지하기 위해 더 많은 리소스를 사용할 것이며, 이로 인해 버퍼 오버플로우가 발생할 수 있습니다. 그리고 정상적인 패킷이 캐시에 입력되지 않을 것입니다.

Genian NAC는 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.

- 감지기간은 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 탈취할 수 있습니다. 만약 악성 단말이 MAC/IP를 복제한 경우 패킷 수준에서 일반 시스템과 도난된 시스템을 구분하는 것은 매우 어렵습니다.

그러나 Genian NAC는 다양한 방법으로 MAC/IP 탈취를 탐지할 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 NAC에서는 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** 위험감지를 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 Executable) 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 NAC는 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 NAC는 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 DHCP 서버 감지

DHCP 서버가 분배하는 DNS 값을 센서에 설정된 DNS와 일치여부를 비교하여, 비정상적인 DHCP 서버를 감지할 수 있습니다.

9.1.7 잘못된 게이트웨이 사용

에이전트는 허용되지 않은 게이트웨이 설정을 즉시 감지할 수 있습니다. 만약 노드에 신뢰할 수 없는 게이트웨이 주소 (또는 기본 게이트웨이)가 설정되어 있다면, 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 복제되었는지를 감지합니다. (설정 필요 없음)

9.1.9 ARP Spoofing

Genian NAC는 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.

- 감지기간은 위험으로 감지하기 위한 기간을 설정합니다.
- 공격횟수 ARP 변조 패킷 횟수를 설정합니다. 감지기간 동안 지정한 횟수 이상의 ARP 변조 패킷을 보낼 경우 위험으로 감지합니다.

ARP Enforcement은 네트워크 장치의 통신을 차단하는데 사용하는 기술이지만, ARP Spoofing은 주로 악성 코드로 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 NAC는 VRRP, HSRP 또는 GLBP 등 알려진 프로토콜에 대하여 감지되지 않도록 예외처리합니다.

9.1.10 알수없는 서비스 요청

Genian NAC는 다양한 방법으로 제공하지 않는 서비스 요청시도를 감지할 수 있습니다. 네트워크센서는 가상의 허니팟을 이용하여 서비스요청을 감지합니다. 만약 가상IP 주소로 제공하지 않는 서비스 요청시도가 감지되면, 일정 기간 내에 지정된 값 이상의 서비스를 요청하면 위험노드로 지정합니다.

- 감지기간은 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 NAC에서는 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. 중요도는 , 위험 정도에 따라 낮음, 중간, 높음 을 선택할 수 있습니다.
4. 적용모드는 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 이벤트를 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
- 대시보드의 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. 위험정의와 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. 조건연산은 **OR** 로 선택합니다.
7. 조건설정의 추가 버튼을 클릭합니다.
8. 아래의 조건설정 항목을 원하는 대로 설정합니다.
 - 항목: 위험감지
 - 조건: 특정위험이 감지되면
 - 설정: (목록 중에 하나를 선택)
9. 추가를 클릭합니다.
10. 필요에 따라 조건설정을 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 정책을 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 나뉘지게 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 시스템을 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 **ON**으로 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 **ON**으로 변경합니다.
6. 저장 버튼을 클릭합니다.

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.

Note: 감사항목의 로그와 리포트에 대한 교육영상을 Online EDU Chapter 4-3에서 확인할 수 있습니다.



The screenshot displays the Genian NAC v10.0 interface. On the left, a navigation menu is visible with 'Log' selected. The main content area shows a 'Log' section with a time-based bar chart (labeled B) and a table of log entries (labeled D). The table columns include Time, Type, Log ID, Detected By, IP, MAC, Username, Full Name, Department, and Description. The table shows various system events like 'Threat Detection', 'Administrator Login', and 'Programs added/detected'. A search and filter sidebar (labeled C) is also visible on the left, and a 'Station & Filters' section (labeled A) is at the bottom left.

10.1 로그 관리

실시간 검색, 필터링, 태그 지정 및 시각화를 통해 특정 데이터를 찾을 수 있습니다. Genian NAC는 심각도에 따라 로그를 제공하고 일반적인 사용법에 따라 사전 정의된 로그 필터를 제공합니다.

10.1.1 감사로그 추가정보 설정하기

기본 감사로그에 저장하는 정보의 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 문자를 사용하여 검색이 가능합니다.

1. Web콘솔 상단메뉴 감사로 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.

설정된 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 검색필터를 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** 메뉴에서 **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** 메뉴에서 **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 **노드그룹**을 생성합니다.
4. **노드그룹**을 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 NAC는 감사로그 포맷 정보를 제공하여 검색필터 설정 및 타 장비와 연동 시 활용 가능합니다.

컬럼 정의

컬럼정보	내용	상세내용
시간	로그 발생 시간	로그 발생 날짜 YYYY-MM-DD , 로그 발생 시각 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 IP 또는 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 사용자명	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 가진
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

기존 검색 필터 사용 또는 새로운 검색 필터 생성

1. 원하는 로그 필터에서 수정 을 클릭합니다.
2. 로그 전송은 알람전송(관리자), SYSLOG, SNMP TRAP, WEBHOOK 을 사용하여 추가로 생성할 수 있습니다.

로그 전송 시 메시지 내용에 매크로 추가

Genian NAC는 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 기본값이 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 NAC|{_VERSION}|{_LOGFILTERNAME}|{_LOGFILTERDESC}|1|rt=
↳{_DATETIME} cs1Label=Log Type cs1={_LOGTYPE} cs2Label=Log ID cs2={_LOGID}
↳dvchost={_SENSORNAME} dst={_IP} dmac={_MAC} msg={_FULLMSG} cs3Label=Detail
↳Message cs3={_DETAILMSG}
```

- SNMP Trap 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}",
  "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}	로그ID 문자열
{_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 호스트명 (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 NAC 정책서버 IP를 "Only accept connection from" 항목에 입력합니다. (선택 사항)
3. NAC의 검색필터에서 SYSLOG 전송을 체크합니다.
4. 다음과 같이 SYSLOG 관련 항목을 입력합니다.
 - 서버주소 : Splunk 서버 IP
 - 프로토콜 : **UDP**
 - 전송포트 : Splunk 에서 정의한 포트 (기본포트는 UDP:514)
 - **SYSLOG 메시지** : {_DATETIME},LOGTYPE={_LOGTYPE},LOGID={_LOGID},IP={_IP},MAC={_MAC},MSG={_MSG},DETAIL={_DETAILMSG}
5. 생성 버튼을 클릭합니다.

SNMP Trap 연동 예제

SNMP Trap은 주로 디바이스 간 이벤트 전송에 활용되고, 설정 방법은 다음과 같습니다.

1. NAC의 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 NAC와 Slack 연동에 대한 정보를 제공합니다. 여기에는 다음 정보가 포함 됩니다.

연동의 목적

연동을 위한 *Slack* 설정

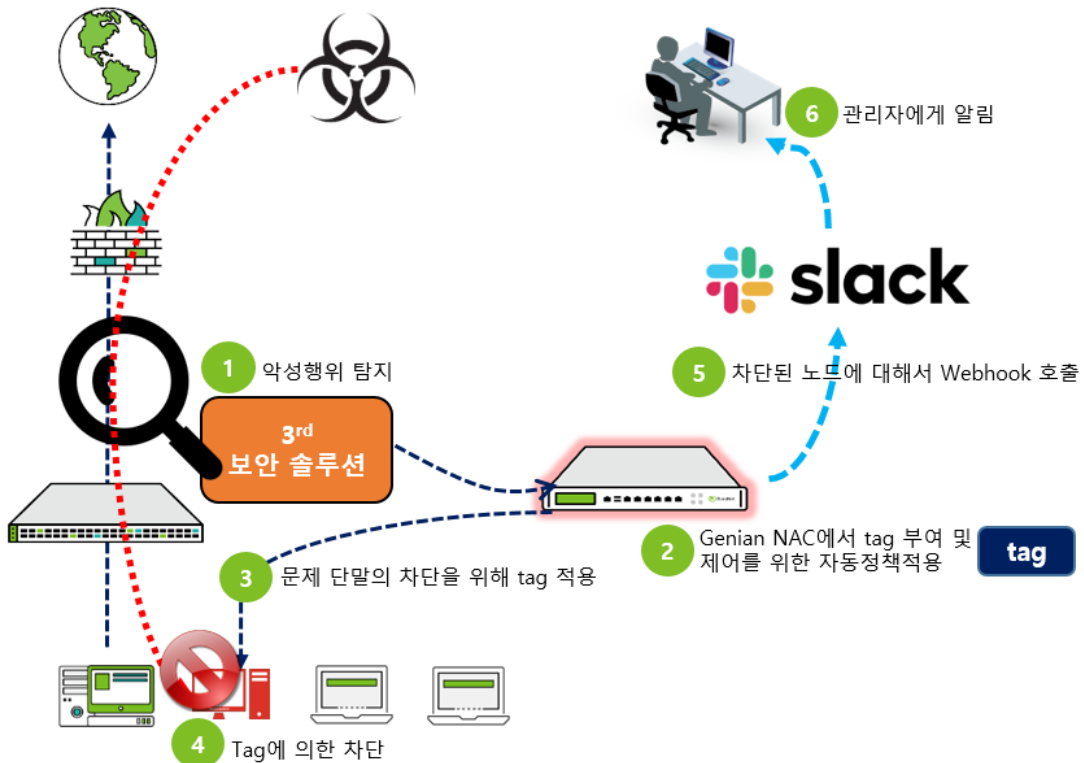
- Slack App(bot) 생성하기
- Slack App 설정 확인

연동을 위한 *Genian NAC* 설정

- 검색필터 설정하기
- Webhook 전송 설정하기

가이드 개요

- 이 가이드는 Genian NAC와 Slack의 연동설정방법 및 활용예시를 제공합니다.
- Genian NAC에서 제공하는 단말의 위협정보, 단말의 정보변경 등의 이벤트 정보를 Slack으로 관리자에게 전송하여, 관리자가 빠르게 인지하고 대응할 수 있도록 도움을 제공합니다.



연동의 목적

Genian NAC와 Slack을 연동하여, 다음과 같은 장점 및 효과를 IT관리자와 사용자에게 제공합니다.

- 노드의 모든 정보를 대상으로 하는 Genian NAC와 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/apps>에 Slack 계정으로 로그인 하신 후, App을 만듭니다.

App의 이름을 정해주고, Slack Workspace를 지정합니다.

- App Name은 Slack에 메시지를 표시하는 Bot의 이름입니다.
- Development Slack Workspace에서 메시지를 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":\n↵:"Hello, World!\n"}' + Webhook URL
```

- 리눅스 터미널에서 실행 시,

```
curl -X POST -H 'Content-type:application/json' --data '{"text":\n↵"Hello, World!"}' + webhook URL
```

연동을 위한 Genian NAC 설정

검색필터 설정하기

1. Genian NAC의 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 NAC는 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 추가해야 합니다. 다른 수신 기준의 경우 다른 규칙을 구성 할 수 있습니다.

1. 필터 오른쪽의 추가 버튼을 클릭하고 팝업 양식을 작성합니다.
2. 필터 이름을 입력합니다.
3. 필터타입의 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 오도록 합니다.
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 수 있는 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 보고할 때 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. 리포트제목의 경우 고유 이름을 입력합니다.
2. 리포트설명의 경우 이 리포트에 대한 설명을 입력합니다.
3. 적용모드에 대해 사용함 을 선택합니다.
4. 자동생성의 경우, 설정 시간에 실행하려면 사용함 을 선택합니다.

세부설정

1. 출력파일의 경우, 드롭다운에서 Excel 또는 CSV 를 선택합니다.

2. 메일수신의 경우, 관리자의 이메일 주소로 전송이 가능합니다.
3. 수행쿼리의 경우, 사용자 지정 쿼리를 추가합니다.
4. 생성을 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 > 리포트로 이동합니다.
2. 좌측 사용자정의 리포트로 이동합니다.
3. 작업선택 > 노드리포트 추가로 이동합니다.

기본설정

1. 리포트제목의 경우 고유 이름을 입력합니다.
2. 리포트설명의 경우 이 리포트에 대한 설명을 입력합니다.
3. 적용모드에 대해 사용함을 선택합니다.
4. 자동생성의 경우, 설정 시간에 실행하려면 사용함을 선택합니다.

세부설정

Note: 세부설정 다음 단계를 반복하여 수집대상을 리포트에 추가합니다.

1. 수집대상의 경우 드롭 다운에서 전체노드 또는 노드그룹을 선택합니다.
2. 노드 그룹을 선택한 경우 대상설정 드롭 다운에서 원하는 그룹을 선택합니다.
3. 항목의 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. 대시보드탭의 경우, Overview, Anomaly 등 대시보드 탭을 설정합니다.
2. 출력파일의 경우, 출력한 파일의 파일 타입을 선택합니다.
3. 메일수신의 경우, 관리자의 이메일 주소로 전송이 가능합니다.

리포트 내보내기

1. 상단 패널의 감사 > 리포트로 이동합니다.
2. 이메일 발송으로 이동하여 원하는 리포트 이름을 클릭합니다.
3. 작업선택 > 즉시수행 (파일을 클릭하여) 하여 리포트를 메일로 발송할 수 있습니다.

리포트를 삭제하는 방법

1. 상단 패널의 감사 > 리포트로 이동합니다.
2. 기본 창에서 삭제할 리포트 이름을 찾아 체크 상자를 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.
변동폭 (전일 비)	오늘과 어제에 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변동폭 (전주 비)	오늘과 이전 주에 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변동폭 (전월 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.
변동폭 (전일 비)	오늘과 어제에 검색필터에 포함된 로그수의 변동폭을 표시합니다.
변동폭 (전주 비)	오늘과 이전 주에 검색필터에 포함된 로그수의 변동폭을 표시합니다.
변동폭 (전월 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 NAC 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**의 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.
변동폭 (전 일 비)	오늘과 어제에 무선랜 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변동폭 (전 주 비)	오늘과 이전 주에 무선랜 노드그룹에 포함된 노드수의 변동폭을 표시합니다.
변동폭 (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

NAC 현황을 보여주는 대시보드 화면을 탭별로 PDF 형태의 파일로 리포트를 제공합니다.

3. 로그 리포트 확인하기

기존 생성된 로그 필터를 기반으로 엑셀(xlsx)과 CSV(comma-separated values) 형태의 텍스트 데이터 파일로 리포트를 제공합니다.

4. 쿼리 리포트 확인하기

관리자가 NAC에서 제공하는 데이터베이스에 쿼리(SQL)를 수행한 결과값에 대해서 엑셀(xlsx, xls)과 CSV(comma-separated values) 형태의 텍스트 데이터 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.

시스템관리

Genian NAC 장비(정책서버, 네트워크센서) 및 서비스, 백업/복원, 관리자 콘솔, 관리자 역할의 환경설정을 확인할 수 있습니다.

11.1 시스템 종료 및 재시작

11.1.1 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.

11.1.2 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.

11.2 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 가진 관리자

Note: 관리자 권한을 부여하려면 계정을 생성하고, 각 계정에 알맞는 관리자 권한을 할당하시기 바랍니다.

11.2.1 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. **사용자용도** 의 경우 **선택안함** 을 선택합니다.
6. **사용자상태** 의 경우 **정상** 을 선택합니다. (일시적으로 계정을 사용 중지하려면 **사용 중지** 를 선택합니다.)
7. **계정사용만료** 의 경우 체크박스를 클릭하여 날짜와 시간을 선택합니다.

8. 태그의 경우 추가를 클릭하여 이 계정에 태그를 추가하도록 선택할 수 있습니다.

비밀번호 설정

1. 비밀번호에 비밀번호를 입력합니다.
2. 비밀번호 확인에 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, (선택) 구분하여 IP 주소를 지정할 수 있습니다. (공란시 제한설정 안함)
7. **인증허용 MAC**의 경우, (선택) 로 구분하여 MAC 주소를 지정할 수 있습니다. (공란시 제한설정 안함)
8. **인증제한 예외노드그룹**의 경우 인증제한이 적용하지 않을 그룹을 할당할 수 있습니다. 할당을 클릭하여 예외노드그룹을 지정합니다.

로그인 설정

1. 관리WEBUI 접속 IP / MAC을 추가합니다. (공란시 제한설정 안함)
2. 사용할 2단계 인증을 선택합니다. SMS인증, OTP 인증, 선택안함을 선택할 수 있습니다.
3. 타임 존을 선택합니다. (Asia / Seoul(GMT +09:00))

알람정보 설정

1. 알람수신설정에서 사용자등록 IP신청 장치신청에 대한 알람 수신여부를 선택합니다. 선택한 항목의 신규 이벤트 발생 알람을 수신할 수 있습니다.
2. SMS수신번호는 알람을 받은 휴대폰 번호를 설정합니다.
3. 발신번호는 SMS에 표시할 발신번호를 입력합니다.
4. 이메일은 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 Client 만이 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.

11.2.2 2단계 인증

SMS, Google OTP 를 활용한 2단계 인증

SMS

Genian NAC는 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 NAC는 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 (심표로 구분 하여 여러 개의 이메일 주소를 입력할 수 있습니다.)
7. 수정 를 클릭하십시오.

Note: 관리자 계정의 2단계 인증을 적용하기 위해서는 정책서버의 2단계 인증 설정도 완료해야 합니다.

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 설정하기 위한 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

미래테크놀로지 Secure AnyOTP

본 가이드는 모바일 OTP 시스템인 미래테크놀로지의 Secure AnyOTP(이하, **AnyOTP** 로 표시함)와 네트워크 접근제어 시스템인 Genian NAC의 연동 기능을 수행하기 위한 설정 방법을 안내합니다.

개요

본 연동은 관리자 계정에 대해서 2-Factor 인증을 위한 연동으로 Genian NAC 관리자 계정에 대해서 보다 안전한 로그인 과정을 수행하기 위해, 2-Factor 인증을 구현하기 위하여, 관리자는 **Genian NAC 관리자 페이지**에 로그인 시 **ID/PW 방식의 Genian NAC 관리자 계정으로 로그인** 이후, 추가적으로 **AnyOTP의 인증**을 거치도록 연동됩니다.

연동의 구성은 Genian NAC가 API 호출방식의 AnyOTP 전용의 연동도구(정책서버 플러그인)를 제공하며, 관리자가 Genian NAC 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 NAC (정책서버)	V5.0 이상	2019.03 이후 Release 버전
Secure AnyOTP		2018.03 이후 Release 버전

연동의 목적

Genian NAC와 AnyOTP 연동은 다음의 효과를 제공합니다.

관리자 로그인 보안을 위한 2-Factor 인증환경 제공

- AnyOTP와 Genian NAC의 정책서버 플러그인 연동을 통해 관리자는 Genian NAC 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 NAC 정책서버 플러그인 준비

Genian NAC는 AnyOTP와 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 AnyOTP 서버의 IP, Port 확인 및 SharedKey 발급

아래의 두개 항목은 연동을 위한 Genian NAC 설정 > Step 2: 정책서버 플러그인 설정 > 3번 항목 설정 시 활용됩니다.

- 1) API 호출을 위해 인증코드 발급을 요청할 AnyOTP 서버의 IP 와 Port 를 확인하시기 바랍니다.
- 2) Genian NAC에서 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 NAC 관리자 페이지에 2단계 인증 진행 시 인증코드를 발급 받을 AnyOTP App을 개인 모바일 단말에 설치하시기 바랍니다.

연동을 위한 Genian NAC 설정

본 과정에서 다루는 Genian NAC의 설정 부분은 AnyOTP와 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 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 NAC 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 NAC와 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 NAC 관리자 페이지에서 2단계 인증 진행 시 인증창에 표시되는 타이틀 문구 입력
URL	/plugin/gwp100003/otpAuth.xhtml?initParameter	AnyOTP 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)

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 Any 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 Any OTP 선택
- 5) 하단부 수정 버튼 클릭

이 과정을 통해서 Genian NAC와 AnyOTP가 연동되어 Genian NAC 관리자 페이지 로그인 수행 시 2-Factor(1단계: Genian NAC 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 등이 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 > 3번 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 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 **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 OTP인증	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 Parameter 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.

11.3 CLI(Command Line Interface)

11.3.1 CLI 접속

Attention: SSH 접속은 허용된 IP에서만 접근 됩니다. 특정IP의 SSH 접근 허용 설정하는 방법은 장비 환경설정 자동으로 세팅하기를 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.

11.3.2 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	사용된 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 지정된 경우 최신 서버 파일로 업그레йд 진행합니다.
halt	시스템 전원 종료 모드 준비
kill pid	PID를 기반으로 프로세스를 종료합니다.
kill pname	이름을 기반으로 프로세스를 종료합니다.
ping	원격 장치에 대한 IP 테스트를 위한 ICMP 요청을 생성합니다.
reboot	시스템을 재부팅합니다.
restart system	OS를 다시 시작합니다.
shutdown service	Genian NAC 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 실행 중인 프로세스를 표시합니다.
show route	현재 구성된 라우트를 표시합니다.
show superadmin	구성된 관리자 계정 목록을 표시합니다.
show time	현재 시스템 시간을 표시합니다.
show uptime	시스템 가동 및 가동 시간 표시합니다.
show version	현재 실행 중인 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
```

11.4 네트워크 구성

CLI (Command Line Interface)를 통해 인터페이스 IP 주소를 변경하거나 DHCP 용 인터페이스를 구성 할 수 있습니다.

11.4.1 인터페이스 IP 주소 변경

인터페이스 IP 주소 변경

변경 전 인터페이스 설정을 확인하세요.

다음과 같이 "show configuration | grep interface [interface name]" 을 입력합니다.

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

인터페이스에 수동설정(IP / 게이트웨이) 및 자동설정(DHCP)이 동시에 활성화 되어있으면 기능이 올바르게 동작하지 않습니다.

Note: 장비에 설정한 Configuration을 검증하고 재부팅을 진행하면, 기본적인 트러블 슈팅이 가능합니다.

인터페이스에 고정 IP 설정

인터페이스(eth0, eth1 등) 또는 VLAN 인터페이스(eth0.10, eth0.20 등)의 IP 주소와 게이트웨이를 정의 하려면 다음을 수행합니다.

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

인터페이스에서 고정 IP 제거

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

인터페이스를 DHCP 클라이언트로 구성

인터페이스 또는 하위 인터페이스를 DHCP 클라이언트로 구성하려면 다음을 수행합니다.

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

인터페이스에서 DHCP 클라이언트 상태를 제거하려면 다음을 수행합니다.

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

11.4.2 센서 인터페이스에 Alias IP 추가

하나의 네트워크에 논리적인 서브넷이 다수 할당되어 있는 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 IP설정을 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. 수정을 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 IP설정을 클릭합니다.
6. Alias IP 우측의 삭제 버튼을 클릭합니다.

11.4.3 센서 인터페이스에 가상 IP 구성

Genian NAC는 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 IP설정을 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 센서설정을 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 IP설정을 클릭합니다.
6. 가상IP의 추가 버튼을 클릭하여 IP주소와 동작모드 > 설정함을 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 IP설정을 클릭합니다.
6. 삭제를 원하는 가상 IP 옆의 삭제 버튼을 클릭합니다.

11.4.4 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 네트워크센서 있는 또 다른 인터페이스를 이용할 수 있습니다.
- 단일 인터페이스인 경우 802.1Q 트렁크 포트를 통해 여러 VLAN을 관리할 수 있습니다.

Note: 장비에 설정한 Configuration을 검증하고 재부팅을 진행하면, 기본적인 트러블 슈팅이 가능합니다.

신규 네트워크센서 추가

새 원격지 관리대역의 네트워크센서가 추가된 경우 정책서버에 연결하는 작업이 필요합니다. 신규 네트워크센서를 추가하는 방법은 네트워크센서 설치를 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 구성해야 합니다.

1. SSH 클라이언트를 통해 네트워크센서에 연결합니다. 관리자 콘솔의 CLI 접속 방법을 참고해주시기 바랍니다.
2. 추가할 각 네트워크센서에 대해 아래 명령을 입력합니다.

아래의 예시에서는 인터페이스 eth0이 이미 구성되어 있습니다. 인터페이스 eth1은 별도의 LAN을 모니터링하도록 구성됩니다.

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

고정 IP를 사용하지 않는 경우 DHCP를 설정합니다.

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

기존 네트워크센서 인터페이스 삭제

Note:

이 기능은 단일 네트워크센서와 모든 노드, 노드정보를 삭제합니다.

1. SSH 클라이언트를 통해 네트워크센서에 연결합니다. 관리자 콘솔의 CLI 접속 방법을 참고해주시기 바랍니다.
2. 삭제할 각 네트워크센서에 대해 아래 명령을 입력합니다.

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

DHCP설정이 되어있는 경우, 설정을 해제 합니다.

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

3. Web콘솔 상단 항목의 시스템으로 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 **Web**콘솔을 통해 추가할 수 없으며, **CLI**콘솔을 통해 기존 **eth0** 또는 **eth1** 인터페이스에 하위 인터페이스를 추가하여 구성해야 합니다.

1. **SSH** 클라이언트 를 통해 네트워크센서에 연결합니다. 관리자 콘솔 의 **CLI** 접속 방법을 참고해주시기 바랍니다.
2. 모니터링할 모든 VLAN 인터페이스를 추가합니다.

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

3. 추가한 각 VLAN 인터페이스별 IP 및 Gateway를 설정합니다.

eth0 이후의 각 VLAN 접미사는 VLAN ID에 의해 결정됩니다. 아래는 VLAN 30에 센서를 추가하는 예시입니다. 모니터링할 모든 VLAN에 대해 아래의 과정을 반복합니다.

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

고정 IP를 사용하지 않는 경우 DHCP를 설정합니다.

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

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 참고해주시기 바랍니다.
2. 모니터링할 모든 VLAN 을 추가하고 삭제할 VLAN 을 제외합니다.

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

3. VLAN 센서 인터페이스를 제거하려면 아래의 명령어를 입력합니다.

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

- DHCP로 설정된 인터페이스를 제거하려면 아래의 명령어를 입력합니다.

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

4. Web콘솔 상단 항목의 시스템 으로 이동합니다.
5. 시스템 관리 패널에서 시스템관리 > 센서관리 로 이동합니다.
6. 변경할 네트워크센서의 IP 주소를 클릭합니다.
7. 대상노드작업 > 삭제 를 클릭합니다.
8. 확인 버튼을 클릭합니다.

11.4.5 네트워크센서 인터페이스 유형 변경

네트워크 구성을 변경하면 네트워크센서의 인터페이스 유형이 액세스 포트에서 트렁크 포트 또는 그 반대로 변경 될 수 있습니다. 이 장에서는 센서 인터페이스 유형을 변경하는 방법을 설명합니다.

Note: 장비에 설정한 Configuration을 검증하고 재부팅을 진행하면, 기본적인 트러블 슈팅이 가능합니다.

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 전송해야 합니다.

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

물리적 인터페이스에 VLAN 인터페이스 생성

```
genian(config)# interface eth0 vlan 10,20,30-35 // 쉼표 또는 하이픈으로
구분된 VLAN ID로 설정합니다.
```

trunk port에 네이티브 VLAN이 있는 경우 eth0은 기본 VLAN이 되며 다른 VLAN 인터페이스 이름은 ethX.VLANID가 됩니다. 네이티브 VLAN이 없으면 eth0 인터페이스 설정을 삭제합니다.

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

VLAN 인터페이스 및 게이트웨이의 고정 IP 설정

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

또는 DHCP 설정 (고정 IP를 사용하지 않는 경우)

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

관리 인터페이스의 다른 구성 설정 (선택 사항)

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

모든 VLAN 인터페이스에 이더넷 고정 IP 또는 DHCP를 제대로 설정되었는지 확인합니다.

VLAN 인터페이스에서 실행 중인 네트워크 센서를 구성하려면 다음을 수행합니다.

1. 관리자 웹 UI에 로그인하고 시스템 메뉴로 이동합니다.
2. 네트워크 센서 IP를 클릭하고 센서 설정 탭으로 이동합니다.
3. 인터페이스 이름을 클릭합니다.
4. 센서 동작 모드를 **Inactive** 에서 **Monitoring** 로 변경합니다.
5. 하단의 수정 버튼을 클릭합니다.

인터페이스가 CLI 설정에서 제거되면 관리 콘솔에 등록된 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 > 센서 관리 를 선택합니다.
3. 원하는 센서에서 IP 를 클릭합니다. (호스트명 열의 인터페이스 이름으로 식별 할 수 있습니다)
4. 하단의 삭제 버튼을 클릭합니다.

Trunk Port 에서 액세스 포트로

VLAN 삭제

```
genian(config)# no interface eth0 vlan 10,20,30-35 // 쉼표 또는 하이픈으로 구분된 VLAN
↳ ID로 교체
```

모든 VLAN 인터페이스 설정 삭제

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

설정 eth0 주소, 게이트웨이 및 기타 설정

11.5 고 가용성 구성(HA구성)

NAC 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

11.5.1 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**

11.5.2 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.

Note: 유튜브를 통해 HA 구성 교육 영상을 확인할 수 있습니다: [Online EDU Chapter 3](#), HA 구성과 설정방법, HA Configuration-en

11.5.3 Primary 정책 서버

```

1. Interactive Wizard
2. Manual Configuration

Select installation type: 2

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

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

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

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

```

(continues on next page)

(continued from previous page)

```

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
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

```

11.5.4 슬레이브 정책 서버

```

1. Interactive Wizard
2. Manual Configuration

Select installation type: 2

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

```

(continues on next page)

(continued from previous page)

```

Re-enter Password:

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

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

```

(continues on next page)

(continued from previous page)

```

hostname SECONDARY

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 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

```

11.5.5 Primary 네트워크센서

```

device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx

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]

```

11.5.6 SECONDARY 네트워크센서

```

device-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx *(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]

```

(continues on next page)

(continued from previous page)

```
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 되는 경우 Failover가 진행됩니다.

11.5.7 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]
```

11.5.8 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]
```

(continues on next page)

(continued from previous page)

```

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
-----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.

11.5.9 Bonding 구성

Bonding은 물리적인 다수의 인터페이스를 논리적으로 하나의 인터페이스로 묶어서 사용하는 기술입니다. **bonding**은 물리적으로 인터페이스가 다운되는 경우를 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 (recommended)
```

Note:

Bonding 설정을 하기전에 인터페이스에는 어떤 설정도 존재해서는 안됩니다.

Bonding parameters 설정 적용을 위해서 장비 리부팅이 필요합니다.

Bonding 인터페이스를 사용하는 경우 장비내 다른 인터페이스의 사용을 금지합니다.

Bonding 인터페이스 상태 확인

Bonding 인터페이스는 Active/Active, Active/Backup 형태의 상태변화가 발생합니다. 아래는 현재 상태를 확인 하는 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
```

(continues on next page)

(continued from previous page)

```
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:0c:29:21:be:b3
Slave queue ID: 0
```

11.6 백업 및 복원

자동백업을 예약하고, 장애 발생 시 복원할 수 있습니다.

Note: Cloud 버전에서는 이 기능을 사용할 수 없습니다.

11.6.1 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	Unix 나 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 암호호화를 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 로컬디스크가 아닌 다른 타입으로 지정할 경우 백업파일 보존여부 설정을 ON으로 설정 시 백업파일 유실에 대응할 수 있습니다.

백업파일 다운로드

1. 상단 패널의 설정으로 이동합니다.
2. 좌측 패널의 환경설정 > 백업으로 이동합니다.
3. 백업파일 다운로드 > 백업목록 버튼을 클릭합니다.
4. 목록에서 백업하려는 파일을 다운로드합니다.

11.6.2 시스템 복원

단일 구성인 경우

1. CLI를 통해 정책서버에 SSH 프로토콜로 연결합니다.
2. CLI 로그인 후 **enable** 및 관리자 비밀번호를 입력하여 **EXEC Mode(#enable)**로 변경합니다.
3. 백업을 복원하려면 "restore <filename> all"을 입력합니다.

HA 구성인 경우

HA 구성이 되어있는 경우 Slack으로 추가 문의 부탁드립니다.

Note: 복원을 수행하기 전에 서비스를 종료해야 합니다.

11.7 외부 전송 이메일 서버 설정

본 문서는 메일서버를 이용하여 외부로 메일을 전송하는 방법을 다루고 있습니다.

11.7.1 전자 메일 계정 설정

1. 상단 패널의 설정으로 이동하십시오.
2. 왼쪽의 환경설정 > 기타설정으로 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.

Note: 유튜브를 통해 Genian NAC와 구글 메일서버 연동 가이드 영상을 확인할 수 있습니다.

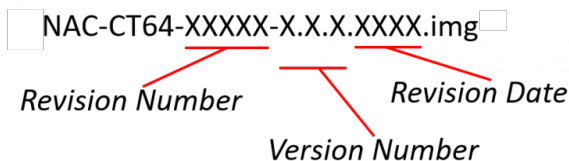


11.8 시스템 업데이트 관리

11.8.1 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.

- **NAC-CT** – 정책서버 이미지
- **NAC-SS** – 네트워크센서 이미지
- **NAC-AGENT** – 에이전트 이미지



정책서버 및 네트워크센서 업데이트

WebUI와 CLI를 통해 정책서버 및 네트워크센서를 업데이트할 수 있습니다.

Warning: 무분별한 업데이트는 NAC 시스템의 치명적인 오류의 원인이 될 수 있습니다. 파트너 엔지니어에게 문의 바랍니다.

Note: Genians Cloud Managed Edition 정책 서버의 경우, 자동으로 업데이트됩니다.

업데이트 이미지 파일 준비하기

파트너 엔지니어에게 문의하여 소프트웨어 이미지 파일을 다운로드합니다.

1. .iso 파일의 내용을 추출합니다.
2. .iso의 /images 디렉터리에서 원하는 소프트웨어 버전을 선택하십시오.
 - 정책서버의 경우 **NAC-CT**로 시작하는 파일 (네트워크센서 파일 포함)
 - 네트워크센서의 경우 **NAC-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. 셸모드에서 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 진행하시기 바랍니다.

1. 셸모드 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. 셸모드 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 NAC 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 NAC에서 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, 노드 그룹 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

11.8.2 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 패널에 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.

11.9 모바일 앱 다운로드

Genian NAC Monitor는 관리자용 앱으로 노드들을 관리하고 사용자의 요청을 처리할 수 있습니다. iOS 및 Android를 모두 지원합니다.

11.9.1 모바일 앱 설치방법

1. 상단 패널의 시스템 로 이동하십시오.
2. 왼쪽 시스템 관리 패널에서 업데이트 관리> 소프트웨어 로 이동하십시오.
3. **Genian NAC 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. 달기 를 클릭하십시오.



11.10 관리 콘솔의 환경 설정

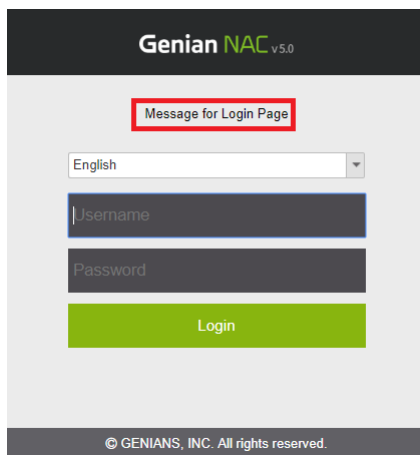
관리자는 관리콘솔 페이지를 통하여 WEB 콘솔의 화면과 CLI 콘솔 접속 화면에 대한 설정을 할 수 있습니다.

11.10.1 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 툴팁에 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 > 미사용IP등록 > 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 > 2단계인증 설정이 추가적으로 필요합니다.)
- **아이디/비밀번호 찾기**: 로그인 상자에 사용자 이름 찾기 / 암호 재설정 표시 여부를 결정할 수 있습니다. 사용을 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 설정 가능합니다.
- **로그인화면 헤더사용**: 로그인페이지 화면 헤더를 사용할지 여부를 선택할 수 있습니다. **On** 으로 변경하면 헤더영역 배경색 및 헤더이미지를 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 저장 가능합니다)

11.10.2 CLI 콘솔

CLI 배너 에서 CLI 접속시 표시될 배너를 설정할 수 있습니다.

11.11 SNMP로 정책 서버 관리

Genian NAC MIB 파일을 다운로드하여 NMS (Network Management System) 유형 솔루션에 사용할 수 있습니다.

11.11.1 Genian NAC MIB 파일 다운로드

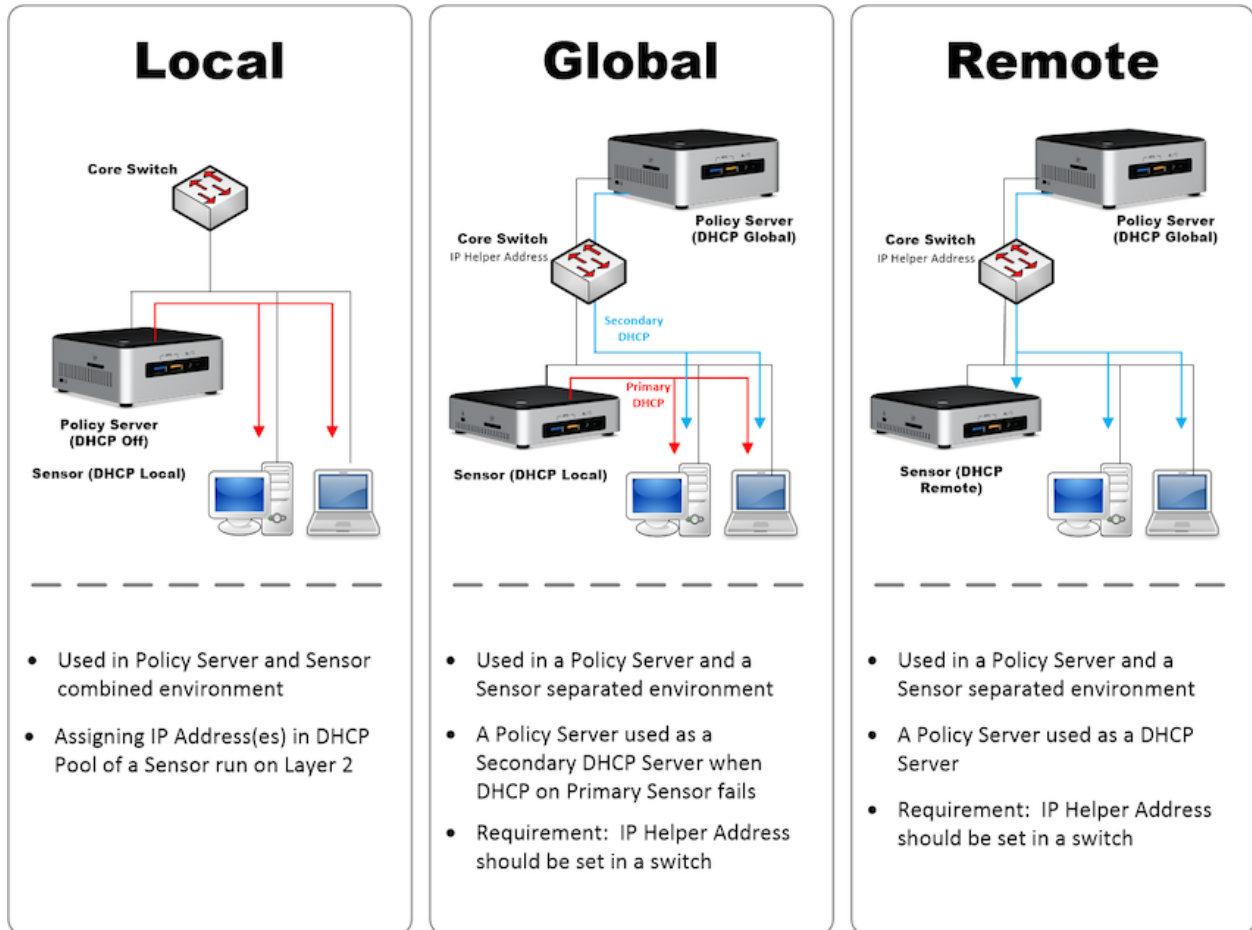
1. 상단 패널의 설정 으로 이동하십시오.
2. 왼쪽 환경 설정 패널에서 환경설정> 감사기록 으로 이동하십시오.
3. 기본 로그 창에서 **SNMP Trap** 수신을 찾으십시오.
4. 사용여부를 **On** 으로 선택하십시오.
5. 커뮤니티 문자열 입력하십시오.
6. 다운로드 **GENIAN MIB** (*Zip* 파일이 로컬 시스템에 다운로드됩니다)
7. 업데이트 를 클릭하십시오.
8. **GENIAN-MIB.zip** 파일의 압축을 풉니다.
9. **GENIAN-MIB.mib** 파일을 원하는 네트워크 관리 시스템에 추가하십시오.

11.12 네트워크센서 DHCP 서비스 설정하기

Genian NAC 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	



11.12.1 네트워크센서 로컬 DHCP 서비스 설정하기

1. 상단 패널에 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.
 - 서비스대상 설정값을 로컬 로 설정합니다.
 - 노드 IP Pool 설정값을 입력합니다.
 - DNS 서버 설정값을 입력합니다.
6. 저장 버튼을 클릭합니다.

11.12.2 네트워크센서 리모트 DHCP 서비스 설정하기

리모트 DHCP 서비스는 자체적으로 DHCP를 제공하지 않으므로 로컬과 리모트 설정된 정책서버가 필요합니다.

1. 상단 패널에 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.
 - 서비스대상 설정값을 리모트 로 설정합니다.
6. 저장 버튼을 클릭합니다.

11.12.3 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 패널에 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.
 - 서비스대상 설정값을 로컬 로 설정합니다.
 - 노드 IP Pool 설정값을 입력합니다.(리모트로 설정된 네트워크센서 대역설정 필수)
 - DNS 서버 설정값을 입력합니다.
6. 저장 버튼을 클릭합니다.

11.12.4 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 DHCP 서버 기능을 제공하지 않고 다른서버에서 DHCP 서비스 제공.
6. 이하 모든 기타 설정 들은 옵션 입니다.
7. 수정 을 클릭합니다.

11.13 네트워크센서 SSH 서비스 설정하기

Genian NAC 네트워크 센서에서 사용하는 SSH(Secure Shell) 서비스 기능에 대해 설정으로 제어하여 사용할 수 있습니다.

11.13.1 네트워크센서 SSH 서비스 활성화 설정하기

1. 상단 페널에 시스템 으로 이동합니다.
2. 왼쪽 시스템 항목에 시스템관리 를 선택합니다.
3. 설정할 네트워크 센서 에 체크박스를 선택합니다.
4. 작업선택 항목에서 장비 일괄 설정 을 선택합니다.
5. 보안설정 항목에서 ssh 활성화 체크박스를 선택한 후 설정을 ON 으로 변경합니다.
6. 저장 버튼을 클릭합니다.

11.13.2 네트워크센서 SSH 서비스 접근제어 설정하기

Note: 네트워크센서 SSH 서비스 활성화 설정 이 ON 으로 설정되어야 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. 기타설정 항목에서 ssh 접근 제어 체크박스를 선택한 후 설정을 ON 으로 변경합니다.
6. 저장 버튼을 클릭합니다.

11.14 SMS 서비스 알람 발신번호 변경하기

발신번호 변경기능은 Genian NAC에서 제공하는 SMS 서비스를 사용할 경우 설정이 가능합니다. Genian NAC에서 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 NAC에서는 노드, 장비, 사용자, IP 신청서, 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(입력 길이제한)	최대/최소 길이가 지정된 문자열 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
멀티라인 문자열 입력	다중행이 지원되는 문자열 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
문자열패턴 입력	패턴에 매칭되는 문자열 입력	노드, 장비, 사용자, IP신청서, 장비 수명주기
멀티라인 문자열패턴 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(필수 항목)	부서명, 직급명으로 정의된 항목 필수 선택	노드, 장비, 사용자, IP신청서, 장비 수명주기
시스템 목록(다중 선택)	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 > IP 신청서 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 IP 사용신청서 기능을 사용해야 합니다.

1. 상단 패널에 설정 으로 이동합니다.
2. 왼쪽 속성관리 항목에서 용도관리 > IP 용도 > IP 신규 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 IP 사용신청서에 추가필드로 설정된 입력값을 뷰 화면에서 확인할 수 있습니다.

1. 상단 패널에 관리 > 신청 로 이동합니다.
2. 왼쪽 IP 사용신청서 항목에 IP 신규/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 NAC에서 제공하는 신청서를 유형에 따라 다양한 형태에 용도를 설정할 수 있습니다. 용도에 따른 신청서 입력사항을 변경하거나, 관리자의 승인방법을 변경할 수 있어 사용자에게 추가적인 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 추가적인 정보를 입력받거나 승인권한을 관리자가 아닌 대상에게 부여할 수 있습니다.

사용자 용도에서 설정할 수 있는 항목은 신청서에 대한 처리옵션과, 신청서에 신청정보 입력과, 신청서에 계정정보 입력으로 나뉩니다.

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 관리자와 피신청자(사용자 계정이 존재하는 대상)으로 세분화 가능
자동승인	별도의 신청서 승인을 수행하지 않음, 신청과 동시에 승인처리

사용자 신청서 신청정보 입력

신청정보는 Genian NAC에서 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.
SMS 문자통보	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 승인 권한을 관리자가 아닌 대상에게 부여할 수 있습니다.

사용자 용도에서 설정할 수 있는 항목은 신청서에 대한 승인방식, 처리옵션, 신청정보 입력으로 나뉘집니다.

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 NAC 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 IP신청서 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 신청서**를 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 **IP신청서 용도별 속성값 설정하기** 참고하시기 바랍니다.

1. 상단 패널에 **관리 > 신청** 으로 이동합니다.
2. 왼쪽 **IP사용신청서** 항목에 하위메뉴(**IP 신규/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 있을 경우 물리적인 조치를 수행하기 이전에 서비스를 재구동을 수행할 수 있습니다.

1. 상단 패널에 시스템 으로 이동합니다.
2. 왼쪽 시스템 관리 항목에 서비스 제어를 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 NAC에서 제공하는 모든 기능이 제공되지 않음으로 변경 시 충분한 검토가 필요합니다.

11.17.3 제공중인 Web 서비스 재구동 기능

Genian NAC에서 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 IP 신청시스템 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 관리를 선택합니다.
3. 디버그 설정을 변경할 네트워크 센서 장비의 체크박스를 선택합니다.(다수의 네트워크 센서 변경 시 대상 체크박스 모두 선택)
4. 작업선택 항목에서 장비 일괄 설정을 선택합니다.
5. 기타설정 항목에서 센서 디버그로그 생성 체크박스를 선택한 후 설정을 ON 으로 변경합니다.
6. 저장위치를 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 정책 서버	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 NAC 장비의 센터디버그를 개별 장비의 CLI 콘솔에 접속하여 설정합니다. 디버그 설정을 통해 Genian NAC 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 않으므로, CLI 모드에서 설정을 해야 합니다.

디버그 설정을 통해 Genian NAC 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** 명령어를 통해 설정모드에 진입합니다.
4. `debug centerd all` 명령어를 입력하여 디버그를 활성화 합니다.
5. **show configuration** 명령어를 입력하여 디버그가 설정됨을 확인합니다. 해당 명령어는 Configuration 모드 가 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 NAC에서 고가용성 기능을 제공하는 VRRP 프로토콜에 대한 디버그를 설정하여 정상적인 상태를 확인 하거나, 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** 명령어를 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 않으므로, 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 원인과약 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 NAC에서 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 NAC 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 NAC에서 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 완료하는데 도움이 되는 유틸리티 또는 기능입니다.
보안 업데이트	제품별 보안 관련 취약점을 위해 널리 배포되는 수정 프로그램입니다. 보안 취약성은 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 패키징된 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 검색하는데 사용됩니다.
중요 업데이트	보안과 관련되지 않은 중요한 버그를 해결하는 특정 문제를 해결하기 위해 널리 릴리스된 수정입니다. 1

11.23 윈도우 업데이트 목록 수동 설정하기

Genian NAC에서 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 정책으로 이동합니다.
2. 왼쪽 정책 항목에서 **Windows 업데이트 정책**을 선택합니다.
3. 생성되어 있는 업데이트 정책 ID를 클릭합니다.
4. 업데이트 설정 탭을 클릭합니다.
5. 설치승인상태가 설치미승인(자동) 항목 중 업데이트 목록에 포함할 업데이트에 체크박스를 선택합니다.
6. 작업선택 메뉴에서 설치승인(관리자)를 선택합니다.
7. 설정 확인 팝업창에 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	<ol style="list-style-type: none"> 1. NAC에서 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, NAC에서 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 정책을 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 CWP 설정 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	NAC 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. NAC 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 참고](#)하시기 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 관리를 선택합니다.
3. 센서 토큰 탭에서 토큰 미사용 센서 차단을 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 불가능합니다.
2. 토큰정보에는 정책서버 접속정보가 들어가 있습니다.
3. 토큰 미사용 센서 차단 기능을 사용하지 않고 토큰을 센서에 설정하는 경우 센서는 토큰에 포함된 정책 서버 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 에이전트를 선택합니다.
3. 기본설정 탭에서 토큰 미사용 에이전트 차단을 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 불가능합니다.
 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.
-

API 가이드

Genian NAC는 정책서버로부터 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 파라미터로 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 NAC에서 제공되는 API의 목록은 아래에서 확인할 수 있습니다.

- [https://\[정책서버IP\]:8443/mc2/swagger/index.html](https://[정책서버IP]:8443/mc2/swagger/index.html) (관리자는 정책 서버에 로그인되어야 합니다.)
- [API Reference Guide for Enterprise Edition](#)
- [API Reference Guide for MSSP](#)

12.1 REST API 활용 가이드

12.1.1 가이드 개요

Genian NAC는 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 NAC의 REST API를 활용하기 위한 요구사항, 인증 방법, 주요 API 등에 대한 안내를 목적으로 합니다.

Note: 유튜브를 통해 REST API 활용 가이드 동영상을 확인할 수 있습니다.



12.1.2 사전 준비사항

Genian NAC 활용 사전 준비사항

외부 장비에서 Genian NAC로 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 Key 방식은 연동을 위한 계정의 API키를 생성하여 Genian NAC의 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 방법을 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 NAC로 Log-in 후 기능을 수행합니다.
- 이후 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 NAC에서 제공하는 REST API는 https 프로토콜(TCP/8443)로 접속합니다.

TCP/8443 포트는 Web콘솔 접속용 포트와 동일합니다. 따라서, 방화벽 등에서 Genian NAC Web콘솔 접속을 위한 설정이 적용된 상태라면, 추가 작업은 하지 않으셔도 됩니다.

12.1.3 API 활용을 위한 상호 인증 방법

Genian NAC와 연동 대상 장비 간의 보안성이 확보된 상태에서 REST API를 활용하기 위해, 상호인증 수행이 우선 진행되어야 합니다.

Genian NAC는 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 Key 값을 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 NAC 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 인식되지 않습니다.
- REST API 사용 시 Get Parameter에 다른 Parameter 값이 존재할 때, 값이 끝나는 부분에 "&"를 이용하여 apiKey를 추가하면 정상적으로 동작됩니다.
 - 예시 : `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 NAC 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 **Subnet**과 **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 NAC와 연동을 위한 주요 API 항목은 NODES, TAGS, USERS, LOGS, NODEGROUPS, CVES 등이 있고, 각각의 내용은 다음과 같습니다.

NODES API

Genian NAC에서 노드(Node)란 IP 와 MAC 을 갖고 있는 장비 또는 엔드포인트를 말합니다.

노드는 NAC에서 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 IP에 대해서 nodeId값을 얻기 위한 목적으로 사용됩니다.
특정 노드에 태그 할당	POST	/nodes/{nodeId}/tags	특정 노드로 판단되는 특정 노드에 차단 태그를 할당하여 네트워크 격리를 수행하기 위한 목적으로 사용됩니다.
특정 노드에 태그 해제	DELETE	/nodes/{nodeId}/tags	특정 노드로 판단되는 특정 노드에 차단 태그를 제거하여 네트워크 진입을 허용하기 위한 목적으로 사용됩니다.
특정 노드의 상세 정보 조회	GET	/nodes/{nodeId}/information	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&
↳page=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 NAC는 노드/사용자를 분류할 때 태그(Tag)를 사용할 수 있습니다. (디폴트 Tag로는 TRUSTED, THREAT, GUEST가 있고, 수정 및 추가가 가능합니다.)

외부장치에서 연동으로 NAC 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 NAC에 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&
→page=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 NAC의 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 tagid 값 혹은 name 정보를 조회합니다.
특정 사용자ID에 태그 할당	POST	/users/{userId}/tags	기존에 할당되지 않은 특정 사용자ID에 차단 태그를 할당하여 네트워크 격리를 수행하기 위한 목적으로 사용됩니다.
특정 사용자ID에 태그 해제	DELETE	/users/{userId}/tags	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 NAC에서 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 NAC의 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-bf4b-fa142353b463}"-H "accept:
↪application/json;charset=UTF-8"
```

NODEGROUPS API

Genian NAC의 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 NAC에 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 NAC는 각 노드별로 공개적으로 알려진 정보 보안 취약성 및 노출에 대한 정보를 제공합니다.

CVES와 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
노 드 의 CVE 내역 조회	GET	/cves	위험노드에 네트워크 격리를 수행하기 위한 목적으로 Genian NAC에서 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 알려줍니다.
400	Bad Request	클라이언트의 요청 구문이 잘못됨
401	Unauthorized	요청 처리를 위해 HTTP 인증 정보가 필요함을 알려줍니다. 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 콘텐츠가 없음을 의미
412	Precondition Failed	클라이언트의 헤더에 있는 전제조건은 서버의 전제조건에 적절하지 않다고 알려줍니다
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 NAC는 API를 활용하는데 도움을 드리고자, Swagger(<http://swagger.io/>)를 제공합니다.

Swagger는 웹페이지를 통해서 REST API 정보와 테스트 도구를 제공합니다.

1단계. Swagger 접속

1. Genian NAC의 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 Code 값이 **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.)
-

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 발생하는 로그
101	GENIAN 장비	GENIAN 장비에서 발생하는 로그
102	동작상태변경	센서의 동작상태 변경 시 발생하는 로그
103	노드정보	노드의 상태 정보 변경 시 발생하는 로그
104	데이터베이스	백업 시 발생하는 로그
107	운영체제 업데이트 동기화	패치파일 업데이트 및 동기화 시 발생하는 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 발생하는 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	NAC 설정 변경 이벤트 로그
906	시스템관리	NAC 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

제품 출시 주기는 어떻게 됩니까?

- Genian NAC는 2021년 2월을 시점으로 격월 정기 릴리즈 버전을 출시합니다.

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* 업데이트의 1 단계를 참고하세요.

에이전트 지원 운영체제는 어떻게 됩니까?

- Genian NAC는 *Windows, macOS, Linux* 운영체제에 대해서 에이전트를 제공합니다.

어떤 백신제품을 지원합니까? ?

- Genian NAC는 국내, 국외의 백신 제품들에 대해서 지속적인 연동을 통해 확대 범위를 넓혀가고 있습니다. [windows](#) 자세히 보기, [macOS](#) 자세히 보기, [Linux](#) 자세히 보기

Genian NAC가 지원하는 무선어댑터는 어떻게 됩니까?

- Genian NAC 무선센서와 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 PC에 CWP 페이지를 표시하는 방식](#)

Web 콘솔 노드관리 화면의 에이전트 아이콘이 회색인 이유는 무엇입니까?

- Web 콘솔 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.

RAID 구성이 가능한가요?

- 별도의 RAID 카드 (ASR-8405E v2)를 추가 장착하여 RAID 0,1 구성이 가능합니다. 자세한 내용은 Sales 부서로 문의주세요.

운영정보 데이터(Genian data)의 업데이트 주기는 언제입니까?

- 운영정보 데이터는 Web콘솔 > 설정 > 기타설정 > 운영정보 자동 업데이트 설정 에서 검사 주기를 설정하고 하단 자동업데이트 항목을 On으로 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 제어를 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.

Active Directory의 사용자 자격 증명을 사용하여 웹 콘솔에 접근할 수 있습니까?

- 인증 연동과 정보 동기화를 설정하면 사용할 수 있습니다. AD 도메인 컨트롤러와 데이터베이스 동기화, 마지막으로 AD 사용자는 Genians 사용자 데이터베이스에서 선택하고 구성해야 합니다.
- 외부 인증서버 설정
- LDAP

노드 타입과 플랫폼 분류 동작 방식은 어떻게 되나요?

- 노드타입과 플랫폼 분류는 운영데이터인 NMDB(NMAP Database, 노드정보 감지 데이터) 와 GPDB(Genian Platform Databases, 운영체제 감지 데이터)를 통해 분류하고 있습니다.
- GDPI

에이전트 로그 수집은 어떻게 진행하나요?

- 에이전트 트레이 아이콘 마우스 우클릭 -> 프로그램 정보 클릭 -> 오류 보고 클릭 -> C:\GnAgent 연월시분.zip 파일 확인

장비도입 후 보안적합성 검증 절차를 반드시 진행해야 하나요?

- 국가사이버안보센터의 안정성 검증필 제품목록으로 등재된 제품의 경우 보안적합성 검증을 생략할 수 있습니다. 현재 NAC는 구간보안 제품군, 네트워크 접근 통제제품으로 등록되어 있습니다.
- 국가사이버보안센터

노드액션과 제어액션의 차이점은 무엇인가요?

- 노드액션은 노드정책에서 사용하는 액션플러그인 정책이며 제어액션은 제어정책에 사용하는 액션정책입니다.
- 노드액션은 등록된 에이전트 플러그인을 모두 사용가능하지만 제어액션에는 지정된 플러그인만 사용가능합니다.

TROUBLESHOOTING

15.1 디버그 수집과 증상분석

15.1.1 NAC 디버그로그와 패킷 수집

NAC는 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.

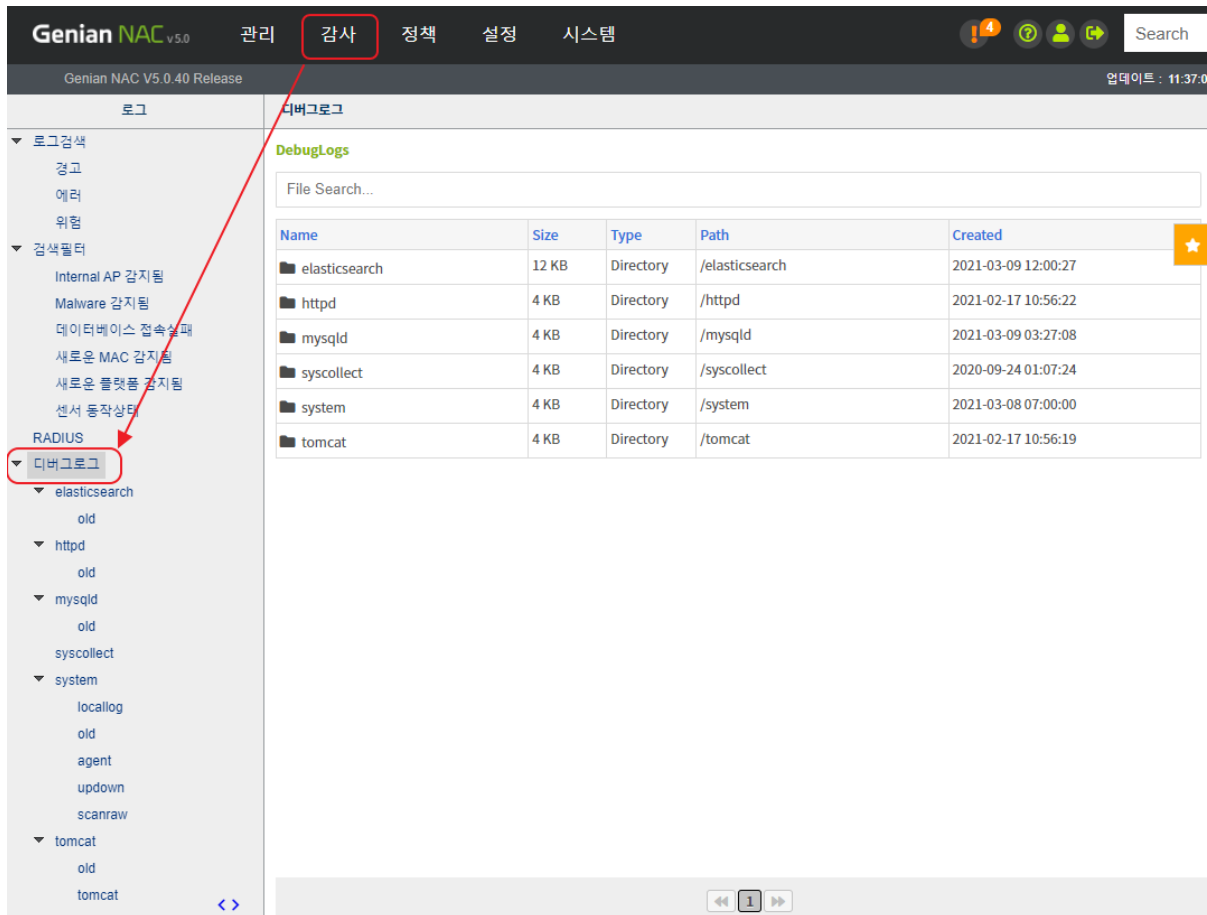
- LINUX 단말의 경우 직접 디버그 저장경로로 이동하여 수집하여야 합니다. "`/var/log/genians`" 입니다.

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)

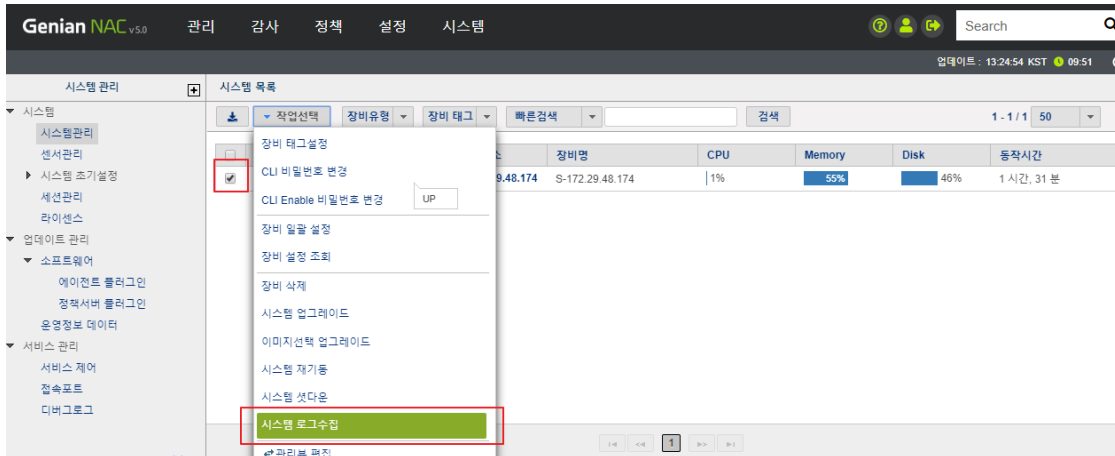


정책서버/네트워크센서 디버그로그 일괄 수집방법 (syscollect)

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
- 셸모드 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 backtrace 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 캡처하고 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: 패킷캡처 결과를 상세하게 출력
-n: 주소 (호스트주소, 포트번호)를 이름으로 변경하지 않고 출력
-e: 패킷캡처결과에 링크레이어 헤더를 출력 (이더넷 주소표시)
-w: 캡처한 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 NAC 분석 방법

이 페이지에서는 NAC에서 문제를 해결하기 위해 검사할 수 있는 주요 프로세스에 대한 개요를 제공한다.

NAC 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: NAC에서 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
cron: 지정된 사이클에서 스크립트 및 명령을 수행하는 데몬
radiusd: 인증을 위한 RADIUS 서버 데몬
```

네트워크센서 프로세스

```
sensord: 네트워크센서 프로세스
nmap: 노드의 네트워크 정보 검색 도구
procmond: NAC에서 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

<p>프로세스명: GnAgent.exe 설명: Genian Agent 기능: 에이전트 무결성 검사, 노드 정책 수신 및 GnPlugin 실행 관리 실행주기: 항상 실행조건: 윈도우즈 로그인 이후 항상</p>
<p>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</p>
<p>프로세스명: GnStart.exe 프로세스명: Genian Starter 기능: 에이전트 무결성 검사, GnAgent 실행 관리, Keepalive 전송 실행 주기: 항상 실행조건: 항상</p>
<p>프로세스명: GnAccount.exe 프로세스명: Genian User Account Manager 기능: OS 로그인 계정 대신 특정 계정으로 GnAgent 프로세스를 실행하는 경우 사용 실행 주기: 이벤트가 발생한 경우 실행조건: 노드정책에 에이전트 실행계정 설정이 되어 있는 경우</p>
<p>프로세스명: GnDump.exe 프로세스명: Genian Agent Dump Utility 기능: 에이전트 디버그로그 수집 실행 주기: 없음 실행조건: 수동 실행 시에만 작동</p>
<p>프로세스명: GnExLib.exe 프로세스명: Genian External Module 기능: 외부 인증 모듈 등록 (예: dll) 실행 주기: 없음 실행조건: 정책적으로 수동 실행시나 인증정보 갱신시</p>
<p>프로세스명: GnScript.exe 프로세스명: Genians Software Install Manager 기능: 에이전트 설치시 실행 주기: 없음 실행조건: 에이전트 설치 중에만 실행</p>
<p>프로세스명: GnUpdate.exe 프로세스명: Genian Updater 기능: 에이전트 자동 업데이트검사 및 업데이트 실행 주기: 6시간 실행조건: 없음</p>
<p>프로세스명: GnUtil.exe 프로세스명: Genian Agent Utility Funciton: 특정 파일의 SHA1 해시 값 계산 실행 주기: 없음 실행조건: 수동으로 실행될 때만 작동함</p>

시스템 디버그 프로세스명

정책서버 로그

Elasticsearch

GENIAN.log: Elasticsearch 프로세스 비정상 종료 및 재시작 오류 로그

httpd

Error_log: httpd 예러 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
 - NAC 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
 procmoud: 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 NAC시스템의 상태를 확인합니다.

- 박스에 표시된 대로 다음 단계를 수행하십시오.
- 정책서버 콘솔에 직접 연결하거나 SSH 통해 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

NAC에서 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 NAC는 다음과 같은 문제가 발생할 수 있습니다.

- NAC 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

The screenshot shows the Genian NAC v5.0 web console interface. The main content area displays a table titled 'System' with columns for 'Node Type', 'Managed Nodes', 'Link', 'IP', and 'MAC'. The 'Link' column for the sensor with IP 192.168.1.240 shows a power icon (indicating a down state), which is highlighted with a green circle. The sensor with IP 172.29.45.240 shows a green checkmark icon (indicating an up state).

Node Type	Managed Nodes	Link	IP	MAC
🟢	4/12	🟢	172.29.45.240	08:60:6E:F6:31:1
🟢	2/2	🔴	192.168.1.240	08:00:27:51:26:4

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-Premises

UDP / 3870 ports

Cloud-managed

(변경가능)

메뉴위치는 시스템 > 서비스 관리 > 접속포트 에서 **Keepalive** 항목에 적혀있는 포트를 허용

The screenshot shows the Genian NAC v5.0 web interface. The top navigation bar includes 'Dashboard', 'Management', 'Log', 'Policy', 'Preferences', and 'System'. The main content area is titled 'Service Port' and contains a table with the following data:

Service	Protocol / Port	Description
HTTP	TCP/80	CWP, Request
HTTPS	TCP/443	CWP, Request, Receiving Policy, Updating Data
KeepAlive	UDP/12320	Console
RADIUS Authentication	UDP/7066	RADIUS Authentication
RADIUS Accounting	UDP/7067	RADIUS Accounting

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 있는 경우 센서에게 알림이 가고 센서는 그에대한 응답을 수행합니다.

센서가 새로운 정책갱신이 필요한것을 인지하게 되면 TCP Port/443 HTTPS를 통하여 정책서버와의 TCP 세션 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 NAC에이전트 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
4. 에이전트가 Keep-Alive 패킷을 생성하지 않는 것

해결방법

정책서버와 에이전트간 통신 확인

- 에이전트와 정책서버간의 Keep-Alive 통신 확인

```
tcpdump -i eth0 host [PC IP] and port 3871
```

- 정책서버와 에이전트 사이에 방화벽이나 타 보안솔루션에서 단말에서 발생하는 패킷이 존재하는지 확인

Keep-Alive 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
- (Windows) 에이전트가 Keep-Alive 패킷을 생성하고 보내는지 확인하려면 추가적인 디버그 설정이 필요
 - 레지스트리에서 HKEY_LOCAL_MACHINE\SOFTWARE\Geni\Genian\Option 또는 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Geni\Genian\Option 을 찾습니다.
 - DWORD:DebugPrint (1) 추가 설정

Keep-Alive 패킷이 감지되는 경우

- Agnet 설치나 정책 서버에 문제가 있을 수 있습니다.
- 기타 케이스에서는 로그를 수집하여 기술지원

참조: [NAC 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 짧을 경우 데이터전송을 하지 못하고 세션이 종료되며 에러로그가 발생합니다.

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

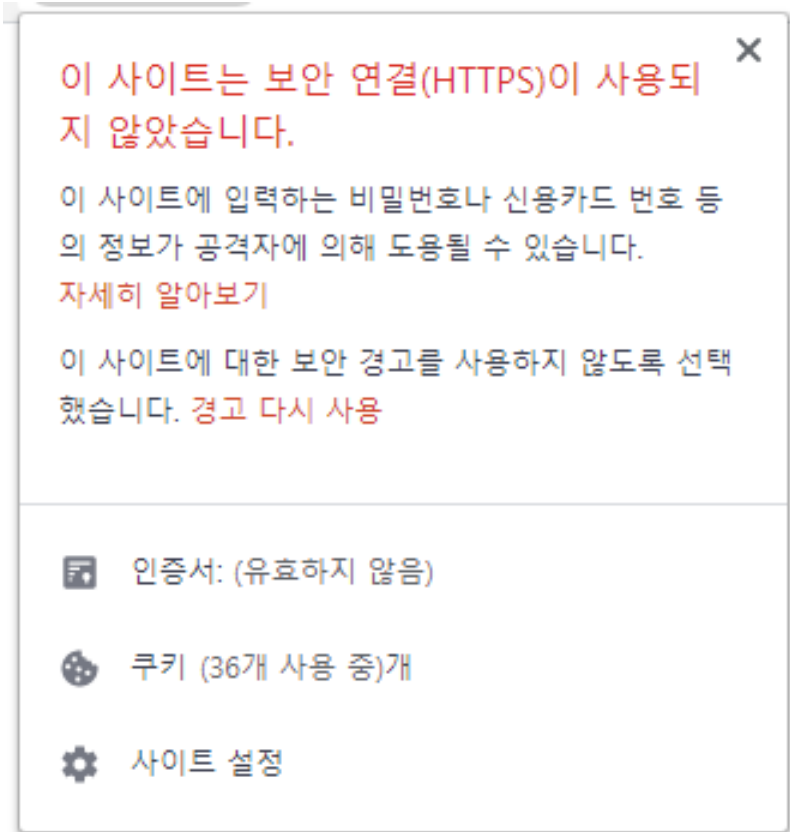
내부AP감지 기능 중지를 수행합니다.

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.

15.2.8 ARP 제어를 통한 네트워크 차단 실패

증상

센서의 모드는 Enforcement 이고 제어정책에 차단 대상 노드가 포함되어 있습니다. 해당 제어정책이 활성화되어 웹 콘솔에 있는 제어정책 관리 뷰에서 차단 노드가 확인되어도 차단이 되지 않고 네트워크 연결이 지속되고 있는 경우

원인

- 일부 IDS/IPS 또는 EDR 솔루션은 ARP Enforcement 작업을 네트워크 공격으로 잘못 식별, 감지하여 차단할 수 있습니다.

해결 방안

충돌하는 보안 제품에서 **Genian NAC**에 대한 예외 추가

해당 문제를 해결하려면, 정책 및 기타 네트워크 보안 솔루션의 구성에 따라 Sensor IP에 대한 예외 처리가 필요합니다.

참조 : ESET Endpoint Security

15.3 설정

15.3.1 노드가 관리UI에 등록되지 않음

증상

네트워크센서를 제외한 모든 노드가 네트워크센서가 설치된 서브넷에서 표시되지 않음

원인

NAC는 연결된 스위치포트의 설정과 네트워크센서 인터페이스 설정과 일치하지 않을 때 노드를 검색할 수 없다.

해결방법

스위치

- NAC가 연결되어 있는 포트가 모니터링하려는 VLAN에 액세스하도록 올바르게 설정되어 있는지 확인하십시오.
- NAC는 표준 액세스 포트 및 802.1q 트렁크포트만 지원합니다.

네트워크센서

- cli에서 `show interface eth[#]` 명령을 사용하여 인터페이스 설정을 확인하십시오.
- eth0 인터페이스는 스위치의 액세스포트나 트렁크포트의 `default vlan`이 설정되어 있는 경우에만 작동합니다.
- 태깅된 모든 VLAN 트래픽은 해당 VLAN의 정의된 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 로그인에 되지 않을 때

증상

인증이 실패하며 "접속권한이 없는 위치입니다." 라는 메시지가 표시되는 증상



원인

- 정책서버는 각 관리자계정에 대한 접속허용 IP 목록을 사용하여 관리 WebUI에 대한 접속을 제어
- 접속허용 목록은 각 관리자 계정의 기본정보탭 > 로그인 설정에서 변경 가능합니다.
- 관리자의 IP 주소가 접속허용 IP에 존재하지 않을 경우 관리자는 관리 WebUI에 접속할 수 없습니다.

해결방법

사용자 관리 수정 권한이 있는 관리자계정이 있는지 확인합니다.

다음:

- 관리 WebUI 접속
- 다음위치로 이동 관리 > 사용자 > 설정을 변경할 사용자 ID 선택 > 로그인 설정
- 접속하려는 IP가 관리 WebUI 접속 IP1에 접속하는 관리자 PC의 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 VLAN 을 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 USER 정보가 사전에 정의되어 있어야 한다. 참조 [Cisco SNMP Configuration](#)

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 **CLI**를 통하여 센서 제어

- 아래와 같이 정책서버 SSH로 접속하고 셸모드로 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 **CLI**에서 센서 동작상태 확인

- 셸모드를 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 적은 경우 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. **Web 콘솔 > 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. **Web 콘솔 > 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 > 관리자 지정 조건**을 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. **Web 콘솔 > 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 NAC로 인한 차단이 의심될때 확인 방법

NAC 운영하는 환경에서 간혹 단말의 네트워크 통신이 실패할 때 NAC와 관련이 있는지에 대한 부분을 확인 하는 방법을 안내합니다.

Genian NAC는 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 NAC와 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 권장 합니다.)
 - 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

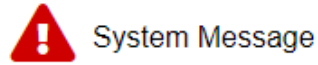
- 에이전트를 통하여 단말을 제어하는 방법은 여러 가지가 있지만 본 상황에서는 네트워크 통신에 대한 부분만 확인합니다.
 - 1) 시작버튼 > 설정 > 네트워크 및 인터넷 > 어댑터 옵션 변경 > 주 사용 네트워크 어댑터가 회색으로 사용 안 함 상태인지 확인합니다.
 - 2) 사용 안 함 상태가 아니라면 에이전트 인터페이스 제어가 수행된 상태는 아닙니다.

15.5 시스템

15.5.1 웹콘솔 시스템 에러

증상

관리WebUI에서 특정 메뉴를 선택하였을 경우 아래와 같은 오류 메시지 표시:



System Message

오류가 발생하였습니다. 관리자에게 문의하세요.

[이전화면](#)

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 오류시

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 NAC 디버그/패킷 수집을 통해 문제를 해결합니다.
 - Syscollect 기능을 이용하여 기술지원 엔지니어와 증상과 로그를 공유하여 기술 지원을 받습니다.

참고: NAC 디버그로그와 패킷 수집

15.5.4 데이터베이스 크래시 발생 시 복구

Genian NAC는 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 있는 경우 Step3로 이동합니다.
genian#
!!! WARNING !!! - SHELL PROMPT IS JUST FOR MAINTENANCE.
!!! WARNING !!! - 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 NAC 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 접속포트를 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 배포에 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 NAC 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 NAC 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
```

Web 콘솔 접속포트 변경하기

Genian NAC 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 NAC 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 **RADIUS**서버 를 선택합니다.
3. **RADIUS Authentication Server** 설정에서 포트번호 (**Authentication**) 를 입력합니다.
4. 수정 버튼을 클릭합니다.

Radius Accounting 서비스에 대한 포트 변경하기

Genian NAC 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 **RADIUS**서버 를 선택합니다.
3. **RADIUS Accounting Server** 설정에서 포트번호 (**Accounting**) 를 입력합니다.
4. 수정 버튼을 클릭합니다.

Data Server 서비스에 대한 포트 변경하기

Genian NAC 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 NAC 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 NAC 장비에 CLI Mode 원격접속에 대한 포트를 변경할 수 있습니다. 기본적으로 사용되는 포트 3910 를 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 NAC WEB 콘솔 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 > SSL 인증서** 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. 서명요청서(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

- NAC는 다음과 같은 방법으로 윈도우 업데이트 서비스를 제공합니다.:
- 윈도우즈 업데이트 검색
- 스케줄링 업데이트
- 윈도우즈 패치검색 서버를 설정 (Genian NAC, Genian Proxy, or Microsoft Servers).
- 윈도우즈 패치 다운로드 서버를 설정 (Genian NAC, 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 (genian-nac-5.0.17)

15.6.3 외부 RADIUS 연동테스트시 secret key mismatched 발생

증상

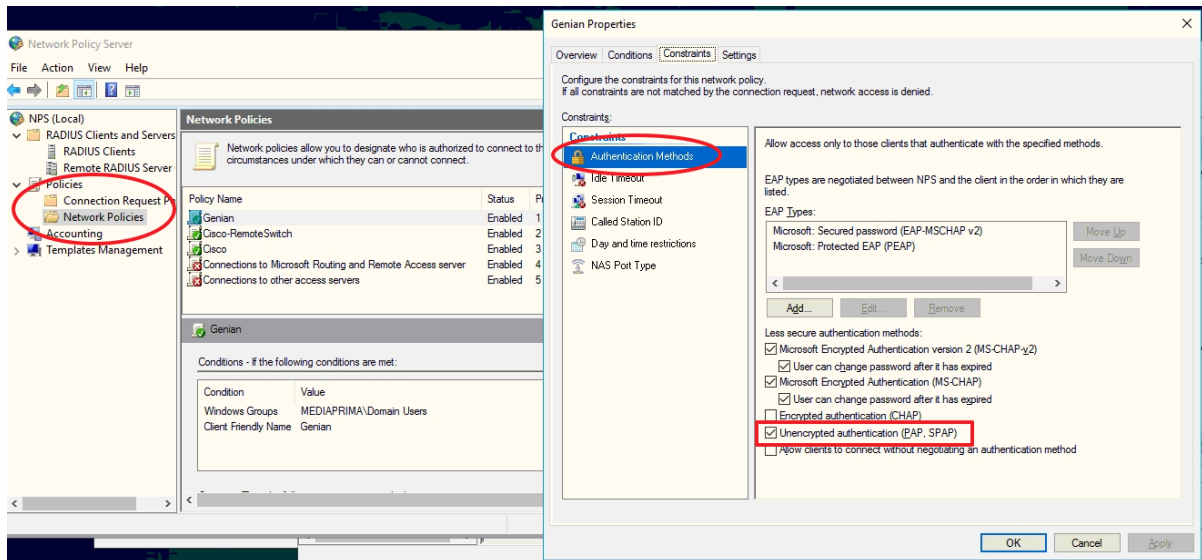
Genian NAC와 외부 RADIUS(Windows) 서버와 연동설정을하고 Web콘솔에서 제공하는 인증테스트 수행시 secret key mismatched 에러 발생

원인

Genian NAC 정책서버는 RADIUS 서버에 요청할때 PAP(비암호화) 방식으로 인증을 요청하는데 RADIUS 서버에 비암호화 인증요청 허용이 되어있지 않은 경우 인증거부 및 인증테스트 창에 위와같은 오류 메시지 표시

해결방법

RADIUS 서버에서 비암호화 방식의 인증요청도 허용하도록 설정



RELEASE NOTES

16.1 업그레이드 가이드

16.1.1 주의사항

- 업그레이드를 하기 전 반드시 업그레이드 가이드, 업그레이드 주의사항, 릴리즈노트를 충분히 읽어보신 뒤 문제되는 사항이 없는지를 확인하신 후 진행하시기 바랍니다.
- 업그레이드 시 모든 데이터는 자동적으로 새로운 버전에 맞게 재수정 됩니다. 하지만 다운그레이드를 하면 제품이 오동작 할 수 있습니다.
- 다운그레이드는 반드시 데이터 초기화를 한 뒤 백업데이터로 복구 하시기 바랍니다.
- 정책서버 및 DB 업그레이드를 하는 경우 *geniup* 수행시 반드시 백업을 수행하는것을 권장합니다.
- 기본버전과 업그레이드 버전간의 버전차이가 큰 경우 다수의 DB테이블 구조변경으로 인한 Migration으로 인해서 업그레이드가 장시간 소요될 수 있습니다. 이때 CLI에 접속하거나 관리콘솔에 접속하면 DB migration중임을 알리는 메시지가 표시됩니다. 이때는 절대로 서비스를 중지하거나 장비를 재부팅해서는 안됩니다.
- 3.0, 4.0 구버전에서 업그레이드 진행시 장비의 CLI 설정정보를 검토 한 후 누락된 사항이 없는지 확인하시기 바랍니다.
- 커스터마이징 설정이 존재하는지 사전 검토바랍니다.

5.0 업그레이드 주의사항

5.0 Major 버전의 경우 기존 3.0, 4.0 제품과 차이점이 많습니다. Major 업그레이드 전에는 주의사항을 꼭 읽고 작업을 진행하시기 바랍니다.

이미지버전 호환성

정책서버 버전 5.0.42 이상으로 업그레이드시 네트워크센서의 버전은 최소 5.0.42 이상을 권고합니다.

업그레이드 이미지 선택

5.0 GNOS 이미지가 정책서버 및 센서 겸용인 CT64와 센서전용인 SS64 두가지로 구분되어 있습니다.

Release NAME	Operation Mode	동작속도	Operation Platform
CT64	Policy, DB, Sensor, Radius	64 Bit	GPC-1000 이상
SS64	Sensor 전용	64 Bit	

Note:

- 5.0 이미지의 용량이 증가하여 512MB 미만의 CF나 DOM을 가진 장비에는 설치가 불가능합니다.
 - 5.0 Console baudrate는 115200 으로 설정하여 접속해야합니다.
-

업그레이드 방법

Genian NAC Ver5.0 이하 제품에서 5.0제품으로 업그레이드 하는 방법은 기존 Minor 업그레이드 방법과 동일합니다.

1. 정책서버 단일장비로 운영중인 경우
 1. 네트워크센서 운영모드를 *Passive* 로 전환합니다.
 2. 정책서버를 업그레이드 합니다.
 3. Web콘솔에 접속 하여 네트워크센서 이미지를 정책서버에 Upload 합니다.
 4. 네트워크센서 CLI에 접속하여 *geniup* 명령어를 통하여 업그레이드 작업을 진행합니다.
2. 정책서버, DB서버 분리구성인 경우
 1. 이중화 구성시 업그레이드 방법을 참고하여 정책서버와 DB서버를 업그레이드합니다.
 2. Web콘솔에 접속 하여 네트워크센서 이미지를 정책서버에 Upload 합니다.
 3. 네트워크센서 CLI에 접속하여 *geniup* 명령어를 통하여 업그레이드 작업을 진행합니다.

Note:

- 정책서버가 5.0으로 업그레이드 된 후에는 3.0 네트워크센서는 정책서버와 연결되지 않습니다.
-

GNOS 이미지 전자서명 추가

5.0 GNOS 이미지 파일에 대한 무결성 및 부인방지를 위한 전자서명 검증기능이 추가 되었습니다. 업그레이드 시 전자서명을 확인하는 절차로 인하여 업그레이드가 실패할 수 있습니다.

Note:

- 3.0과 4.0.12 미만 버전에서 5.0으로 업그레이드 시 최초 1회 비 Sign 이미지를 이용하여 업그레이드를 진행해야합니다.
 - 비 Sign 이미지는 기술지원센터 를 통하여 전달 받을 수 있습니다.
-

에이전트 업데이트

3.0과 4.0버전의 에이전트는 5.0버전에서 사용할 수 없습니다. 또한 정책서버를 5.0으로 업그레이드 하면 에이전트가 동작하지 않게 됩니다.

정책서버가 5.0으로 업그레이드 된 후, 센터의 배포용 에이전트는 기존 버전의 에이전트를 유지하게 됩니다.

따라서 소프트웨어 관리 메뉴에 5.0버전의 에이전트를 upload 해야 합니다.

- 구 버전의 에이전트 플러그인의 설정이 5.0에서 상이한 내용이 있을 수 있기때문에 수동으로 점검이 필요합니다.
- 정책서버에 5.0 버전의 에이전트가 등록되면 구버전 에이전트는 업데이트 주기(6시간)에 맞추어 자동으로 업데이트 됩니다.

16.1.2 업그레이드 진행

WEBUI를 이용한 진행

- 센서와 같이 대량으로 업그레이드를 해야하는 경우 WEBUI를 사용한 업그레이드를 권장합니다.

CLI를 이용한 진행

- 정책서버 또는 DB서버와 같이 주요한 서버를 업그레이드 할 경우 CLI를 통한 업그레이드를 추천합니다.

16.1.3 정책서버/센서 구성시 업그레이드 방법

둘간의 버전이 다른경우 비정상동작하는 경우가 많습니다. 따라서 반드시 두 버전을 동일버전으로 맞추어 줍니다. 정책서버와 센서가 서로다른 버전인 상태로 동작하지 않도록 하기위해 다음과 같은 절차를 통하여 업그레이드 합니다.

- 정책서버 서비스 중지
- 정책서버 업그레이드 (재부팅하지 않음)
- 센서 업그레이드
- 정책서버 재부팅

16.1.4 정책서버/DB서버 분리구성시 업그레이드 방법

정책서버 업그레이드 과정에서 DB서버가 업그레이드 되지 않도록 주의해야 합니다. 그를 위해 다음과 같은 절차로 업그레이드를 수행합니다.

- 정책서버 동작중지
- DB서버 업그레이드- DB서버 재부팅 후 정상동작 확인
- 정책서버 업그레이드

16.1.5 이중화 구성시 업그레이드 방법

업그레이드 과정에서 MASTER시스템이 변경되지 않도록 하는 것이 불필요한 문제를 줄이는 방법입니다. 그를 위해서 다음과 같은 절차로 업그레이드를 수행합니다.

- SLAVE시스템의 서비스를 중지 합니다.
- SLAVE시스템을 업그레이드 합니다. 단, 자동재부팅 되지 않도록 합니다.
- MASTER시스템의 서비스를 중지 합니다.
- MASTER시스템을 업그레이드 합니다. 단, 자동재부팅 되지 않도록 합니다.
- MASTER시스템을 재부팅하고 서비스를 체크합니다.
- SLAVE시스템을 재부팅하고 서비스를 체크합니다.
- 만일 DB서버도 업그레이드 하는 경우 정책서버의 서비스를 중지하고 DB서버를 업그레이드 한 뒤 DB 서버 정상동작을 확인하고 정책서버를 업그레이드 합니다.

16.2 Current Versions

16.2.1 Genian NAC 5.0.61 (R) Release Notes (2024-04-01)

Last Updated: 2024-04-01

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
125418	GN-27711	RADIUS	RADIUS 와 AD 인증연동 환경에서 사용자의 패스워드가 AD서버에서 변경되었을 경우 패스워드 prompt 가 나올수 있도록 개선	
125418	GN-27706	WebUI	WEBUI 2단계인증 시 1차 ID/PW 로그인 인증 실패 횟수가 포함되도록 개선	
125418	GN-27697	Center	Webhook 인증연동시 패스워드를 SHAxxx 결과로 전달할 수 있도록 추가	
125418	GN-27691	WebUI	[5.0] 외부 서비스 연동 API 기능 추가	
125418	GN-27662	Windows Agent	Kaspersky 신규 백신 제품 (Kaspersky Endpoint Security 12 for Windows)에 대한 정보 수집기능 추가	
125418	GN-27499	Windows Agent	무선랜제어 플러그인에서 허용 무선랜 설정에 대한 설명 수정	
125418	GN-27335	Center	802.1x Account 패킷의 calling-station-id 에 단말의 IP가 들어가 있는 경우 Framed IP로 처리하도록 개선	
125418	GN-27294	IPMGMT, Sensor	IP 정책을 센서별로 생성할 수 있도록 개선	
125418	GN-26663	macOS Agent	macOS 비밀번호 유효성 검사 플러그인 추가	
125418	GN-26589	WebUI	CLI 비밀번호를 변경 할 수 없는 범용OS 및 클라우드 장비에 변경불가 안내메시지 표시되도록 개선	
125418	GN-25876	WebUI	관리자 2단계 인증 실패 시 감사로그 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
125418	GN-27954	Center	RADIUS Account 패킷으로 노드의 IP를 업데이트하면서 IP/MAC이 동일한 노드가 복수개 만들어지는 문제	5.0.36
125418	GN-27911	WebUI	관리콘솔의 접근허용 IP설정에서 Subnet 지원 옵션이 오 동작하는 문제	6.0.21 (R), 5.0.61 (R)
125418	GN-27895	Windows Agent	외부인증연동 플러그인에 등록된 프로그램이 계속 수행되는 문제.	6.0.18, 5.0.58
125418	GN-27894	Center	신규노드 호스트명제한 기능이 정상 동작하지 못하는 문제	6.0.21 (R), 5.0.61 (R)
125418	GN-27848	GNOS, Sensor	[GNOS] 센서장비의 syslog 서비스가 외부로 OPEN 되어 동작하는 문제	
125418	GN-27808	Center	vpn 연결 실패도중에 vpn 기능을 off / on을 하면 불필요한 로그가 남는 문제	5.0.42 (LTS), 6.0.0
125418	GN-27797	WebUI	IP정책을 센서 대역으로 적용한 경우 빠른검색 등에서 IP 검색시 다중으로 출력되는 문제	6.0.21 (R), 5.0.61 (R)
125418	GN-27733	WebUI	노드 목록과 노드 상세 화면의 마지막 동작시각이 일치하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
125418	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
125418	GN-27657	WebUI	감사로그 내보내기 한 엑셀 파일이 Windows Excel에서 정상적으로 열리지 않는 문제	6.0.11

16.2.2 Genian NAC 5.0.55 (LTS) Release Notes (2023-07-21)

Last Updated: 2024-04-04

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
125400	GN-27107	WebUI	권한 없는 관리자로 인한 Tomcat 재구동 명령 수행으로 서비스 무력화	5.0.41	2.7
125328	GN-27242	WebUI	NAC 5.0에서 사용자 검색 화면을 통해서 sql injection이 가능한 취약점	5.0.15	4.8
123778	GN-26393	WebUI	접근 권한 없는 페이지에 직접 URL을 입력하여 정보 수정이 가능한 취약점		3.1
123254	GN-26390	WebUI	감사로그 REST API를 통한 권한 없는 관리자의 파일 내보내기 권한 우회 취약점		3.1
122614	GN-27492	WebUI	Tomcat Version Upgrade (8.5.94 -> 8.5.96 / 9.0.81 -> 9.0.83)		7.5
121389	GN-26315	WebUI	2단계 인증에서 인증코드 입력값 횡수제한, 시간제한하도록 개선		4.3
120866	GN-27278	WebUI	Tomcat Version Upgrade (8.5.94 / 9.0.81)		7.5
120379	GN-26935	WebUI	부서명으로 출력된 html tag가 tree에서 실행되는 취약점	5.0.0	1.2
120379	GN-26865	WebUI	대시보드 위젯 설정에서 XSS 입력 취약점		1.2
120379	GN-26835	Center	데이터 업데이트에 사용되는 SQL을 통한 Command Injection 취약점		6.6
120379	GN-26833	Sensor	센서의 NMDB 업데이트 과정에서 nmap 스크립트 변조 취약점		4.1
120379	GN-26814	Center	Bufferoverflow 에 대한 코드 개선		2
120379	GN-26725	Linux Agent, macOS Agent, Windows Agent	[Agent] 센터 및 센서에서 전송된 이벤트에 대한 유효성 검사 추가		6.3
120379	GN-26696	Sensor	센서의 수신 이벤트에 대한 검증 미흡		6.3
120379	GN-26694	Center	다운로드 URL 검증 미흡으로 인한 Parameter Injection 취약점		6.6
120379	GN-26383	WebUI	html/script 코드 주입 가능한 취약점		5.3
120379	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
125153	GN-27973	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 3.0.13, 1.1.1w 업데이트 - X.509 정책 제약 조건을 확인하는 과정에서 과도한 리소스 사용	4.0.0, 5.0.0, 6.0.0
123469	GN-27625	Sensor	센서 운영모드 및 정책변경시 public ip를 가져오지 못할 경우 반영되지 않는 문제 개선	
122691	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
122238	GN-27164	VRRPD	[범용OS] 이중화 구성 master 상태로 전환 후 인터페이스 상태검사 실패로 인해 slave 상태로 전환되는 문제	5.0.42 (LTS)
122215	GN-27402	WebUI	MAC 정책 수정 시 시작/종료 시각을 설정할 수 있도록 API 개선	
122178	GN-27390	Center, WebUI	리포트 보존개수 설정 시 /disk/data/report 디렉토리의 데이터도 삭제하도록 개선	
121929	GN-27241	macOS Agent	macOS 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121892	GN-27248	Linux Agent	Linux Agent, 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121742	GN-26627	WebUI	CWP 웹 페이지 출력 상태에서 에이전트 인증 후 CWP 웹에서 인증 화면이 다시 출력되지 않도록 개선	
121119	GN-27269	- Unknown/None	apache / tomcat 관련 디렉토리 및 파일의 불필요한 권한 제거	
120558	GN-26325	GNOS	httpd 구동 스크립트 실행 시 procmound에 의해 중복 실행되는 문제 개선	
120405	GN-27146	Center	extauth 를 통한 외부인증연동 실패시 사용자가 입력한 패스워드가 센터디버그파일에 남는 문제	
120379	GN-27207	Windows Agent	다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
120379	GN-27206	Center, Sensor	센터에서 신뢰할 수 있는 nodeid 를 센서와 에이전트로 내려보내는 기능 추가	
120379	GN-27142	Windows Agent	알약 신규버전에 대응하는 연동 모듈 변경	
120379	GN-27121	Center, macOS Agent	macOS 에이전트 신규 OS 14.0 (Sonoma) 지원	
120379	GN-27046	WebUI	노드 등록, 노드 일괄등록, 노드 속성 가져오기에 IP/MAC 추가필드 항목을 추가	
120379	GN-27045	WebUI	노드관리 목록에 신규로 추가된 IP, MAC 추가필드 출력 기능 추가	

continues on next page

Table 1 - continued from previous page

Revision	Key	Components	Description	Affects Versions
120379	GN-27038	WebUI	openssh 버전업 이후 webssh 접속되지 않는 문제 개선	
120379	GN-27031	Center, Sensor	[범용OS] Ubuntu OverlayFS 모듈에서 발생하는 로컬 권한 상승 취약점	
120379	GN-27013	WebUI	markdown으로 설정된 항목을 변환할 수 있도록 개선	
120379	GN-27010	GenianOS	GNOS OpenSSH 버전 업그레이드 (8.6p1->9.3p2)	
120379	GN-26988	macOS Agent	macOS 파일 배포 플러그인 V2 사용시 승인창 표시되지 않도록 기능개선	
120379	GN-26987	Linux Agent	Linux Agent, 파일 배포 플러그인 V2 사용시 승인창 표시되지 않도록 기능개선	
120379	GN-26981	Center, Linux Agent, macOS Agent, WebUI, Windows Agent	배포 플러그인 V2 사용시 승인창 표시 되지 않도록 기능 개선	
120379	GN-26879	WebUI	IP/MAC 추가필드 관리 기능 추가	
120379	GN-26838	Ubuntu(Debian)	[범용OS] ICMP Timestamp 지원 기능 제거	
120379	GN-26792	Center, Sensor	정책서버 수신 이벤트 검증 강화	
120379	GN-26791	WebUI	노드 일괄 등록시 (csv 파일 업로드) 사용 가능한 커스텀필드 20개 까지 확장	
120379	GN-26789	Genian Syncer	지니안싱커로 동기화 되는 운영정보데이터의 전자서명 검증	
120379	GN-26778	Center	IP/MAC 추가필드 관련 노드그룹 조건 추가	
120379	GN-26766	Center, macOS Agent	macOS Sigstore 전자서명을 기반한 배포 플러그인 개발	
120379	GN-26730	macOS Agent	macOS 에이전트 ZTNA 신규 아이콘 적용 및 연결표시 변경	
120379	GN-26729	macOS Agent	macOS 에이전트 백신정보수집 플러그인 사용시 AhnLab V3 정보를 수집 못 하는 증상	
120379	GN-26724	Sensor	Axgate 80D, 200AX 모델 포팅 모듈 커널 업그레이드 (2.6.38->4.14.196) 개선	
120379	GN-26644	Windows Agent	센터 CA 인증서 설치 옵션을 기본 ON으로 변경 및 수행 주기 변경	
120379	GN-26563	Sensor	센서 인터페이스에 Alias IP 설정없이 Alias IP대역을 센서가 관리할 수 있도록 개선	
120379	GN-26479	Sensor	센서 reboot / poweroff 명령을 통해서 종료하는 경우 차단 노드에 대해서 차단해제되도록 개선	
120379	GN-26462	WebUI	관리UI 로그인 화면에서 고객정보가 노출되지 않도록 개선	
120379	GN-26381	WebUI	사용자관리 목록에 조직명(USER_COMPANY) 컬럼 추가	

continues on next page

Table 1 - continued from previous page

Revision	Key	Components	Description	Affects Versions
120379	GN-26359	Windows Agent	윈도우의 'Wi-Fi 임의 하드웨어 주소 옵션'을 사용하지 않도록 강제화하는 기능 추가	
120379	GN-26329	Windows Agent	화면보호기 제어시 Windows 로그인 화면 표시 설정을 강제로 해제할 수 있는 기능 추가	
120379	GN-26321	WebUI	장치그룹화면의 OS 종류 콤보박스가 빈값으로 출력되는 문제	
120379	GN-26192	WebUI	SAML Service Provider Metadata 생성 기능	
120379	GN-26186	Center	event key 불일치로 인한 감사로그 타입이 맞지 않는 부분 개선	5.0.33
120379	GN-26183	WebUI	IP신청시스템의 IP신청시 사용종료일이 당일로 기본 출력되지 않도록 수정	
120379	GN-26171	CWP	CWP 공지사항에 관리자의 아이디가 노출되지 않도록 개선	
120379	GN-26167	Authsync	SCRAM-SHA-256 인증방식 지원을 위한 postgresql 패키지 업그레이드	
120379	GN-26123	WebUI	사용자 계정신청 후 전송된 메일의 DateTime 값에 밀리세컨드 값이 출력되는 부분 개선	
120379	GN-26105	WebUI	노드관리 동작상태차트의 너비(width)의 개선	
120379	GN-26043	Sensor	SNMP Agent 구동시 인증 및 암호화 알고리즘 선택가능하도록 개선	
120379	GN-26037	WebUI	사용자신청서 상세페이지에서 승인/거부처리시 사유입력 팝업창이 나타나도록 개선	
120379	GN-26031	Center, Database	Agent에 의해 수집된 시스템정보(마더보드)를 이용한 노드그룹 조건 추가	
120379	GN-25993	Center	GPDB/NMDB 업데이트 이전 버전 원복 기능	
120379	GN-25959	Center	자동반납 시 감사로그를 남기도록 개선	
120379	GN-25940	Linux Agent	Linux Agent, Offline 설치 패키지 제작 툴 개발	
120379	GN-25921	Linux Agent	Linux Agent, Log 정리 기능 추가	
120379	GN-25540	GenianOS	CA 인증서 유효기간 10년으로 변경	
120379	GN-23316	Center	정책서버 이미지에 센서/에이전트 포함하여 업그레이드 간편화	
120379	GN-22197	Center	OAuth 2.0 ROPC 인증연동 가능하도록 기능 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
125372	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)
125299	GN-27972		SSL 인증서의 유효기간이 10년으로 생성되는 문제	6.0.15, 5.0.55 (LTS)
125279	GN-28003	Windows Agent	파일배포 플러그인 V2에서 배포파일 검증방법이 Sigstore Keyless Signing일 경우 실패하는 문제	5.0.42 (LTS), 4.0.155, 6.0.15, 5.0.56 (50 LTS)
125176	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
125164	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)
124337	GN-27442	WebUI	노드관리 목록화면에서 마지막 동작시각 컬럼의 정렬이 동작하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
124088	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
123749	GN-27550	WebUI	트리구조의 데이터 컴포넌트가 출력되지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS), 6.0.17, 5.0.57
123440	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
123232	GN-27399	macOS Agent	macOS 내부/외부 상태에 맞지 않게 플러그인이 동작하는 문제	6.0.5, 5.0.48

continues on next page

Table 2 - continued from previous page

Revision	Key	Components	Description	Affects Versions
123154	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)
123138	GN-27496	Linux Agent	Linux Agent, 간헐적으로 액션 시스템 정보 전송이 일부 누락되는 문제	5.0.50, 6.0.15
123126	GN-27401	Sensor	센서장비에서 동일한 이벤트를 받는 경우 센서프로세스가 비정상 종료 되는 문제	4.0.64
123060	GN-24708	Center	많은 센서 디버그를 센터로 전송하는 환경에서 센터 재부팅시 오래된 디버그 삭제 동작으로 부하가 발생할 수 있는 문제	5.0.0
123051	GN-27575	Center	ES 로그필터쿼리 결과가 2K보다 크면 로그필터액션이 동작하지 않는 문제	4.1.M6
122951	GN-27574	Center	ES로그 정리주기에 로그필터를 위한ES인덱스(nac-filter)가 삭제되는 문제	5.0.50, 6.0.11
122853	GN-27480	WebUI	노드그룹 조건 중 부서선택 타입의 조건을 검색할 수 없는 문제	5.0.31, 6.0.0
122843	GN-27561	Center	[범용OS] LDAP 설정파일이 범용OS 에서 잘못된 파일에 설정되는 문제로 ldapsearch 명령 결과가 실패하는 문제	5.0.42 (LTS)
122592	GN-27502	Center	Keepalive 에 의한 에이전트/센서 다운 체크과정이 오래 걸리는 경우 에이전트 로그온 API 처리가 지연되는 문제	5.0.42 (LTS)
122508	GN-27504	Center	KeepAlive 수신 시 NodeID 관련 DB 오류 (Illegal mix of collations) 감사로그 발생되지 않도록 개선	
122458	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)
122447	GN-26487	WebUI	CVE 상세화면에서 값이 없을 경우 에러페이지 출력되는 문제 수정	5.0.24
122429	GN-27510	Center, Sensor	[범용OS] NAC패키지 업그레이드 후 추가된 라이브러리를 찾지 못하는 문제	5.0.42 (LTS)
122379	GN-27404	Center, macOS Agent	macOS 업데이트 플러그인의 설치모드 사용시 정상적으로 설치되지 않는 문제	5.0.11
122306	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

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122259	GN-27437	Center, macOS Agent	macOS Sonoma 단말의 OS 정보가 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
122118	GN-27384	Windows Agent	윈도우 방화벽 제어 플러그인의 프로그램 경로 설정 오류 수정	5.0.45
122086	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)
122074	GN-27385	GenianOS	iptables 명령이 동시 실행시 실패될 수 있는 문제 개선	5.0.0, 6.0.0
121882	GN-27398	Linux Agent	Linux Agent, 조건만 검사 액션 수행 결과가 변경되어도 업데이트 안되는 문제	5.0.50, 6.0.15
121837	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
121755	GN-27387	WebUI	OpenPort 현황 화면에서 내보내기 기능 동작하지 않는 문제	5.0.6
121710	GN-27380	Windows Agent	액션검사조건에 에이전트가 지원하는 매크로 이외에 '%' 문자가 존재하면 비정상 종료되는 문제	5.0.0, 6.0.0
121624	GN-26858	WebUI	5.0 버전 2단계 인증으로 구글 OTP 사용 시 인증코드에 숫자 외의 문자가 포함될 경우 오류 발생하는 문제	5.0.50, 5.0.53
121587	GN-27393	WebUI	IP,MAC 추가필드 사용자선택기에서 설정된 맵핑 키펀키가 동작하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
121530	GN-27270	macOS Agent	macOS AD 대체인증시 허용 도메인명에 .com 생략시 인증되지 않는 문제	4.0.108, 5.0.5

continues on next page

Table 2 - continued from previous page

Revision	Key	Components	Description	Affects Versions
121510	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
121466	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
121457	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)
121411	GN-27209	WebUI	IP 신청 승인 완료 및 요청 Email 알림이 가지 않는 문제	5.0.46, 6.0.4
121399	GN-27388	Center	[범용OS] webssh 접속 안되는 문제	5.0.42 (LTS)
121376	GN-27203	Windows Agent	불특정하게 액션수행결과가 변경되어도 일정시간(5분) 후에 전송하는 문제	5.0.0, 6.0.0
121202	GN-27322	Center, Sensor	[범용OS] 시스템관리 > 환경설정 > 타임존 설정이 우분투 NAC 에서 동작 안하는 문제	5.0.50
121183	GN-27259	Linux Agent	Linux Agent, 특정 패키지로 에이전트 설치시 동작하지 않는 문제	5.0.45, 6.0.2
121169	GN-27356	Sensor	패치 Proxy 서비스설정 on 설정임에도 cache 서비스가 구동되지 않는 문제	5.0.55 (LTS), 4.0.157
121136	GN-27359	gnlogin, VR-RPD	이벤트재전송처리가 필요없는 프로세스에서도 이벤트큐 처리가 동작하여 Same event already exist in queue 디버그 로그가 발생하는 문제	5.0.42 (LTS)
121022	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)
120745	GN-27290	WebUI	센서명에 '%' 가 포함되는 경우 센서트리가 정상적으로 표시되지 않는 문제	5.0.43, 6.0.0
120643	GN-27292	WebUI	노드상세에서 정책 설정 시 IP/MAC 목록을 선택하여도 선택항목이 입력되지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)

continues on next page

Table 2 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120608	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)
120540	GN-27091	Center, procmond	센서에서 보내는 이벤트로그(procmond 프로세스)가 정책 서버에서 unknown center did 에러 발생하면서 로그 저장 안되는 문제	5.0.42 (LTS)
120525	GN-27113	Center	Slave 장비에서 전송되는 업데이트 정보(sysinfo)를 unknown devid 로 업데이트 실패하는 문제	4.0.145, 5.0.42 (LTS), 6.0.1
120511	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
120501	GN-27177	Backup	백업 파일에 에이전트 zip 파일이 포함되어 용량이 증가하는 문제	6.0.16 (LTS), 5.0.55 (LTS)
120443	GN-27224	Windows Agent	에이전트 인증창으로 화면이 잠겨있는 상태에서 입력대화상자 출력 안됨	5.0.49, 6.0.7
120431	GN-27153	WebUI	관리자 노드관리범위 제한을 센서그룹으로 설정하고 노드 등록 시 관리센서 선택할 수 없는 문제	5.0.31
120424	GN-27191	WebUI	감사로그 화면에서 브라우저가 멈추는 문제	5.0.54, 6.0.15
120379	GN-27237	Center, Sensor	관리콘솔에서 센서에 등록된 에이전트노드삭제시 센서에 의해서 노드가 즉시 재등록 안되는 문제	5.0.42 (LTS)
120379	GN-27215	WebUI	5.0버전에서 관리 > 스위치 > 그룹 클릭 시 오류 페이지 출력 문제	5.0.42 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120379	GN-27187	CLOUD	신규 Cloud 정책서버에서 agent 정보가 정상적으로 표시되지 않는 문제	5.0.45, 6.0.2
120379	GN-27183	Center, Sensor	정책서버에서 센서로 전송하는 재등록이벤트(REGISTER_REQ)가 센서에서 처리되지 않는 문제	5.0.42 (LTS)
120379	GN-27176	macOS Agent	macOS 업데이트 플러그인이 비정상 동작하는 문제	5.0.11
120379	GN-27162	Sensor	[범용OS] 장비 부팅후 gdcid 데몬이 구동되지 않는 문제	5.0.42 (LTS)

continues on next page

Table 2 - continued from previous page

Revision	Key	Components	Description	Affects Versions
120379	GN-27158	WebUI	사용자 설정목록 타입의 IP 추가필드 변경 시 노드정보 업데이트 할 수 없는 오류	6.0.16 (LTS), 5.0.55 (LTS)
120379	GN-27154	WebUI	스위치 관리에서 스위치를 삭제하였으나 노드 목록에서 접속장치 컬럼의 링크가 동작하는 문제	5.0.38
120379	GN-27152	WebUI	동일 아이피의 여러 노드가 있을 경우 잘못된 노드가 매트릭스 뷰에 출력되는 문제	4.0.8
120379	GN-27151	geniup	마이그레이션 도중 명령어가 종료되어 마이그레이션이 정상 수행되지 않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120379	GN-27137	macOS Agent	macOS 메시지 팝업 내용이 보이지 않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 6.0.14
120379	GN-27136	macOS Agent	macOS USB 차단 동작하지 않는 문제	5.0.50, 6.0.9
120379	GN-27132	gnlogin	mysql 패스워드에 % 문자열 존재시 센터 비정상 동작하는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120379	GN-27127	Windows Agent	윈도우즈 업데이트 플러그인을 통한 Offline PMS 수행 실패	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120379	GN-27106	Center	노드정책 즉시적용 시 일부 노드만 적용되는 문제	5.0.42 (LTS), 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
120379	GN-27089	macOS Agent	macOS Agent 관리콘솔에 의한 무결성 체크 명령시 Gn-Daemon 재기동 되는 문제	5.0.42 (LTS), 5.0.54, 6.0.15, 5.0.56 (50 LTS)
120379	GN-27085	WebUI	SAML로 관리콘솔 로그인시 기존접속을 끊고 접속함(강제로 로그인) 기능이 동작하지 않는 문제	5.0.48, 6.0.6
120379	GN-27084	WebUI	XSS 검사로직에서 URLEncode 처리된 파라미터에 대한 오답으로 인해 감사로고가 남는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120379	GN-27074	WebUI	5.0.55 버전에서 피방문자 이메일 승인 대상이 관리자임에도 일반 사용자가 검색되는 문제	5.0.55 (LTS)
120379	GN-27066	Windows Agent	파일배포V2에서 스크립트 수행시 CMD창 표시 오류 수정	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120379	GN-27058	Windows Agent	PC 재시작시 내/외부 상태에 따라 수행 설정한 액션이 오 동작하는 문제	5.0.43, 6.0.0
120379	GN-27053	WebUI	노드속성 가져오기 기능에서 AUTHUSER (인증사용자) 킬럼을 사용할 수 없는 문제	5.0.30
120379	GN-27047	WebUI	툰갯 구동시 Elastic 관련 초기화 중 오류가 발생하여 Elastic Percolate가 초기화 되지 않는 문제	5.0.53, 6.0.14
120379	GN-27037	MGMT	[범용 OS] 관리콘솔 포트와 HTTPS 포트를 동일하게 설정하는 경우 apache 구동 안되는 문제	5.0.42 (LTS)
120379	GN-27016	Sensor	localconf의 서비스포트가 센서데몬에 의해서 불특정 값으로 변경되는 문제	NoVersion
120379	GN-27000	WebUI	노드관리목록 > 인증사용자 킬럼의 링크로 사용자 상세 화면 이동 시 유효하지 않은 파라미터 메시지 출력되는 문제	6.0.5, 5.0.50
120379	GN-26973	macOS Agent	macOS 사용자 알림메시지 주기적 수행시 팝업 되지 않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 6.0.14

continues on next page

Table 2 - continued from previous page

Revision	Key	Components	Description	Affects Versions
120379	GN-26972	Center	SLAVE 장비가 존재하는 경우 'BadQuery=Illegal mix of col-lations' 오류가 발생하는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120379	GN-26970	Center	Push Notification 이벤트처리 개선버전 에이전트임에도 정책서버에서 과거 이벤트처리방식으로 이벤트처리하는 문제	5.0.42 (LTS), 4.0.155
120379	GN-26969	WebUI	Get Parameter(QueryString) 관련 XSS 오탐 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
120379	GN-26957	macOS Agent	macOS 플러그인 적용 범위와 무관하게 액션 즉시수행시 액션이 수행되는 문제	6.0.5, 5.0.48
120379	GN-26956	WebUI	인증연동 설정 수정시 Exception 오류 메시지가 출력되는 문제	6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120379	GN-26938	Linux Agent	Linux Agent, 로컬 네트워크 변경 감지 오류로 신규 노드 등록이 되지 않는 문제	5.0.51, 6.0.11
120379	GN-26931	Center	마더보드 정보(updateinfo)가 삭제되지 않는 문제	5.0.52, 6.0.13
120379	GN-26930	Center	알람 전송 실패 메시지 사용안함 설정 시 검색필터 관련 기능이 동작하지 않는 문제	5.0.39
120379	GN-26901	Sensor	[AXGATERALINK] 잘못된 엔디안으로 빌드하여 정책업데이트가 되지 않은 문제	6.0.5, 5.0.48
120379	GN-26895	macOS Agent	macOS Mac mini M2 모델에서 소프트웨어 정보수집을 하지 못하는 현상	5.0.11
120379	GN-26887	WebUI	센서모드 전환시 노드목록의 제어정책 컬럼의 툴팁이 갱신되지 않는 문제	5.0.50, 6.0.11
120379	GN-26870	WebUI	EDR 에서 NAC 연동을 통한 대응 정책 설정시 NAC 노드에 태그가 할당되지 않는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
120379	GN-26785	Center	장치제어 정책 사용 시, 다른 노드 그룹의 장치제어 정책을 수신할 수 있는 문제	5.0.23
120379	GN-26687	WebUI	노드관리 마지막동작시각 컬럼의 시각이 관리자의 타임존이 적용되지 않고 출력되는 문제	4.1.M4
120379	GN-26643	Windows Agent	에이전트 자체인증창 액션정책을 제거해도 이전에 표시된 인증창이 계속 표시되는 문제	5.0.0, 6.0.0
120379	GN-26606	macOS Agent	macOS 인증창에서 엔터키 1회 입력시 로그인 수행되지 않는 문제	5.0.15

continues on next page

Table 2 - continued from previous page

Revision	Key	Components	Description	Affects Versions
120379	GN-26566	WebUI	노드 정보 업데이트 후, 탭 이동 시 변경한 정보가 갱신되어 보여지지 않는 문제	5.0.50
120379	GN-26551	macOS Agent	macOS 에이전트 다수의 액션 수행 조건 검사 시 마지막 조건의 결과만 표시됨	5.0.21, 6.0.0
120379	GN-26497	Windows Agent	무선연결관리자에서 무선프로파일(EAP-TTLS)의 서버 인증서 검증을 끄면 연결안됨	5.0.49, 6.0.7
120379	GN-26467	Windows Agent	비밀번호유효성검사 액션으로 검증 이후에도 간헐적으로 미검증 사유로 팝업창이 출력됨.	5.0.6, 6.0.0
120379	GN-26448	WebUI	Compose 방식 설치후 시스템 목록에서 정책서버 정보가 출력되지 않는 오류	5.0.6
120379	GN-26444	WebUI	노드그룹 조건의 소프트웨어 설정 창에서 한글검색이 안되는 증상	5.0.35
120379	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)
120379	GN-26335	Windows Agent	PC 원격 접속시 에이전트 트레이 아이콘 미표시 문제	5.0.0, 6.0.0
120379	GN-26317	WebUI	방문자 용도의 용도 설정에서 사용자/신규신청 옵션에 동일 조건 추가시 오류 발생	4.0.11
120379	GN-26288	WebUI	사용자 정의 필드 수정후 목록 출력이 이상해지는 오류	4.0.11
120379	GN-26272	Center	SMTP 인증연동 - [계정@[도메인] ID 형식인 경우 사용자 인증 비정상 문제	5.0.53
120379	GN-26250	Linux Agent	Linux Agent, 일부 Network interface 정보 수집이 누락되는 문제	5.0.51, 6.0.12
120379	GN-26204	Center	정책서버 설치시에 "File read failed. ERRMSG=Is a directory" 디버그가 발생하는 문제	5.0.42 (LTS), 4.0.152
120379	GN-26194	Sensor	http / https 포트 설정변경시 중복으로 IPTABLES가 생성되는 문제	4.0.17
120379	GN-26181	Linux Agent	Linux Agent, 이미 로그인된 사용자로 전환시 트레이 아이콘 표시 안되는 문제	5.0.41, 6.0.0
120379	GN-26097	WebUI	노드관리 엑셀 Export 시 진행되지 않는 문제	4.0.2
120379	GN-26027	Center	미사용 IP에 대해 변경금지를 설정한 노드등록시 IPM 아이콘이 출력되지 않는 문제	4.0.8
120379	GN-26026	Sensor	센서장비 구동시 센터와 시간차이로 인해서 스케줄러가 비정상 동작하면서 센서가 다운상태로 표시되는 문제	5.0.50
120379	GN-26023	Center	custom 인증서 만료로그가 정상적으로 남지 않는 문제	5.0.0
120379	GN-25970	CLI/gnlogin	[범용 OS] CLI 콘솔 접속 IP 미설정 시 SSH 접근이 허용되는 문제	5.0.42 (LTS), 6.0.0
120379	GN-25831	WebUI	용도 관리의 필드 할당 추가/제거 시 입력타입이 변경되는 문제	4.0.11
120379	GN-25148	WebUI	WebUI 스마트도움말 설정이 표기되지 않는 오류	5.0.49, 6.0.7

16.2.3 Genian NAC 5.0.56 (50 LTS) Release Notes (2023-07-21)

Last Updated: 2024-04-04

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
125401	GN-27107	WebUI	권한 없는 관리자로 인한 Tomcat 재구동 명령 수행으로 서비스 무력화	5.0.41	2.7
125327	GN-27242	WebUI	NAC 5.0에서 사용자 검색 화면을 통해서 sql injection이 가능한 취약점	5.0.15	4.8
123777	GN-26393	WebUI	접근 권한 없는 페이지에 직접 URL을 입력하여 정보 수정이 가능한 취약점		3.1
123255	GN-26390	WebUI	감사로그 REST API를 통한 권한 없는 관리자의 파일 내보내기 권한 우회 취약점		3.1
122615	GN-27492	WebUI	Tomcat Version Upgrade (8.5.94 -> 8.5.96 / 9.0.81 -> 9.0.83)		7.5
121388	GN-26315	WebUI	2단계 인증에서 인증코드 입력값 횟수제한, 시간제한하도록 개선		4.3
120865	GN-27278	WebUI	Tomcat Version Upgrade (8.5.94 / 9.0.81)		7.5
120392	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
120315	GN-26383	WebUI	html/script 코드 주입 가능한 취약점		5.3
118279	GN-26935	WebUI	부서명으로 출력된 html tag가 tree에서 실행되는 취약점	5.0.0	1.2
117609	GN-26865	WebUI	대시보드 위젯 설정에서 XSS 입력 취약점		1.2
117494	GN-26835	Center	데이터 업데이트에 사용되는 SQL을 통한 Command Injection 취약점		6.6
117494	GN-26833	Sensor	센서의 NMDB 업데이트 과정에서 nmap 스크립트 변조 취약점		4.1
117494	GN-26814	Center	Bufferoverflow 에 대한 코드 개선		2
117494	GN-26725	Linux Agent, macOS Agent, Windows Agent	[Agent] 센터 및 센서에서 전송된 이벤트에 대한 유효성 검사 추가		6.3
117494	GN-26696	Sensor	센서의 수신 이벤트에 대한 검증 미흡		6.3
117494	GN-26694	Center	다운로드 URL 검증 미흡으로 인한 Parameter Injection 취약점		6.6

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
125152	GN-27973	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 3.0.13, 1.1.1w 업데이트 - X.509 정책 제약 조건을 확인하는 과정에서 과도한 리소스 사용	4.0.0, 5.0.0, 6.0.0
123468	GN-27625	Sensor	센서 운영모드 및 정책변경시 public ip를 가져오지 못할 경우 반영되지 않는 문제 개선	
122690	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
122239	GN-27164	VRRPD	[범용OS] 이중화 구성 master 상태로 전환 후 인터페이스 상태검사 실패로 인해 slave 상태로 전환되는 문제	5.0.42 (LTS)
122179	GN-27390	Center, WebUI	리포트 보존개수 설정 시 /disk/data/report 디렉토리의 데이터도 삭제하도록 개선	
121928	GN-27241	macOS Agent	macOS 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121891	GN-27248	Linux Agent	Linux Agent, 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121118	GN-27269	- Unknown/None	apache / tomcat 관련 디렉토리 및 파일의 불필요한 권한 제거	
120559	GN-26325	GNOS	httpd 구동 스크립트 실행 시 procmond에 의해 중복 실행되는 문제 개선	
120406	GN-27146	Center	extauth 를 통한 외부인증연동 실패시 사용자가 입력한 패스워드가 센터디버그파일에 남는 문제	
120181	GN-27207	Windows Agent	다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
120024	GN-27206	Center, Sensor	센터에서 신뢰할 수 있는 nodeid 를 센서와 에이전트로 내려보내는 기능 추가	
119951	GN-27013	WebUI	markdown으로 설정된 항목을 변환할 수 있도록 개선	
119815	GN-27121	Center, macOS Agent	macOS 에이전트 신규 OS 14.0 (Sonoma) 지원	
119720	GN-27142	Windows Agent	알약 신규버전에 대응하는 연동 모듈 변경	
119668	GN-27031	Center, Sensor	[범용OS] Ubuntu OverlayFS 모듈에서 발생하는 로컬 권한 상승 취약점	
119034	GN-27038	WebUI	openssh 버전업 이후 webssh 접속되지 않는 문제 개선	
118995	GN-26987	Linux Agent	Linux Agent, 파일 배포 플러그인 V2 사용시 승인창 표시되지 않도록 기능개선	
118571	GN-26988	macOS Agent	macOS 파일 배포 플러그인 V2 사용시 승인창 표시되지 않도록 기능개선	
118336	GN-27010	GenianOS	GNOS OpenSSH버전 업데이트 (8.6p1->9.3p2)	
118212	GN-26981	Center, Linux Agent, macOS Agent, WebUI	배포 플러그인 V2 사용시 승인창 표시되지 않도록 기능개선	561

Issues Fixed

Revision	Key	Components	Description	Affects Versions
125373	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)
125298	GN-27972		SSL 인증서의 유효기간이 10년으로 생성되는 문제	6.0.15, 5.0.55 (LTS)
125280	GN-28003	Windows Agent	파일배포 플러그인 V2에서 배포파일 검증방법이 Sigstore Keyless Signing일 경우 실패하는 문제	5.0.42 (LTS), 4.0.155, 6.0.15, 5.0.56 (50 LTS)
125175	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
125163	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)
124087	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
123441	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
123288	GN-27517	WebUI	Nodes REST API 에서 특정 항목이 수정되지 않는 오류	5.0.8, 4.0.111
123237	GN-27399	macOS Agent	macOS 내부/외부 상태에 맞지 않게 플러그인이 동작하는 문제	6.0.5, 5.0.48
123151	GN-27460	GenianOS	[범용 OS] 초기동작시 aes256 명령이 실행되지 않는 문제	5.0.42 (LTS), 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
123137	GN-27496	Linux Agent	Linux Agent, 간헐적으로 액션 시스템 정보 전송이 일부 누락되는 문제	5.0.50, 6.0.15
123127	GN-27401	Sensor	센서장비에서 동일한 이벤트를 받는 경우 센서프로세스가 비정상 종료 되는 문제	4.0.64

continues on next page

Table 3 - continued from previous page

Revision	Key	Components	Description	Affects Versions
123061	GN-24708	Center	많은 센서 디버그를 센터로 전송하는 환경에서 센터 재부팅시 오래된 디버그 삭제 동작으로 부하가 발생할 수 있는 문제	5.0.0
123052	GN-27575	Center	ES 로그 필터 쿼리 결과가 2K보다 크면 로그 필터 액션이 동작하지 않는 문제	4.1.M6
122952	GN-27574	Center	ES 로그 정리주기에 로그 필터를 위한 ES 인덱스 (nac-filter) 가 삭제되는 문제	5.0.50, 6.0.11
122844	GN-27561	Center	[범용OS] LDAP 설정 파일이 범용OS 에서 잘못된 파일에 설정되는 문제로 ldapsearch 명령 결과가 실패하는 문제	5.0.42 (LTS)
122593	GN-27502	Center	Keepalive 에 의한 에이전트/센서 다운 체크 과정이 오래 걸리는 경우 에이전트 로그인 API 처리가 지연되는 문제	5.0.42 (LTS)
122507	GN-27504	Center	KeepAlive 수신 시 NodeID 관련 DB 오류 (Illegal mix of col- lations) 감사로그 발생되지 않도록 개선	
122457	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)
122446	GN-26487	WebUI	CVE 상세화면에서 값이 없을 경우 에러페이지 출력되는 문제 수정	5.0.24
122430	GN-27510	Center, Sen- sor	[범용OS] NAC패키지 업그레이드 후 추가된 라이브러리를 찾지 못하는 문제	5.0.42 (LTS)
122378	GN-27404	Center, ma- cOS Agent	macOS 업데이트 플러그인의 설치모드 사용시 정상적으로 설치되지 않는 문제	5.0.11
122333	GN-27467	WebUI	노드액션 설명에 XSS를 추가하면 정책 적용 팝업화면에서 XSS가 실행되는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
122260	GN-27437	Center, ma- cOS Agent	macOS Sonoma 단말의 OS 정보가 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
122117	GN-27384	Windows Agent	윈도우 방화벽 제어 플러그인의 프로그램 경로 설정 오류 수정	5.0.45

continues on next page

Table 3 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122085	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)
122073	GN-27385	GenianOS	iptables 명령이 동시 실행시 실패될 수 있는 문제 개선	5.0.0, 6.0.0
121881	GN-27398	Linux Agent	Linux Agent, 조건만 검사 액션 수행 결과가 변경되어도 업데이트 안되는 문제	5.0.50, 6.0.15
121838	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
121756	GN-27387	WebUI	OpenPort 현황 화면에서 내보내기 기능 동작하지 않는 문제	5.0.6
121709	GN-27380	Windows Agent	액션검사조건에 에이전트가 지원하는 매크로 이외에 '%' 문자가 존재하면 비정상 종료되는 문제	5.0.0, 6.0.0
121625	GN-26858	WebUI	5.0 버전 2단계 인증으로 구글 OTP 사용 시 인증코드에 숫자 외의 문자가 포함될 경우 오류 발생하는 문제	5.0.50, 5.0.53
121529	GN-27270	macOS Agent	macOS AD 대체인증시 허용 도메인명에 .com 생략시 인증되지 않는 문제	4.0.108, 5.0.5
121511	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
121465	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
121456	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)
121412	GN-27209	WebUI	IP 신청 승인 완료 및 요청 Email 알림이 가지 않는 문제	5.0.46, 6.0.4

continues on next page

Table 3 - continued from previous page

Revision	Key	Components	Description	Affects Versions
121401	GN-27388	Center	[범용OS] webssh 접속 안되는 문제	5.0.42 (LTS)
121377	GN-27203	Windows Agent	불특정하게 액션수행결과가 변경되어도 일정시간(5분) 후에 전송하는 문제	5.0.0, 6.0.0
121203	GN-27322	Center, Sensor	[범용OS] 시스템관리 > 환경설정 > 타임존 설정이 우분투 NAC 에서 동작 안하는 문제	5.0.50
121175	GN-27259	Linux Agent	Linux Agent, 특정 패키지로 에이전트 설치시 동작하지 않는 문제	5.0.45, 6.0.2
121170	GN-27356	Sensor	패치 Proxy 서비스설정 on 설정임에도 cache 서비스가 구동되지 않는 문제	5.0.55 (LTS), 4.0.157
121137	GN-27359	gnlogin, VR-RPD	이벤트재전송처리가 필요없는 프로세스에서도 이벤트큐 처리가 동작하여 Same event already exist in queue 디버그 로그가 발생하는 문제	5.0.42 (LTS)
121023	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)
120742	GN-27290	WebUI	센서명에 '%' 가 포함되는 경우 센서트리가 정상적으로 표시되지 않는 문제	5.0.43, 6.0.0
120638	GN-27265	WebUI	5.0.56(LTS) 버전에서 노드관리의 부서단계 표시가 advance 설정과 다르게 나타나는 문제	5.0.56 (50 LTS)
120609	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)
120539	GN-27091	Center, procmond	센서에서보내는 이벤트로그(procmond 프로세스)가 정책 서버에서 unknown center did 에러 발생하면서 로그 저장 안되는 문제	5.0.42 (LTS)
120524	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
120512	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

continues on next page

Table 3 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120502	GN-27177	Backup	백업 파일에 에이전트 zip 파일이 포함되어 용량이 증가하는 문제	6.0.16 (LTS), 5.0.55 (LTS)
120444	GN-27224	Windows Agent	에이전트 인증창으로 화면이 잠겨있는 상태에서 입력대화상자 출력 안됨	5.0.49, 6.0.7
120377	GN-27215	WebUI	5.0버전에서 관리 > 스위치 > 그룹 클릭 시 오류 페이지 출력 문제	5.0.42 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120147	GN-27237	Center, Sensor	관리콘솔에서 센서에 등록된 에이전트노드삭제시 센서에 의해서 노드가 즉시 재등록 안되는 문제	5.0.42 (LTS)
120134	GN-27176	macOS Agent	macOS 업데이트 플러그인이 비정상 동작하는 문제	5.0.11
120107	GN-26887	WebUI	센서모드 전환시 노드목록의 제어정책 컬럼의 툴팁이 갱신되지 않는 문제	5.0.50, 6.0.11
120005	GN-27154	WebUI	스위치 관리에서 스위치를 삭제하였으나 노드 목록에서 접속장치 컬럼의 링크가 동작하는 문제	5.0.38
119994	GN-27000	WebUI	노드관리목록 > 인증사용자 컬럼의 링크로 사용자 상세 화면 이동 시 유효하지 않은 파라미터 메시지 출력되는 문제	6.0.5, 5.0.50
119827	GN-27137	macOS Agent	macOS 메시지 팝업 내용이 보이지 않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 6.0.14
119805	GN-27058	Windows Agent	PC 재시작시 내/외부 상태에 따라 수행 설정한 액션이 오 동작하는 문제	5.0.43, 6.0.0
119735	GN-27183	Center, Sensor	정책서버에서 센서로 전송하는 재등록이벤트 (REGISTER_REQ)가 센서에서 처리되지 않는 문제	5.0.42 (LTS)
119542	GN-27162	Sensor	[범용OS] 장비 부팅후 gdcid 데몬이 구동되지 않는 문제	5.0.42 (LTS)
119518	GN-27151	geniup	마이그레이션 도중 명령어가 종료되어 마이그레이션이 정상수행되지 않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
119442	GN-27135	WebUI	업그레이드 이후 파일패포V2 항목 최초 수정시에 글로벌 설정으로 등록 안되는 오류	5.0.42 (LTS), 5.0.50, 4.0.156, 5.0.56 (50 LTS)

continues on next page

Table 3 – continued from previous page

Revision	Key	Components	Description	Affects Versions
119408	GN-27132	gnlogin	mysql 패스워드에 % 문자열 존재시 센터 비정상 동작하는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
119377	GN-27085	WebUI	SAML로 관리콘솔 로그인시 기존접속을 끊고 접속함(강제로 로그인) 기능이 동작하지 않는 문제	5.0.48, 6.0.6
119368	GN-27084	WebUI	XSS 검사로직에서 URLEncode 처리된 파라미터에 대한 오답으로 인해 감사로고가 남는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
119358	GN-27127	Windows Agent	윈도우즈 업데이트 플러그인을 통한 Offline PMS 수행 실패	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
119273	GN-26676	gnlogin	[범용 OS] gnlogin 명령시 감사기록에 ADMIN, ADMINIP 가 남지 않는 문제	5.0.23
119162	GN-27106	Center	노드정책 즉시적용 시 일부 노드만 적용되는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
119101	GN-27089	macOS Agent	macOS Agent 관리콘솔에 의한 무결성 체크 명령시 Gn-Daemon 재기동 되는 문제	5.0.42 (LTS), 5.0.54, 6.0.15, 5.0.56 (50 LTS)
119009	GN-26938	Linux Agent	Linux Agent, 로컬 네트워크 변경 감지 오류로 신규 노드 등록이 되지 않는 문제	5.0.51, 6.0.11
118937	GN-26972	Center	SLAVE 장비가 존재하는 경우 'BadQuery=Illegal mix of col-lations' 오류가 발생하는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15

continues on next page

Table 3 - continued from previous page

Revision	Key	Components	Description	Affects Versions
118842	GN-27037	MGMT	[범용OS] 관리콘솔 포트와 HTTPS 포트를 동일하게 설정하는 경우 apache 구동 안되는 문제	5.0.42 (LTS)
118785	GN-27066	Windows Agent	파일배포 V2에서 스크립트 수행시 CMD창 표시 오류 수정	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
118606	GN-26956	WebUI	인증연동 설정 수정시 Exception 오류 메시지가 출력되는 문제	6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
118603	GN-26870	WebUI	EDR 에서 NAC 연동을 통한 대응 정책 설정시 NAC 노드에 태그가 할당되지 않는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
118483	GN-26895	macOS Agent	macOS Mac mini M2 모델에서 소프트웨어 정보수집을 하지 못하는 현상	5.0.11
118452	GN-26957	macOS Agent	macOS 플러그인 적용 범위와 무관하게 액션 즉시수행시 액션이 수행되는 문제	6.0.5, 5.0.48
118392	GN-26973	macOS Agent	macOS 사용자 알림메시지 주기적 수행시 팝업 되지않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 6.0.14
118368	GN-27016	Sensor	localconf의 서비스포트가 센서데몬에 의해서 불특정 값으로 변경되는 문제	NoVersion
118285	GN-26785	Center	장치제어 정책 사용 시, 다른 노드 그룹의 장치제어 정책을 수신할 수 있는 문제	5.0.23
118226	GN-26969	WebUI	Get Parameter(QueryString) 관련 XSS 오탐 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
117923	GN-26970	Center	Push Notification 이벤트처리 개선버전 에이전트임에도 정책서버에서 과거 이벤트처리방식으로 이벤트처리하는 문제	5.0.42 (LTS), 4.0.155
117494	GN-24713	procmond	정책서버를 센서전용 이미지로 변경시 데몬구동 오류가 발생하는 문제	5.0.0

16.3 Previous Versions

16.3.1 Genian NAC 5.0.60 Release Notes (2024-03-04)

Last Updated: 2024-04-01

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
125402	GN-27107	WebUI	권한 없는 관리자로 인한 Tomcat 재구동 명령 수행으로 서비스 무력화	5.0.41	2.7
125325	GN-27242	WebUI	NAC 5.0에서 사용자 검색 화면을 통해서 sql injection이 가능한 취약점	5.0.15	4.8

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
125151	GN-27973	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 3.0.13, 1.1.1w 업데이트 - X.509 정책 제약 조건을 확인하는 과정에서 과도한 리소스 사용	4.0.0, 5.0.0, 6.0.0
124658	GN-27699	WebUI	WEBUI 2단계인증 인증코드 입력 시 마스킹 되어 표시되도록 개선	
124658	GN-27651	macOS Agent	macOS off-line 로그 (감사 기록) 전송 기능 개발	
124658	GN-27645	Center, Sensor	FTP/SFTP 백업시 서버연결timeout 시간을 설정할 수 있도록 개선	
124658	GN-27626	Center, procmond	프로세스검사데몬 (procmond) 에서 센터데몬 SOAP API HealthCheck 하도록 개선	
124658	GN-27620	Center, Sensor	파일 다운로드 수행 시 타임아웃 설정 가능하도록 개선	5.0.42 (LTS), 6.0.3
124658	GN-27537	VRRPD	Multicast 패킷운영이 불가능한 환경에서 VRRP Unicast mode 를 통해서 HA 가능하도록 개선	
124658	GN-27524	macOS Agent	macOS 에이전트 비정상종료 원인분석을 위한 디버깅 정보 저장	
124658	GN-27518	WebUI	관리콘솔 SAML 인증 연동시 JIT provisioning 기능 지원	
124658	GN-27372	WebUI	노드그룹 목록의 적용 노드 수 가져오는 구조 개선	
124658	GN-27065	Center	인증코드 검증 실패시 감사로그 추가 및 비밀번호 수정시 by 정보 추가	
124658	GN-26877	Center	노드그룹 조건에서 매크로를 사용할 수 있도록 추가	
124658	GN-26847	WebUI	CWP설정 > 확인버튼 URL의 설명 보강	
124658	GN-26595	WebUI	정책 수정 시 적용된 노드의 수량을 포함한 경고 메시지 출력	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
125371	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)
125351	GN-27968	WebUI	설정의 인증서 관리에서 인증서 관련 업로드시 저장 및 수정이 안되는 문제	6.0.19, 5.0.59
125297	GN-27957	procmond	[범용OS] 센서 장비에서 프로세스 검사 수행되지 않는 문제	5.0.60
125292	GN-27972		SSL 인증서의 유효기간이 10년으로 생성되는 문제	6.0.15, 5.0.55 (LTS)
125241	GN-27991	CLOUD	Cloud에서 NAC 5.0버전의 사이트를 삭제할 때 감사로그 미삭제 문제	5.0.42 (LTS)
125171	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
125161	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)
124899	GN-27932	Center	센터 업그레이드 또는 재부팅할 때 다량의 Keep Alive 디버그 로그로 인한 부하 문제 개선	6.0.19, 5.0.59
124883	GN-27904	MySQL	SSD 사용 장비에서 MySQL 8.0 구동 실패하는 문제	6.0.18, 5.0.58
124873	GN-27936	RADIUSD	Radius 데몬 업그레이드 이후 TLS 1.0 으로 유/무선 연결시 인증실패로 연결안되는 문제	6.0.19, 5.0.59
124658	GN-27989	Genian Syncer	지니안싱커로 GenianData를 동기화할 때 무결성 검증에 실패하는 문제	4.0.156, 6.0.16 (LTS), 5.0.55 (LTS)
124658	GN-27722	macOS Agent	macOS 장치 차단시 로그에 차단 정책ID가 잘못 표시되는 문제	6.0.3, 5.0.46
124658	GN-27709	Windows Agent	신규로 파악된 백신의 엔진 업데이트 수행시 '실시간검사'가 미동작으로 보고되는 문제	6.0.19, 5.0.59
124658	GN-27664	WebUI	IP관리센서 목록에서 한개의 센서에서만 DHCP Pool 사용현황이 출력되는 문제	5.0.42 (LTS)
124658	GN-27632	WebUI	로그인 한 관리콘솔 언어가 CWP 지원언어에 포함되어 있지 않은 경우 다국어입력기 출력 문제	5.0.31
124658	GN-27617	Windows Agent	운영체제 정보 수집 액션으로 AD서버에 빈암호 사용여부를 체크하여 AD계정이 잠기는 문제	4.0.109, 5.0.6, 6.0.0
124658	GN-27579	CWP	노드정책 > 비밀번호 사용 옵션을 off로 했을때 CWP 사용자 정보 확인 화면이 정상적으로 동작하지 않는 문제	4.0.M8
124658	GN-27576	WebUI	노드그룹 필터 설정 팝업영역이 화면을 벗어나는 오류	5.0.31, 6.0.0
124658	GN-27571	WebUI	노드부가 제한된 관리자로 새로운 노드부를 생성 후 사용시, 해당 부 항목이 증가되는 현상	5.0.42 (LTS)
124658	GN-27566	WebUI	에이전트 OS 아이콘이 잘못나오는 문제 수정	4.1.M5
124658	GN-	WebUI	CONF Update API 사용시 오류 발생하는 문제 수정	5.0.20
16.3. Previous Versions				571
124658	GN-27543	dbmigration	레지스트리 설정의 데이터 마이그레이션시 값이 잘못 변환되는 문제	6.0.5, 5.0.48
124658	GN-27522	WebUI	노드액션의 플러그인 변경 후 정책적용 시 변경된 플러그인의 이름으로 출력되지 않는 문제	5.0.45, 6.0.2

16.3.2 Genian NAC 5.0.59 Release Notes (2024-02-05)

Last Updated: 2024-02-29

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
124618	GN-27568	Windows Agent	유선 및 무선 연결관리자의 802.1x 인증 (GTC) 에서 TLSv1.3 지원	
123983	GN-27612	WebUI	멀티라인 텍스트 입력형식의 추가필드에 읽기전용 옵션 추가	
123983	GN-27602	WebUI	멀티라인 입력 추가필드 항목에 READONLY 옵션 설정 추가	
123983	GN-27473	Windows Agent	정책 재적용 할때마다 반복되는 액션 정책 로그 개선	
123983	GN-27456	WebUI	ipmgmt 신청결과에 승인 사유 컬럼 추가	
123983	GN-27455	Windows Agent	하우리 바이로봇 API 변경 (VrInfo.dll ver 2023.11.10.0)	
123983	GN-27447	Linux Agent	Linux Agent, 소프트웨어 정보수집에서 Snap을 통해 설치된 소프트웨어도 수집되도록 개선	
123983	GN-27357	WebUI	SAML idp의 IP-Port 출력형식에 대한 개선 및 관련 코드 정리	
123983	GN-27348	WebUI	오류 페이지 출력 개선	
123983	GN-27315	WebUI	대시보드 '센터/센서 장비상태 현황' 위젯 기능 개선	
123983	GN-27229	WebUI	임시사용자 IP 신청서 비밀번호 입력란에 필수입력 표시 추가	
123983	GN-27225	Windows Agent	하우리 Virobot Security 1.0 백신 정보 수집	
123983	GN-27214	WebUI	시스템 기본설정의 Timezone 기본값을 Browser Timezone으로 변경	
123983	GN-27212	WebUI	Cloud 환경에서 정책서버 Timezone 설정 가능하도록 개선	
123983	GN-27199	WebUI	IP/MAC 추가필드 빠른검색 조건에 추가	
123983	GN-27133	WebUI	대시보드 센서맵에 센서 상태에 따라 마커의 색상이 구분되도록 개선	
123983	GN-26667	WebUI	정책에 액션 일괄적용 기능 추가	
123983	GN-26539	WebUI	관리 상세 페이지 수정 버튼 위치 변경	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
124618	GN-27464	Windows Agent	Openssl3.0 적용된 무선연결관리자를 통해 GTC 인증실패 & 무선연결안됨 (임시조치)	6.0.19, 5.0.59
124318	GN-27648	WebUI	감사로그에 An error occurred when requesting the page. StatusCode=404, 403 Warning 로그가 남는 문제	6.0.19, 5.0.59
124086	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
124034	GN-27742	Center	Cloud NAC에서 메일전송 실패하는 문제	6.0.19, 5.0.59
123983	GN-27678	Windows Agent	모양 및 개인설정 플러그인에서 화면보호기 정보 수집안 되는 문제	5.0.59
123983	GN-27619	Center	GNOS 센터에 Ubuntu NAC 센서 소프트웨어 업로드 안되는 문제	5.0.42 (LTS)
123983	GN-27590	WebUI	노드그룹의 백신정보 관련 조건에 백신명을 직접입력할 수 없는 문제	6.0.6, 5.0.49
123983	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
123983	GN-27572	Backup	[범용OS] 백업 파일에 에이전트 zip 파일이 포함되어 용량이 증가하는 문제	5.0.31
123983	GN-27514	Center	노드정책의 인증방식 순서에 따라 일부 인증방식의 실패 로그가 남지 않는 문제	5.0.16
123983	GN-27508	Windows Agent	모양 및 개인설정 액션에 액션즉시적용 명령으로 설정되어있는 화면보호기 동작하지 않는 문제.	4.1.M8, 5.0.0, 6.0.0
123983	GN-27482	WebUI	무선랜 그룹 복사 시 오류 발생하는 문제	4.1.4
123983	GN-27458	Center	CLOUD 버전 에이전트 로그 수집되지 않는 문제	5.0.42 (LTS)
123983	GN-27443	Windows Agent	PC부팅시 백신 실시간 감시상태가 미동작으로 보고되는 문제	5.0.0, 6.0.0
123983	GN-27442	WebUI	노드관리 목록화면에서 마지막 동작시각 컬럼의 정렬이 동작하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
123983	GN-27429	Center	Openssl 3.0을 사용 할 때 라이선스정보를 읽어오지 못하는 문제	6.0.19
123983	GN-27420	WebUI	노드 관리범위 제한이 걸린 센서그룹에 센서를 추가하는 경우 해당 관리자의 트리에 즉시 반영되지 않는 문제	5.0.31
123983	GN-27413	WebUI	다국어 메시지 컴포넌트에서 국문항목만 수정시 타언어 설정값이 반영안되는 문제	4.1.M3, 4.0.17
123983	GN-27409	Sensor	AD 서버에 최신 업데이트 설치 시 Agentless AD SSO 기능이 동작하지 않는 문제	

continues on next page

Table 4 - continued from previous page

Revision	Key	Components	Description	Affects Versions
123983	GN-27405	WebUI	무선랜 정책복사 후 수정이 안되는 문제	4.0.8
123983	GN-27396	WebUI	노드목록 내보내기 시 마지막동작시각 컬럼의 내용이 잘 못출력되는 문제	6.0.16 (LTS), 5.0.55 (LTS)
123983	GN-27371	WebUI	적용범위가 없는 같은 단독 플러그인이 정책에 다중 할당 가능한 문제	5.0.43, 6.0.0
123983	GN-27308	Elastic-Search, Ubuntu(Debian)	[범용 OS] 로그서버가 싱글모드일 때, elasticsearch의 nac_nodegrptreesnapshot 인덱스의 복제본이 생기는 문제	
123983	GN-27285	WebUI	password 타입의 입력란이 상위 옵션과 관계없이 빈 값일 경우, 저장이 안되는 문제	6.0.17, 5.0.57
123983	GN-27247	WebUI	WMI 수집정보 위젯의 링크를 통해 노드 목록 이동 시 결과 출력되지 않는 문제	5.0.33
123983	GN-27238	WebUI	영문 ID/비밀번호 찾기 문구에 클라우드 버전 ID/비밀번호 찾기 문구가 무조건 출력되는 문제	5.0.31
123983	GN-27236	WebUI	CWP 세션 만료 페이지의 문구가 시스템 로케일로 출력되는 문제	5.0.14
123983	GN-27218	Database	운영체제 정보수집 액션에 의한 정책서버의 "Unknown CODEMAP" 디버그 발생	5.0.48, 6.0.6
123983	GN-27205	WebUI	관리콘솔 세션 타임아웃이 60분을 넘어가는 경우 남은 시간 표시 영역에 시간이 정상적으로 표시 되지 않는 문제	4.1.2
123983	GN-27173	Center	스위치 삭제 시 노드의 접속장치/접속포트 정보가 삭제되지 않는 문제	
123983	GN-27125	GenianOS	[범용 OS] 이미지 업그레이드 이후 서비스 구동되지 않도록 개선	
123983	GN-27120	WebUI	노드정책의 노드액션 할당에서 할당항목을 취소하게 되면 할당가능한 목록에 보이지 않는 문제	6.0.17, 5.0.57
123983	GN-27099	Sensor	글로벌 DHCP 환경으로 DHCP IP 할당 시 노드의 Active 상태를 확인하도록 개선	
123983	GN-27064	Windows Agent	안전모드 부팅 후 장치제어 플러그인 버전이 변경되면 이전 정책으로만 제어되는 문제	5.0.0, 6.0.0
123983	GN-26900	Sensor	사용 중인 IP를 DHCP IP로 할당하는 문제	4.0.149
123983	GN-26559	WebUI	사용자 등록 페이지의 기간 설정 처리 시 관리자의 타임존에 맞게 설정되도록 개선	4.1.M4
123983	GN-26253	WebUI	로그인 직후 플랫폼 상태별 카운트 위젯에서 이동시 현재 위치 경로에 null이 표시되는 문제	4.0.0
123136	GN-27496	Linux Agent	Linux Agent, 간헐적으로 액션 시스템 정보 전송이 일부 누락되는 문제	5.0.50, 6.0.15

16.3.3 Genian NAC 5.0.58 Release Notes (2023-12-19)

Last Updated: 2024-02-21

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
123776	GN-26393	WebUI	접근 권한 없는 페이지에 직접 URL을 입력하여 정보 수정이 가능한 취약점		3.1
123285	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
123467	GN-27625	Sensor	센서 운영모드 및 정책변경시 public ip를 가져오지 못할 경우 반영되지 않는 문제 개선	
122824	GN-27491	WebUI	SAML 인증 연동시 IdP-initiated SSO 인증 요청에 대해 인증 가능하도록 개선	
122715	GN-27476	WebUI	SAML 로그인시 기존 로그인 버튼과 구분하기 위해 구분선을 추가와, 다중 IdP 설정시 로그인 버튼 출력 개선	
122715	GN-27344	Center	Secondary Webhook 인증연동을 할 수 있도록 기능 개선	
122715	GN-27320	WebUI	외부 접근 허용 시 출력되는 알람에 대한 개선	
122715	GN-27243	Authsync	응답헤더에 포함된 페이징파라미터를 이용할 수 있도록 REST API Server 타입 정보동기화 개선	
122715	GN-27201	WebUI	노드 속성 변경에 IP / MAC 추가필드 항목 추가	
122715	GN-27077	Sensor	이벤트소켓 생성시 event socket not configured 로그 발생에 대한 예외처리 개선	
122715	GN-27068	WebUI	노드그룹 조건필터 목록을 탐색 할 수 있도록 개선	
122715	GN-26955	- Unknown/None	ES 계정 변경 시 sysinspect 스크립트가 변경된 ES 계정으로 동작하도록 개선	
122715	GN-26942	WebUI	장비 수정 API 호출 시 오류 로그 남는 문제 개선	
122715	GN-26929	Database	'USB 정보' 추가/삭제 감사로그에 장치정보 추가	
122715	GN-26921	Windows Agent	에이전트를 통한 외부인증연동 플러그인 개발	
122715	GN-26913	Windows Agent	엑소스피어 백신 정보 수집	
122715	GN-26907	Center	검색필터 Webhook 설정 시 복수의 URL 설정이 가능하도록 개선	
122715	GN-26873	WebUI	Top 메뉴의 빠른검색에서 (IP/장비)소유자, 소유부서 검색이 되도록 개선	
122715	GN-26855	MySQL	[범용OS] mysql 비밀번호 재사용 방지하도록 개선	
122715	GN-26842	Center	CLOUD GPDB 갱신시 mysqldump 수행오류	
122715	GN-26575	IPMGMT	ipmgmt 페이지 기능 사용하지 않을 시 접근 불가 설정	
122715	GN-26545	GenianOS	GNOS 커널 버전 업그레이드 (5.15.0)	
122715	GN-26482	Authsync, Database	부서코드 저장 시, 사이즈 초과를 방지하기 위해 해시 함수로 압축	5.0.45, 6.0.2
122715	GN-26325	GNOS	httpd 구동 스크립트 실행 시 procmound에 의해 중복 실행되는 문제 개선	
122715	GN-26284	Center	제품내 self-sign 인증서 자동 갱신 기능	
122715	GN-25533	Center	Proxy 서비스설정시 cache 삭제 옵션 추가	
122715	GN-25333	RADIUSD	RADIUS EAP-TTLS 지원 (MSCHAPv2, PAP)	
576	25333			Chapter 16. Release Notes
122715	GN-22567	Database	GNOS MySQL 8.0 업그레이드	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
123770	GN-27674	MySQL	SSD가 있는 장비에서 mysql 8.0 버전 이미지로 업그레이드 후 데몬이 실행되지 못하는 문제	6.0.18, 5.0.58
123747	GN-27550	WebUI	트리구조의 데이터 컴포넌트가 출력되지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS), 6.0.17, 5.0.57
123498	GN-27646	Authsync	정보동기화의 사용자 부서ID 컬럼명에 MySQL 함수 사용하는 경우, 부서 동기화 실패하여 잘못된 정책이 할당될 수 있는 문제	6.0.18, 5.0.58
123419	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
123341	GN-27399	macOS Agent	macOS 내부/외부 상태에 맞지 않게 플러그인이 동작하는 문제	6.0.5, 5.0.48
123302	GN-27573	WebUI	사용자그룹별 현황에서 각 그룹 인원수 클릭시 목록이 출력되지 않는 문제	4.0.156, 6.0.16 (LTS), 5.0.57
123294	GN-27401	Sensor	센서장비에서 동일한 이벤트를 받는 경우 센서프로세스가 비정상 종료 되는 문제	4.0.64
123287	GN-27517	WebUI	Nodes REST API 에서 특정 항목이 수정되지 않는 오류	5.0.8, 4.0.111
123267	GN-27460	GenianOS	[범용 OS] 초기동작시 aes256 명령이 실행되지 않는 문제	5.0.42 (LTS), 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
123169	GN-27519	Sensor	지속적으로 센서모드 변경시 데드락이 발생하여 센서 시스템이 멈추는 증상	5.0.57, 4.0.157, 6.0.19
123136	GN-27496	Linux Agent	Linux Agent, 간헐적으로 액션 시스템 정보 전송이 일부 누락되는 문제	5.0.50, 6.0.15
123059	GN-24708	Center	많은 센서 디버그를 센터로 전송하는 환경에서 센터 재부팅시 오래된 디버그 삭제 동작으로 부하가 발생할 수 있는 문제	5.0.0
123050	GN-27575	Center	ES 로그필터쿼리 결과가 2K보다 크면 로그필터액션이 동작하지 않는 문제	4.1.M6
122950	GN-27574	Center	ES로그 정리주기에 로그필터를 위한 ES인덱스(nac-filter)가 삭제되는 문제	5.0.50, 6.0.11
122842	GN-27561	Center	[범용 OS] LDAP 설정파일이 범용 OS 에서 잘못된 파일에 설정되는 문제로 ldapsearch 명령 결과가 실패하는 문제	5.0.42 (LTS)
122715	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 5 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122715	GN-27397	WebUI	operator 계정으로 RADIUS 정책 생성 수정 못하는 오류	5.0.30
122715	GN-27389	Center, CLOUD	CLOUD 정책서버 업그레이드 시 범용 OS 센서 자동 업그레이드 수행되지 않는 문제	
122715	GN-27368	WebUI	관리범위에 따른 관리자별 일일리포트 생성시 집계가 잘 못된 문제	6.0.17, 5.0.57
122715	GN-27321	WebUI	노드/제어 정책 수정되지 않는 문제	4.0.157, 6.0.18, 5.0.58
122715	GN-27148	WebUI	2차인증 사용하여 관리콘솔 로그인 시 로그인 성공 후 로그인 실패 카운트 초기화 되지 않는 문제	4.0.10
122715	GN-27119	Windows Agent	에이전트인증창 URL 버튼에서 정의된 이름값 출력이 모두 출력되지 않는 문제	5.0.42 (LTS), 6.0.0
122715	GN-27111	Authsync	직급동기화 시 로컬DB에 직급정보가 없을 때 직급동기화가 실패하는 문제	6.0.6, 5.0.49
122715	GN-27110	WebUI	CWP 사용자 등록 신청결과조회 화면에서 사용자 정보 수정 후 다시 신청결과조회 화면 접근시 인증이 안되는 문제	5.0.32
122715	GN-27059	WebUI	태그명을 공백(Space)으로 입력이 가능한 문제	4.0.M7
122715	GN-27057	procmond	tomcat 재시작시 tomcat9 버전이 아님에도 감사기록에 tomcat9 라고 남는 문제	5.0.53, 6.0.15
122715	GN-27048	WebUI	로그인화면 3줄 이상 입력 시, 레이어 새로 영역 겹치는 문제	6.0.8
122715	GN-27040	Center	에이전트에서 수집된 '알수없음', '정보없음' 날짜 정보가 '1970-01-01'로 표시되는 문제	
122715	GN-27017	Elastic-Search, gnlogin	로그서버 구동 전 로그서버 인증 정보 변경 시 감사로그 저장되지 않는 문제	
122715	GN-27006	WebUI	CLOUD 버전에서 서비스 제어 메뉴 제거했으나 상단 메뉴에서 접근이 가능한 문제	5.0.29
122715	GN-26993	WebUI	감사로그, 노드상세 이력관리 화면에서 ip, mac에 툴팁으로 표시되는 정보표기 오류	6.0.4, 5.0.47
122715	GN-26992	Center	에이전트 플러그인이 정책서버의 타임존 기준으로 동작하는 문제	
122715	GN-26965	WebUI	[5.0] ipmgmt3 접속 시 게스트 용도 설정값이 없을 경우 접속 오류 페이지 출력되는 문제	4.0.114, 5.0.11
122715	GN-26951	Windows Agent	백신정보수집 플러그인으로 바이러스 치료 감사기록이 되지 않는 문제	4.0.144, 5.0.41
122715	GN-26941	WebUI	ConfEngine 의 AddRemove 컴포넌트 내 항목 수정시 잘못 수정되는 문제	5.0.18
122715	GN-26933	WebUI	일부 날짜 입력필드에 사용되는 달력 컴포넌트가 영문으로만 표시되는 문제	5.0.20, 6.0.0
122715	GN-26904	WebUI	노드관리 > 위험 컬럼의 아이콘 미출력 문제	5.0.53, 6.0.13
122715	GN-26864	Windows Agent	간헐적으로 정보수집플러그인의 최신정보가 업데이트되지 않는 문제	5.0.0, 6.0.0
122715	GN-26859	Linux Agent	Linux Agent, 파티션이 나뉘져 있지 않은 저장 장치 정보가 수집되지 않는 문제	5.0.41, 6.0.0

continues on next page

Table 5 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122715	GN-26777	WebUI	노드/제어정책의 노드그룹 수정 시 갱신시각 업데이트 되지 않는 문제	6.0.18
122715	GN-26742	Sensor	센서 노드정보 검사 설정의 "NMAP TCP SCAN" 사용안함 적용되지 않는 문제	5.0.40
122715	GN-25805	WebUI	IP Matrix View에서 IP변경금지 (지정 IP대역) - 단일 IP 위반됨 아이콘 표시되지 않는 문제	4.0.8

16.3.4 Genian NAC 5.0.57 Release Notes (2023-10-11)

Last Updated: 2023-12-19

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
122612	GN-27492	WebUI	Tomcat Version Upgrade (8.5.94 -> 8.5.96 / 9.0.81 -> 9.0.83)		7.5
121387	GN-26315	WebUI	2단계 인증에서 인증코드 입력값 횟수제한, 시간제한하도록 개선		4.3
120864	GN-27278	WebUI	Tomcat Version Upgrade (8.5.94 / 9.0.81)		7.5
120388	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
122689	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
122665	GN-25714	WebUI	보안서약 만료일 설정 옵션 추가	
122237	GN-27164	VRRPD	[범용OS] 이중화 구성 master 상태로 전환 후 인터페이스 상태검사 실패로 인해 slave 상태로 전환되는 문제	5.0.42 (LTS)

continues on next page

Table 6 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122214	GN-27402	WebUI	MAC 정책 수정 시 시작/종료 시각을 설정할 수 있도록 API 개선	
122165	GN-27390	Center, WebUI	리포트 보존개수 설정 시 /disk/data/report 디렉토리의 데이터도 삭제하도록 개선	
121927	GN-27241	macOS Agent	macOS 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121890	GN-27248	Linux Agent	Linux Agent, 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
121744	GN-26627	WebUI	CWP 웹 페이지 출력 상태에서 에이전트 인증 후 CWP 웹에서 인증 화면이 다시 출력되지 않도록 개선	
121117	GN-27269	- Unknown/None	apache / tomcat 관련 디렉토리 및 파일의 불필요한 권한 제거	
120831	GN-27319	WebUI	Tomcat 구동시 jdbc 연결에 serverTimezone 설정 추가	
120404	GN-27146	Center	extauth 를 통한 외부인증연동 실패시 사용자가 입력한 패스워드가 센터디버그파일에 남는 문제	
120334	GN-27174	WebUI	ConfEngine File (40) 타입에서 기본 출력되는 콤보박스의 데이터 선택할 수 있도록 개선	
120334	GN-27163	Sensor	센서데몬의 주기적으로 데드락 여부를 검사하는 기능 추가	
120334	GN-27160	Center	인증 연동 시 사용자 도메인을 사용할 때 로컬DB 계정 연결 방식 수정	
120334	GN-27049		macOS 파일배포 폴더 정규식 지원하도록 개선	
120334	GN-26875	WebUI	호스트명 제한시 CWP에 출력되는 메시지 수정	
120334	GN-26843	Center	센터데몬 초기 구동시 에이전트 패키지를 두번 생성하는 문제	
120334	GN-26827	WebUI	백업수행 지금시작 버튼의 팝업 메시지 수정	
120334	GN-26803	Windows Agent	플러그인을 통한 공유폴더제어에 대한 감사기록 추가	
120334	GN-26801	WebUI	WEBUI 의 primefaces 기본 시스템 오류가 출력되는 문제 개선	
120334	GN-26763	WebUI	데일리 리포트 내 전일 동안 추가된 항목을 선택할 수 있도록 개선	
120334	GN-26760	WebUI	데일리 리포트 생성 및 발송 시 관리자 별로 (관리범위에 따른) 관리되도록 개선	
120334	GN-26753	WebUI	쿼리리포트에 쿼리 문자열 끝에 세미콜론 입력시 오류 메시지 출력하도록 개선	
120334	GN-26734	WebUI	관리>노드>장비속성 에서 내용연수 시작일/만료일 잘못된 날짜를 입력시 오류메시지 개선	
120334	GN-26668	CWP	CWP SSL 사용 기본 설정을 On으로 변경	
120334	GN-26665	WebUI	정책 생성시 에이전트 액션 할당시 "사용가능 OS 종류" 의 드롭다운 UI 를 추가	
120334	GN-26653	WebUI	노드관리목록>노드속성변경시 같은 카테고리의 항목은 하나만 선택할 수 있도록 개선	

continues on next page

Table 6 – continued from previous page

Revision	Key	Components	Description	Affects Versions
120334	GN-26640	WebUI	노드그룹 조건 계속추가 시 이전 항목이 선택되어 있도록 변경	
120334	GN-26610	Center	사용자 기본 로케일 설정과 상관없이 에이전트 설치 시 영문으로 표시되는 문제	
120334	GN-26555	Sensor	네트워크객체에서 FQDN을 사용시 센서에 캐시된 IP 정보를 확인하는 gnlogin 명령 추가	
120334	GN-26544	GNOS	GNOS 커널 최신패치 적용 (5.10.181)	
120334	GN-26491	WebUI	노드 관리 설명 컬럼의 내용이 컬럼 사이즈만큼 출력되도록 개선	
120334	GN-26473	Sensor	입력한 SNMP Agent의 버전분리 및 Community와 Passwd를 정규식 검사하도록 개선	
120334	GN-26468	WebUI	노드상세의 소프트웨어/이력관리 목록의 페이지당 목록 출력 갯수를 변경 가능하도록 개선	
120334	GN-26464	WebUI	설정 > 공지사항에서 이미지 업로드 및 미리보기 시 이미지가 깨져보이는 문제 개선	
120334	GN-26450	WebUI	이력관리 목록에서 페이지 이동 시 스크롤이 상단으로 이동하도록 개선	
120334	GN-26412	WebUI	관리자 세션 강제종료시 로그인 화면으로 전환되도록 수정	
120334	GN-26410	CWP, WebUI	SAML 인증연동시 IdP 인증 후 SP에서 오류가 발생시 아무런 메시지가 출력되지 않는 문제	
120334	GN-26407	WebUI	IP 관리 매트릭스 뷰에서 정책서버 표시될 수 있도록 수정	
120334	GN-26312	WebUI	노드 일괄 등록시 csv 중복노드 존재하면 이후 작업이 진행되지 않는 문제	
120334	GN-26300	WebUI	CWP 장치신청서 및 알람메시지 타임존 맞지 않는 문제	
120334	GN-26187	WebUI	사용자 등록 페이지의 피방문자 검색을 관리자의 이메일로 조회할 수 있도록 개선	
120334	GN-25759	WebUI	캘린더에 양식에 맞지 않는 값 입력시, 영문 메시지가 출력되는 문제	
120334	GN-19829	CLOUD	On-Prem 백업파일을 Cloud에 Restore 할 수 있도록 한다	
120180	GN-27207	Windows Agent	다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
122591	GN-27502	Center	Keepalive 에 의한 에이전트/센서 다운 체크과정이 오래 걸리는 경우 에이전트 로그온 API 처리가 지연되는 문제	5.0.42 (LTS)
122567	GN-27480	WebUI	노드그룹 조건 중 부서선택 타입의 조건을 검색할 수 없는 문제	5.0.31, 6.0.0
122545	GN-27495	WebUI	서비스 제어 > 정책적용 다이얼로그에서 닫기 버튼 클릭 시 정책 적용 이벤트가 호출되지 않도록 수정	6.0.17, 5.0.57

continues on next page

Table 7 – continued from previous page

Revision	Key	Components	Description	Affects Versions
122505	GN-27504	Center	KeepAlive 수신 시 NodeID 관련 DB 오류 (Illegal mix of collations) 감사로그 발생되지 않도록 개선	
122455	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)
122428	GN-27510	Center, Sensor	[범용OS] NAC패키지 업그레이드 후 추가된 라이브러리를 찾지 못하는 문제	5.0.42 (LTS)
122377	GN-27404	Center, macOS Agent	macOS 업데이트 플러그인의 설치모드 사용시 정상적으로 설치되지 않는 문제	5.0.11
122305	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
122258	GN-27437	Center, macOS Agent	macOS Sonoma 단말의 OS 정보가 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
122116	GN-27384	Windows Agent	윈도우 방화벽 제어 플러그인의 프로그램 경로 설정 오류 수정	5.0.45
122084	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)
122072	GN-27385	GenianOS	iptables 명령이 동시 실행시 실패될 수 있는 문제 개선	5.0.0, 6.0.0
121880	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 7 - continued from previous page

Revision	Key	Components	Description	Affects Versions
121835	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
121708	GN-27380	Windows Agent	액션검사조건에 에이전트가 지원하는 매크로 이외에 '%' 문자가 존재하면 비정상 종료되는 문제	5.0.0, 6.0.0
121655	GN-27387	WebUI	OpenPort 현황 화면에서 내보내기 기능 동작하지 않는 문제	5.0.6
121623	GN-26858	WebUI	5.0 버전 2단계 인증으로 구글 OTP 사용 시 인증코드에 숫자 외의 문자가 포함될 경우 오류 발생하는 문제	5.0.50, 5.0.53
121585	GN-27393	WebUI	IP,MAC 추가필드 사용자선택기에서 설정된 맵핑 컬럼키가 동작하지 않는 문제	6.0.16 (LTS), 5.0.55 (LTS)
121528	GN-27270	macOS Agent	macOS AD 대체인증시 허용 도메인명에 .com 생략시 인증되지 않는 문제	4.0.108, 5.0.5
121508	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
121464	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
121453	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)
121397	GN-27388	Center	[범용OS] webssh 접속 안되는 문제	5.0.42 (LTS)
121201	GN-27322	Center, Sensor	[범용OS] 시스템관리 > 환경설정 > 타임존 설정이 우분투 NAC 에서 동작 안하는 문제	5.0.50
121168	GN-27356	Sensor	패치 Proxy 서비스설정 on 설정임에도 cache 서비스가 구동되지 않는 문제	5.0.55 (LTS), 4.0.157
121163	GN-27259	Linux Agent	Linux Agent, 특정 패키지로 에이전트 설치시 동작하지 않는 문제	5.0.45, 6.0.2
121135	GN-27359	gnlogin, VR-RPD	이벤트재전송처리가 필요없는 프로세스에서도 이벤트큐 처리가 동작하여 Same event already exist in queue 디버그 로그가 발생하는 문제	5.0.42 (LTS)

continues on next page

Table 7 - continued from previous page

Revision	Key	Components	Description	Affects Versions
121077	GN-27289	WebUI	사용자정의 리포트 생성시 리포트 파일이 생성되지 않는 문제	6.0.17, 5.0.57
121020	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)
120818	GN-27262	Center	정책서버와 DB서버의 Timezone 설정이 다른경우 노드의 변경된 제어정책이 센서로 전달 안되는 문제	6.0.17, 5.0.57
120775	GN-24372	CLOUD	Docker compose 정책서버에서 백업 동작안하는 문제	5.0.42 (LTS)
120741	GN-27290	WebUI	센서명에 '%' 가 포함되는 경우 센서트리가 정상적으로 표시되지 않는 문제	5.0.43, 6.0.0
120606	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)
120537	GN-27091	Center, procmond	센서에서 보내는 이벤트로그 (procmond 프로세스)가 정책서버에서 unknown center did 에러 발생하면서 로그 저장 안되는 문제	5.0.42 (LTS)
120522	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
120509	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
120497	GN-27177	Backup	백업 파일에 에이전트 zip 파일이 포함되어 용량이 증가하는 문제	6.0.16 (LTS), 5.0.55 (LTS)
120430	GN-27153	WebUI	관리자 노드관리범위 제한을 센서그룹으로 설정하고 노드 등록 시 관리센서 선택할 수 없는 문제	5.0.31
120376	GN-27215	WebUI	5.0버전에서 관리 > 스위치 > 그룹 클릭 시 오류 페이지 출력 문제	5.0.42 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)

continues on next page

Table 7 - continued from previous page

Revision	Key	Components	Description	Affects Versions
120360	GN-27191	WebUI	감사로그 화면에서 브라우저가 멈추는 문제	5.0.54, 6.0.15
120334	GN-26976	Center	[범용OS] 업데이트 실패 시, 장비가 제대로 동작하지 못하는 문제	5.0.56 (50 LTS), 6.0.17
120334	GN-26899	Center	Self-Signed 인증서 재발급 되지 않는 문제	5.0.45, 6.0.2
120334	GN-26845	WebUI	윈도우즈 업데이트 액션이 할당되어 있을 경우 에이전트를 삭제했지만 노드목록에서 에이전트 존재하는 것처럼 출력되는 문제	4.0.M1, 5.0.0, 6.0.0
120334	GN-26836	WebUI	태그가 포함된 부서명이 존재하면 노드그룹 조건에 부서 정보 검색 오류	5.0.42 (LTS), 6.0.0
120334	GN-26815	WebUI	감사 > 리포트 > 노드 리포트 > 노드그룹 선택 > 내용 출력되지 않는 문제	5.0.24
120334	GN-26771	Center	gnlogin 을 통해서 정책서버 Enable(node-server enable) 후 센터데몬 프로세스가 정상 구동되지 않는 문제	5.0.42 (LTS)
120334	GN-26751	Sensor	sensord deadlock 감지시 잘못 데드락을 체크하는 문제	6.0.16 (LTS), 5.0.57
120334	GN-26692	WebUI	시스템관리의 소프트웨어에서 파일 선택없이 업로드 처리시 프로그레스가 종료되지 않는 현상	5.0.2
120334	GN-26689	Center	변경금지 설정 제거 디버그에 노드 IP 잘못 출력되는 문제	5.0.43, 6.0.0
120334	GN-26683	WebUI	노드 상세화면 목록화면의 검색바에서 임의의 문자 및 검색 조건의 형태에 맞지 않는 값을 입력했을때 오류 페이지 출력되는 문제	5.0.22
120334	GN-26680	Center	비밀번호 Blacklist 파일의 마지막 라인 단어가 사용금지 (제한)되지 않는 문제	4.0.106
120334	GN-26676	gnlogin	[범용OS] gnlogin 명령시 감사기록에 ADMIN, ADMINIP 가 남지 않는 문제	5.0.23
120334	GN-26673	Center	신규노드 정책: MAC차단 인 경우 변경금지(지정IP대역) 설정된 노드의 IP 사용시간 만료 시 MAC허용 노드가 차단되는 문제	4.1.M5
120334	GN-26652	WebUI	노드관리 목록 > 노드속성 가져오기 수행시 IP 시작/종료 시각이 입력한 값과 9시간 차이나는 문제	4.1.M4
120334	GN-26605	Center	새로운 무선랜 AP 감지, 무선랜AP 정보변경 감사로그 형식 수정	6.0.0
120334	GN-26586	WebUI	노드그룹 복사시 '변경 정책 적용' 버튼이 출력되지 않고 즉시 적용되는 문제	5.0.31
120334	GN-26578	WebUI	IP사용신청서 결과조회에서 사용자ID, 부서명 컬럼이 공백으로 출력되는 문제	4.1.4
120334	GN-26573	WebUI	관리콘솔 설정값 확인 연동변경 및 언어설정 파라미터 변경	6.0.0
120334	GN-26560	WebUI	노드관리 화면에서 검색어에 AND가 존재할 경우 검색되지 않는 문제	5.0.38
120334	GN-26558	WebUI	네트워크 객체의 네트워크 주소 중 FQDN 옵션의 TTL 값만 수정 시 수정되지 않는 문제	5.0.19
120334	GN-26529	WebUI	센서 IP사용률 Top 현황(구버전) 위젯에서 잘못된 센서의 IP/Mask 설정으로 인한 오류 페이지 출력 개선	4.1.4

continues on next page

Table 7 - continued from previous page

Revision	Key	Components	Description	Affects Versions
120334	GN-26489	Center	우분투/클라우드 버전에서 디버그 파일의 스레드 ID가 정상적으로 남지 않는 문제	6.0.0
120334	GN-26487	WebUI	CVE 상세화면에서 값이 없을 경우 에러페이지 출력되는 문제 수정	5.0.24
120334	GN-26463	GenianOS	syscollect 정상 동작하지 않을 수 있는 문제	5.0.0
120334	GN-26432	Windows Agent	Windows 인증창, 무선연결관리자에서 로고가 좌측 상단에 출력되는 문제	5.0.39, 6.0.0
120334	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
120334	GN-26408	Sensor	노드그룹에 노드그룹에 속하지 않는 조건을 넣을 때 간헐적으로 센서데몬이 죽는 문제	4.0.114, 5.0.11
120334	GN-26382	WebUI	사용자 인증 > 인증연동 > SAML2 인증연동에서 SAML IdP 설정 또는 추가할때 Http Status 400 - Bad Request가 발생할 수 있는 문제	5.0.25
120334	GN-26380	WebUI	IPMGMT 에서 IP 신청서 양식 다운로드 되지 않는 문제	5.0.43, 6.0.0
120334	GN-26369	WebUI	노드/로그/무선랜 리포트에서 전년도 검색시 날짜 표시가 잘못 출력되는 문제	5.0.34
120334	GN-26354	Center	인증연동 시 연결되지 않은 로컬DB 계정정보 표시하는 문제	5.0.53
120334	GN-26314	WebUI	IP 신청 목록 설정에서 부서명 등을 제거하면 IP 신청서에서 라벨이 보이지 않는 문제	4.0.11
120334	GN-26235	macOS Agent	macOS 에이전트 신규 모델 mac의 메인보드 정보를 얻어 오지 못하는 문제	5.0.41, 6.0.0
120334	GN-25815	WebUI	IP 신규/반납 신청서의 승인/거부 팝업이 활성화되어있는 상태에서 승인/거부시 대기상태가 되는 문제	4.1.3
120146	GN-27237	Center, Sensor	관리콘솔에서 센서에 등록된 에이전트노드삭제시 센서에 의해서 노드가 즉시 재등록 안되는 문제	5.0.42 (LTS)
118284	GN-26785	Center	장치제어 정책 사용 시, 다른 노드 그룹의 장치제어 정책을 수신할 수 있는 문제	5.0.23
114066	GN-26566	WebUI	노드 정보 업데이트 후, 탭 이동 시 변경한 정보가 갱신되어 보여지지 않는 문제	5.0.50
113315	GN-26496	CLOUD	Cloud site 최초 생성시 로그 통계 데이터가 보이지 않는 문제	5.0.50, 6.0.12

16.3.5 Genian NAC 5.0.50 Release Notes ()

Last Updated:

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
114720	GN-26368	WebUI	관리자의 API 키가 다른 관리자에게 노출되는 취약점		5.3
114214	GN-26392	WebUI	권한 없는 관리자가 디버그 로그 다운로드 가능한 취약점		2.9
113219	GN-26460	Windows Agent	에이전트를 통해 일반 사용자가 PC 관리자 권한을 획득할 수 있는 취약점	5.0.0, 6.0.0	4.6
112785	GN-26286	WebUI	Google OTP 2단계 인증에서 보안키를 신규로 발급받아 2단계 인증을 통과할 수 있는 문제		6.5
111886	GN-26150	WebUI	Tomcat version upgrade (9.0.68 -> 9.0.72, 8.5.78 -> 8.5.86)		
111844	GN-26205	Database	mysql 버전 업그레이드 5.7.40 -> 5.7.41		
111681	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
111338	GN-26000	MySQL	mysql 버전 업그레이드 5.7.33 -> 5.7.40		
111257	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
111018	GN-25982	WebUI	WebUI Response Header에 CSP, HSTS Header 추가		
110496	GN-25875	Windows Agent	에이전트가 웹브라우저 실행할 때 High권한 가지는 문제	4.0.0, 5.0.0, 6.0.0	3.3
110418	GN-25811	IPMGMT	IP 신청시스템에서 frontpage를 통해 사용자ID만으로 로그인 가능한 문제		4.9
110230	GN-25925	IPMGMT, WebUI	IP 신청시스템 > IP신청 화면 XSS 가능한 문제		5.4
110145	GN-25740	WebUI	감사 > 로그 > 로그검색바에서 XSS가 가능한 문제		5.6
109992	GN-25847	WebUI	CWP 화면에서 사용자 정보 수정 페이지 접근시 재인증 절차 추가		4.2
	GN-26051	WebUI	5.0 WebUI lib 취약점 항목 점검		
	GN-25250	WebUI	HTML Tag 문자열 뒤에 /를 붙이는 경우 XSS가 가능한 문제		4.9
	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
118280	GN-26838	Ubuntu(Debian)	[범용 OS] ICMP Timestamp 지원 기능 제거	
117757	GN-26702	WebUI	정책서버에서 외부로 접근이 허용되면 경고를 출력하는 기능	
117448	GN-26769	Linux Agent	Linux Agent, Sigstore 전자서명을 기반한 배포 플러그인 개발	
116767	GN-26826	geniup	UEFI 시스템에서 geniup 수행시 디스크부족 발생하는 문제	
116532	GN-26705	Center	SLSA를 통한 업데이트서버 배포 데이터 전자서명 검증	
116395	GN-26844	Center, Sensor	센서에서 외부로 접근가능여부를 센서정보(공인IP)에 표시	
115885	GN-26786	Center	업데이트서버로부터 받은 WSUSSCN2.CAB 에 대한 전자서명 검증	
114255	GN-26328	WebUI	노드그룹 엑셀다운로드시 노드 그룹명이 포함되게 개선	
112249	GN-26255	WebUI	OTP 입력길이를 32자까지 확대	
111632	GN-26135	macOS Agent	macOS 파일배포 옵션 추가 및 파일 실행 관련 로직 개선	5.0.35
111187	GN-25994	macOS Agent	macOS 하드웨어 정보 수집 플러그인에 USB 장치 정보 추가	
110538	GN-25579	Center	노드 스냅샷 정리기능 누락	
110499	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
109979	GN-25656	RADIUS	[RADIUS] AD 인증연동시 실패감사로그를 상세하게 출력하도록 변경	
109641	GN-25446	Linux Agent	Linux Agent, Sophos Linux 백신 정보 추가 수집 기능 개발	
107294	GN-25095	Linux Agent	Linux Agent, 파일 배포 액션 플러그인 개발	
	GN-26171	CWP	CWP 공지사항에 관리자의 아이디가 노출되지 않도록 개선	
	GN-25601	WebUI	IP 사용 신청서 수정화면에서 신청정보 비활성화되는 문제	
	GN-25496	macOS Agent	macOS 에이전트 자동업데이트 부하 분산 가능하도록 체크 주기 변경	
	GN-25494	Windows Agent	비밀번호 유효성검사에서 비밀번호 변경감지하여 검증창이 자동으로 종료될 수 있도록 수정	
	GN-25479	WebUI	장치 사용 신청서 처리 알림 메시지의 html 구문 제거	
	GN-25477	macOS Agent	macOS 잠자기 모드에서 무선랜제어 플러그인 사용시 Popup 메시지 중복처리	
	GN-25457	WebUI	REST API를 통한 '인스턴스 메시지' 전송	

continues on next page

Table 8 - continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-25416	Linux Agent	Linux Agent, 정책서버에서 서로다른 표준시간대 사용에 대한 예외처리	
	GN-25388	Windows Agent	무선랜제어 플러그인에 "허용SSID-정규식" 옵션에 대한 도움말 추가	
	GN-25322	WebUI	사용자 관리뷰에 마지막 인증해제시각 컬럼 추가	
	GN-25316	GNOS	"잘못된 DHCP 서버 수집 정보" 관련 위험 감사로그 항상 출력 옵션 추가	
	GN-25273	GenianOS	[범용 OS] apache2 설정을 custom 하게 사용할 수 있도록 개선	6.0.3
	GN-25266	Windows Agent	비밀번호 검증 플러그인 시작 시 디버그로그에 빈암호 사용 여부 표시	
	GN-25231	WebUI	노드그룹 조건 중 MAC 주소 조건 클릭시 로딩이 오래 걸리는 문제 개선	
	GN-25223	Linux Agent	Linux Agent, 트레이 아이콘을 통한 웹 브라우저 접속 시, snap에서 다운받은 웹 브라우저 연동 추가	
	GN-25212	WebUI	CWP 신규 사용자 등록 화면의 기간(날짜시각입력 형태) 입력 항목 출력 개선	
	GN-25205	WebUI	노드상세 - 운영체제 업데이트 정보탭의 최근 수행결과 출력 개선	
	GN-25191	WebUI	'에이전트 서비스 중지' 시 변경된 상태를 Image Icon으로 확인 할 수 있게 제공	
	GN-25189	CLI/gnlogin	mgmt-port CLI 입력시 mgmt-local-port 가 적용되도록 개선	5.0.44, 6.0.2
	GN-25161	Center	제어정책을 통한 Switch Port VLAN 변경시 Port Bounce 처리	
	GN-25096	Center	RADIUS MAC 인증 노드그룹검사를 Calling-Station-Id 를 가지고 비교할 수 있도록 개선	
	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	
	GN-24820	WebUI	감사> 로그 화면에 로그데이터 사용량 표기 기능 추가	
	GN-23573	Windows Agent	에이전트 자동업데이트 부하 분산 가능하도록 체크 주기 변경	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
117427	GN-26213	WebUI	노드정책 생성 후 노드그룹을 할당시에 변경하지 않는 옵션값이 변경된 것으로 나타나는 문제	5.0.44
117233	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

continues on next page

Table 9 - continued from previous page

Revision	Key	Components	Description	Affects Versions
117182	GN-26770	Center, Sensor	[범용OS] 센서가 배포서버로 동작하지 않는 문제	5.0.29
116853	GN-26839	Center, Sensor	정책서버/센서 메모리 릭(지니업데이트 및 노드스캔(https)) 발생 문제	4.0.14
116616	GN-26779	WebUI	로그서버(elasticsearch) 정상상태 임에도 경고 메시지 출력되는 문제	5.0.23
116581	GN-26758	Windows Agent	에이전트가 로컬시스템으로 동작하면 프로그램제거 플러그인을 통하여 Store 앱 삭제 실패	5.0.42 (LTS), 6.0.0
116343	GN-26623	WebUI	노드관리의 뷰가 IP 관리뷰 일 때 액셀 내보내기시 IP만료 시각이 표기되지 않는 문제	5.0.50
115785	GN-26749	Elastic-Search	[범용OS] Elastic과 통신이 Iptables 정책에 의해서 차단되어 간헐적으로 ES가 정상 구동 안하는 문제	5.0.31
115639	GN-26727	Sensor	[범용OS] 센서와 동일한 DNS를 할당하는 DHCP 서버가 비정상적인 DHCP서버로 감지되는 문제	
115493	GN-25887	WebUI	현황&필터의 노드그룹 내에 다단계의 카테고리 구조에서 하위 카테고리가 표시되지 않음	5.0.42 (LTS), 5.0.45, 6.0.2
115289	GN-26719	WebUI	정책 > 객체 > 시간 메뉴에서 시간 객체 생성시 System Timezone과 관리자 Timezone이 다른 경우 날짜가 잘못 저장되는 문제	5.0.34
115122	GN-26428	Center	콘솔UI를 통한 deb 이미지 업그레이드시 OS 종류에 따라 실패할 수 있는 문제	5.0.42 (LTS), 6.0.12
115022	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
114668	GN-25626	WebUI	피방문자 이메일 승인 대상이 관리자임에도 일반 사용자가 검색되는 문제	4.0.M8
114312	GN-26597	WebUI	DB/Log 서버 분리구성 일 경우 쿼리리포트 생성되지 않는 문제	5.0.37
114300	GN-26532	WebUI	NIC 벤더별 현황의 수량 맞지 않는 문제 개선	
114265	GN-26609	WebUI	노드추가필드(사용자선택기-맵핑컬럼명) 사용하여 노드 등록 시 오류 발생하는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
114197	GN-26440	WebUI	태그의 변동사항이 없는데 노드 상세정보 수정 시 함께 업데이트 처리 되는 문제	5.0.22, 6.0.4
114197	GN-26425	WebUI	노드그룹 조건의 사용자 부서 선택 시 데이터에 상위부서가 포함되지 않는 문제	5.0.35
114153	GN-26280	Center	멀티 센서 장비 삭제 이후 재등록될때 센서 승인 상태로 등록되는 문제	6.0.8, 5.0.50
114066	GN-26566	WebUI	노드 정보 업데이트 후, 탭 이동 시 변경한 정보가 갱신되어 보이지 않는 문제	5.0.50
113986	GN-26476	WebUI	액션별 수행결과 현황 페이지 오류 수정	5.0.50

continues on next page

Table 9 - continued from previous page

Revision	Key	Components	Description	Affects Versions
113769	GN-25776	Center	패스워드가 없는 사용자 및 동기화된 사용자(READ ONLY) 에 대해서 비밀번호 변경 만료 알림메시지가 나오지 않도록 개선	4.0.18
113594	GN-26319	WebUI	감사로그 화면에서 관리장비명 클릭시 노드관리 검색되지 않고 모두 출력되는 문제	5.0.38
113556	GN-26448	WebUI	Compose 방식 설치후 시스템 목록에서 정책서버 정보가 출력되지 않는 오류	5.0.6
113541	GN-26540	Windows Agent	영문관리콘솔의 플러그인 '적용OS' 선택에서 Windows 11 이 Windows 10으로 잘못 표시됨.	5.0.42 (LTS), 6.0.0
113486	GN-26267	WebUI	감사 > 로그에서 KST 기준 9시 이전에는 오늘의 감사로그가 출력되지 않는 문제	4.0.17
113400	GN-26357	WebUI	신규 노드그룹 상세화면의 대상노드리스트에서 기본현황으로 돌아갈때 구 버전 상세화면 출력되는 문제	5.0.35
113357	GN-26322	macOS Agent	macOS 알림메세지 수신시 CPU 점유율 높아지는 문제	5.0.27
113343	GN-26446	Center	LDAP 연결 실패 시 center 데몬의 fd가 증가하는 문제	5.0.41, 4.0.145, 6.0.0
113322	GN-26444	WebUI	노드그룹 조건의 소프트웨어 설정 창에서 한글검색이 안되는 증상	5.0.35
113136	GN-26130	macOS Agent	macOS 하드웨어 정보수집 플러그인 사용시 크래시 발생하는 문제	5.0.38
113084	GN-26040	WebUI	변경노드관리 전체 노드 선택 시 관리자 확인 기능 동작 않는 문제	5.0.26
113044	GN-26414	Windows Agent	비밀번호 검증창의 고정옵션이 off 임에도 주기적으로 화면 중앙으로 위치되는 문제	5.0.42 (LTS), 6.0.12, 5.0.53
113024	GN-26433	Sensor	게이트웨이 IP추가시 IP Rule 이 잘못생성되어 센서 통신이 안될 수 있는 문제	5.0.42 (LTS)
112771	GN-26160	Authsync, Center	CSV를 다운로드 받아 사용자정보 동기화 진행할 때 실패할 수 있는 문제	5.0.0
112754	GN-26385	Packaging	C30G,C50G장비 모니터 출력 안되는 문제	5.0.44, 6.0.1
112674	GN-26259	Elastic-Search	Advance 페이지의 Elasticsearch 관리툴에서 샤드 정보표시 오류	5.0.17
112643	GN-26223	WebUI	노드 상세화면에서 태그할당 시 태그가 50개만 출력되는 문제	5.0.22
112598	GN-26242	WebUI	구름OS(Linux)에 설치된 에이전트가 관리콘솔의 노드목록에 Windows 아이콘으로 표시 되는 문제	6.0.8, 5.0.50
112511	GN-26227	Center	[범용OS] 서버인증서에 Subject Alternative Names 이 없어서 INVALID COMMON NAME 인증서 오류 발생하는 문제	5.0.23
112389	GN-26208	WebUI	검색창에 <문자가 포함된 검색어를 입력할 경우 XSS 감지로그가 남는 문제	6.0.7, 5.0.50, 4.0.152
112371	GN-26178	WebUI	상세 감사로그 메세지에 포함된 ->로 인해 XSS 발견 로그가 남는 문제	6.0.7, 5.0.50, 4.0.152

continues on next page

Table 9 – continued from previous page

Revision	Key	Components	Description	Affects Versions
112122	GN-25936	WebUI	관리역할 권한설정에 상관없이 동작하는 노드 작업명령이 동작하지 않는 문제	5.0.44, 6.0.1
112106	GN-26219	WebUI	정책 복사 시 액션에 라벨이 존재할 경우 오류가 발생하는 문제	4.0.113, 5.0.10
112065	GN-26170	WebUI	영문 관리콘솔의 CWP 디자인 템플렛의 컴포넌트 추가/삭제가 정상동작하지 않는 문제	5.0.48, 6.0.7
111954	GN-26200	Center	ZTNA 및 NAC 최신버전에서 CVE 목록 갱신되지 않는 문제	5.0.50, 6.0.12, 5.0.53
111828	GN-26188	IPMGMT	IP신청시스템 임시사용자 자동로그인 되지 않는 문제	5.0.50, 4.0.153, 6.0.11
111738	GN-25998	Windows Agent	(비밀번호 검증 플러그인) 계정의 비밀번호 변경시각이 계속 변경되어 보고되는 문제	4.0.M5, 5.0.0, 6.0.0
111729	GN-25565	Center	Syslog TLS 전송시 센터데몬 비정상 종료	4.1.M7
111670	GN-26175	Center	GDPI를 사용하는 Cloud 서비스에서 GPDB를 계속 다운로드 하는 현상	5.0.41
111620	GN-26106	Windows Agent	네트워크 공유폴더제어에서 공유허용시간 설정시 공유 해제되지 않는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
111587	GN-26137	WebUI	CWP 디자인 템플릿 설정 페이지에서 CWP 페이지 미리 보기 화면이 보이지 않는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
111559	GN-26161	GenianOS	procmond에서 sshd 재구동 오류 수정	5.0.23
111463	GN-26028	Windows Agent	프로세스 강제종료 액션정책이 여러 개 존재할 경우 강제 종료 미동작 문제 수정	5.0.25
111171	GN-26068	WebUI	[5.0]자동 생성된 대시보드 리포트 클릭 시 다운로드 되지 않고 빈 화면으로 이동되는 문제	5.0.50
111067	GN-26063	IPMGMT	CWP에서 IP사용신청 자동로그인 기능이 동작하지 않는 문제	5.0.50, 4.0.153, 6.0.11
111039	GN-26008	WebUI	노드그룹 상세화면에서 정책복사 기능 동작 하지 않는 문제	5.0.31
110998	GN-26047	WebUI	[4.0/5.0] 대시보드 > 센서맵 출력되지 않는 문제 수정	5.0.42 (LTS)
110983	GN-26029	CLOUD	Cloud NAC 사용자정보 동기화 안되는 문제	6.0.3, 5.0.50
110975	GN-26045	CLOUD	신규 Cloud Site 생성시 GDPI API를 사용하도록 설정이 되지 않는 문제	5.0.50, 6.0.10
110914	GN-25900	Linux Agent	Linux Agent 장기 사용시 서버로부터 정책을 받는 횟수가 증가하는 문제	5.0.41, 6.0.0
110851	GN-25832	WebUI	PC 시간 변경시 관리콘솔 세션타임이 변경되는 문제	5.0.48, 6.0.7
110794	GN-26018	WebUI	IP신규/반납 신청서의 상세보기 화면에서 승인시 오류 발생	5.0.49, 6.0.8

continues on next page

Table 9 - continued from previous page

Revision	Key	Components	Description	Affects Versions
110786	GN-25995	WebUI	IP 주소 관리에서 노드등록 시 노드삭제금지 적용 안되는 문제	5.0.40
110781	GN-25964	Windows Agent	에이전트 인증창 업그레이드 후 인증 후 실행 옵션이 사라지는 문제	5.0.42 (LTS), 6.0.3, 5.0.46
110530	GN-25893	WebUI	5.0 노드상세정보에서 노드선택 후 작업선택의 노드대상 작업지시 명령이 수행안되는 문제.	5.0.44, 6.0.1
110443	GN-25880	Center	[범용OS] favicon 출력 안되는 문제	5.0.37
110351	GN-25931	CWP	On Premise에서 Domain을 사용하는 경우 SAML 인증시 IP주소로 인증요청이 발생하여 인증이 되지 않는 문제	5.0.48
110323	GN-25888	Center	메일서버 및 정보동기화 시, 구글 인증 코드 발급이 안되는 증상	5.0.16, 6.0.0
110210	GN-25903	macOS Agent	macOS 파일패포 플러그인 파일 미업로드시 에이전트 오 동작하는 문제	5.0.31, 6.0.0
110174	GN-25796	Center	에이전트에 의한 신규노드 등록 시 노드타입이 지정된 경우에도 노드타입 변경되는 문제	5.0.33
110155	GN-25885	Sensor	스위치 포트정보가 수집 안되는 문제	6.0.4, 5.0.47
110062	GN-25863	WebUI	노드관리 검색어에 &가 있을 경우 동작하지 않는 문제	5.0.42 (LTS), 5.0.49, 6.0.8
110024	GN-25905	WebUI	[5.0] 위젯 및 현황 화면에서 잘못된 노드목록 링크 수정	5.0.48
109975	GN-25868	Center	간헐적으로 노드(에이전트) 업다운 로그가 남지 않는 문제	5.0.49
109950	GN-25699	WebUI	현황&필터의 에이전트 액션의 필터 결과가 상세조회 내역과 다른 문제 및 엑셀다운로드가 안되는 현상	6.0.4, 5.0.48
109755	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
109725	GN-25750	Windows Agent	인증창에서 잘못된 URL으로 웹브라우저가 열리는 문제	5.0.0, 4.0.123
	GN-26655	WebUI	Compose 버전에서 노드관리 엑셀 export 시 오류 페이지 발생	5.0.48, 6.0.6
	GN-25979	Center	RADIUS 정책을 여러번 변경시 정책적용 큐가 정상동작 하지 않는 문제	5.0.23
	GN-25978	WebUI	스위치 상세화면에서 수정시 패스워드 변경을 하지 않았는데 패스워드 길이 오류 출력되는 문제	5.0.17
	GN-25864	Genian Mobile	Genian NAC Monitor 에서 센터에 접속되지 않는 문제	5.0.49, 6.0.9
	GN-25815	WebUI	IP 신규/반납 신청서의 승인/거부 팝업이 활성화되어있는 상태에서 승인/거부시 대기상태가 되는 문제	4.1.3
	GN-25745	Linux Agent	Linux Agent, "파일 패포" 플러그인에서 Root 권한으로 파일 실행이 안되는 문제	6.0.8, 5.0.50
	GN-25734	Windows Agent	에이전트 알림메세지에서 하이퍼링크 클릭시 IE가 표시 되는 현상	6.0.4, 5.0.47
	GN-25652	WebUI	대시보드의 CVE 현황 위젯에서 플랫폼 수량을 클릭하여 이동했을 때, 목록 버튼 클릭시 오류 발생	5.0.43, 6.0.0

continues on next page

Table 9 - continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-25642	WebUI	5.0 버전에서 개선된 노드그룹 조건설정 UI 가 안나오는 문제	5.0.49
	GN-25574	macOS Agent	macOS 에이전트내의 메시지 관련 ID를 정상적으로 가져 오지 못하는 문제	5.0.50, 6.0.9
	GN-25559	Windows Agent	무선연결관리자를 통하여 한글 SSID 프로파일이 잘못 등록되어 연결못하는 문제	4.0.5, 5.0.0, 6.0.0
	GN-25549	dbmigration	CLOUD 고객사 사이트 생성후 RADIUS Accounting 동작 하지 않는 문제	5.0.33
	GN-25498	macOS Agent	macOS 모양 및 개인설정 플러그인의 화면보호기 옵션이 적용되지 않는 문제	5.0.15, 5.0.45, 6.0.2
	GN-25462	Genian Monitor	윈도우용 Genian Monitor에서 상세항목 클릭시 웹페이지 오류 표시 문제	5.0.19, 6.0.0
	GN-25443	Center	custom 인증서 사용중에도 인증서 만료로그가 장비인증서 기준으로 남는 문제	5.0.0
	GN-25439	Center	GPDB 수동 업데이트 시 에이전트 설치 노드의 플랫폼이 Unknown으로 변경되는 문제	
	GN-25428	Ubuntu(Debian)	[범용 OS] 에이전트 파일 restore 후, 에이전트 설치 파일 업로드 및 다운로드 안되는 문제	5.0.23, 6.0.0
	GN-25418	GenianOS	[범용 OS] 파일 내보내기(Excel Export) 기능이 동작하지 않는 문제	
	GN-25399	Center, Database	Windows 업데이트 액션 라벨 할당 시 Windows 업데이트 현황의 노드 수가 잘못 표시되는 문제	4.0.113, 5.0.10
	GN-25390	Sensor	FQDN 네트워크 객체 사용시 권한이 정상동작하지 않는 문제	5.0.27
	GN-25381	Center, CLOUD	CLOUD 버전에서 인증서 재발급 버튼으로 인증서가 재발급되지 않는 증상	5.0.45, 6.0.2
	GN-25364	WebUI	CONF On/Off 버튼을 부모로 설정했을 때 자식 설정의 visible 처리가 정상적으로 처리되지 않는 문제	5.0.16
	GN-25350	WebUI	IP신규신청의 이메일 승인/거부 후 로그인 되어 있는 관리자 UI 세션이 종료 되는 문제	4.1.0
	GN-25345	Center	[범용 OS] 정책서버 업그레이드시 센서 자동 업그레이드 기능 동작하지 않는 문제	5.0.43, 6.0.0
	GN-25340	macOS Agent	macOS 운영체제 정보수집 플러그인에서 설치 날짜를 가져오지 못하는 문제	6.0.4, 5.0.47
	GN-25339	WebUI	로그검색 및 검색필터의 수정상태에서 새로고침 버튼 클릭 시 분석차트페이지로 전환되는 현상	5.0.22
	GN-25319	WebUI	노드목록에서 NodeType 조건을 여러개 입력해서 조회할 때 오류 페이지 출력되는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
	GN-25317	Center	노드그룹 조건의 시간객체 종료시각 이후에도 노드그룹에서 해제되지 않는 문제	4.1.3
	GN-25289	macOS Agent	macOS 장치제어 플러그인 동작 오류 및 로그 개선	6.0.3, 5.0.46
	GN-25279	WebUI	노드타입 위젯에서 일부 노드타입의 링크로 이동된 노드 목록에서 결과가 잘못출력되는 문제	5.0.43, 6.0.0
	GN-25271	Center	기본/보조DNS 조건 정책 적용시 링크 UP 된 인터페이스만 정책검사되도록 수정	5.0.0
	GN-25259	Windows Agent	노드정책의 에이전트 사용여부를 OFF으로 변경해도 이전 액션수행 결과가 남아있는 문제	5.0.0, 6.0.0

continues on next page

Table 9 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-25253	Windows Agent	장치제어 차단 후 감사로그에 'ID=숫자' 형태로 출력되어 정책 이름으로 수정	5.0.25, 6.0.0
	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
	GN-25219	Center	[범용OS] HA 이중화 구성에서 Master 파일이 Slave로 동기화되지 않는 문제	
	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
	GN-25159	WebUI	URL 호출에서 설정된 헤더 목록이 모두 삭제되지 않는 문제	5.0.15
	GN-25152	IPMGMT	IP관리정책위반인 상태에서 IP사용신청 시 페이지 오류	5.0.11
	GN-25147	WebUI	디폴트 노드그룹을 모두 업데이트 했는데 업데이트 가능 수량이 있다고 표시될 수 있는 문제	5.0.27
	GN-25144	Center	인증연동 서버주소에 공백이 포함된 경우 서버 연결에 실패하는 문제	
	GN-25117	WebUI	에이전트 관련 위젯에서 노드목록 이동시 검색되지 않는 문제	5.0.33
	GN-25081	WebUI	IP 신청서 REST API에서 장비변경 승인이 처리되지 않는 문제	5.0.7, 4.0.110

16.3.6 Genian NAC 5.0.53 Release Notes ()

Last Updated:

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
116659	GN-26814	Center	Bufferoverflow 에 대한 코드 개선		2
114720	GN-26368	WebUI	관리자의 API 키가 다른 관리자에게 노출되는 취약점		5.3
114214	GN-26392	WebUI	권한 없는 관리자가 디버그 로그 다운로드 가능한 취약점		2.9
113219	GN-26460	Windows Agent	에이전트를 통해 일반 사용자가 PC 관리자 권한을 획득할 수 있는 취약점	5.0.0, 6.0.0	4.6
112785	GN-26286	WebUI	Google OTP 2단계 인증에서 보안키를 신규로 발급받아 2단계 인증을 통과할 수 있는 문제		6.5
111886	GN-26150	WebUI	Tomcat version upgrade (9.0.68 -> 9.0.72, 8.5.78 -> 8.5.86)		
111844	GN-26205	Database	mysql 버전 업그레이드 5.7.40 -> 5.7.41		
111681	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
111257	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
118280	GN-26838	Ubuntu(Debian)	[범용OS] ICMP Timestamp 지원 기능 제거	
117757	GN-26702	WebUI	정책서버에서 외부로 접근이 허용되면 경고를 출력하는 기능	
117448	GN-26769	Linux Agent	Linux Agent, Sigstore 전자서명을 기반한 배포 플러그인 개발	
116767	GN-26826	geniup	UEFI 시스템에서 geniup 수행시 디스크부족 발생하는 문제	
116532	GN-26705	Center	SLSA를 통한 업데이트서버 배포 데이터 전자서명 검증	
116395	GN-26844	Center, Sensor	센서에서 외부로 접근가능여부를 센서정보(공인IP)에 표시	
115885	GN-26786	Center	업데이트서버로부터 받은 WSUSSCN2.CAB 에 대한 전자서명 검증	
114255	GN-26328	WebUI	노드그룹 엑셀다운로드시 노드 그룹명이 포함되게 개선	
112651	GN-26337	macOS Agent	macOS 액션 수행 조건에 사용자 경로에 대한 매크로 추가	
112523	GN-26163	Sensor	Dnsmasq Cache 기능을 사용하도록 변경	
112450	GN-25704	Sensor	PROXY 를 통한 연결시에도 CWP 리다이렉트 동작하도록 수정	
112249	GN-26255	WebUI	OTP 입력길이를 32자까지 확대	
111932	GN-25550	WebUI	노드/제어 액션의 상세화면에서 사용처에 대한 목록 출력 및 삭제 가능하도록 개선	
111632	GN-26135	macOS Agent	macOS 파일배포 옵션 추가 및 파일 실행 관련 로직 개선	5.0.35
111418	GN-25739	WebUI	사용자 일괄등록시 관리역할 추가	
	GN-25990	WebUI	SAML Assertion Attribute(사용자정보)를 통한 사용자 추가/갱신 기능	
	GN-25630	Center	감사로그검색필터 WEBHOOK 외부연동기능시 BULK 전송 가능하도록 개선	
	GN-25517	WebUI	노드목록에서 컨버터 적용으로 인해 정렬이 불가능한 컬럼에 대한 개선	
	GN-25337	WebUI	매일 특정 시간대에 발생한 감사로그를 검색필터로 설정 가능하도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
117427	GN-26213	WebUI	노드정책 생성 후 노드그룹을 할당시에 변경하지 않는 옵션값이 변경된 것으로 나타나는 문제	5.0.44
117233	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
117182	GN-26770	Center, Sensor	[범용OS] 센서가 배포서버로 동작하지 않는 문제	5.0.29
116853	GN-26839	Center, Sensor	정책서버/센서 메모리 릭(지니업데이트 및 노드스캔(https)) 발생 문제	4.0.14
116616	GN-26779	WebUI	로그서버 (elasticsearch) 정상상태 임에도 경고 메시지 출력되는 문제	5.0.23
116581	GN-26758	Windows Agent	에이전트가 로컬시스템으로 동작하면 프로그램제거 플러그인을 통하여 Store 앱 삭제 실패	5.0.42 (LTS), 6.0.0
116343	GN-26623	WebUI	노드관리의 뷰가 IP 관리뷰 일 때 엑셀 내보내기시 IP만료 시각이 표기되지 않는 문제	5.0.50
115785	GN-26749	Elastic-Search	[범용OS] Elastic과 통신이 Iptables 정책에 의해서 차단되어 간헐적으로 ES가 정상 구동 안하는 문제	5.0.31
115639	GN-26727	Sensor	[범용OS] 센서와 동일한 DNS를 할당하는 DHCP 서버가 비정상적인 DHCP서버로 감지되는 문제	
115493	GN-25887	WebUI	현황&필터의 노드그룹 내에 다단계의 카테고리 구조에서 하위 카테고리가 표시되지 않음	5.0.42 (LTS), 5.0.45, 6.0.2
115289	GN-26719	WebUI	정책 > 객체 > 시간 메뉴에서 시간 객체 생성시 System Timezone과 관리자 Timezone이 다른 경우 날짜가 잘못 저장되는 문제	5.0.34
115122	GN-26428	Center	콘솔UI를 통한 deb 이미지 업그레이드시 OS 종류에 따라 실패할 수 있는 문제	5.0.42 (LTS), 6.0.12
115022	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
114824	GN-26647	WebUI	시스템 관리화면에 Disk 컬럼 내용 출력되지 않는 문제 개선	5.0.23
114668	GN-25626	WebUI	피방문자 이메일 승인 대상이 관리자임에도 일반 사용자가 검색되는 문제	4.0.M8
114312	GN-26597	WebUI	DB/Log 서버 분리구성 일 경우 쿼리리포트 생성되지 않는 문제	5.0.37
114300	GN-26532	WebUI	NIC 벤더별 현황의 수량 맞지 않는 문제 개선	
114265	GN-26609	WebUI	노드추가필드(사용자선택기-맵핑컬럼명) 사용하여 노드 등록 시 오류 발생하는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
114197	GN-26440	WebUI	태그의 변동사항이 없는데 노드 상세정보 수정 시 함께 업데이트 처리 되는 문제	5.0.22, 6.0.4

continues on next page

Table 10 – continued from previous page

Revision	Key	Components	Description	Affects Versions
114197	GN-26425	WebUI	노드그룹 조건의 사용자 부서 선택 시 데이터에 상위부서가 포함되지 않는 문제	5.0.35
114153	GN-26280	Center	멀티 센서 장비 삭제 이후 재등록될때 센서 승인 상태로 등록되는 문제	6.0.8, 5.0.50
114066	GN-26566	WebUI	노드 정보 업데이트 후, 탭 이동 시 변경한 정보가 갱신되어 보여지지 않는 문제	5.0.50
113986	GN-26476	WebUI	액션별 수행결과 현황 페이지 오류 수정	5.0.50
113970	GN-26299	Center	인증연동 사용자도메인과 다른 도메인인 경우에도 인증 허용 문제	5.0.53
113961	GN-26272	Center	SMTP인증연동 - [계정@[도메인] ID 형식인 경우 사용자 인증 비정상 문제	5.0.53
113769	GN-25776	Center	패스워드가 없는 사용자 및 동기화된 사용자 (READ ONLY) 에 대해서 비밀번호 변경 만료 알림메시지가 나오지 않도록 개선	4.0.18
113732	GN-26549	Sensor	간헐적 dnsmasq 데몬 재시작 증상	6.0.12, 5.0.53
113655	GN-26554	Sensor	우분투NAC 센터/센서장비에서 Too many open file 에러 발생 및 센서 상태 Down 되는 문제	5.0.51, 6.0.11
113594	GN-26319	WebUI	감사로그 화면에서 관리장비명 클릭시 노드관리 검색되지 않고 모두 출력되는 문제	5.0.38
113556	GN-26448	WebUI	Compose 방식 설치후 시스템 목록에서 정책서버 정보가 출력되지 않는 오류	5.0.6
113541	GN-26540	Windows Agent	영문관리콘솔의 플러그인 '적용OS' 선택에서 Windows 11 이 Windows 10으로 잘못 표시됨.	5.0.42 (LTS), 6.0.0
113486	GN-26267	WebUI	감사 > 로그에서 KST 기준 9시 이전에는 오늘의 감사로그가 출력되지 않는 문제	4.0.17
113400	GN-26357	WebUI	신규 노드그룹 상세화면의 대상노드리스트에서 기본현황으로 돌아갈때 구 버전 상세화면 출력되는 문제	5.0.35
113373	GN-26518	Center	에이전트가 수집한 정보 (updateinfo) 가 삭제될수 있는 문제	5.0.52, 6.0.13
113357	GN-26322	macOS Agent	macOS 알림메세지 수신시 CPU 점유율 높아지는 문제	5.0.27
113343	GN-26446	Center	LDAP 연결 실패 시 center 데몬의 fd가 증가하는 문제	5.0.41, 4.0.145, 6.0.0
113322	GN-26444	WebUI	노드그룹 조건의 소프트웨어 설정 창에서 한글검색이 안되는 증상	5.0.35
113315	GN-26496	CLOUD	Cloud site 최초 생성시 로그 통계 데이터가 보이지 않는 문제	5.0.50, 6.0.12
113136	GN-26130	macOS Agent	macOS 하드웨어 정보수집 플러그인 사용시 크래시 발생하는 문제	5.0.38
113084	GN-26040	WebUI	변경노드관리 전체 노드 선택 시 관리자 확인 기능 동작 않는 문제	5.0.26
113044	GN-26414	Windows Agent	비밀번호 검증창의 고정옵션이 off 임에도 주기적으로 화면 중앙으로 위치되는 문제	5.0.42 (LTS), 6.0.12, 5.0.53

continues on next page

Table 10 – continued from previous page

Revision	Key	Components	Description	Affects Versions
113024	GN-26433	Sensor	게이트웨이 IP추가지 IP Rule 이 잘못생성되어 센서 통신이 안될 수 있는 문제	5.0.42 (LTS)
112771	GN-26160	Authsync, Center	CSV를 다운로드 받아 사용자정보 동기화 진행할 때 실패할 수 있는 문제	5.0.0
112754	GN-26385	Packaging	C30G,C50G 장비 모니터 출력 안되는 문제	5.0.44, 6.0.1
112674	GN-26259	Elastic-Search	Advance 페이지의 Elasticsearch 관리툴에서 샤드 정보표시 오류	5.0.17
112643	GN-26223	WebUI	노드 상세화면에서 태그할당 시 태그가 50개만 출력되는 문제	5.0.22
112634	GN-26276	Elastic-Search	Elasticsearch 이중화 구성 되지 않는 문제	5.0.51, 6.0.11
112598	GN-26242	WebUI	구름OS(Linux)에 설치된 에이전트가 관리콘솔의 노드목록에 Windows 아이콘으로 표시 되는 문제	6.0.8, 5.0.50
112530	GN-26316	Center	과거 비밀번호 재사용 방지 기능 사용 시에도 최근 사용 비밀번호로 변경 가능한 문제	3.0_1007
112511	GN-26227	Center	[범용OS] 서버인증서에 Subject Alternative Names 이 없어서 INVALID COMMON NAME 인증서 오류 발생하는 문제	5.0.23
112504	GN-26324	Sensor	5.0.53 버전 이후 버전에서 디스크정보(NAC장비) 수집 안되는 문제	5.0.53
112389	GN-26208	WebUI	검색창에 < 문자가 포함된 검색어를 입력할 경우 XSS 감지로그가 남는 문제	6.0.7, 5.0.50, 4.0.152
112371	GN-26178	WebUI	상세 감사로그 메시지에 포함된 ->로 인해 XSS 발견 로그가 남는 문제	6.0.7, 5.0.50, 4.0.152
112122	GN-25936	WebUI	관리역할 권한설정에 상관없이 동작하는 노드 작업명령이 동작하지 않는 문제	5.0.44, 6.0.1
112106	GN-26219	WebUI	정책 복사시 액션에 라벨이 존재할 경우 오류가 발생하는 문제	4.0.113, 5.0.10
112065	GN-26170	WebUI	영문 관리콘솔의 CWP 디자인 템플렛의 컴포넌트 추가/삭제가 정상동작하지 않는 문제	5.0.48, 6.0.7
111954	GN-26200	Center	ZTNA 및 NAC 최신버전에서 CVE 목록 갱신되지 않는 문제	5.0.50, 6.0.12, 5.0.53
111893	GN-26072	Linux Agent	Linux Agent, GUI Module 미사용으로 동작시 행걸리는 문제	6.0.12
111828	GN-26188	IPMGMT	IP신청시스템 임시사용자 자동로그인 되지 않는 문제	5.0.50, 4.0.153, 6.0.11
111738	GN-25998	Windows Agent	(비밀번호 검증 플러그인)계정의 비밀번호 변경시각이 계속 변경되어 보고되는 문제	4.0.M5, 5.0.0, 6.0.0
111729	GN-25565	Center	Syslog TLS 전송시 센터데몬 비정상 종료	4.1.M7
111670	GN-26175	Center	GDPI를 사용하는 Cloud 서비스에서 GPDB를 계속 다운로드 하는 현상	5.0.41

continues on next page

Table 10 – continued from previous page

Revision	Key	Components	Description	Affects Versions
111620	GN-26106	Windows Agent	네트워크 공유폴더제어에서 공유허용시간 설정시 공유 해제되지 않는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
111587	GN-26137	WebUI	CWP 디자인 템플릿 설정 페이지에서 CWP 페이지 미리 보기 화면이 보이지 않는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
111559	GN-26161	GenianOS	procmond에서 sshd 재구동 오류 수정	5.0.23
	GN-26655	WebUI	Compose 버전에서 노드관리 엑셀 export 시 오류 페이지 발생	5.0.48, 6.0.6
	GN-25944	WebUI	소프트웨어 업데이트 관리에서 메이저 버전이 더 낮지만 업데이트 버튼이 출력되는 문제	5.0.20
	GN-25815	WebUI	IP 신규/반납 신청서의 승인/거부 팝업이 활성화 되어있는 상태에서 승인/거부시 대기상태가 되는 문제	4.1.3

16.3.7 Genian NAC 5.0.54 Release Notes (2023-04-12)

Last Updated: 2023-07-20

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
114720	GN-26368	WebUI	관리자의 API 키가 다른 관리자에게 노출되는 취약점		5.3
114214	GN-26392	WebUI	권한 없는 관리자가 디버그 로그 다운로드 가능한 취약점		2.9
113419	GN-26391	WebUI	권한 없는 관리자가 디버그로그 실시간 보기 가능한 취약점	5.0.0, 6.0.0	2.9
113219	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
117757	GN-26702	WebUI	정책서버에서 외부로 접근이 허용되면 경고를 출력하는 기능	
117448	GN-26769	Linux Agent	Linux Agent, Sigstore 전자서명을 기반한 배포 플러그인 개발	
116767	GN-26826	geniup	UEFI 시스템에서 geniup 수행시 디스크부족 발생하는 문제	
116532	GN-26705	Center	SLSA를 통한 업데이트서버 배포 데이터 전자서명 검증	
116395	GN-26844	Center, Sensor	센서에서 외부로 접근가능여부를 센서정보(공인IP)에 표시	
115885	GN-26786	Center	업데이트서버로부터 받은 WSUSSCN2.CAB 에 대한 전자서명 검증	
114255	GN-26328	WebUI	노드그룹 엑셀다운로드시 노드 그룹명이 포함되게 개선	
114197	GN-26568	WebUI	노드그룹 조건의 소프트웨어 명 포함/미포함 설정 시, 직접 입력 가능하도록 개선	
112796	GN-26148	Center	에이전트 로그인 시 기존 노드와 다른 장비로 판단되면 노드 정보를 즉시 업데이트할 수 있도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
117427	GN-26213	WebUI	노드정책 생성 후 노드그룹을 할당시에 변경하지 않는 옵션값이 변경된 것으로 나타나는 문제	5.0.44
117233	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
117182	GN-26770	Center, Sensor	[범용OS] 센서가 배포서버로 동작하지 않는 문제	5.0.29
117122	GN-26773	WebUI	노드 목록 조회 API에서 노드그룹 조건이 동작하지 않는 문제	5.0.54, 6.0.14
116853	GN-26839	Center, Sensor	정책서버/센서 메모리 릭(지니업데이트 및 노드스캔(https)) 발생 문제	4.0.14
116696	GN-26768	WebUI	노드 추가필드 - 사용자 선택기 설정 옵션이 반영되지 않는 오류	5.0.22
116625	GN-26816	WebUI	노드그룹의 CWP 메시지에 태그가 있는 경우, 출력이 깨지는 오류	5.0.37
116616	GN-26779	WebUI	로그서버(elasticsearch) 정상상태 임에도 경고 메시지 출력되는 문제	5.0.23
116581	GN-26758	Windows Agent	에이전트가 로컬시스템으로 동작하면 프로그램제거 플러그인을 통하여 Store앱 삭제 실패	5.0.42 (LTS), 6.0.0
116343	GN-26623	WebUI	노드관리의 뷰가 IP 관리뷰 일 때 엑셀 내보내기시 IP만 표시가 표시되지 않는 문제	5.0.50
115785	GN-26749	Elastic-Search	[범용OS] Elastic과 통신이 Iptables 정책에 의해서 차단되어 간헐적으로 ES가 정상 구동 안하는 문제	5.0.31

continues on next page

Table 11 - continued from previous page

Revision	Key	Components	Description	Affects Versions
115639	GN-26727	Sensor	[범용OS] 센서와 동일한 DNS를 할당하는 DHCP 서버가 비정상적인 DHCP서버로 감지되는 문제	
115611	GN-26706	WebUI	'노드 추가필드 - 사용자선택기' 텍스트 입력 불가 옵션인 경우 검색팝업 동작하도록 수정	5.0.22
115493	GN-25887	WebUI	현황&필터의 노드그룹 내에 다단계의 카테고리 구조에서 하위 카테고리가 표시되지 않음	5.0.42 (LTS), 5.0.45, 6.0.2
115300	GN-26601	WebUI	관리자의 관리범위를 센서그룹으로 설정 시 매트릭스뷰에서 미사용 IP 선택하지 못하는 문제	4.0.117, 5.0.14
115289	GN-26719	WebUI	정책 > 객체 > 시간 메뉴에서 시간 객체 생성시 System Timezone과 관리자 Timezone이 다른 경우 날짜가 잘못 저장되는 문제	5.0.34
115122	GN-26428	Center	콘솔UI를 통한 deb 이미지 업그레이드시 OS 종류에 따라 실패할 수 있는 문제	5.0.42 (LTS), 6.0.12
115109	GN-26571	Enforcer	CWP사용안함으로 설정해도 센서에서 SYN-ACK 응답이 발생하여 차단 노드가 통신되는 것처럼 보이는 문제	5.0.0
115022	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
114881	GN-26654	macOS Agent	macOS 화면보호기 설정을 사용자가 수동으로 변경시 강제화 안됨	5.0.45, 6.0.2
114824	GN-26647	WebUI	시스템 관리화면에 Disk 컬럼 내용 출력되지 않는 문제 개선	5.0.23
114668	GN-25626	WebUI	피방문자 이메일 승인 대상이 관리자임에도 일반 사용자가 검색되는 문제	4.0.M8
114614	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
114534	GN-26620	Enforcer	IP충돌보호 unknown mac 설정 시 정상 mac이더라도 충돌보호가 걸리는 문제	4.0.17
114312	GN-26597	WebUI	DB/Log 서버 분리구성 일 경우 쿼리리포트 생성되지 않는 문제	5.0.37
114265	GN-26609	WebUI	노드추가필드(사용자선택기-맵핑컬럼명) 사용하여 노드 등록 시 오류 발생하는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
114241	GN-26430	WebUI	클라우드 환경에서 장치사용신청서의 부서트리가 나타나지 않는 문제	5.0.52, 6.0.13
114197	GN-26465	WebUI	노드그룹 조건의 에이전트 액션 수정 시, 기존 설정 값이 기본값으로 선택되지 않는 문제	5.0.45
114197	GN-26440	WebUI	태그의 변동사항이 없는데 노드 상세정보 수정 시 함께 업데이트 처리 되는 문제	5.0.22, 6.0.4
114197	GN-26425	WebUI	노드그룹 조건의 사용자 부서 선택 시 데이터에 상위부서가 포함되지 않는 문제	5.0.35

continues on next page

Table 11 – continued from previous page

Revision	Key	Components	Description	Affects Versions
114153	GN-26280	Center	멀티 센서 장비 삭제 이후 재등록될때 센서 승인 상태로 등록되는 문제	6.0.8, 5.0.50
114066	GN-26566	WebUI	노드 정보 업데이트 후, 탭 이동 시 변경한 정보가 갱신되어 보이지 않는 문제	5.0.50
113986	GN-26476	WebUI	액션별 수행결과 현황 페이지 오류 수정	5.0.50
113972	GN-26587	WebUI	노드관리 부서명 컬럼의 내용이 정상출력되지 않는 문제 개선	6.0.5, 5.0.50
113970	GN-26299	Center	인증연동 사용자도메인과 다른 도메인인 경우에도 인증 허용 문제	5.0.53
113961	GN-26272	Center	SMTP인증연동 - [계정@[도메인] ID형식인 경우 사용자 인증 비정상 문제	5.0.53
113769	GN-25776	Center	패스워드가 없는 사용자 및 동기화된 사용자 (READ ONLY) 에 대해서 비밀번호 변경 만료 알림메시지가 나오지 않도록 개선	4.0.18
113732	GN-26549	Sensor	간헐적 dnsmasq 데몬 재시작 증상	6.0.12, 5.0.53
113655	GN-26554	Sensor	우분투NAC 센터/센서장비에서 Too many open file 에러 발생 및 센서 상태 Down 되는 문제	5.0.51, 6.0.11
113556	GN-26448	WebUI	Compose 방식 설치후 시스템 목록에서 정책서버 정보가 출력되지 않는 오류	5.0.6
113541	GN-26540	Windows Agent	영문관리콘솔의 플러그인 '적용OS' 선택에서 Windows 11 이 Windows 10으로 잘못 표시됨.	5.0.42 (LTS), 6.0.0
113486	GN-26267	WebUI	감사 > 로그에서 KST 기준 9시 이전에는 오늘의 감사로그가 출력되지 않는 문제	4.0.17
113400	GN-26357	WebUI	신규 노드그룹 상세화면의 대상노드리스트에서 기본현황으로 돌아갈때 구 버전 상세화면 출력되는 문제	5.0.35
113373	GN-26518	Center	에이전트가 수집한 정보 (updateinfo) 가 삭제될수 있는 문제	5.0.52, 6.0.13
113357	GN-26322	macOS Agent	macOS 알림메세지 수신시 CPU 점유율 높아지는 문제	5.0.27
113343	GN-26446	Center	LDAP 연결 실패 시 center 데몬의 fd가 증가하는 문제	5.0.41, 4.0.145, 6.0.0
113322	GN-26444	WebUI	노드그룹 조건의 소프트웨어 설정 창에서 한글검색이 안되는 증상	5.0.35
113315	GN-26496	CLOUD	Cloud site 최초 생성시 로그 통계 데이터가 보이지 않는 문제	5.0.50, 6.0.12
113149	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
113129	GN-26353	Authsync	Google G Suite 정보 동기화 시 고정값 설정되지 않는 문제	
113044	GN-26414	Windows Agent	비밀번호 검증창의 고정옵션이 off 임에도 주기적으로 화면 중앙으로 위치되는 문제	5.0.42 (LTS), 6.0.12, 5.0.53
113024	GN-26433	Sensor	게이트웨이 IP추가시 IP Rule 이 잘못생성되어 센서 통신이 안될 수 있는 문제	5.0.42 (LTS)

continues on next page

Table 11 – continued from previous page

Revision	Key	Components	Description	Affects Versions
112796	GN-26655	WebUI	Compose 버전에서 노드관리 엑셀 export 시 오류 페이지 발생	5.0.48, 6.0.6
112796	GN-26119	Windows Agent	무선랜제어에서 대소문자 비교 오류로 인한 연결허용된 AP가 차단되는 문제	4.0.0, 5.0.0, 6.0.0
112796	GN-26118	Windows Agent	프린터정보 수집에서 가상 프린터 수집 제외 설정시 일부 프린터가 제외되는 문제	4.0.0, 5.0.0, 6.0.0
112674	GN-26259	Elastic-Search	Advance 페이지의 Elasticsearch 관리툴에서 샤드 정보표시 오류	5.0.17

16.3.8 Genian NAC 5.0.52 Release Notes (2023-02-22)

Last Updated: 2023-02-22

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
111357	GN-25874	Center	센터 api status 로깅 주기 변경 (1일->10분)	
111357	GN-25860	WebUI	태그 추가 시 감사로그에 설명이 저장될 수 있도록 개선	
111357	GN-25752	WebUI	메모리 위젯 출력의 세분화 및 동작방식 개선	
111357	GN-25710	Center	procmo에서 syslog-ng를 모니터링하도록 추가	
111357	GN-25622	build	실시간 네트워크 인터페이스 트래픽량을 확인할 수 있는 스크립트 추가	
111357	GN-25440	Center	장비 인증 사용 시 미사용노드 자동로그아웃에 의해 일부 노드가 인증해제되는 문제 개선	
111357	GN-24094	Sensor	센서 업그레이드 실패 감사기록 상세화	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
111357	GN-26020	Windows Agent	내용이 없는 프린터 정보 수집으로 대시보드에서 빈정보 출력	4.1.0, 5.0.0, 6.0.0
111357	GN-26019	Center	검색필터 알람전송 SMS 내용에 {_FULLMSG} 포함 시 국제 SMS 전송 실패하는 문제	5.0.19
111357	GN-26005	Genian Syncer	지니안싱커로 한글경로의 파일이 업로드되지 않는 문제	4.0.0, 5.0.0, 6.0.0
111357	GN-25999	Windows Agent	인터페이스 제어 액션으로 무선인터페이스가 유선으로 오탐하여 차단되는 문제	5.0.0, 6.0.0
111357	GN-25927	Ubuntu(Debian)	[범용OS] 웹서버 상태 모니터링 (FTSS) 할 수 있도록 개선	5.0.23
111357	GN-25908	Center	[범용OS] CENTERD STAT - HTTPD가 아닌 APACHE2를 Count 하도록 수정	5.0.50
111357	GN-25846	Database	Ad hoc 네트워크 연결 위험감지의 "알려진 네트워크 자동 포함" 설정 적용되지 않는 문제	5.0.21
111357	GN-25817	WebUI	에이전트 버전현황 위젯에서 노드목록으로 이동 후 페이지 이동 및 작업 수행 시 잘못된 검색조건이 추가되는 문제	5.0.26
111357	GN-25756	Windows Agent	로컬시스템으로 에이전트 동작 시 수동 프록시 설정 않는 문제	4.0.0, 5.0.0, 6.0.0
111357	GN-25675	Center	LDAP 인증연동 설정값이 없으면 Agentless AD SSO 기능 동작하지 않는 문제	5.0.44, 6.0.1
111357	GN-25002	Center	NAT IP 노드등록 기능으로 등록된 노드의 플랫폼 및 타입이 unknown으로 변경되는 문제	4.0.27
111357	GN-24674	WebUI	장치사용신청서에서 부서 할당시 부서 출력 화면에 error: 문구 표시	5.0.42 (LTS), 6.0.0
111039	GN-26008	WebUI	노드그룹 상세화면에서 정책복사 기능 동작 하지 않는 문제	5.0.31
110323	GN-25888	Center	메일서버 및 정보동기화 시, 구글 인증 코드 발급이 안되는 증상	5.0.16, 6.0.0

16.3.9 Genian NAC 5.0.51 Release Notes (2023-02-10)

Last Updated: 2023-03-03

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
111338	GN-26000	MySQL	mysql 버전 업그레이드 5.7.33 -> 5.7.40		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
111187	GN-25994	macOS Agent	macOS 하드웨어 정보 수집 플러그인에 USB 장치 정보 추가	
111028	GN-25928	Genian Syncer	지니안싱커에 불필요하게 출력되는 패치모음 설정 항목 제거	
111028	GN-25891	Windows Agent	수집되는 오픈포트의 개수 제한기능 추가	
111028	GN-25735	WebUI	라이선스 현황 화면에서 라이선스에 에이전트 제한 수량이 있을 경우 출력	
111028	GN-25727	Ubuntu(Debian)	[범용OS] history 이력에 timestamp 출력	5.0.0, 6.0.0
111028	GN-25666	Center	[RADIUS] 감사로그를 로그필터를 통해서 외부 전송할 수 있도록 개선	
111028	GN-25657	WebUI	임시사용신청의 신청서처리결과를 IP 관리에서 메뉴 추가 삭제 가능하도록 수정	
111028	GN-25639	CLI/gnlogin, Database	ssh port 변경시 DB에 즉시 반영되도록 개선	
111028	GN-25625	WebUI	필수항목으로 사용자 추가 필드를 생성하는 경우 필수항목을 표시하도록 수정	
111028	GN-25604	Center	CWP 에이전트설치 메시지 삭제 시 에이전트설치 아이콘 출력되지 않는 문제	3.0_0910
111028	GN-25567	Linux Agent	Linux Agent, 네트워크 정보 수집시 다중 IP, DNS 설정 정보 (IPv4, IPv6) 수집 가능하도록 개선	
111028	GN-25564	Linux Agent	Linux Agent, 로컬 네트워크 변경시 감지 및 관련 추가작업 개발	
111028	GN-25480	Sensor	[범용OS] 디스크 정보 수집시 블록 디바이스 정보가 수집되도록 개선	
111028	GN-25280	WebUI	사용자 생성 wizard 기능 추가	
111028	GN-25269	Center	RADIUS 정책 추가속성에 USER 매크로를 사용가능하도록 개선	
111028	GN-24938	WebUI	이메일 발송의 즉시수행시 수행시점의 노드그룹 데이터로 메일을 발송하도록 수정	
111028	GN-24755	Center	geniupdate 를 통한 BP 공지사항을 NAC 에 적용	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
113084	GN-26040	WebUI	변경노드관리 전체 노드 선택 시 관리자 확인 기능 동작 않는 문제	5.0.26
111241	GN-26035	WebUI	IP 사용 신청서 상세보기에서 다운로드 이미지 클릭시 오류 페이지 발생	5.0.42 (LTS), 5.0.50, 6.0.10
111171	GN-26068	WebUI	[5.0]자동 생성된 대시보드 리포트 클릭시 다운로드 되지 않고 빈 화면으로 이동되는 문제	5.0.50
111067	GN-26063	IPMGMT	CWP에서 IP사용신청 자동로그인 기능이 동작하지 않는 문제	5.0.50, 4.0.153, 6.0.11
111039	GN-26008	WebUI	노드그룹 상세화면에서 정책복사 기능 동작 하지 않는 문제	5.0.31
111028	GN-25979	Center	RADIUS 정책을 여러번 변경시 정책적용 큐가 정상동작 하지 않는 문제	5.0.23
111028	GN-25978	WebUI	스위치 상세화면에서 수정시 패스워드 변경을 하지 않았는데 패스워드 길이 오류 출력되는 문제	5.0.17
111028	GN-25859	Enforcer, Sensor	[범용OS] ubuntu 커널 버전에 대한 nac.ko 모듈 생성 실패로 인한 센서 오작동	5.0.39, 6.0.0
111028	GN-25797	WebUI	선택 노드바구니 비우기 기능 오동작 문제 수정	5.0.44, 6.0.1
111028	GN-25760	WebUI	노드의 IP 정책이 정상적으로 반영되지 않는 문제	4.0.116, 5.0.13
111028	GN-25730	WebUI	노드상세화면에서 ZTNA VPN 으로 등록된 노드 동작방식 잘못출력되는 문제	5.0.32
111028	GN-25712	Windows Agent	DNS제어 플러그인을 통한 Hosts 파일 제어시 한글이 포함되어있으면 오동작하는 문제	4.1.0, 5.0.0, 6.0.0
111028	GN-25694	WebUI	노드의 관리센서를 센서 Alias 로 설정할 수 있는 문제 수정	4.0.119, 5.0.16
111028	GN-25686	Windows Agent	무선연결관리자 OFF 상태에서 트레이아이콘에 무선관련 메뉴 표시 오류	5.0.0, 6.0.0
111028	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
111028	GN-25608	Windows Agent	유선인증관리자로 GTC인증 후 다시 인증정보 받지 않고 자동 인증 되는 문제	5.0.17, 6.0.0
111028	GN-25575	WebUI	노드리포트 검색바에서 달력에 날짜를 선택하면 선택한 날짜와 다른 날짜가 선택되는 문제	5.0.8
111028	GN-25553	WebUI	감사로그 Excel Exporter시 상세정보의 내용이 깨지는 현상	5.0.21
111028	GN-25543	WebUI	SAML2로 사용자 인증 후 노드목록 인증사용자 컬럼에 아이콘 미출력 문제 수정	5.0.19
111028	GN-25507	WebUI	노드 액션의 조건설정에서 조건컬럼에 나타나는 아이콘에 톨팁이 표시되지 않음	4.0.M1
111028	GN-25489	WebUI	노드 관리의 노드 삭제 명령 전송 건수에 상관없이 '(1 건)'으로 표시되는 문제	5.0.44
111028	GN-25242	CLOUD	cloud ztna site 삭제시 elasticsearch index 가 삭제되지 않는 문제	6.0.5

16.3.10 Genian NAC 5.0.49 Release Notes (2022-10-11)

Last Updated: 2022-12-20

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
109588	GN-25753	WebUI	CWP 에서 PAGEFW 파라미터를 통한 불법 경로로 리다이렉트 하지 않도록 개선		4.2
109191	GN-25561	WebUI	노드검색바 Blind SQL Injection 취약점		5.3
108512	GN-25184	Sensor	DNS Cache Poisoning 공격방어를 위해서 Dns-masq 에서 쿼리 결과를 캐쉬하지 않도록 수정		3.7
108069	GN-25193	WebUI	[범용 OS Ubuntu] 관리콘솔 > CWP Design Template 목록 페이지 'X-Frame-Options' Header 가 allowall로 표시되는 문제		6.5
108069	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
109075	GN-25640	WebUI	사용자정의 리포트 트리 메뉴에 내가생성한 리포트만 출력되도록 수정	
108809	GN-25615	Linux Agent	NAC 설치 및 업그레이드 시 리눅스 에이전트 등록 및 업그레이드 누락 추가	
108768	GN-25468	WebUI	액션조건 설정시 레지스트리 값에 공백 허용	
108635	GN-25404	WebUI	[5.0] 노드목록에서 변경정책 적용 버튼 클릭 후 검색된 내용 그대로 출력되도록 개선	
108632	GN-25075	WebUI	공지사항 이미지 업로드 기능 추가	
108465	GN-24693	Windows Agent	인증창 잠금화면에 배경이미지 지원	
108069	GN-25417	macOS Agent	macOS 에이전트 인증창 종료 금지	
108069	GN-25201	macOS Agent	macOS 에이전트 상태 재검사 기능	
108069	GN-25164	GenianOS	인증시마다 소유자를 재설정 시 정보가 갱신된 경우에만 감사로그를 남기도록 개선	
108069	GN-25138	Windows Agent	GnPMS 수행결과를 윈도우즈 업데이트 액션의 결과메시지로 제공	
108069	GN-25137	Linux Agent	Linux Agent, ARP 관리 액션 플러그인 개발	
108069	GN-25112	Linux Agent	Linux Agent, 에이전트 삭제 방식 옵션에 따른 동작 기능 개발	
108069	GN-25100	Database	mysql이 활성화 되지 않은 서버에서 mysql client 동작시 Port 관련 경고 제거	
108069	GN-25089	WebUI	메뉴얼 링크 개선	
108069	GN-25078	Windows Agent	에이전트 인증창으로 화면잠금을 사용중에 모니터 확장에 대한 고려	
108069	GN-25058	WebUI	WAS로 들어오는 요청항목에 대한 전처리 기능 추가	
108069	GN-25054	Linux Agent	Linux Agent, 오류 보고를 위한 Agent 전체 로그 압축 기능 추가	
108069	GN-25046	Enforcer	kernel debug 기능에 권한정보도 출력할 수 있도록 개선	
108069	GN-25033	RADIUS	RADIUS 인증서 등록 개선 및 Windows 11 단말에서 EAP-TLS 연결 실패하는 문제	5.0.42 (LTS)
108069	GN-25027	WebUI	감사로그 필터의 입력항목 글자수 제한 확대	
108069	GN-25025	Windows Agent	무선연결관리자를 통하여 "EAP-TTLS" 인증방법 제공	
108069	GN-25001	WebUI	사용자 화면에서 부서명으로 사용자 검색 기능 추가	
108069	GN-24975	WebUI	엑셀 내보내기 된 파일의 로딩 속도 개선	
108069	GN-24966	WebUI	정책 관리화면에서 링크를 통한 노드목록 이동시 노드관점으로 출력될 수 있도록 파라미터 추가	
108069	GN-24950	Windows Agent	유선인증관리자를 통하여 "EAP-TTLS" 인증방법 제공	
108069	GN-24907	WebUI	[5.0] 노드목록의 컬럼 사이즈 조절 기능 추가	
108069	GN-24903	WebUI	노드그룹 상세화면 조건 목록에 검색기능 추가	
108069	GN-24898	WebUI	리포트 인메이플 선택 목록 조회 관련 기능 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
109433	GN-25755	WebUI	엑셀로 사용자 내보내기시 특정 컬럼 누락 현상	5.0.47
109324	GN-25708	macOS Agent	macOS 에이전트 크래시 발생하는 문제	5.0.45, 6.0.2
109235	GN-25663	macOS Agent	인터넷연결 차단 환경에서 macOS 에이전트 설치 시 IP 입력창 출력	5.0.27, 6.0.0
109214	GN-25720	IPMGMT	임시사용자 IP신규신청이 안되는 문제	4.0.149, 6.0.6, 5.0.49
109161	GN-25645	Center	DHCP노드IP변경시 변경전IP로 만들어진 플랫폼탐지데이터파일(scanraw)이 정리 안되는 문제	4.0.M7
109154	GN-25589	Center	IP변경노드 삭제에 의해서 노드 삭제시 Bad type conversion 에러 발생	5.0.46, 6.0.5
108777	GN-25482	WebUI	정책 그룹의 조건설정을 수정하는 경우, 신규 추가되는 문제	6.0.6, 5.0.49
108772	GN-25481	dbmigration	액션조건 중 레지스트리 설정 관련 데이터 마이그레이션 오류 발생	5.0.48
108769	GN-25032	WebUI	태그해제시각을 무제한으로 설정했음에도 태그에 설정된 기간설정이 적용되는 문제 수정	5.0.21
108727	GN-25086	WebUI	카테고리 미지정에 속하는 리포트 항목 클릭시 오류 발생	5.0.38, 6.0.0
108691	GN-25129	CWP, WebUI	AWS에 AMI 이미지로 운영되는 정책서버에서 SAML 인증연동이 안되는 문제	5.0.19
108399	GN-25520	Center	GPDB를 통한 플랫폼 감지 시 확장 노드타입이 설정되지 않는 문제	5.0.48
108176	GN-25532	WebUI	CWP 에서 사용자 패스워드 변경 시 USER_LASTPWCHANGE 값이 갱신되지 않는 문제	6.0.6, 5.0.49, 4.0.151
108069	GN-25456	macOS Agent	macOS 에이전트 업로드시 Duplicate entry 로그 발생하는 문제	5.0.45, 6.0.2
108069	GN-25402	macOS Agent	macOS 호스트명 변경 플러그인 성공여부 오류	5.0.34, 6.0.0
108069	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
108069	GN-25386	macOS Agent	macOS 프로세스 강제종료 플러그인 동작하지 않음	5.0.0, 6.0.0
108069	GN-25361	Windows Agent	허용된 AP의 SSID가 한글일 때 무선랜제어 플러그인 동작오류	5.0.0, 6.0.0
108069	GN-25357	WebUI	IP신규/반납 신청서의 상세보기 화면에서 승인시 오류 발생	5.0.13
108069	GN-25354	macOS Agent	macOS 공유폴더명에 마침표가 포함되면 정보 수집하지 못하는 문제	6.0.4, 5.0.47
108069	GN-25343	Windows Agent	PC부팅시마다 관리폴더에 대한 공유제어 알림팝업이 띄워지는 문제	5.0.0, 6.0.0

continues on next page

Table 12 - continued from previous page

Revision	Key	Components	Description	Affects Versions
108069	GN-25318	Windows Agent	취약한 비밀번호 사용에도 비밀번호유효성검사 팝업창을 닫을 수 있는 문제	5.0.13, 6.0.0
108069	GN-25301	macOS Agent	macOS 네트워크 공유폴더 해제 오작동 및 글자 깨지는 문제	6.0.4, 5.0.47
108069	GN-25296	Windows Agent	영문 윈도우에서 에이전트 인증창의 기본로고가 한글로 표시됨.	5.0.8, 6.0.0
108069	GN-25222	Linux Agent	Linux Agent, 장기 사용시 간헐적으로 Database Access 오류	6.0.4, 5.0.47
108069	GN-25218	WebUI	fontawesome 아이콘 클릭시 로딩바 출력 문제	6.0.3, 5.0.46
108069	GN-25211	WebUI	설정 > 환경설정 > 관리콘솔 > 인증 > 세션 타임아웃 설정 오류	6.0.1
108069	GN-25163	Windows Agent	노드가 삭제되고 신규로 다시 등록된 노드에 백신정보수집이 바로 되지 않는 문제	5.0.0, 6.0.0
108069	GN-25151	Center	동일한 이름을 가지는 소프트웨어가 여러개 있는 경우 소프트웨어 버전이 같으면/다르면 노드그룹 매칭이 안되는 문제	5.0.37
108069	GN-25136	WebUI	노드 관리 화면에서 만족함/만족안함 컬럼의 카운트가 잘못 출력되는 문제	5.0.33
108069	GN-25130	Genian Monitor	윈도우용 Genian Monitor에서 항목 및 설정 등을 수정 할 수 없음	5.0.0, 6.0.0
108069	GN-25115	WebUI	관리콘솔에서 IP 관리의 신청결과 목록의 컬럼에서 IP주소 컬럼을 제거했으나 반영되지 않는 문제	5.0.10
108069	GN-25091	WebUI	특정 관리역할 할당 후 감사로그 IP, MAC 클릭시 노드 목록 검색 필터가 안되는 증상	4.1.M1
108069	GN-25080	Authsync, Center	관리콘솔에서 설정 변경 시 정보동기화 수행주기 시점에 동기화 수행되지 않는 문제	
108069	GN-25074	Center	폐쇄망에서 이미지 업그레이드시 GPDB를 이용한 신규 기능이 정상동작 하지 않을 수 있는 문제	5.0.0, 6.0.0
108069	GN-25048	Linux Agent	Linux Agent, Tray Icon 간헐적으로 표시 안되는 문제	5.0.42 (LTS), 6.0.0
108069	GN-25044	WebUI	Genian Software 파일업로드시 문제	5.0.2
108069	GN-25029	macOS Agent	macOS Agent에서 무선랜제어 차단시 메시지 팝업되지 않음	5.0.27, 6.0.0
108069	GN-25016	WebUI	신규 노드그룹의 백신정보의 조건 출력 오동작 수정	5.0.31
108069	GN-24998	Authsync	부서정보, 직급정보 동기화시 데이터소스 구분값 설정이 변경되면 동기화가 정상수행되지 않는 문제	4.0.0
108069	GN-24990	WebUI	IP 다중신청서 업로드시 용도 설정이 되지 않은 경우 동일한 검증 메시지가 출력되는 문제	4.0.106, 4.0.148
108069	GN-24972	WebUI	[5.0] 대시보드 탭 수정시 위젯의 위치가 변경되는 문제	5.0.34
108069	GN-24947	WebUI	사용자수정 API 호출 시 비밀번호 마지막 변경시각 컬럼이 수정되지 않는 문제	5.0.43, 6.0.0, 4.0.146
108069	GN-24835	Center	에이전트로 인해 등록되는 노드등록시 MAC정보가 소문자로 저장될 수 있는 문제	6.0.4

continues on next page

Table 12 – continued from previous page

Revision	Key	Components	Description	Affects Versions
108069	GN-24676	WebUI	REST-API 서비스 이용시에 관리자 세션이 유지되는 오류	5.0.14
108069	GN-24675	Ubuntu(Debian)	[범용 OS] NAC deb 파일 생성시 각이 관리콘솔에서 잘못 표시되는 문제	5.0.41

16.3.11 Genian NAC 5.0.48 Release Notes (2022-08-08)

Last Updated: 2022-10-19

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
107566	GN-25438	Center, Sensor	_filelist.html 파일을 센터마다 다르게 생성하도록 개선		3
106931	GN-25306	WebUI	사용하지 않는 HTTP-Method를 통해 사용가능 method 정보가 출력되는 문제		5.3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
108654	GN-24847	WebUI	관리콘솔 인증을 SAML 방식으로 인증하도록 기능 개발	
108399	GN-22808	Center	확장 노드타입을 이용한 노드그룹조건 추가	
108047	GN-25409	WebUI	디버그로그 화면의 접근권한 설정 개선	
107251	GN-25160	Windows Agent	Sophos Endpoint Agent 백신정보 업데이트	
107047	GN-21428	macOS Agent	macOS Agent 단말 네트워크의 내/외부 상태에 따른 액션 정책 적용	
106711	GN-22592	CWP	CWP 디자인템플릿 컴포넌트 설정을 off 했다가 on 할 경우 컴포넌트 위치가 최하단으로 떨어지는 문제	
106691	GN-24962	WebUI	노드 등록시에 설명을 입력할 수 있는 UI 추가	
106677	GN-24961	WebUI	노드 목록 내보내기(다운로드)시에 진행률 표시	
106605	GN-25206	macOS Agent	macOS 에이전트 데몬동작 중단시 프로세스 완전종료	
106605	GN-25149	Windows Agent	윈도우 게스트 계정에 대한 정보수집 가능하도록 개선	
106605	GN-25071	Linux Agent	Linux Agent, 노드 재등록 시 액션이 다시 수행되도록 기능 추가	
106605	GN-25047	WebUI	노드 등록 API 에 노드 커스텀필드 수정 기능 추가	
106605	GN-24983	Linux Agent	Linux Agent, Sophos server protection 정보 수집 기능 추가	
106605	GN-24945	WebUI	노드 목록의 엑셀 출력시 IP소유자/IP소유부서 출력 형태 수정	
106605	GN-24925	WebUI	REST API 사용시 인증에 대한 설명 수정	
106605	GN-24921	Center	ldap 인증연동 및 ldap 정보동기화에서 인증서를 이용한 LDAP서버 연결이 가능하도록 수정	
106605	GN-24894	Enforcer	NAC 커널(Enforcer) 에서 udp 이벤트패킷 전송시 패킷사이즈가 mtu 사이즈보다 크면 정책서버로 패킷전송 안되는 문제	
106605	GN-24879	Linux Agent	Linux Agent, 최신 플랫폼 버전 정보 추가	
106605	GN-24876	WebUI	사용자신청서 용도에 MAC/장비 인증제한 처리옵션 추가	
106605	GN-24862	WebUI	IP/장비 소유자 설정에서 사용자 이름 검색 가능하도록 기능 추가	
106605	GN-24816	Windows Agent	에이전트 인증창에 비밀번호 입력 자동 전환 기능 추가	
106605	GN-24787	Center	동작상태관련 감사로그의 관리장비명이 센서이름으로 표시도록 수정	
106605	GN-24786	WebUI	local.conf의 data-server username 앞뒤에 공백이 있는 경우 웹 콘솔 구동되지 않는 문제 개선	
106605	GN-24768	Linux Agent	Linux Agent 프로세스 강제 종료 플러그인 개발	
106605	GN-24664	Linux Agent	Linux Agent package 전자서명 기능 추가	
614				Chapter 16. Release Notes
106605	GN-24600	Center	사용자 계정 시작 시각 기능 추가	
106605	GN-24330	Windows Agent	KB국민은행 PentaSSO 지속적으로 인증연동가능하도록 수정	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
107843	GN-24914	Genian Syncer	지니안싱커를 통하여 업로드된 패치파일을 다운로드 받지 못하는 문제	5.0.44, 6.0.1
107712	GN-25308	WebUI	관리콘솔이 유희 상태에서 깨어난 후 세션 타임 아웃 시간이 지나도 세션이 유지되는 문제	5.0.42 (LTS), 6.0.0
107423	GN-25380	Sensor	SNMP v2 Community 설정값에 특수문자 포함 시 스위치 등록에 실패하는 문제	6.0.4, 5.0.47
107224	GN-25099	WebUI	사용자등록신청서의 메일 승인시 사용만료일이 반영되지 않는 문제	4.0.M8, 5.0.41
107157	GN-25370	Windows Agent	윈도우 XP에 NAC V5.0 에이전트 설치시 DLL 오류 문제	5.0.47
106972	GN-25287	WebUI	노드상세 정책 > MAC 정책 > 변경금지의 IP LIST 수정시 IPChange Event 호출이 되지 않는 문제	5.0.41
106956	GN-25298	macOS Agent	macOS 에이전트에서 '주기적 수행' 주기의 액션 수행시 수행결과가 '수행전 만족'으로 유지	5.0.11, 6.0.0
106671	GN-25257	WebUI	리포트 메뉴에서 노드 리포트의 필터 메뉴에서 Excel 다운로드 시도 시 오류 발생	5.0.36
106639	GN-25277	Windows Agent	에이전트 빌드시 전자서명 검증 오류 수정	4.0.0, 5.0.0, 6.0.0
106605	GN-25225	Windows Agent	모니터 정보수집 플러그인으로 인한 GnPlugin.exe 비정상 종료	5.0.0, 6.0.0
106605	GN-25215	Windows Agent	운영체제 정보수집 플러그인으로 인한 GnPlugin 미동작 문제	5.0.37, 6.0.0
106605	GN-25200	WebUI	영문UI에서 관리역할 메뉴제한 항목내에 특정항목 한글로 출력되는 오류	4.1.0
106605	GN-25094	macOS Agent	macOS 에이전트에서 AD계정 대체인증시 반복하여 재인증	5.0.7, 6.0.0
106605	GN-25043	MGMT	등록된 외부인증서로 웹서버 (httpd) 구동 안되는 문제	5.0.42 (LTS)
106605	GN-25000	Linux Agent	Linux Agent, 액션 수행 결과 메시지가 잘못 표시되는 문제	5.0.42 (LTS), 6.0.0
106605	GN-24984	Sensor	Secondary IP 가 설정된 인터페이스에 대해서 마지막 Secondary IP 대역만 서브넷스캔 동작하는 문제	5.0.42 (LTS)
106605	GN-24981	Windows Agent	PC에 Teredo Tunneling Pseudo-Interface가 존재할 경우 MAC/IP Clone 탐지 오류	5.0.0, 6.0.0
106605	GN-24967	WebUI	상위 부서의 정보 변경시 부서에 속한 하위 부서 정보가 변경되지 않는 문제	4.0.M9
106605	GN-24946	WebUI	Radius 정책 수정시 오류 메시지 출력 및 변경정책 적용이 정상적으로 되지 않는 문제 수정	5.0.30
106605	GN-24939	Authsync	REST API Server 를 통해서 정보동기화시 Pageing 파라미터값이 잘못적용되어 API 를 호출하는 문제	5.0.38
106605	GN-24919	WebUI	상제리포트 타입으로 정의된 이메일 즉시수행시 오류 발생	5.0.43, 6.0.0
106605	GN-24896	WebUI	IP 다중 신청 목록이 용도에 설정된 IP 처리 대역보다 많은 경우 서브넷을 변경하여 할당하지 않는 문제	4.1.0
106605	GN-24867	Windows Agent	프린터 공유폴더에 대한 공유제어가 안되는 문제	4.0.125, 5.0.22, 6.0.0

continues on next page

Table 13 – continued from previous page

Revision	Key	Components	Description	Affects Versions
106605	GN-24845	WebUI	IP신청시스템 자동거부처리 API 에서 예러가 나타나는 문제	5.0.14
106605	GN-24839	WebUI	IP/MAC 현황에서 엑셀 내보내기 시 오류 페이지 발생하는 문제	4.0.M7
106605	GN-24811	Windows Agent	무선연결관리자에서 사용자ID/PW 저장 해제 후 값이 다시 채워지는 문제	5.0.0, 6.0.0
106605	GN-24798	Center	Google G Suite 정보동기화 및 SAML 인증연동 시 노드의 인증사용자가 검색되지 않는 문제	5.0.19
106605	GN-24792	Linux Agent	Linux Agent, 인증 허용 MAC 정책 기능 동작하지 않는 문제	5.0.41, 6.0.0
106605	GN-24784	IPMGMT	IP사용신청서 결과조회시에 locale값이 변경되는 오류	4.0.114, 5.0.11
106605	GN-24741	WebUI	노드 상세에서 장비내 노드의 다른 노드 이동시 해당 노드의 상세화면이 출력되지 않는 문제	5.0.38
106605	GN-24725	Linux Agent	Linux Agent Debian11 기반 플랫폼에서 트레이 아이콘 표시 안되는 문제	5.0.0, 6.0.0
106605	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
106605	GN-24625	Center	에이전트버전 업그레이드시 에이전트소프트웨어 신규 추가로 처리 되어 대시보드에 업그레이드 현황이 잘못 나오는 문제	4.0.M8
106605	GN-24580	Windows Agent	문서검색&삭제 커스텀 플러그인에서 삭제 실패시 사용자에게 표시되는 메시지 없음	5.0.42 (LTS)
103940	GN-24685	WebUI	차단된 IP 허용옵션을 사용시, 사용예정으로 설정된 차단 IP가 할당되는 문제	4.0.12

16.3.12 Genian NAC 5.0.47 Release Notes (2022-06-10)

Last Updated: 2022-08-19

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
106031	GN-25104	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1q)		5.3
105840	GN-25064	WebUI	웹서비스 취약점 Apache WAS 정보를 노출하지 않도록 개선	4.0.119, 5.0.16	2.5
105198	GN-23947	Windows Agent	윈도우 에이전트 시큐어코딩 점검결과 취약점 패치	5.0.0, 6.0.0	

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
106259	GN-24451	macOS Agent	macOS 네트워크 공유폴더 플러그인 개발	
105732	GN-25062	macOS Agent	macOS 에이전트의 macOS Ventura 지원	
105279	GN-24791	WebUI	매트릭스 뷰에서 관리IP제어범위 설정시 설정된 범위의 내역만 확인하도록 기능 개선	
105198	GN-24924	WebUI	노드목록 가져오기(GET /nodes) API 에 인증사용자 아이디 파라미터 추가	
105198	GN-24918	WebUI	IP할당 시 관리IP 제어범위 옵션에 따라 IP가 제한되게 출력되도록 개선	6.0.4, 5.0.47
105198	GN-24832	WebUI	관리 > 노드 목록 화면에 트리의 전체노드 선택시 미사용 아이피 출력될 수 있도록 개선	
105198	GN-24728	IPMGMT, WebUI	IP사용 신청서에서 Email 승인/거부 버튼링크 파라미터 암호화	
105198	GN-24643	WebUI	위젯 데이터 기준 관점(노드/장비)으로 노드목록을 출력하도록 개선	
105198	GN-24633	WebUI	노드그룹 조건 설정시 '특정시간내에~' 조건의 경우 시간 단위 이외의 단위를 설정 못하는 문제	
105198	GN-24616	Linux Agent	Linux Agent, 정책 및 관리 서버 정보에 대한 무결성 검증 기능 개발	
105198	GN-24562	Windows Agent	에이전트에서 사용되는 웹브라우저 기본값을 "기본 웹브라우저"로 변경	
105198	GN-24548	WebUI	감사 > 로그 > IP 링크에 노드 정보가 tooltip으로 표시되도록 개선	
105198	GN-24545	WebUI	IP 신청 REST API에 센서의 서브넷 파라미터를 추가하여 해당 서브넷의 미사용 IP로 자동할당 될 수 있도록 개선	
105198	GN-24507	Linux Agent	[CC] Linux Agent, 신규 플랫폼 (한컴 구름) 정보 추가	
105198	GN-24464	macOS Agent	macOS Agent 운영체제 정보수집 플러그인에 설치시각 정보 추가	
105198	GN-24463	Linux Agent	[CC] Linux Agent, TLS 통신시 Cipher Suite 고정되도록 개선	
105198	GN-24450	Linux Agent	[CC]Linux Agent, 인증코드를 통한 에이전트 삭제 기능 추가	
105198	GN-24433	Linux Agent	Linux Agent, OS 최신 업데이트 체크를 버전이 아닌 업데이트 항목으로 검사하도록 개선	
105198	GN-24156	WebUI	노드 일괄 등록 시 MAC허용 - 변경금지(지정IP) 설정 가능하도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
106373	GN-25220	Backup	백업 시 비밀번호가 암호화되어 실패하는 문제	6.0.3, 5.0.46
106366	GN-25179	Center	첨부파일메일전송시 MIME 형식이 잘못되어서 첨부파일 사이즈가 0kB 로 표시되고 읽을수 없는 문제	5.0.16
106049	GN-25090	Sensor	호스트명 변경 실시간 감지기능 사용시 메모리 할당 실패에 대한 예외처리 누락으로 센서 죽는 문제	4.0.114, 5.0.11
105962	GN-25132	WebUI	범용OS 우분투 버전에서 '에이전트상태'로 분류된 항목으로 노드그룹 조건추가시 에러 발생	5.0.42 (LTS), 5.0.43, 6.0.1
105739	GN-25085	Center	노드생성시 등록일자/업다운상태 노드그룹 조건에 잘못 매칭되는 문제	4.0.0
105669	GN-24936	WebUI	노드그룹 생성 조건에 출력되는 컴포넌트 항목 수정	5.0.31
105640	GN-25060	Center	장기간 다운에 의한 에이전트 정보 삭제 후 에이전트 재설치 및 로그인 이후에도 에이전트 플랫폼 정보가 업데이트 안되는 문제	5.0.0, 4.0.61
105632	GN-25067	Center, Sensor	[범용OS] 디버그로그가 복수개의 파일에 중복으로 쌓이는 문제	5.0.42 (LTS)
105625	GN-25003	Sensor	센서에서 수집된 노드의 DHCP 정보 전송 실패 이후 센터 재구동되는 문제	4.0.114, 5.0.11
105617	GN-25068	macOS Agent	macOS 모양 및 개인설정 액션 사용시 플러그인 종료되는 문제	5.0.15, 6.0.0
105532	GN-25037	WebUI	노드관리 화면에서 현황 및 필터의 노드그룹 메뉴를 통해 목록 확인 후 재검색 시 오류 발생	5.0.38
105511	GN-25050	Enforcer	Enforcer 커널 모듈에서 메모리 할당 실패 문제	5.0.40
105411	GN-24885	WebUI	사용자 정의 버튼에서 이미지 업로드 시 목차 페이지가 넘어가지 않는 문제	5.0.12
105393	GN-24999	Sensor	가상센서 32개까지만 추가되는 문제	5.0.32
105198	GN-24971	Sensor	센서데몬 hang 증상 문제	4.0.117
105198	GN-24905	Center	스위치 ARP 테이블 정보를 이용해서 노드를등록하는 환경에서 에이전트가 Down상태인데 노드는 UP 상태로 변경되는 문제	6.0.4, 5.0.47
105198	GN-24897	macOS Agent	macOS 모양 및 개인설정 액션 관련 데이터베이스 오류 발생하는 문제	5.0.45, 6.0.2
105198	GN-24864	WebUI	관리콘솔 로그인시 Internal Server Error 발생하면서 로그인이 안되는 문제	5.0.47
105198	GN-24846	WebUI	IP 사용 신청서의 IP 리스트가 용도에 설정된 IP 할당 대역으로 표시되지 않는 문제	5.0.13
105198	GN-24802	Windows Agent	V3백신에 대한 실시간 감시 강제화 제어 옵션이 동작안함.	5.0.0, 6.0.0
105198	GN-24797	Sensor	SNMP 정보수집시 잘못된 데이터형식으로 인한 수집오류	4.1.4
105198	GN-24767	Sensor	NETBIOS 스캔에 의해서 노드의 도메인정보가 업데이트 되지 않는 문제	4.0.M3

continues on next page

Table 14 - continued from previous page

Revision	Key	Components	Description	Affects Versions
105198	GN-24733	Windows Agent	스크립트 수행플러그인에서 수행할 스크립트 내용이 많을 경우 액션정책이 수행안됨.	4.0.16, 5.0.0, 6.0.0
105198	GN-24729	IPMGMT, WebUI	IP사용신청서 Email 승인시 다중신청항목 일괄승인시 오류	4.0.113, 5.0.10
105198	GN-24707	WebUI	관리 > 노드 > 현황및필터 > 액션 > 노드목록 이동 시 결과 출력되지 않는 문제	5.0.33
105198	GN-24701	Windows Agent	외부인증연동 기능 사용시 BASE64 암호화 방식을 사용할 경우 인증연동 미동작 문제	5.0.0, 6.0.0
105198	GN-24665	Backup	외부저장장치를 통해서 백업을 수행하는 경우 로컬디스크에 대한 여유공간확보가 동작 안하는 문제	4.0.19
105198	GN-24649	Center, Windows Agent	제어정책에 권한객체가 다중등록되어있으면 윈도우 방화벽 제어 플러그인에 의한 차단 오동작	5.0.28, 6.0.0
105198	GN-24645	WebUI	현황&필터 태그 화면에서 관리부 편집이 반영되지 않는 문제	5.0.9
105198	GN-24630	WebUI	센터에 등록된 노드의 제어정책 컬럼 툴팁이 잘못 출력되는 문제 수정	5.0.27
105198	GN-24628	macOS Agent	macOS Agent에서 무결성 검사 기능이 정상동작하지 않는 문제	5.0.27, 6.0.0
105198	GN-24626	WebUI	노드상세화면에서 목록 단기 버튼 클릭시 오류 로그 출력되는 문제	5.0.38
105198	GN-24620	WebUI	노드관리 트리의 노드바구니 클릭 후 필터 및 현황의 메뉴 조회시 노드목록 출력되지 않는 문제	5.0.42 (LTS), 6.0.0
105198	GN-24608	Documents	Web 콘솔 스마트도움말과 링크된 DOCS문서 404 에러	5.0.43
105198	GN-24592	WebUI	시스템 로그수집완료시 생성되는 버튼으로 이동된 페이지에 관련 데이터가 나타나지 않는 문제	5.0.40
105198	GN-24568	Windows Agent	무선랜제어로 허용된 AP 가 차단되는 문제	
105198	GN-24560	Windows Agent	에이전트 인증창의 실행옵션에 "%ProgramFiles%" 사용시 "C:\Program Files (x86)" 경로의 파일 수행 안됨.	5.0.0, 6.0.0
105198	GN-24554	WebUI	구(舊) 노드그룹 상세화면에서 조건 삭제 시 페이징 출력 옵션이 원복되는 문제 (255 설정시 50으로 변경)	5.0.12
105198	GN-24523	WebUI	사용자 내보내기시 특정 컬럼 누락 현상(엑셀 형식)	4.0.7
105198	GN-24502	WebUI	노드정책 복사 후 정책 수정시 변경안한 옵션의 값이 수정되는 문제	5.0.44
105198	GN-24449	Windows Agent	프로그램제거 플러그인에서 '선택삭제'버튼 무반응 문제	5.0.42 (LTS), 6.0.0
105198	GN-21894	Center	노드타입: 미분류 노드가 IP/MAC 사용시간 만료시 삭제되지 않는 문제	5.0.31

16.3.13 Genian NAC 5.0.46 Release Notes (2022-04-12)

Last Updated: 2022-06-20

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
104950	GN-24908	WebUI	Tomcat version upgrade (8.5.78)		8.6
104928	GN-24917	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1o)		9.8
104658	GN-24851	Center	Apache HTTP Server 2.4.53 업그레이드		9.8

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
104358	GN-24852	WebUI	노드 관리화면의 노드그룹 트리 출력 쿼리 개선	
	GN-24546	WebUI	관리콘솔의 IP관리에서 할당대상 IP가 차단된 IP 할당을 허용할 때 차단된 IP를 할당가능하게 개선	
	GN-24545	WebUI	IP 신청 REST API에 센서의 서버넷 파라미터를 추가하여 해당 서버넷의 미사용 IP로 자동할당 될 수 있도록 개선	
	GN-24493	macOS Agent	macOS 백신정보 수집 플러그인에 ESET Endpoint Security 정보 추가	
	GN-24469	Center	센서 DHCP노드 IP갱신 기능을 스위치를 통한 노드등록 시에서 적용할 수 있도록 개선	
	GN-24458	Windows Agent	연결할 수 있는 AP가 없으면 무선연결관리자 출력되지 않도록 수정	
	GN-24319	Linux Agent	Linux Agent, 노드 삭제시 재 등록 이벤트 처리 기능 추가	
	GN-24316	Windows Agent	DNS제어 플러그인에서 IP주소와 Host를 매칭되는 설정 값을 제거 할 수 있도록 수정.	
	GN-24312	syslog	syslog TLS 사용시 TLS 1.0 사용하지 않도록 syslog-ng 설정 수정	
	GN-24294	RADIUS	RADIUS 데몬 구동되지 않는 문제 (ADSDOMAINNAME not defined)	
	GN-24281	WebUI	노드명령 REST API 개선	
	GN-24278	WebUI	상태그룹에서 '노드액션'의 플러그인이 할당되었을 때, 노드 액션에서 플러그인을 변경할 수 있도록 개선	
	GN-24267	Center	Agentless AD SSO - 3개 이상의 서버 설정 가능하도록 개선	
	GN-24263	Center	SMTP 인증시 인증 사용자 ID 를 도메인까지 포함해서 표시 하도록 개선 및 인증 감사로그에 인증소스 추가	
	GN-24262	IPMGMT, WebUI	IP 신청서 작성시 승인자를 설정하지 않은 경우 모두전달 옵션에 따라 모든 사용자에게 메일이 전달되는 문제 개선	
	GN-24178	Linux Agent	[CC] Linux Agent Clam antivirus 정보 수집 기능 추가	
	GN-24044	Center	백업을 위한 sftp 설정 시 패스워드가 평문으로 저장되는 문제	
	GN-17595	macOS Agent	macOS 에이전트 장치 제어 플러그인 제작	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
105184	GN-24989	Sensor	DHCP 서버포트(UDP/목적지포트 67)로 dhcp 가 아닌 패킷을 센서가 수신하는 경우에 센서데몬 메모리 증가하는 문제	4.0.11
104996	GN-24906	Center	백신정보/서약동의 정보의 시간관련 노드그룹 조건이 경과하더라도 노드그룹이 변경되지 못하는 증상	3.0_0910

continues on next page

Table 15 - continued from previous page

Revision	Key	Components	Description	Affects Versions
104992	GN-24933	Center	[5.0] keepalive 로그가 옵션에 상관없이 출력되는 부분 개선	5.0.44
104928	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
104907	GN-24789	Sensor	에이전트설치 단말의 FQDN 정보가 센서 NETBIOS 스캔에 의해서 변경되는 문제	4.0.146
104775	GN-24920	WebUI	정보동기화 조건문에 "%" 입력시 에러페이지뜨는 현상	5.0.42 (LTS), 5.0.45, 6.0.2
104775	GN-24829	WebUI	정상적인 정책 적용 데이터 인데 XSS 발견 감사로그가 남는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
104578	GN-24838	macOS Agent	macOS monterey 환경에서 '모니터 정보 수집' 플러그인 사용 시 GnPlugin 프로세스 실행 안됨	5.0.17
104572	GN-24837	macOS Agent	macOS monterey 환경에서 '파일배포' 액션동작시 pkg 설치 파일 실행불가	5.0.45
104246	GN-24817	WebUI	하위 부서별 사용자 목록이 출력이 되지 않는 문제	5.0.45, 6.0.4
104209	GN-24819	Windows Agent	불특정하게 액션정책 무결성 체크 실패로 액션정책이 수행안됨.	5.0.0, 6.0.0
104158	GN-24661	WebUI	백신 관련 노드그룹 필수항목값 누락으로 인한 그룹조건 즉시 수정 안되는 오류	5.0.23
104128	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
104020	GN-24673	VRRPD	[범용OS] HA 환경에서 M->S 전환시 인터페이스 MAC주소가 변경되는 문제	5.0.42 (LTS), 6.0.0
103977	GN-24430	Center	IP관리 메시지 우선: On 설정 시 노드정책에 설정된 CWP 디자인 템플릿이 적용되지 않는 문제	5.0.14
103883	GN-24307	Center, Sensor	IP 로만 구성된 노드그룹의 IP들이 변경 될때 노드롤이 센서로 전달되지 않는 증상 발생	5.0.11, 6.0.0
	GN-24668	Center	수동등록된 스위치를 통해서 등록된 노드의 UP/DOWN 상태가 센서와 동기화 안되는 문제	5.0.36
	GN-24660	Center	노드의 플랫폼 정보가 Microsoft Windows 에서 Unknown Platform 으로 변경되는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
	GN-24631	WebUI	IP신규신청 일괄승인시 미할당IP가 있음에도 할당IP가 없다고 나타나는 문제	6.0.3, 5.0.46
	GN-24577	macOS Agent	macOS 액션조건이 불만족인데도 주기가 항상수행인 일부 플러그인이 동작하는 문제	5.0.0, 6.0.0
	GN-24563	Windows Agent	액션조건이 불만족인데도 주기가 항상수행인 일부 플러그인이 동작하는 문제	5.0.0, 6.0.0
	GN-24496	Center	노드정보 호스트명(NL_FQDN)이 센서 노드정보검사 후 변경되는 문제	4.0.25
	GN-24424	WebUI	노드그룹 상세화면의 대상노드리스트 탭에서 노드 상세 화면으로 이동 후 돌아가기 버튼의 오동작 문제	5.0.31
	GN-24418	Windows Agent	인증창 종료금지상태에서 외부 프로그램에 의하여 종료 될 수 있는 문제	4.1.0, 5.0.0, 6.0.0

continues on next page

Table 15 - continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-24410	CWP	CWP 템플릿 사용시 IP관리메세지 우선 설정 이후 사용자 인증 킴포넌트 사용하면 정상 동작 안하는 오류	4.0.143, 5.0.40
	GN-24407	IPMGMT, WebUI	IP 신규신청 일괄 승인 시 할당 가능한 IP 주소가 부족함에도 동일 IP 주소로 일괄 승인되는 문제	4.1.4
	GN-24406	IPMGMT, WebUI	REST API 를 통한 IP 신규 신청 시 자동승인 미동작	5.0.8
	GN-24360	Windows Agent	에이전트 설치 노드가 에이전트 센서 설치후에도 센터 관리 대역에 계속 존재하는 문제	5.0.40, 6.0.0
	GN-24338	Windows Agent	Windows 보안설정 액션에 대한 반복적인 디버그로그 남는 문제 수정	4.0.109, 5.0.6, 6.0.0
	GN-24329	Windows Agent	알림메시지 및 공지사항 표시할 때 태그 표시 오류	5.0.42 (LTS), 6.0.0
	GN-24327	WebUI	대시보드 위젯 감사로그 필터 추가 시 오류 페이지 발생	4.0.13
	GN-24314	WebUI	대상노드작업의 접속인증페이지(CWP) 조회 시 내 정보 IP 표기 오류	5.0.40
	GN-24303	WebUI	노드그룹 IP/MAC 정보 CSV 일괄 설정시 항목에 조건항목이 출력되는 오류	5.0.43, 6.0.0
	GN-24301	Center	SFTP 백업시 LOG는 SFTP 전송이 되지 않는 문제	5.0.45, 6.0.2
	GN-24300	Windows Agent	에이전트 인증창에서 "인증 후 실행" 옵션 동작 안하는 문제	5.0.0, 6.0.0
	GN-24290	GenianOS	NAC 점검 스크립트(sysinspect) 'Check Setup Config' 수행 시 Warning 발생	4.0.120, 5.0.17
	GN-24245	Windows Agent	정책서버와 통신되지 않는 상황에서 내부네트워크로 표시되는 문제	5.0.43, 6.0.0
	GN-24244	Center	이중화 설정되어있는 장비에서 백업시 오류 메시지가 화면에 표시되는 문제	4.0.119, 5.0.16
	GN-24241	Center	동일 대역에 여러대의 센서가 존재하는 경우 노드타입과 플랫폼이 일반 노드로 등록되는 문제	6.0.0
	GN-24187	Windows Agent	무선연결관리자의 '유선 사용시 숨김' 옵션이 동작하지 않는 문제	5.0.0
	GN-24181	macOS Agent	macOS Agent '에이전트 삭제방식' 적용되지 않는 문제	5.0.41, 6.0.0
	GN-23710	macOS Agent	macOS 에이전트 인증창에서 인증 제한 기능을 사용할 경우 인증 해제 되지 않는 이슈	5.0.17, 6.0.1
	GN-23285	Windows Agent	윈도우셸이 explorer가 아닐 경우 에이전트가 동작하지 않는 문제	4.0.0, 5.0.0, 6.0.0
	GN-22689	WebUI	CLI(conf terminal)에서 hostname 변경시 시스템관리 > 시스템 목록에 장비명(System Name)이 변경되지 않는 문제	5.0.33

16.3.14 Genian NAC 5.0.45 Release Notes (2022-02-09)

Last Updated: 2022-04-12

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
103839	GN-24689	WebUI	감사> 로그> 로그검색에서 XSS가 가능한 문제		4.3
103673	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
103642	GN-24687	WebUI	디버그로그 화면에서 상대경로로 파일 접근 가능한 문제		3.83
102688	GN-24535	WebUI	logstash 제거		5.9

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
103664	GN-24471	WebUI	노드목록에서 부서, 직급, 태그에 관련된 항목을 converter로 출력하도록 개선	
103418	GN-24648	WebUI	노드목록에서 IP소유자 컬럼이 있을 경우 검색 결과가 느려지는 문제 개선	
103069	GN-24302	Center	Webhook 인증 연동 암호화방식 MD5(MD5B64) 가능하도록 매크로 추가 및 응답메세지 캡처기능 제공	
103060	GN-24257	Center	LDAP 인증연동 시 서버 연결 타임아웃 설정 가능하도록 개선	
103056	GN-24198	WebUI	네트워크 객체의 네트워크주소에 특정 도메인이 등록되지 않는 문제	
102925	GN-24557	Center, RADIUS	RADIUS 인증시 노드등록 기능을 옵션설정 기능으로 제공	
102431	GN-24172	WebUI	Bad Request(400) 발생 시 톱캣 버전 정보 출력하지 않도록 수정	
102431	GN-24165	WebUI	인스턴스메시지 내용 입력시 html 태그를 변환하지 않도록 수정	
102431	GN-24082	WebUI	/nodes/{nodeId}/tags API를 통해 노드 태그 외 다른 태그도 추가로 조회할 수 있도록 개선	
102431	GN-24020	WebUI	Applications REST API 에 추가된 기능에 대한 파라미터 추가	
102431	GN-24010	WebUI	센서명 변경시 해당 센서에 속한 노드들의 센서명이 즉시 변경되도록 수정	
102431	GN-23980	Center	쿼리리포트 메일 전송 시 다중 메일 계정으로 메일이 전송되도록 개선	

continues on next page

Table 16 - continued from previous page

Revision	Key	Components	Description	Affects Versions
102431	GN-23964	WebUI, Windows Agent	노드정보-인터페이스 정보에서 연결방식에 가상타입 표시	
102431	GN-23953	WebUI	Self-Sign 인증서 재생성 및 외부에서 생성된 SSL 인증서 등록기능	
102431	GN-23943	Center	영문 감사로그 생성시 한글이 표기되는 부분 개선	
102431	GN-23918	WebUI	하나의 노드정책에 동일한 단독플러그인액션이 둘 이상 들어갈 수 있는 문제	
102431	GN-23880	Linux Agent	Linux Agent, OS 로그인 사용자 변경 또는 로그아웃 & 재로그인시 에이전트 비정상 동작하는 문제	
102431	GN-23869	Windows Agent	5.0 버전 "http URL 인증" 커스텀 플러그인 추가	
102431	GN-23865	Windows Agent	5.0 버전 호스트명 인증 커스텀 플러그인 추가	
102431	GN-23825	Linux Agent	Linux Agent, 센터 접속이 안될 경우 이전 정책으로 액션이 동작하도록 기능 추가	
102431	GN-23817	IPMGMT, WebUI	IP신청시스템 Email 단계별 승인 방식 개선	
102431	GN-23802	WebUI	소프트웨어 업데이트 안내 방식 개선 - 패치 및 업그레이드 분리 제공	
102431	GN-23752	Linux Agent	Linux Agent, 신규 배포판 및 버전 정보 추가	
102431	GN-23749	Linux Agent	Linux Agent, TmaxOS 최신 업데이트 체크 기능 개발	
102431	GN-23722	Linux Agent	Linux Agent, 인터페이스 제어 액션 개발	
102431	GN-23644	GenianOS	부팅시 일부 파일시스템 검사 누락된것 추가	
102431	GN-23468	Center	Webhook API 호출 결과를 이용해서 다른 Webhook API 호출가능하도록 개선	
102431	GN-23221	Windows Agent	IE보안옵션제어 플러그인에 Chrome,Edge 옵션 제어 추가	
102431	GN-23189	macOS Agent	macOS Agent 모양 및 개인설정 플러그인 - 화면보호기, 바탕화면 제어 추가	
102431	GN-22690	WebUI	감사로그 제한 기능 - 노드 관리 범위 제한이 걸려있어도 감사로그는 모든 로그가 표시되는 문제	
102431	GN-22074	WebUI	SAML 인증연동을 2개 이상의 IdP(인증 정보 제공자)를 지원 가능하도록 개선	
102431	GN-21279	CLOUD	AWS SES를 통한 Email 전송시 파일첨부 가능하도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
103820	GN-24691	Center	스위치를 통해서 등록된 노드가 센서에 의해서 등록됨 으 로 로그가 생성되는 문제	5.0.43, 6.0.0
103763	GN-24683	Sensor	센서데몬이 dhcp scan 시작 후 잘못된 메모리 참조로 비정상 종료되는 문제	4.0.2
103728	GN-24724	Windows Agent	외부에서 내부 네트워크 상태로 전환된 후 에이전트 액션 정책이 늦게 적용되는 문제	5.0.40, 6.0.0
103622	GN-24682	WebUI	IP 용도 용도별 승인방식이 자동승인인 경우 역순으로 IP 할당되지 않는 문제	5.0.44, 6.0.2
103616	GN-24684	WebUI	라이선스 화면에서 계정 (genians.com) 로그인시 반응이 없는 문제	5.0.20
103610	GN-24192	WebUI	사용자 태그부여 시 사용자 목록에서 태그가 인증된 노드의 개수 만큼 표기되는 증상	4.0.138, 5.0.35
103519	GN-24617	WebUI	추가된 노드타입 (가상센서, Agent 센서) 이 노드그룹의 설정리스트와 노드목록의 검색필드 조건 항목에서 누락된 문제	5.0.40
103490	GN-24597	Center	에이전트 버전비교 조건대로 노드그룹이 포함되지 못하는 문제	5.0.16, 6.0.0
103388	GN-24678	Sensor	SNMP v3 스위치정보 수집시 일부 정보가 누락되는 문제	5.0.44, 6.0.1
103344	GN-23923	Windows Agent	정보수집 플러그인에서 빈정보 수집하여 노드정보가 삭제되는 문제	5.0.0
103250	GN-24619	Center	수동등록스위치의 노드타입이 노드정보스캔에 의해서 네트워크장비로 변경되는 문제	5.0.14
103217	GN-24644	Center	ARP관리 플러그인 정보 갱신시 간헐적으로 센터데몬이 죽는 문제	5.0.43, 6.0.0, 4.0.146
103103	GN-24485	macOS Agent	macOS Agent 메모리가 지속적으로 증가하는 문제	4.0.0, 5.0.0, 6.0.1
103095	GN-24586	Windows Agent	소프트웨어정보수집 플러그인으로 일부SW가 수집되지 않고 DB에러 발생	5.0.43, 6.0.0
103051	GN-24603	Center	신규제어정책 추가 또는 제어정책 사용함/안함 변경시 제어정책권한 cache를 업데이트 안하는 문제	4.0.M2
102990	GN-24593	Enforcer	가상센서에 등록된 노드에 대해서 healthcheck 를 수행해서 노드상태가 down으로 변경되는 문제	5.0.32
102972	GN-24582	Center	미러센서에서 제어정책 복사시 권한객체가 동작하지 않는 증상	4.0.116, 5.0.13
102967	GN-24598	Enforcer, Sensor	노드그룹 조건에서 '속하지 않으면' AND '속하지 않으면' 설정 시 earlyrole 비정상 동작 수정	4.0.114, 5.0.11
102953	GN-24358	Center	가상센서가 아닌 일반 노드에도 가상센서와 IP가 동일하면 에이전트센서로 설정되는 문제	5.0.40
102924	GN-24559	WebUI	[5.0] 개선된 노드그룹에서 조건설정 변경시 UI에 반영되지 않는 문제	5.0.37
102870	GN-24544	Sensor	WOL 패킷이 잘못된 인터페이스로 전송되는 문제	5.0.40
102839	GN-24375		ES 백업 (Snapshot) 정리 안되는 문제	5.0.42 (LTS)

continues on next page

Table 17 - continued from previous page

Revision	Key	Components	Description	Affects Versions
102799	GN-24350	WebUI	사용중인 노트액션의 설정 변경 시 설정 UI가 정상적으로 출력되지 않는 문제	5.0.45, 6.0.2
102561	GN-24364	WebUI	IP충돌보호 - 다중 MAC 설정되지 않는 문제	5.0.42 (LTS), 6.0.0
102516	GN-24467	WebUI	노드관리 목록에서 직급컬럼 추가시 목록 출력이 되지 않는 문제	5.0.33
102503	GN-24479	WebUI	라이선스가 초과되지 않았는데 NAC 라이선스초과 문구가 출력될 수 있는 문제	4.1.M3
102431	GN-24434	WebUI	노드 상세화면에서 노트타입을 지정 체크박스를 선택했지만 해당 내용이 저장되지 않는 문제	5.0.44, 6.0.1
102431	GN-24415	Authsync	Cloud NAC Oracle 정보동기화 시 라이브러리 경로 오류	5.0.45, 6.0.2
102431	GN-24346	Authsync	[CLOUD] 정보 동기화 수행 완료시까지 오랜 시간이 소요되는 문제	5.0.23
102431	GN-24268	WebUI	노드 스냅샷 리포트 자동생성 실패하는 문제	6.0.0
102431	GN-24261	Center	HA VIP 노드의 Device Type 이 NODE 로 등록되는 문제	5.0.40
102431	GN-24254	RADIUSD	RADIUS 데몬 STOP시 winbind 데몬은 STOP 안되고 계속 남아 있는 문제	5.0.35
102431	GN-24194	Center	사용자 패스워드 업데이트시 사용자 그룹 재적용 안되는 문제	5.0.44
102431	GN-24188	WebUI	메일승인대기 항목의 신청서 우선사용승인 처리 후 화면 이동이 없는 문제	5.0.13
102431	GN-24153	WebUI	IP관리 > 매트릭스 뷰에서 정상적으로 출력되지 않는 매트릭스 존재	4.0.12
102431	GN-24147	WebUI	감사로그 설명 컬럼 툴팁의 태그 표시 문제 수정	5.0.22
102431	GN-24139	Windows Agent	저장장치 정보 수집에 Storage 총용량 잘못수집되는 문제	4.1.0, 5.0.0, 6.0.0
102431	GN-24136	WebUI	노드 액션명에 ,(comma)가 존재하는 경우 노드그룹 설정 값에 이미지 경로가 표시되는 문제	5.0.14
102431	GN-24120	WebUI	관리역할 관리화면 > 서비스역할 생성시 오류 발생	5.0.42 (LTS)
102431	GN-24113	WebUI	관리역할 수정시 메뉴제한 설정 disabled 처리 안되는 오류	5.0.0
102431	GN-24110	Windows Agent	Smart NAC 대체 인증 플러그인으로 잘못된 인증값이 연동되는 문제	5.0.41
102431	GN-24092	WebUI	노드그룹 조건 설정 시, 선택항목에 따라 입력항목이 변경되지 않는 문제	5.0.20
102431	GN-24071	WebUI	CWP 신규 사용자 등록 화면에 본인인증 항목이 출력되지 않는 문제	5.0.42 (LTS), 6.0.0
102431	GN-24011	RADIUSD	RADIUS Attribute 의 갯수가 많은 경우 RADIUS 인증이 실패하는 문제	5.0.24
102431	GN-24005	Center	파일배포 플러그인 https URL 사용시 다운로드하지 못하는 문제	4.0.0, 5.0.0
102431	GN-24002	Linux Agent	Linux Agent, 트레이 아이콘 표시 안되는 문제	5.0.42 (LTS), 6.0.0

continues on next page

Table 17 – continued from previous page

Revision	Key	Components	Description	Affects Versions
102431	GN-23997	WebUI	권한객체의 조건설정에서 객체에 대한 수정 버튼 클릭시 에러 메시지 출력되는 문제	5.0.25
102431	GN-23962	WebUI	권한 객체 ID에 특수문자가 포함된 경우 제어정책에 할당되지 않는 문제	4.0.M8
102431	GN-23952	IPMGMT	http 사용시 IP신청시스템에서 자동로그인 및 로그인이 안되는 문제	5.0.27
102431	GN-23950	Authsync	https를 사용해 csv 정보동기화 시 동기화되지 않는 문제	4.0.5
102431	GN-23949	CWP	신규 사용자 등록 시 피방문자 이메일 승인을 사용 안함에도 승인 요청 메일이 발송되는 문제	4.0.M8
102431	GN-23917	Sensor	가상IP 수동 추가 시 등록되지 않는 문제	5.0.41, 6.0.0
102431	GN-23855	Center	스위치 수동 등록시, 다른 네트워크 대역의 ip로 같은 스위치가 존재하는 경우, 센서 트리 스위치의 정보가 갱신 되도록 개선	4.0.117, 5.0.14
102431	GN-23835	Center	장비 수명주기 관리 추가필드(NI_CUSTOM) 관련 노드그룹 조건을 설정할 수 없는 문제	4.0.129, 5.0.26
102431	GN-23819	WebUI	tomcat webapps 폴더 링크 존재하지 않아 Custom Web Application을 설정할 수 없는 오류	5.0.40
100309	GN-23925	Sensor	Alias IP 로 추가된 인터페이스에 대한 로컬네트워크패킷이 Default Gateway 로 전달 되는 문제	5.0.42 (LTS)

16.3.15 Genian NAC 5.0.44 Release Notes (2021-12-08)

Last Updated: 2022-02-16

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
101696	GN-24305	GNOS	Apache 취약점 조치를 위한 2.4.52 버전 업그레이드		9.8
101621	GN-24253	WebUI	log4j 취약점 개선		9.8

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
104135	GN-23367	Center, RA-DIUSD	RADIUS 2차 SMS 인증 및 속성 (Axcgate-Auth-Type) 추가	
102133	GN-24279	WebUI	[gndbcp] local.conf 에 저장된 DB 패스워드 복호화시 쓰레기 값은 제거하고 복호화 될 수 있도록 수정	
102073	GN-24251	WebUI	OTP 인증키 분실 시 재발급 방법 변경	
101681	GN-24304	WebUI	IP 신청시스템 승인 신청이 느린 문제 개선	
101545	GN-24315	Documents	5.0.44 Global Release	
101504	GN-24265	macOS Agent	macOS Agent 네트워크 정보에 연결된 무선랜의 BSSID 정보 추가	5.0.0
101487	GN-24149	GnBrowser	GnBrowser에서 노드삭제등 일부 기능 동작 안되는 문제	
101421	GN-24190	Center, MySQL	MYSQL/CENTERD 메모리 사용량감소를 위한 conf 설정 변경 및 jemalloc 메모리 할당자 사용	
100942	GN-24432	CLOUD, Containerization, Docker	Update Genian NAC Policy Server Marketplace Product with new AMI (includes log4j fixes)	5.0.44
100942	GN-24151	WebUI	IP신청시스템 용도별 사용 가능 센서 설정 및 조회 API 추가	
100942	GN-24132	macOS Agent	macOS Agent 무선랜제어 플러그인 정보에 프로토콜 정보 추가	
100942	GN-24077	WebUI	mysql 인증 플러그인을 sha256_password로 변경해도 웹 접속 가능하도록 수정	
100942	GN-24059	WebUI	IP신청시 역순 할당 기능 추가	
100942	GN-24020	WebUI	Applications REST API 에 추가된 기능에 대한 파라미터 추가	
100942	GN-23930	WebUI	Custom 암호화 알고리즘 방식 지원	
100942	GN-23896	WebUI	노드 상세화면의 목록쿼리 조회시 JOIN 쿼리 제거 등의 성능 개선	
100942	GN-23895	Authsync	Oracle Database 19c 까지 연동 가능하도록 개선	
100942	GN-23771		시스템 재기동 KeepAlive Down 시에도 가능 하도록	
100942	GN-23658	Sensor	MDNS를 통한 호스트명 탐지 개선	
100942	GN-23635	WebUI	관리역할 편집기능 기본제공	
100942	GN-23618	WebUI	노드관리에서 하드웨어(hardwareinfo) 검색 컬럼에 대한 설명 보강	
100942	GN-23602	gnlogin	DB migration 진행상태를 좀더 알기쉽게 표시	
100942	GN-23583	WebUI	노드관리 목록에서 관리뷰에 사용자정보의 부서명을 추가할 시 부서명 단계가 표시되도록 개선	5.0.41
100942	GN-23570	WebUI	IP 매트릭스뷰에서 다중 선택/해제 가능하도록 기능 추가	
100942	GN-23516	Windows Agent	시스템종료 플러그인에서 종료시 응용프로그램 종료 옵션 추가	
100942	GN-23391	GNOS	최신 드라이버 지원을 위한 Kernel 버전 업그레이드 (5.10)	
100942	GN-23388	WebUI	Agentless ADSSO 설정은 LDAP 인증연도에서 분리	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
102417	GN-24428	WebUI	노드관리 목록에서 관리뷰에 사용자정보의 부서명의 코드가 없을 시에 오류 발생	5.0.44
102412	GN-24506	WebUI	[5.0] 시스템 > 서비스 제어 > 웹어플리케이션 재구동이 정상동작하지 않는 문제	5.0.41
102313	GN-24400	Windows Agent	전자서명 인증서 변경으로 인한 폐쇄망 환경에서 에이전트 업데이트 문제	5.0.0, 6.0.0
102264	GN-24239	WebUI	노드관리 검색에서 태그명으로 검색 되지 않는 문제	4.0.144, 5.0.41
102107	GN-24365	WebUI	액션 수정시 동일한 멀티 플러그인의 액션이 정책에 할당되어 있을때 수정되지 않는 문제	5.0.43, 6.0.0
102094	GN-24341	Center	네트워크대역에 에이전트센서가 등록되어있는 상태에서 동일한 네트워크대역의 에이전트센서가 재등록되는 문제	5.0.40
102041	GN-24176	WebUI	노드 상세화면에서 변경된 항목이 화면 갱신이 없으면 반영되지 않아 보이는 문제	5.0.22
102034	GN-24417	WebUI	노드그룹 조건 중 MAC 주소가 소문자이면 노드가 인식되지 않는 문제	5.0.31
101863	GN-24374	Windows Agent	윈도우즈 xp 에서 에이전트 동작 안되는 문제	4.0.144, 5.0.41
101849	GN-24293	WebUI	노드관리 > 작업선택 > 노드그룹 지정/해제 명령 동작하지 않는 문제	5.0.44, 6.0.1
101793	GN-24362		RADIUSD 에서 정책서버로 SOAP 호출시 417 Expectation Failed 발생하는 문제	5.0.42 (LTS)
101781	GN-24264		네트워크제어 플러그인에서 '자동 규칙 설정'으로 제어시 이상 동작	5.0.28
101739	GN-23675	Genian Syncer	지니안싱커에서 라이선스 파일등록이 안되는 문제	4.0.144, 5.0.41
101705	GN-24167	Center, Sensor	센서관리대상 노드 정보에 센서인터페이스정보가 비어있어 센서에서 노드를 관리할 수 없는 문제	5.0.36
101664	GN-24284	WebUI	IP 신청서 승인화면에서 직접할당시 관리센서를 변경한 후 승인을 할 경우 오류 발생문제	5.0.13
101530	GN-24310	macOS Agent, Windows Agent	5.0.43이상 버전의 에이전트 업데이트시 에이전트 무한반복 재실행되는 문제	5.0.43, 6.0.0
101337	GN-24259	WebUI	소프트웨어 업데이트 UI에서 현재버전(revision이 100000번 이상일때)보다 낮은 버전이 업그레이드 가능에 표시되는 문제	5.0.20
101281	GN-24260	Center	에이전트지정액션 이벤트 전송시 비정상적인 이벤트 프레임이 생성되면서 센터데몬 비정상 종료되는 문제	3.3.1.1009
101266	GN-24202	Center	노드그룹조건이 노드그룹에 속하면(하지않으면) 인데 조건에 해당하는 노드그룹이 사용안함 또는 없는 경우 노드 그룹매칭이 비정상 동작하는 문제	5.0.35
101144	GN-24015	procmond, RADIUSD	정책서버 이중화 구성에서 radius 데몬이 지속적으로 재시작 되는 문제	4.0.143, 5.0.40
101021	GN-24078	Center	스위치 동작상태가 DOWN으로 잘못설정되는 문제	5.0.35

continues on next page

Table 18 – continued from previous page

Revision	Key	Components	Description	Affects Versions
101008	GN-24124	WebUI	노드그룹에서 그룹조건으로 OR연산으로 IP관련조건 추가 시 정책적용시간이 느려지는 현상	5.0.11
100942	GN-24200	WebUI	센서 서버넷 23비트로 설정 후 IP신청서에서 할당 시 2번째 대역 목록 표시가 안되는 문제	5.0.13
100942	GN-24161	WebUI	라이선스 수량이 초과되지 않았지만 노드관리 화면에서 라이선스 수량이 초과되었다는 메시지가 출력되는 문제	5.0.3
100942	GN-24122	WebUI	노드 관리에서 관리뷰 추가 시 설정한 컬럼의 내용이 출력되지 않는 문제	5.0.42 (LTS)
100942	GN-24118	macOS Agent	macOS Agent 소프트웨어 정보수집 플러그인에서 일부 누락되는 문제	5.0.0
100942	GN-24114	WebUI	사용자 목록에서 태그 출력에 대한 문제 수정	5.0.34, 5.0.39
100942	GN-24072	WebUI	Tomcat Context.xml에서 local.conf에 등록된 db 패스워드를 사용하지 못하는 문제	4.0.146, 5.0.44, 6.0.1
100942	GN-24066	Authsync	정상 파일인 경우에도 읽기 실패로 CSV 정보 동기화 실패하는 문제	4.0.146, 5.0.44, 6.0.1
100942	GN-24025	WebUI	작업선택의 노드바구니에 담기 기능이 동작하지 않는 문제	5.0.44, 6.0.1
100942	GN-23948	Sensor	SNMP v3 스위치 SNMP 정보수집이 비정상적인 문제	5.0.41
100942	GN-23845	WebUI	감사로그 > 분석차트로 출력되는 위젯이 로그필터로 필터링 될때 오류 메시지 출력되는 문제	4.0.14
100942	GN-23804	WebUI	스위치 포트 관리자 Down 시 에러메세지 출력 형식 수정	4.0.106
100942	GN-23788	WebUI	IP사용신청서 결과조회 화면에서 사용위치 정렬시 데이터 검색하지 못하는 문제	4.1.0, 4.0.23
100942	GN-23773	WebUI	디버그로그 화면에서 파일 및 폴더 목록 가져오기 개선	
100942	GN-23755	WebUI	[4.0.1] 설정 > 환경설정 > 감사기록에서 Syslog 감사기록 필터 추가/삭제가 정상 동작하지 않는 문제	4.0.145
100942	GN-23625	WebUI	관리콘솔 관리자 계정 AllowIP 설정에 X.X.X.X/0로 설정 시 로그인페이지에서 오류 발생 문제	5.0.41
100942	GN-23609	WebUI	노드 상태검사 최소 주기 옵션 최소값 수정	5.0.38
100942	GN-23599	WebUI	노드 상세화면에서 태그 할당 후 화면갱신 하지 않은 상태에서 삭제 시 삭제되지 않는 문제	5.0.22
100942	GN-23571	WebUI	사용자 정의 버튼 업로드 파일 삭제 후 수정버튼 클릭시 필수입력 값으로 오류출력나지만 파일이 삭제되는 문제	4.0.106
100942	GN-23553	CWP	CWP 사용자 등록 페이지에서 파일 업로드 에러 출력시 html 태그 출력되는 문제	4.0.106
100942	GN-23534	Center	에이전트로 인해 등록되는 노드의 DPI 링크가 표시되지 않는 증상	5.0.39
100942	GN-23519	WebUI	소프트웨어 현황의 수량과 노드관리의 노드 수가 일치하지 않는 문제	5.0.38
100942	GN-23440	Windows Agent	백신정보수집 플러그인을 통하여 백신전체 검사시 네트워크드라이브가 포함되는 문제	4.1.0, 5.0.0
100942	GN-23408	Center	사용자ID에 '문자가 들어가 있는 경우 db 쿼리 에러 발생하는 문제	5.0.18

continues on next page

Table 18 – continued from previous page

Revision	Key	Components	Description	Affects Versions
100942	GN-23275	WebUI	노드리포트 chart에서 UTC 시간으로 표시되는 문제	5.0.22
100942	GN-23217	Authsync	csv 사용자 정보동기화시 csv read 오류가 발생할 경우 전체 사용자가 삭제될수 있는 문제	4.0.1
100942	GN-23026	IPMGMT	IPMGMT 파일업로드 추가필드 기능 오류	5.0.36

16.3.16 Genian NAC 5.0.43 Release Notes (2021-10-06)

Last Updated: 2021-12-09

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
99347	GN-23866		Sophos Anti-Virus 정보 제공 확대	
98871	GN-23723	Sensor	SNMP Switch 정보수집시 Juniper Switch MAC 정보 수집	
98871	GN-23639		노드그룹 목록에서 사용 가능한 OS 이미지가 출력되지 않는 문제(CLOUD)	
98871	GN-23435	Center, CLI/gnlogin	센서 상태 확인 CLI 명령어(show sensor) 필터 개선	
98871	GN-23348	WebUI	정책 > 서비스 객체 생성 및 수정할때 ICMP 프로토콜에 포트 넘버 입력 가능한 문제 개선	
98871	GN-23323	WebUI	노드 > 현황 & 필터 > 위험노드 현황 목록 출력 개선	
98871	GN-23185	WebUI	사용자 기본정보에서 비밀번호변경 강제 시 감사로그 추가	
98871	GN-23175	Center	SNMP를 통한 연결방식 감지시 무선이 우선하도록 개선	
98871	GN-23110	Sensor	에이전트 단말과 센서의 네트워크설정(netmask)이 다른 경우 에이전트에서 keepalive 를 받지 못하는 문제	
98871	GN-22847	Windows Agent	Nets 업체의 ESSO 시스템과 인증 연동되는 SSO 플러그인 개발	
98871	GN-22607	WebUI	노드그룹 IP/MAC 주소 같은면 조건의 다중입력 사항을 CSV 파일을 통해 입력되도록 기능 추가	
98871	GN-22591	WebUI	무선랜 일괄등록 기능 추가	
98871	GN-22542	WebUI	위험노드 현황 기능 추가(내보내기, 검색)	
98871	GN-22536	Windows Agent	에이전트 확장 플러그인 패키지 추가	
98871	GN-21203	Windows Agent	ESTsoft 알약4.0, 5.0 백신 제품 연동	
100321	GN-22966	IPMGMT, WebUI	IP신청시스템에서 신규신청시 엑셀파일을 이용할 때 사용종료일이 반영되지 않는 문제	
100156	GN-23858	macOS Agent	에이전트와 정책서버에서 서로다른 표준시간대 사용에 대한 예외처리 (MacAgent)	5.0.0, 6.0.0
100156	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
99933	GN-23991	Center	에이전트에 의한 노드 등록상태에서 수동스위치에 의한 노드등록시 중복노드 발생	4.0.117, 5.0.14
99919	GN-23891		LDAP 인증연동시 Primary Server 에서 연결실패하는 경우에도 인증시도 하는 문제	5.0.15, 4.0.137

continues on next page

Table 19 – continued from previous page

Revision	Key	Components	Description	Affects Versions
99898	GN-23957		KeepAlive 전송시 센터 도메인에 대한 IP를 캐쉬하는 문제	5.0.15
99579	GN-23890		macOS Agent AD 대체 인증설정 후 OS재부팅시 인증 해제 되는 증상	4.0.124, 5.0.21, 6.0.0
99467	GN-23351	Center, Sensor	NODEPOISONSTATUS를 Agent 설치단말에 한하여 전송하도록 개선	3.4.M6
99439	GN-23935	syslog	로그필터 syslog TLS 연동시 SSL 연결에 대한 Timeout 이 동작하도록 센터데몬 수정	4.0.137, 5.0.34
99427	GN-23946	Sensor	AD SSO 계정 정보에 특정 특수문자 포함 시 syntax 에러 발생하는 문제	5.0.25
99161	GN-23911	Center	SSDP Multicast 를 통해서 User-Agent 정보가 수집된 단말에 대해서 오탐보고가 안되는 문제	5.0.31
98871	GN-23780	WebUI	사용자 관리화면에서 사용자 가져오기 시 USER_PASSCRYPTTYPE 컬럼값이 csv 에 입력한 값으로 저장되지 않는 문제	5.0.41
98871	GN-23761	WebUI	노드정책 생성시 파일패포 액션 할당 불가	5.0.36
98871	GN-23489	WebUI	플랫폼 명에 '(apostrophe)가 포함된 경우 링크 이동하지 않는 문제(노드 플랫폼 위젯)	5.0.20
98871	GN-23460	Windows Agent	인터페이스 제어 플러그인을 통하여 인터넷 연결 공유가 해제되지 않는 문제	4.1.0, 5.0.0
98871	GN-23426	WebUI	라이선스 정보의 장비수와 클릭시 보여지는 노드목록의 노드수가 일치하지 않는 문제	5.0.26
98871	GN-23404	Center	센서의 관리대상 IP에 속하지 않는 노드 삭제시 노드그룹에서 삭제되지 않는 문제	3.5.0
98871	GN-23310	WebUI	전체현황 위젯의 전체 에이전트 수와 노드 검색에서의 수와 일치하지 않는 문제	5.0.22
98871	GN-23306	Sensor	에이전트가 있음에도 센서가 수집한 domain 명으로 노드 정보가 업데이트 되는 문제	4.0.0
98871	GN-23292	Center	무선랜 AP 가 삭제 되어도 노드의 접속 AP 정보는 계속 남아있는 문제	4.0.0
98871	GN-23220	Authsync	CSV 사용자, 부서, 직급 동기화를 하나의 설정으로 사용하는 경우 동기화가 실패하는 문제	4.0.0
98871	GN-23214	WebUI	노드목록 화면과 노드상세 화면에서의 [메모리 전체]가 상이하게 출력되는 문제	5.0.22
98871	GN-23187	Database	SNMP Version 2 (snmpv2) 스위치의 정보가 수집되지 않는 문제	5.0.17
98871	GN-23152	WebUI	리포트 > 이메일발송의 default 제공 일일리포트 메일 폼 수정	5.0.32
98871	GN-23127	WebUI	노드 조건검색에서 AgentActionName 검색시 할당되지 않은 노드가 검색되는 문제	5.0.26
98871	GN-23119	Authsync	정보 동기화 오류 발생 시 WebUI의 최근 동기화 상태정보가 업데이트되지 않는 문제	5.0.17
98871	GN-22821	WebUI	'노드 타입' 위젯에서 에이전트 센서, 가상센서 노드타입이 미표시되는 문제	5.0.40
98871	GN-22720	WebUI	노드상세 화면에서 정책 변경시 수정 버튼이 출력되지 않는 현상(특정 케이스 한함)	4.1.3
98770	GN-23851	Center	노드 IP 변경시 MAC 이 동일함에도 노드가 신규로 등록 되는 문제	4.0.118, 5.0.15

continues on next page

Table 19 – continued from previous page

Revision	Key	Components	Description	Affects Versions
101202	GN-23938		Scheduler 타입이 한번 실행 (ONCE_AFTER) 인 경우 Scheduler 비정상 동작문제	5.0.42 (LTS)
100960	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
100871	GN-24133	Center	OR 조건으로 노드그룹 업데이트시 노드그룹이 변경되지 않는 문제	5.0.11
100858	GN-24166	WebUI	적용범위가 포함된 노드액션에서 적용범위를 전체로 수정시 오류 메시지 발생	5.0.43, 6.0.0
100828	GN-24162		잘못된 인터페이스의 MAC 주소를 가지고 서버넷스캔 수행하는 문제	3.4.M2
100500	GN-24085	WebUI	사용자 관리화면에서 사용자 가져오기 시 패스워드 입력되지 않는 문제	5.0.40
100471	GN-24129	Center	노드 관리범위 제한설정시 로그필터에 의한 감사기록 전송 안되는 문제	5.0.36
100443	GN-24101	Sensor	네트워크객체 및 권한객체 생성시 커널에서 네트워크 객체 참조 오류	3.5.0, 4.0.0, 5.0.0, 6.0.0
100397	GN-24089	Windows Agent	Keep Alive 소켓 생성에 실패할 경우 에이전트 재시작 전까지 노드 DOWN으로 유지되는 문제	4.0.142, 5.0.39
100361	GN-24070	WebUI	에이전트 트레이 메뉴를 통한 사용자 인증 페이지 호출시 오류 메시지 출력되는 문제	5.0.14
100315	GN-24075		외부인증 연동시 사용자패스워드에 특수문자(, ' , ")를 사용하는 경우 인증실패 발생하는 문제	4.0.145, 5.0.42 (LTS), 6.0.1
100301	GN-24074		에이전트(4.x) 정보 업데이트(updateinfo) 요청이 SQL Injection 구문으로 탐지되어 업데이트 실패하는 문제	4.0.145, 5.0.42 (LTS)
100275	GN-23914		사용자ID 정규식 적용시 센터데몬 비정상 종료되는 문제	5.0.41

16.3.17 Genian NAC 5.0.42 (LTS) Release Notes (2021-08-03)

Last Updated: 2024-02-02

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
99990	GN-23981	macOS Agent, Windows Agent	에이전트에 UDP 이벤트의 패킷 조작을 통한 비정상 종료 문제		3.4
99971	GN-23966	WebUI	CWP 사용자 신청시 Excel 파일로 신청되는 경우 XSS 공격 가능 취약점		6.8
99958	GN-23965	WebUI	Agent Download 페이지에서 상대경로를 통한 내부 파일 다운로드 취약점	5.0.37	5.2
99939	GN-23967	WebUI	REST API Command Injection		6.7

continues on next page

Table 20 – continued from previous page

Revision	Key	Components	Description	Affects Versions	CVSS Score
99906	GN-23970	WebUI	모바일 앱을 이용한 관리자 로그인 우회 취약점		6.1
99893	GN-24014	Center	HTTP로 호출가능한 SOAP/REST 제한		2.5
99808	GN-23972	Center, Sensor	UDP event 패킷처리시 데몬 비정상 종료 가능한 문제	5.0.36	6.4
99621	GN-23700	Center	(KVE-2021-1061) 노드에 인증된 사용자가 아님에도 비밀번호를 변경할 수 있는 취약점		8.7
99370	GN-23794	WebUI	REST API 호출시 유효한 인증 토큰이 존재하지 않아도 호출 가능한 문제		4.9
98838	GN-23708	Center	인증처리가 미비한 센서관련 API 보완		4.6
98803	GN-23701	Windows Agent	(KVE-2021-1062) Agent 파일 생성시 상대경로를 사용할 수 있는 취약점		6.1
98787	GN-23714	Center	인증처리가 미비한 에이전트관련 API 보완		4.6
98177	GN-23743	Center	API를 통한 서비스 거부 공격(DoS, Denial of Service) 취약점 개선		6.4
98077	GN-23705	WebUI	(KVE-2021-1062) Conf Engine 에서 파일 업로드 컴포넌트의 이름 유효성 체크 강화		6.7
98062	GN-23488	WebUI	[SaaS] SaaS 보안인증 WAS(Tomcat) 취약점 개선		7.5
98026	GN-23699	Center, Sensor	(KVE-2021-1061) 센서정보 없이 모든 노드의 정보를 얻을 수 있는 취약점		
97987	GN-23706	Center	내부적으로 사용되는 SOAP API가 RPC를 통해 외부로 노출된 취약점		
97918	GN-23702	WebUI	(KVE-2021-1062) CWP Design Template 에서 SSTI 취약점		
97654	GN-23663	macOS Agent, Windows Agent	에이전트 OpenSSL 1.1.11 업데이트		9.8
97647	GN-23662	GNOS	openssl 버전 1.1.11로 업그레이드	4.0.146, 5.0.44, 6.0.1	9.8
97400	GN-23358	WebUI	[CC] Web 취약성 점검결과 보안		6.5
97376	GN-23563	Center	Command injection 공격 방어를 위한 수정		8
97135	GN-23578	WebUI	REST API 취약점 개선		6.8
97106	GN-23446	gnlogin, WebUI	비밀번호에 특정단어를 사용할 수 없도록 처리		8.7
96939	GN-23500	Center	SQL Injection 방어 처리방법 개선		8.7
96917	GN-23499	GNOS	GNOS 내부 취약한 LD_LIBRARY_PATH 환경 변수 제거		
96905	GN-23533	Center	사용불가 플러그인이 에이전트로 전달되지 않도록 개선		7.6

continues on next page

Table 20 – continued from previous page

Revision	Key	Components	Description	Affects Versions	CVSS Score
96752	GN-26051	WebUI	5.0 WebUI lib 취약점 항목 점검		
96752	GN-25119	macOS Agent	macOS Agent, OpenVPN(2.5.7) 및 OpenSSL(1.1.1q) 최신 버전으로 업그레이드		5.3
96752	GN-23377	GNOS	openssh 버전 8.6p1 으로 업그레이드		
96752	GN-23237	GenianOS	Apache httpd(2.4.48) / tomcat(8.5.63) 업그레이드		7.5
96752	GN-23233	Elastic-Search	[CC] elasticsearch 5.6.16 버전으로 업그레이드		8.8
96752	GN-23055	WebUI	시큐어코딩 점검 결과 취약점 패치 - javascript	5.0.42 (LTS)	
96752	GN-22473	Center	시큐어코딩 점검 결과 개선 - 불충분한 랜덤 값 사용		7.5
121387	GN-26315	WebUI	2단계 인증에서 인증코드 입력값 횟수제한, 시간제한하도록 개선		4.3
120388	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
118679	GN-26383	WebUI	html/script 코드 주입 가능한 취약점		5.3
117607	GN-26865	WebUI	대시보드 위젯 설정에서 XSS 입력 취약점		1.2
117077	GN-26835	Center	데이터 업데이트에 사용되는 SQL을 통한 Command Injection 취약점		6.6
116659	GN-26814	Center	Bufferoverflow 에 대한 코드 개선		2
116166	GN-26833	Sensor	센서의 NMDB 업데이트 과정에서 nmap 스크립트 변조 취약점		4.1
115661	GN-26725	Linux Agent, macOS Agent, Windows Agent	[Agent] 센터 및 센서에서 전송된 이벤트에 대한 유효성 검사 추가		6.3
114952	GN-26696	Sensor	센서의 수신 이벤트에 대한 검증 미흡		6.3
114940	GN-26694	Center	다운로드 URL 검증 미흡으로 인한 Parameter Injection 취약점		6.6
114720	GN-26368	WebUI	관리자의 API 키가 다른 관리자에게 노출되는 취약점		5.3
114214	GN-26392	WebUI	권한 없는 관리자가 디버그 로그 다운로드 가능한 취약점		2.9
113219	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 20 – continued from previous page

Revision	Key	Components	Description	Affects Versions	CVSS Score
112785	GN-26286	WebUI	Google OTP 2단계 인증에서 보안키를 신규로 발급받아 2단계 인증을 통과할 수 있는 문제		6.5
111844	GN-26205	Database	mysql 버전 업그레이드 5.7.40 -> 5.7.41		
111338	GN-26000	MySQL	mysql 버전 업그레이드 5.7.33 -> 5.7.40		
111257	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
111018	GN-25982	WebUI	WebUI Response Header에 CSP, HSTS Header 추가		
110496	GN-25875	Windows Agent	에이전트가 웹브라우저 실행할 때 High권한 가지는 문제	4.0.0, 5.0.0, 6.0.0	3.3
110230	GN-25925	IPMGMT, WebUI	IP 신청시스템 > IP 신청 화면 XSS 가능한 문제		5.4
110145	GN-25740	WebUI	감사 > 로그 > 로그검색바에서 XSS가 가능한 문제		5.6
109992	GN-25847	WebUI	CWP 화면에서 사용자 정보 수정 페이지 접근시 재인증 절차 추가		4.2
109588	GN-25753	WebUI	CWP 에서 PAGEFW 파라미터를 통한 불법 경로로 리다이렉트 하지 않도록 개선		4.2
109191	GN-25561	WebUI	노드검색바 Blind SQL Injection 취약점		5.3
108512	GN-25184	Sensor	DNS Cache Poisoning 공격방어를 위해서 Dns-masq 에서 쿼리 결과를 캐시하지 않도록 수정		3.7
107566	GN-25438	Center, Sensor	_filelist.html 파일을 센터마다 다르게 생성하도록 개선		3
106931	GN-25306	WebUI	사용하지 않는 HTTP-Method를 통해 사용가능 method 정보가 출력되는 문제		5.3
106031	GN-25104	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1q)		5.3
105840	GN-25064	WebUI	웹서비스 취약점 Apache WAS 정보를 노출하지 않도록 개선	4.0.119, 5.0.16	2.5
104950	GN-24908	WebUI	Tomcat version upgrade (8.5.78)		8.6
104928	GN-24917	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1o)		9.8
104658	GN-24851	Center	Apache HTTP Server 2.4.53 업그레이드		9.8
103839	GN-24689	WebUI	감사>로그>로그검색에서 XSS가 가능한 문제		4.3

continues on next page

Table 20 – continued from previous page

Revision	Key	Components	Description	Affects Versions	CVSS Score
103673	GN-24651	Center, macOS Agent, Windows Agent	OpenSSL 최신버전으로 업데이트 (OpenSSL 1.1.1n)	4.0.0, 5.0.0, 6.0.0	7.5
103642	GN-24687	WebUI	디버그로그 화면에서 상대경로로 파일 접근 가능한 문제		3.83
102688	GN-24535	WebUI	logstash 제거		5.9
101696	GN-24305	GNOS	Apache 취약점 조치를 위한 2.4.52 버전 업데이트		9.8
101621	GN-24253	WebUI	log4j 취약점 개선		9.8
100546	GN-24030	GNOS	제품에 포함된 netcat(nc) 명령에서 reverse shell 기능 제거		
100181	GN-23977	macOS Agent, Windows Agent	에이전트에서 인스턴트 메시지 표시할 때 존재하는 XSS 취약점 수정		6.8

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
98450	GN-23626		비밀번호 암호화 방식 SHA256 에서 BASE64_DECODE(UNHEX(HASH)) 된 HASH 값 지원	
98219	GN-23396	WebUI	XSS Filter 적용 개선	
97909	GN-23568	WebUI	관리 > 노드 상세에서 오탐보고시 감사로그에 XSS 탐지 로그가 남는 문제	
97598	GN-23622		부팅시 syslog 구동에 오랜시간이 소요되는 문제 해결을 위한 debug 로그 처리 방법 개선	
97530	GN-23564	Linux Agent	Linux Agent, 도메인을 통한 센터 접속 및 동작 기능 개발	
97530	GN-23443	Linux Agent	Linux Agent 사용자 인증 기능 추가	
97530	GN-23350	Linux Agent	Linux Agent 트레이 메뉴 및 프로그램 정보 화면 표시 기능 개발	
97530	GN-23211	Linux Agent	Linux Agent Tray Icon 표시 기능 추가	
97530	GN-23084	Linux Agent	Linux Agent 액션 수행 조건 검사기능 추가	
97530	GN-22890	Linux Agent	Linux Agent 수행 조건만 검사 액션 추가	
97231	GN-22531	Center, Sensor	Cloud 센터와 On-Prem 센서간의 SSL 터널을 통한 정보동기화 및 인증연동	

continues on next page

Table 21 – continued from previous page

Revision	Key	Components	Description	Affects Versions
97192	GN-23015	macOS Agent, Windows Agent	에이전트 삭제방식 옵션을 글로벌옵션에서 노드 정책으로 변경	
97188	GN-22891	Linux Agent	Linux Agent 액션 정책 할당 및 수행 결과 전송 기능 추가	
97188	GN-22247	Windows Agent	에이전트 알림메시지 사용시 자동 팝업 옵션 추가	
97188	GN-22123	Windows Agent	에이전트 인증창에서 인증전에 특정 URL을 표시할 수 있는 기능 제공	
96928	GN-22798	Center	RADIUS 인증패킷을 이용한 노드등록시 인증이 실패하는 경우에도 노드 등록되는 문제	
96924	GN-22961	Center	RADIUS Attribute를 이용한 장비/노드 정보 업데이트	
96874	GN-22594	WebUI	관리 > 노드 > 그룹 트리 및 노드그룹에 속한 노드 목록 쿼리 개선	
96752	GN-24546	WebUI	관리콘솔의 IP관리에서 할당대상 IP가 차단된 IP할당을 허용할 때 차단된 IP를 할당가능하게 개선	
96752	GN-23369	Windows Agent	에이전트 액션 검사조건의 해쉬값 옵션에 SHA2-256도 체크가능하도록 추가	
96752	GN-23260	Windows Agent	에이전트 윈도우 11 지원	
96752	GN-23190	macOS Agent	macOS 에이전트의 macOS Monterey 지원	
96752	GN-23131	Windows Agent	인터페이스제어 플러그인에서 반복된 제어 관련한 불필요 로그 제거	
96752	GN-23049	CWP	CWP 신규 사용자 등록 화면에 본인인증 기능 추가	
96752	GN-23047	WebUI	인증만료 전 알림 기능 OFF 설정 가능하도록 개선	
96752	GN-23003	Linux Agent	Linux Agent 액션 수행 주기 설정 기능 추가	
96752	GN-22997	WebUI	노드 관리범위 제한이 센서그룹인 경우 IP주소 관리에서 제한된 센서만 출력되도록 개선	
96752	GN-22982	Windows Agent	백신연동 플러그인에 Check Point Endpoint security 제품의 상세정보 추가	
96752	GN-22968	WebUI	IP사용신청서 결과조회 화면에서 신청일자 기간 검색 기능 제공	
96752	GN-22967	WebUI	IP사용신청서 결과조회 화면에서 커스텀 필드에 대한 빠른검색 제공	
96752	GN-22960	Windows Agent	백신연동 플러그인에 Trend Micro APEX one 제품의 상세정보 추가	
96752	GN-22956	Windows Agent	GnBrowser에 관리되는 접속목록에 대한 표시이름 설정기능 추가	
96752	GN-22885	WebUI	노드정책 상세화면에서 위험감지 할당 다이얼로그에 아이콘 추가	
96752	GN-22856	WebUI	IP신청서 다중신청시 1건의 메일로 결과를 받을 수 있도록 개선	4.1.3

continues on next page

Table 21 – continued from previous page

Revision	Key	Components	Description	Affects Versions
96752	GN-22852	macOS Agent	macOS 에이전트 설치시 정책서버 IP 정보가 없으면 입력 받도록 개선	
96752	GN-22823	Windows Agent	소프트웨어 정보수집 플러그인에 Microsoft Store 항목 추가	
96752	GN-22813	Center	센서 이미지 업데이트 명령 수행에 대한 감사기록 추가	
96752	GN-22698	WebUI	메일서버/SMS 설정 사용안함 기능 추가	
96752	GN-22694	WebUI	IP 신청 시스템의 IP 검색기 다이얼로그에서 검색시 빈괄호가 표시되는 문제	
96752	GN-22597	WebUI	이메일 발송기능에 사용자정의 리포트 파일첨부 기능 추가	
96752	GN-22595	WebUI	사용자정의 리포트의 노드 리포트(추이리포트) 생성시 수행주기를 주기적 수행만 동작하도록 개선	
96752	GN-21939	Windows Agent	프로그램제거 플러그인으로 Microsoft Store 로 설치된 항목 제거	
96752	GN-19733	Database	기본 로그필터에 IP Conflict 로그필터 추가	
96752	GN-16843	WebUI	관리 > IP관리 목록에 DHCP 사용현황 정보 추가	
122237	GN-27164	VRRPD	[범용OS] 이중화 구성 master 상태로 전환 후 인터페이스 상태검사 실패로 인해 slave 상태로 전환되는 문제	5.0.42 (LTS)
121890	GN-27248	Linux Agent	Linux Agent, 다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
120404	GN-27146	Center	extauth 를 통한 외부인증연동 실패시 사용자가 입력한 패스워드가 센터디버그파일에 남는 문제	
120180	GN-27207	Windows Agent	다중정책서버를 사용할 때 에이전트에서 서버 이벤트 검증 가능하도록 개선	
120022	GN-27206	Center, Sensor	센터에서 신뢰할 수 있는 nodeid 를 센서와 에이전트로 내려보내는 기능 추가	
119948	GN-27013	WebUI	markdown으로 설정된 항목을 변환할 수 있도록 개선	
119667	GN-27031	Center, Sensor	[범용OS] Ubuntu OverlayFS 모듈에서 발생하는 로컬 권한 상승 취약점	
119029	GN-27038	WebUI	openssh 버전업 이후 webssh 접속되지 않는 문제 개선	
118334	GN-27010	GenianOS	GNOS OpenSSH버전 업그레이드(8.6p1->9.3p2)	
118211	GN-26981	Center, Linux Agent, macOS Agent, WebUI, Windows Agent	배포 플러그인 V2 사용시 승인창 표시 되지 않도록 기능 개선	
117757	GN-26702	WebUI	정책서버에서 외부로 접근이 허용되면 경고를 출력하는 기능	

continues on next page

Table 21 – continued from previous page

Revision	Key	Components	Description	Affects Versions
117372	GN-26755	Center, Linux Agent, macOS Agent, WebUI, Windows Agent	Sigstore 전자서명을 기반한 배포 플러그인 개발	
116767	GN-26826	geniup	UEFI 시스템에서 geniup 수행시 디스크부족 발생하는 문제	
116681	GN-26792	Center, Sensor	정책서버 수신 이벤트 검증 강화	
116532	GN-26705	Center	SLSA를 통한 업데이트서버 배포 데이터 전자서명 검증	
116395	GN-26844	Center, Sensor	센서에서 외부로 접근가능여부를 센서정보(공인IP)에 표시	
115885	GN-26786	Center	업데이트서버로부터 받은 WSUSSCN2.CAB 에 대한 전자서명 검증	
111632	GN-26135	macOS Agent	macOS 파일배포 옵션 추가 및 파일 실행 관련 로직 개선	5.0.35
110499	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
108047	GN-25409	WebUI	디버그로그 화면의 접근권한 설정 개선	
105732	GN-25062	macOS Agent	macOS 에이전트의 macOS Ventura 지원	
101681	GN-24304	WebUI	IP 신청시스템 승인 신청이 느린 문제 개선	
101421	GN-24190	Center, MySQL	MYSQL/CENTERD 메모리 사용량감소를 위한 conf 설정 변경 및 jemalloc 메모리 할당자 사용	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
99898	GN-23957		KeepAlive 전송시 센터 도메인에 대한IP를 캐쉬하는 문제	5.0.15
99161	GN-23911	Center	SSDP Multicast 를 통해서 User-Agent 정보가 수집된 단말에 대해서 오탐보고가 안되는 문제	5.0.31
98925	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
98900	GN-23786	Center	가상센서에 다수의 스위치를 등록시 노드가 업다운 되는 오류 개선	5.0.35
98850	GN-23824	Center	감사기록 보존기한이 지나지 않은 감사기록이 삭제될 수 있는 문제	4.1.3

continues on next page

Table 22 – continued from previous page

Revision	Key	Components	Description	Affects Versions
98770	GN-23851	Center	노드 IP 변경시 MAC 이 동일함에도 노드가 신규로 등록되는 문제	4.0.118, 5.0.15
98717	GN-23828	WebUI	[5.0] 대시보드 > 센서맵이 출력되지 않는 문제	5.0.41
98697	GN-23739		Microsoft Store 로 설치된 일부 앱이 삭제 후 프로그램 제거 플러그인 삭제 리스트에 설치상태로 표시되는 문제 수정	5.0.42 (LTS)
98331	GN-23565	Windows Agent	인테페이스 제어 정책을 통해 기본 장치를 제외한 인터페이스 차단시 IP가 변경되면 오동작하는 문제	4.0.0, 5.0.0, 6.0.0
98260	GN-23419	Sensor	AXGATE 센서에서 네트워크 객체 변경시 갱신되지 않는 문제	5.0.40
98246	GN-23581	Center	2차 인증 사용시 패스워드변경 강제 동작하지 않는 문제	4.0.145, 5.0.42 (LTS), 6.0.0
98241	GN-23641	Sensor	SNMPv3 password가 변경될 경우 switch discovery 동작오류 수정	5.0.17
98198	GN-23725	WebUI	사용자 정의 버튼에서 정보수집 버튼 사용시 장비 수명 주기 항목 입력 안되는 오류	5.0.11
98193	GN-23729	WebUI	사용자 생성시 패스워드 암호화 방식이 HMAC-SHA256 으로만 설정되는 오류	5.0.42 (LTS)
98169	GN-23707	Center	webhook 인증연동시 x-www-form-urlencoded 방식이 지원되지 않는 문제	5.0.35
98036	GN-23395	Windows Agent	GnPlugin 미동작시 반복 재실행되도록 수정	4.0.0, 5.0.0
97901	GN-23142	Enforcer	CWP Redirection 이 아닌 패킷 차단에 대한 제한감사기록 동작하지 않는 문제	5.0.40
97889	GN-23656	WebUI	SNMP Switch 일괄설정시 v3 설정이 불가능한 문제	5.0.17
97875	GN-23630	WebUI	RADIUS 정책 수정에서 연산이 변경되지 않는 문제	5.0.30
97866	GN-23529	Sensor	soap 통신 실패 후 recovery 동작시 누락된 정보를 가져오도록 개선	4.0.123, 5.0.20
97675	GN-23616		VPN사용환경하의 macOS Agent에서 TouchBar MacAddress 사용으로 인한 중복노드 발생	4.0.0, 5.0.0, 6.0.1
97649	GN-23637		macOS BigSur 화면보호기 정보가 '사용 안함'으로 수집되는 증상	5.0.15, 6.0.0
97625	GN-23673	Authsync	정보동기화시 \$문자를 이용한 치환식이 포함된 컬럼명이 있는 경우 정보동기화 실패 문제	5.0.42 (LTS), 6.0.0
97612	GN-23669	Windows Agent	윈도우 64비트에서 NAC 4.X 버전을 5.0 버전으로 업데이트할 때 정책서버 IP 입력 대화상자 표시 오류	5.0.41, 6.0.0
97609	GN-23586		사용자정의 버튼의 파일 업로드 시 Slave와 동기화되지 않는 문제	5.0.36
97605	GN-23664	WebUI	log2migration이 정상동작하지 않는 문제	5.0.41
97479	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
97418	GN-23617	Sensor	센서가 센터보다 먼저 업그레이드된 경우 노드 동작 상태가 계속해서 UP/DOWN 반복 변경되는 문제	5.0.38
97412	GN-23612	WebUI	빠른검색에서 노드목록으로 이동 후 페이지 처리가 되지 않는 문제	5.0.38

continues on next page

Table 22 – continued from previous page

Revision	Key	Components	Description	Affects Versions
97386	GN-23528	WebUI	노드의 에이전트액션(파일 배포) 수행시 패스워드 확인에 실패하는 문제	4.0.4
97350	GN-23606	WebUI	노드정책 노드액션 설정 중 패스워드 입력 후 진행이 되지 않는 문제	5.0.42 (LTS)
97339	GN-23590		4.0 업그레이드시 관리콘솔이 구동되지 않는 문제	4.1.M5
97317	GN-23601		grub.conf에 GNTARGET=S_i686 설정된 장비 업그레이드시 부팅불가 현상	4.0.12
97288	GN-23595	Center	netsnmp lib 업그레이드로 인한 정책서버 snmptrap 전송 실패	4.0.145, 5.0.42 (LTS)
97112	GN-23575	WebUI	정책에서 액션할당할때 관리자 인증을 거쳐야 하는 플러그인임에도 인증 다이얼로그가 출력되지 않는 문제	5.0.41
97064	GN-23562	Database	제품 업그레이드 이후 백업시 오류메시지가 발생하는 문제	5.0.41
96853	GN-23498		사용자정보 동기화 수행시 MySQL 오류 발생되면 무한루프에 빠지는 문제	3.3.3
96768	GN-23397	WebUI	노드관리 화면에 IP 매트릭스 뷰 전환 버튼이 사라지는 문제	5.0.38
96752	GN-27135	WebUI	업그레이드 이후 파일배포V2 항목 최초 수정시에 글로벌 설정으로 등록 안되는 오류	5.0.42 (LTS), 5.0.50, 4.0.156, 5.0.56 (50 LTS)
96752	GN-26676	gnlogin	[범용OS] gnlogin 명령시 감사기록에 ADMIN, ADMINIP 가 남지 않는 문제	5.0.23
96752	GN-26101	WebUI	5.0.42 LTS 에서 개선된 UI의 노드그룹 조건설정에서 선택한 선택항목으로 내용이 반영되지 않는 문제	5.0.31
96752	GN-25815	WebUI	IP 신규/반납 신청서의 승인/거부 팝업이 활성화되어있는 상태에서 승인/거부시 대기상태가 되는 문제	4.1.3
96752	GN-25319	WebUI	노드목록에서 NodeType 조건을 여러개 입력해서 조회할 때 오류 페이지 출력되는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
96752	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
96752	GN-25043	MGMT	등록된 외부인증서로 웹서버(httpd) 구동 안되는 문제	5.0.42 (LTS)
96752	GN-24981	Windows Agent	PC에 Teredo Tunneling Pseudo-Interface가 존재할 경우 MAC/IP Clone 탐지 오류	5.0.0, 6.0.0
96752	GN-24971	Sensor	센서데몬 hang 증상 문제	4.0.117
96752	GN-24675	Ubuntu(Debian)	[범용OS] NAC deb 파일 생성시각이 관리콘솔에서 잘못 표시되는 문제	5.0.41
96752	GN-24660	Center	노드의 플랫폼정보가 Microsoft Windows 에서 Unknown Platform 으로 변경되는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
96752	GN-24523	WebUI	사용자 내보내기시 특정 컬럼 누락 현상(엑셀 형식)	4.0.7

continues on next page

Table 22 - continued from previous page

Revision	Key	Components	Description	Affects Versions
96752	GN-24300	Windows Agent	에이전트 인증창에서 "인증 후 실행" 옵션 동작 안하는 문제	5.0.0, 6.0.0
96752	GN-23442	WebUI	IP 매트릭스뷰에서 센서가 출력되지 않는 문제	5.0.40
96752	GN-23411	WebUI	노드리스트 엑셀 다운로드시 노드 관점으로만 출력되는 문제	5.0.38
96752	GN-23328	Sensor	ARP Bomb 위험감지 설정의 임계치를 초과하지 않아도 위험노드로 감지되는 문제	4.0.106
96752	GN-23298	Center	cloud 환경에서 시스콜렉트 동작 오류 문제	5.0.33
96752	GN-23215	WebUI	누락된 리소스 번들 내용 추가	5.0.30, 5.0.41
96752	GN-23214	WebUI	노드목록 화면과 노드상세 화면에서의 [메모리 전체]가 상이하게 출력되는 문제	5.0.22
96752	GN-23172	WebUI	IP신규신청 시 /24 Prefix 보다 작은 네트워크센서의 유동 IP 할당 문제	4.1.M3
96752	GN-23141	macOS Agent	macOS 파일배포 시 지정경로에 파일이 저장되지 않는 문제	5.0.0
96752	GN-23102	WebUI	CONF값 초기화 시 캐스팅 오류로 초기화 중단되지 않도록 개선	
96752	GN-23092	WebUI	사용자 신청서 결과조회 사용기간 항목이 '항상'으로 표시되는 문제(일반계정 용도)	4.0.5
96752	GN-23071	CLOUD	[CLOUD] 원격 센서의 디버그 파일이 호스트명(IP)으로 구분되지 않는 문제	5.0.27
96752	GN-23024	Center	USER_CUSTOM 매크로가 동작하지 않는 문제	4.0.114, 5.0.11
96752	GN-22996	WebUI	센서 트리에서 센서 그룹 대상 내보내기 시 전체 노드로 내보내기 되는 문제	5.0.38
96752	GN-22969	WebUI	IP신청서 추가필드명 변경사항이 IP사용신청서 결과조회 화면의 조건검색에 반영 안되는 문제	4.0.M9
96752	GN-22935	WebUI	노드그룹 조건 설정에서 IP 주소 영역 입력시 마지막 IP 설정이 변경되는 문제	4.0.M8
96752	GN-22932	Sensor	미러환경에서 가상센서단말에 대한 제어가 동작하지 않는 문제	5.0.32
96752	GN-22909	WebUI	관리노드에서 파일 내보내기 엑셀 자료에 장비명/센서명이 누락되는 문제	5.0.38
96752	GN-22861	WebUI	노드관리 검색의 NIC Vendor가 정상적으로 검색되지 않는 문제	5.0.38
96752	GN-22855	WebUI	MAC 주소 형태의 검색 시 빠른검색과 노드검색시 결과가 상이한 문제	5.0.38
96752	GN-22851	WebUI	웹플러그인 Verify.gnc 파일이 정상적으로 생성되지 않아 플러그인 업로드시 오류 발생 문제	5.0.41
96752	GN-22839	WebUI	노드 그룹 카테고리 생성 팝업 시 화면 멈춤 현상	5.0.36
96752	GN-22815	WebUI	관리콘솔에서 오류 발생시 로그가 출력되지 않는 문제	5.0.41
96752	GN-22791	WebUI	관리역할 추가/삭제 시 감사로그 생성되지 않는 문제	4.0.M5

continues on next page

Table 22 - continued from previous page

Revision	Key	Components	Description	Affects Versions
96752	GN-22755	WebUI	시스템관리의 장비유형 검색시 페이지 오류 발생	5.0.36
96752	GN-22749	WebUI	노드목록에서 동작상태가 ACTIVE인 경우 마지막 동작 시각이 현재시간으로 표시되는 문제	5.0.26
96752	GN-22715	WebUI	감사 > 로그 > 디버그로그 화면에서의 기능오류	5.0.40
96752	GN-22681	WebUI	현황&필터 및 위젯에서 링크 이동 후에 관점이나 목록 수를 변경하면 타이틀이 전체노드로 변경되는 문제	5.0.38
96752	GN-22618	WebUI	사용자(관리자) 설정 화면 오류	5.0.22
96752	GN-22481	Windows Agent	윈도우를 통한 GTC 인증 수행시 인증대화상자가 여러개 겹쳐출력되는 문제	5.0.17
96752	GN-22464	macOS Agent	macOS 업데이트시 지정시각 검사를 사용할 경우 오동작 하는 문제	5.0.11
96752	GN-22395	macOS Agent	macOS 에이전트 설치가 안되는 문제	5.0.0
95819	GN-23340	Center	ldap 인증연동/정보동기화 실패하는 문제	5.0.42 (LTS)
121835	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
121508	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
121453	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)
121397	GN-27388	Center	[범용OS] webssh 접속 안되는 문제	5.0.42 (LTS)
121374	GN-27203	Windows Agent	불특정하게 액션수행결과가 변경되어도 일정시간(5분) 후에 전송하는 문제	5.0.0, 6.0.0
121201	GN-27322	Center, Sensor	[범용OS] 시스템관리 > 환경설정 > 타임존 설정이 우분투 NAC 에서 동작 안하는 문제	5.0.50
121163	GN-27259	Linux Agent	Linux Agent, 특정 패키지로 에이전트 설치시 동작하지 않는 문제	5.0.45, 6.0.2
121135	GN-27359	gnlogin, VR-RPD	이벤트재전송처리가 필요없는 프로세스에서도 이벤트큐 처리가 동작하여 Same event already exist in queue 디버그 로그가 발생하는 문제	5.0.42 (LTS)

continues on next page

Table 22 – continued from previous page

Revision	Key	Components	Description	Affects Versions
121020	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)
120606	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)
120537	GN-27091	Center, procmond	센서에서 보내는 이벤트로그 (procmond 프로세스)가 정책 서버에서 unknown center did 에러 발생하면서 로그 저장 안되는 문제	5.0.42 (LTS)
120522	GN-27113	Center	Slave 장비에서 전송되는 업데이트 정보 (sysinfo)를 unknown devid 로 업데이트 실패하는 문제	4.0.145, 5.0.42 (LTS), 6.0.1
120509	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
120376	GN-27215	WebUI	5.0버전에서 관리 > 스위치 > 그룹 클릭 시 오류 페이지 출력 문제	5.0.42 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
120146	GN-27237	Center, Sensor	관리 콘솔에서 센서에 등록된 에이전트노드삭제시 센서에 의해서 노드가 즉시 재등록 안되는 문제	5.0.42 (LTS)
120003	GN-27154	WebUI	스위치 관리에서 스위치를 삭제하였으나 노드 목록에서 접속장치 컬럼의 링크가 동작하는 문제	5.0.38
119826	GN-27137	macOS Agent	macOS 메시지 팝업 내용이 보이지 않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 6.0.14
119732	GN-27183	Center, Sensor	정책서버에서 센서로 전송하는 재등록이벤트 (REGISTER_REQ)가 센서에서 처리되지 않는 문제	5.0.42 (LTS)

continues on next page

Table 22 - continued from previous page

Revision	Key	Components	Description	Affects Versions
119539	GN-27162	Sensor	[범용OS] 장비 부팅후 gdcid 데몬이 구동되지 않는 문제	5.0.42 (LTS)
119516	GN-27151	geniup	마이그레이션 도중 명령어가 종료되어 마이그레이션이 정상 수행되지 않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
119406	GN-27132	gnlogin	mysql 패스워드에 % 문자열 존재시 센터 비정상 동작하는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
119366	GN-27084	WebUI	XSS 검사로직에서 URLEncode 처리된 파라미터에 대한 오답으로 인해 감사로그가 남는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
119354	GN-27127	Windows Agent	윈도우즈 업데이트 플러그인을 통한 Offline PMS 수행 실패	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
119158	GN-27106	Center	노드정책 즉시적용 시 일부 노드만 적용되는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
119099	GN-27089	macOS Agent	macOS Agent 관리콘솔에 의한 무결성 체크 명령시 Gn-Daemon 재기동 되는 문제	5.0.42 (LTS), 5.0.54, 6.0.15, 5.0.56 (50 LTS)

continues on next page

Table 22 - continued from previous page

Revision	Key	Components	Description	Affects Versions
118935	GN-26972	Center	SLAVE 장비가 존재하는 경우 'BadQuery=Illegal mix of col-lations' 오류가 발생하는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
118840	GN-27037	MGMT	[범용OS] 관리콘솔 포트와 HTTPS 포트를 동일하게 설정하는 경우 apache 구동 안되는 문제	5.0.42 (LTS)
118784	GN-27066	Windows Agent	파일배포V2에서 스크립트 수행시 CMD창 표시 오류 수정	5.0.42 (LTS), 4.0.156, 6.0.16 (LTS), 5.0.55 (LTS), 5.0.56 (50 LTS)
118601	GN-26870	WebUI	EDR 에서 NAC 연동을 통한 대응 정책 설정시 NAC 노드에 태그가 할당되지 않는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
118391	GN-26973	macOS Agent	macOS 사용자 알림메시지 주기적 수행시 팝업 되지 않는 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 6.0.14
118367	GN-27016	Sensor	localconf의 서비스포트가 센서데몬에 의해서 불특정 값으로 변경되는 문제	NoVersion
118224	GN-26969	WebUI	Get Parameter(QueryString) 관련 XSS 오탐 문제	5.0.42 (LTS), 5.0.50, 5.0.53, 5.0.54, 4.0.155, 6.0.15
117922	GN-26970	Center	Push Notification 이벤트처리 개선버전 에이전트임에도 정책서버에서 과거 이벤트처리방식으로 이벤트처리하는 문제	5.0.42 (LTS), 4.0.155
117233	GN-26852	Center, Ge-nian Syncer	Syncer 를 통한 지니데이터 업로드시 Mobilebrowser 데이터가 업데이트 안되는 문제 및 CVE 데이터 버전 갱신 안되는 문제	4.1.0
117182	GN-26770	Center, Sensor	[범용OS] 센서가 배포서버로 동작하지 않는 문제	5.0.29
116853	GN-26839	Center, Sensor	정책서버/센서 메모리 릭(지니업데이트 및 노드스캔(https)) 발생 문제	4.0.14
116616	GN-26779	WebUI	로그서버(elasticsearch) 정상상태 임에도 경고 메시지 출력되는 문제	5.0.23
116581	GN-26758	Windows Agent	에이전트가 로컬시스템으로 동작하면 프로그램제거 플러그인을 통하여 Store 앱 삭제 실패	5.0.42 (LTS), 6.0.0

continues on next page

Table 22 - continued from previous page

Revision	Key	Components	Description	Affects Versions
115785	GN-26749	Elastic-Search	[범용OS] Elastic과 통신이 Iptables 정책에 의해서 차단되어 간헐적으로 ES가 정상 구동 안하는 문제	5.0.31
115639	GN-26727	Sensor	[범용OS] 센서와 동일한 DNS를 할당하는 DHCP 서버가 비정상적인 DHCP서버로 감지되는 문제	
115493	GN-25887	WebUI	현황&필터의 노드그룹 내에 다단계의 카테고리 구조에서 하위 카테고리가 표시되지 않음	5.0.42 (LTS), 5.0.45, 6.0.2
115289	GN-26719	WebUI	정책 > 객체 > 시간 메뉴에서 시간 객체 생성시 System Timezone과 관리자Timezone이 다른 경우 날짜가 잘못 저장되는 문제	5.0.34
115122	GN-26428	Center	콘솔UI를 통한 deb 이미지 업그레이드시 OS 종류에 따라 실패할 수 있는 문제	5.0.42 (LTS), 6.0.12
115022	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
114668	GN-25626	WebUI	피방문자 이메일 승인 대상이 관리자임에도 일반 사용자가 검색되는 문제	4.0.M8
114312	GN-26597	WebUI	DB/Log 서버 분리구성 일 경우 쿼리리포트 생성되지 않는 문제	5.0.37
114300	GN-26532	WebUI	NIC 벤더별 현황의 수량 맞지 않는 문제 개선	
114265	GN-26609	WebUI	노드추가필드(사용자선택기-맵핑컬럼명) 사용하여 노드 등록 시 오류 발생하는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
114197	GN-26440	WebUI	태그의 변동사항이 없는데 노드 상세정보 수정 시 함께 업데이트 처리 되는 문제	5.0.22, 6.0.4
114197	GN-26425	WebUI	노드그룹 조건의 사용자 부서 선택 시 데이터에 상위부서가 포함되지 않는 문제	5.0.35
113769	GN-25776	Center	패스워드가 없는 사용자 및 동기화된 사용자(READ ONLY)에 대해서 비밀번호 변경 만료 알림메시지가 나오지 않도록 개선	4.0.18
113594	GN-26319	WebUI	감사로그 화면에서 관리장비명 클릭시 노드관리 검색되지 않고 모두 출력되는 문제	5.0.38
113556	GN-26448	WebUI	Compose 방식 설치후 시스템 목록에서 정책서버 정보가 출력되지 않는 오류	5.0.6
113541	GN-26540	Windows Agent	영문관리콘솔의 플러그인 '적용OS' 선택에서 Windows 11이 Windows 10으로 잘못 표시됨.	5.0.42 (LTS), 6.0.0
113486	GN-26267	WebUI	감사 > 로그에서 KST 기준 9시 이전에는 오늘의 감사로그가 출력되지 않는 문제	4.0.17
113357	GN-26322	macOS Agent	macOS 알림메세지 수신시 CPU 점유율 높아지는 문제	5.0.27
113343	GN-26446	Center	LDAP 연결 실패 시 center 데몬의 fd가 증가하는 문제	5.0.41, 4.0.145, 6.0.0

continues on next page

Table 22 - continued from previous page

Revision	Key	Components	Description	Affects Versions
113322	GN-26444	WebUI	노드그룹 조건의 소프트웨어 설정 창에서 한글검색이 안되는 증상	5.0.35
113044	GN-26414	Windows Agent	비밀번호 검증창의 고정옵션이 off 임에도 주기적으로 화면 중앙으로 위치되는 문제	5.0.42 (LTS), 6.0.12, 5.0.53
113024	GN-26433	Sensor	게이트웨이 IP추가시 IP Rule 이 잘못생성되어 센서 통신이 안될 수 있는 문제	5.0.42 (LTS)
112771	GN-26160	Authsync, Center	CSV를 다운로드 받아 사용자정보 동기화 진행할 때 실패할 수 있는 문제	5.0.0
112754	GN-26385	Packaging	C30G,C50G장비 모니터 출력 안되는 문제	5.0.44, 6.0.1
112674	GN-26259	Elastic-Search	Advance 페이지의 Elasticsearch 관리툴에서 샤드 정보표시 오류	5.0.17
112511	GN-26227	Center	[범용OS] 서버인증서에 Subject Alternative Names 이 없어서 INVALID COMMON NAME 인증서 오류 발생하는 문제	5.0.23
111738	GN-25998	Windows Agent	(비밀번호 검증 플러그인) 계정의 비밀번호 변경시각이 계속 변경되어 보고되는 문제	4.0.M5, 5.0.0, 6.0.0
111620	GN-26106	Windows Agent	네트워크 공유폴더제어에서 공유허용시간 설정시 공유 해제되지 않는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
111587	GN-26137	WebUI	CWP 디자인 템플릿 설정 페이지에서 CWP 페이지 미리 보기 화면이 보이지 않는 문제	5.0.42 (LTS), 5.0.50, 6.0.11
111559	GN-26161	GenianOS	procmond에서 sshd 재구동 오류 수정	5.0.23
111463	GN-26028	Windows Agent	프로세스 강제종료 액션정책이 여러 개 존재할 경우 강제 종료 미동작 문제 수정	5.0.25
110998	GN-26047	WebUI	[4.0/5.0] 대시보드 > 센서맵 출력되지 않는 문제 수정	5.0.42 (LTS)
110786	GN-25995	WebUI	IP 주소 관리에서 노드등록 시 노드삭제금지 적용 안되는 문제	5.0.40
110781	GN-25964	Windows Agent	에이전트 인증창 업그레이드 후 인증 후 실행 옵션이 사라지는 문제	5.0.42 (LTS), 6.0.3, 5.0.46
110210	GN-25903	macOS Agent	macOS 파일배포 플러그인 파일 미업로드시 에이전트 오 동작하는 문제	5.0.31, 6.0.0
110062	GN-25863	WebUI	노드관리 검색어에 &가 있을 경우 동작하지 않는 문제	5.0.42 (LTS), 5.0.49, 6.0.8
109755	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
109725	GN-25750	Windows Agent	인증창에서 잘못된 URL으로 웹브라우저가 열리는 문제	5.0.0, 4.0.123

continues on next page

Table 22 – continued from previous page

Revision	Key	Components	Description	Affects Versions
106972	GN-25287	WebUI	노드상세 정책 > MAC 정책 > 변경금지의 IP LIST 수정시 IPMChange Event 호출이 되지 않는 문제	5.0.41
106366	GN-25179	Center	첨부파일메일전송시 MIME 형식이 잘못되어서 첨부파일 사이즈가 0kB 로 표시되고 읽을수 없는 문제	5.0.16
106049	GN-25090	Sensor	호스트명 변경 실시간 감지기능 사용시 메모리 할당 실패에 대한 예외처리 누락으로 센서 죽는 문제	4.0.114, 5.0.11
105962	GN-25132	WebUI	범용OS 우분투 버전에서 '에이전트상태'로 분류된 항목으로 노드그룹 조건추가시 에러 발생	5.0.42 (LTS), 5.0.43, 6.0.1
105640	GN-25060	Center	장기간 다운에 의한 에이전트 정보 삭제 후 에이전트 재설치 및 로그인 이후에도 에이전트 플랫폼 정보가 업데이트 안되는 문제	5.0.0, 4.0.61
105632	GN-25067	Center, Sensor	[범용OS] 디버그로그가 복수개의 파일에 중복으로 쌓이는 문제	5.0.42 (LTS)
105511	GN-25050	Enforcer	Enforcer 커널 모듈에서 메모리 할당 실패 문제	5.0.40
105184	GN-24989	Sensor	DHCP 서버포트(UDP/목적지포트 67)로 dhcp 가 아닌 패킷을 센서가 수신하는 경우에 센서데몬 메모리 증가하는 문제	4.0.11
104928	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
104775	GN-24920	WebUI	정보동기화 조건문에 "%" 입력시 에러페이지뜨는 현상	5.0.42 (LTS), 5.0.45, 6.0.2
104775	GN-24829	WebUI	정상적인 정책 적용 데이터 인데 XSS 발견 감사로그가 남는 문제	5.0.42 (LTS), 5.0.45, 6.0.2
104209	GN-24819	Windows Agent	불특정하게 액션정책 무결성 체크 실패로 액션정책이 수행안됨.	5.0.0, 6.0.0
104158	GN-24661	WebUI	백신 관련 노드그룹 필수항목값 누락으로 인한 그룹조건 즉시 수정 안되는 오류	5.0.23
104020	GN-24673	VRRPD	[범용OS] HA 환경에서 M->S 전환시 인터페이스 MAC주소가 변경되는 문제	5.0.42 (LTS), 6.0.0
103883	GN-24307	Center, Sensor	IP 로만 구성된 노드그룹의 IP들이 변경 될때 노드롤이 센서로 전달되지 않는 증상 발생	5.0.11, 6.0.0
103763	GN-24683	Sensor	센서데몬이 dhcp scan 시작 후 잘못된 메모리 참조로 비정상 종료되는 문제	4.0.2
103519	GN-24617	WebUI	추가된 노드타입(가상센서, Agent 센서)이 노드그룹의 설정리스트와 노드목록의 검색필드 조건 항목에서 누락된 문제	5.0.40
103051	GN-24603	Center	신규제어정책 추가 또는 제어정책 사용함/안함 변경시 제어정책관련 cache를 업데이트 안하는 문제	4.0.M2
102924	GN-24559	WebUI	[5.0] 개선된 노드그룹에서 조건설정 변경시 UI에 반영되지 않는 문제	5.0.37
102839	GN-24375		ES 백업(Snapshot) 정리 안되는 문제	5.0.42 (LTS)
102561	GN-24364	WebUI	IP충돌보호 - 다중 MAC 설정되지 않는 문제	5.0.42 (LTS), 6.0.0

continues on next page

Table 22 - continued from previous page

Revision	Key	Components	Description	Affects Versions
102516	GN-24467	WebUI	노드관리 목록에서 직급컬럼 추가시 목록 출력이 되지 않는 문제	5.0.33
102503	GN-24479	WebUI	라이선스가 초과되지 않았는데 NAC 라이선스초과 문구가 출력될 수 있는 문제	4.1.M3
102412	GN-24506	WebUI	[5.0] 시스템 > 서비스 제어 > 웹어플리케이션 재구동이 정상동작하지 않는 문제	5.0.41
102313	GN-24400	Windows Agent	전자서명 인증서 변경으로 인한 폐쇄망 환경에서 에이전트 업데이트 문제	5.0.0, 6.0.0
102264	GN-24239	WebUI	노드관리 검색에서 태그명으로 검색되지 않는 문제	4.0.144, 5.0.41
102094	GN-24341	Center	네트워크대역에 에이전트센서가 등록되어있는 상태에서 동일한 네트워크대역의 에이전트센서가 재등록되는 문제	5.0.40
102041	GN-24176	WebUI	노드 상세화면에서 변경된 항목이 화면 갱신이 없으면 반영되지 않아 보이는 문제	5.0.22
101863	GN-24374	Windows Agent	윈도우즈 xp 에서 에이전트 동작 안되는 문제	4.0.144, 5.0.41
101793	GN-24362		RADIUSD 에서 정책서버로 SOAP 호출시 417 Expectation Failed 발생하는 문제	5.0.42 (LTS)
101705	GN-24167	Center, Sensor	센서관리대상 노드 정보에 센서인터페이스정보가 비어있어 센서에서 노드를 관리할 수 없는 문제	5.0.36
101337	GN-24259	WebUI	소프트웨어 업데이트 UI에서 현재버전(revision이 100000번 이상일때)보다 낮은 버전이 업그레이드 가능에 표시되는 문제	5.0.20
101281	GN-24260	Center	에이전트지정액션 이벤트 전송시 비정상적인 이벤트 프레임이 생성되면서 센터데몬 비정상 종료되는 문제	3.3.1.1009
101266	GN-24202	Center	노드그룹조건이 노드그룹에 속하면(하지않으면) 인데 조건에 해당하는 노드그룹이 사용안함 또는 없는 경우 노드 그룹매칭이 비정상 동작하는 문제	5.0.35
101202	GN-23938		Scheduler 타입이 한번 실행 (ONCE_AFTER) 인 경우 Scheduler 비정상 동작문제	5.0.42 (LTS)
101021	GN-24078	Center	스위치 동작상태가 DOWN으로 잘못설정되는 문제	5.0.35
101008	GN-24124	WebUI	노드그룹에서 그룹조건으로 OR연산으로 IP관련조건 추가시 정책적용시간이 느려지는 현상	5.0.11
100871	GN-24133	Center	OR 조건으로 노드그룹 업데이트시 노드그룹이 변경되지 않는 문제	5.0.11
100828	GN-24162		잘못된 인터페이스의 MAC 주소를 가지고 서버넷스캔 수행하는 문제	3.4.M2
100443	GN-24101	Sensor	네트워크객체 및 권한객체 생성시 커널에서 네트워크 객체 참조 오류	3.5.0, 4.0.0, 5.0.0, 6.0.0
100301	GN-24074		에이전트(4.x) 정보 업데이트(updateinfo) 요청이 SQL Injection 구문으로 탐지되어 업데이트 실패하는 문제	4.0.145, 5.0.42 (LTS)
100275	GN-23914		사용자ID정규식 적용시 센터데몬 비정상 종료되는 문제	5.0.41

16.3.18 Genian NAC 5.0.41 Release Notes (2021-06-01)

Last Updated: 2021-08-03

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
94598	GN-22872	- Unknown/None-	openssl 1.1.1k 패치		7.4
94598	GN-22747	Database	GNOS MySQL 5.7 업그레이드		
94598	GN-22558	- Unknown/None-	DNSMASQ 취약점 수정을 위한 버전 업그레이드		8.1
94598	GN-22551	WebUI	시큐어코딩 점검 결과 취약점 패치 - 자바 코드		9.3
94598	GN-22475	Center	시큐어코딩점검결과 개선 - 조치없이 오류 조건 감지		1.8
94598	GN-21728	- Unknown/None-	OpenSSL 업그레이드 (1.0.2u -> 1.1.1j)		9.8

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
95399	GN-22918	Authsync	사용자가 소속된 멤버십이 10개를 초과하는 경우 AD 정보동기화 시 멤버십 동기화되지 않는 문제	
95050	GN-23174	WebUI	라이선스 유지보수 만료일 적용 개선 - 최근(큰 값) 날짜 우선	
94959	GN-22613	Install Wizard	Install Wizard 에서 VLAN DHCP 설정여부를 선택할 수 있도록 개선	
94959	GN-22438	Windows Agent	에이전트 설치시 정책서버 IP정보가 없으면 입력받도록 개선	
94598	GN-22942	Windows Agent	CMD 명령을 통한 에이전트 중지 기능 제거	
94598	GN-22771	- Unknown/None	NAC Proxy(Cache) 기반 PMS 사용시에도 대량의 외부 트래픽 발생하는 문제	
94598	GN-22707	WebUI	브라우저의 Width가 좁아지면서 관리화면 메뉴바의 레이아웃이 깨지는 문제 개선	
94598	GN-22676	WebUI	관리콘솔의 노드정책에서 노드액션 할당 후 정책적용 팝업에 노드액션 이름으로 출력되게끔 개선	
94598	GN-22635	Install Wizard	Install Wizard 에서 Timezone 설정 제거	
94598	GN-22621	Center	감사로그 부서명 저장 단계 설정 기능	
94598	GN-22619	Windows Agent	에이전트 인증창에서 로그인 시도 카운트 유지하도록 개선	
94598	GN-22522	Windows Agent	부팅 구성 정보(BCD) 수집기능 옵션화	
94598	GN-22516	macOS Agent	macOS Agent 신규 M1 칩 기기 CPU 정보 수집 오류	
94598	GN-22501	Windows Agent	장치제어 차단로그에 모델명, 시리얼 정보 추가	
94598	GN-22484	Center	사용자정의버튼 URL 에 대해서 MACRO 처리를 통해서 노드/사용자 정보 전달 가능하도록 기능 추가	
94598	GN-22471	macOS Agent	macOS Agent 사용자에 의한 에이전트 삭제기능 추가	
94598	GN-22463	WebUI	노드그룹/노드목록 정렬관련 개선	
94598	GN-22455	WebUI	IPAM 버전일 경우 IPAM 전용 로고로 출력될 수 있도록 수정	
94598	GN-22449	WebUI	장치사용 신청서 등록/조회 화면에서 신청사유/처리사유 항목 추가	
94598	GN-22301	Center	Cloud NAC 플랫폼 탐지 GDPI API 사용하도록 변경	
94598	GN-22261	WebUI	2단계 인증 OTP 관련 사용자 입력창 및 OTP앱에 표시되는 내용 개선	
94598	GN-22210	Windows Agent	'파일관리' 액션으로 파일 복사나 이동시 존재하지 않는 폴더경로 처리	
94598	GN-22159	Windows Agent	NetMan SSO 커스텀 플러그인 개발 ("외부인증연동(암호화레지스트리)")	
94598	GN-20165	WebUI	위험감지 감지범위 식별을 위한 사용성 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
96722	GN-23455	Center	logrotate 미동작으로 로그들이 정리되지 않는 문제	5.0.41
96646	GN-23438	Windows Agent	GnPlugin.exe 메모리 누수현상 발생	4.1.0, 5.0.0
96558	GN-23405	GenianOS	장비 부팅에 오랜 시간이 소요되는 문제	4.0.144, 5.0.41
96544	GN-23432	Center	윈도우에이전트설치단말의 PLID가 잘못 설정되는 문제	5.0.39
95898	GN-23299	Windows Agent	에이전트 수행계정이 로컬시스템계정에서 PC로그인계정으로 변경되지 않는 문제	5.0.38
95829	GN-23283	WebUI	노드정책에서 액션 라벨 할당할때 오류 발생하는 문제	5.0.30
95819	GN-23340	Center	ldap 인증연동/정보동기화 실패하는 문제	5.0.42 (LTS)
95797	GN-23272	Database	SSDEV 를 사용하는 장비에서 mysql 심볼릭 링크 잘못 생성되는 문제	5.0.41
95790	GN-23287	macOS Agent	macOS Agent 도메인명 설치파일로 Agent 설치시 센터의 Agent 동작상태 갱신되지 않는 문제	5.0.36, 6.0.0
95773	GN-23294	Windows Agent	잘못된 보안센터 정보로 인하여 삭제된 백신정보가 보고 되는 문제	5.0.0
95651	GN-23108	macOS Agent	macOS Agent에서 MacAddress가 없는 인터페이스 정보를 서버로 전송하는 문제	4.0.0, 5.0.0
95599	GN-23007	Sensor	센서 DHCP 사용시 WINS 서버를 여러개 설정하면 DHCP 패킷이 정상적으로 만들어지지 않는 문제	4.0.0, 5.0.0
95350	GN-23120	WebUI	노드 조건검색에서 [같지 않으면/일부가 같지 않으면] 검색 결과 문제	5.0.38
95318	GN-23266	WebUI	쿼리리포트 생성 및 수정이 되지 않는 문제	5.0.41
95044	GN-23100	WebUI	일일리포트 로그필터 항목들의 오늘 Count가 0으로 나오는 증상	5.0.36
94935	GN-23128	Authsync	정보 동기화를 통한 노드 정보 갱신 시 감사로그의 노드 IP가 역순으로 표시되는 문제	5.0.1, 4.0.108
94851	GN-23192	CLI/gnlogin	센서 장비의 CLI 접속 시 라이센스 관련 불필요한 디버그 출력되는 문제	5.0.41
94817	GN-23088	Authsync	mysql 정보동기화시 한글이 깨지는 문제	5.0.36
94789	GN-23157	Windows Agent	플러그인으로 수집된 백신정보의 이름이 공백으로 출력 되는 문제.	5.0.17
94598	GN-22938	Center	Keepalive 처리시 센터데몬 비정상 종료 문제	4.0.117, 5.0.15
94598	GN-22884	Windows Agent	에이전트보다 플러그인이 먼저 업데이트될 경우 동작 오류 수정	4.0.0, 5.0.0
94598	GN-22834	WebUI	정책관리에서 할당된 노드액션 및 제어액션 삭제시 모호한 메시지 출력과 수정이 안되는 현상	5.0.41
94598	GN-22801	Windows Agent	무선연결관리자의 자동재연결옵션이 무선연결중 변경되면 반영안되는 문제	5.0.0

continues on next page

Table 23 – continued from previous page

Revision	Key	Components	Description	Affects Versions
94598	GN-22800	WebUI	모바일에서 사용자 신청서 처리시 임시계정 신청서 정상 출력 안되는 오류	5.0.22
94598	GN-22788	Windows Agent	운영체제 정보수집플러그인을 통한 사용자계정정보 수집시 도메인사용자 누락되는 문제	4.1.0, 5.0.0
94598	GN-22763	WebUI	MAC + IP Clone 이벤트정의 설정의 감지 주체가 센터로 표기되는 문제	3.3.4
94598	GN-22751	WebUI	태그현황 위젯에서 카운트 클릭시 노드/사용자 관리 화면에 내용이 출력되지 않는 문제	5.0.33, 4.0.138
94598	GN-22736	macOS Agent	[CC 인증] macOS 에이전트 훼손 후 무결성 점검 시 복구 실패되는 문제	5.0.33
94598	GN-22724	WebUI	Cloud 정책서버인 경우 center 항목이 트리에 표현되지 않는 문제	4.1.M8
94598	GN-22708	WebUI	노드 상세 목록에서 노드 선택 후 태그 설정 시 오류 메시지 출력되는 문제	5.0.25
94598	GN-22684	WebUI	노드정책, 제어정책 생성후 변경정책 적용 시 불필요 및 잘못된 정보 출력되는 오류	5.0.16, 5.0.22, 5.0.36, 5.0.38
94598	GN-22677	CWP	CWP 인증창에서 로그인 잠금이 정상적으로 동작하지 않는 문제	5.0.9
94598	GN-22674	WebUI	노드액션에서 사용중인 무선랜정책을 삭제할 수 있는 문제	4.0.5
94598	GN-22651	WebUI	IP사용신청서 IP신규/반납 신청정보 용도 수정시 화면 깨지는 현상	5.0.36
94598	GN-22649	WebUI	노드 대상 'MAC허용 - 변경금지 (지정 IP대역)' 설정시 감사로그가 발생 안되는 문제	5.0.22
94598	GN-22623	CLI/gnlogin	CLI dhcp 명령어에서 batch mode 가 동작안하는 문제	4.1.2
94598	GN-22584	Windows Agent	특정상황에서 운영체제 시작시 재인증 기능이 동작안함	4.0.12, 5.0.0
94598	GN-22568	WebUI	노드관리 검색시 충돌보호 위반, 변경금지(지정 IP대역) 위반이 정상적으로 검색되지 않는 문제	5.0.38
94598	GN-22560	Windows Agent	화면보호기 정보를 얻지 못하였을 때 사용안함으로 전송되는 문제	4.1.0
94598	GN-22543	Authsync	장비수명주기정보 동기화시 감사기록 남지 않는 문제	5.0.11
94598	GN-22517	WebUI	빠른검색 결과와 상세보기 결과가 일치하지 않는 문제	5.0.38
94598	GN-22514	Windows Agent	프로그램 제거 액션을 통한 한컴오피스 프로그램 제거 안되는 문제	4.1.0, 5.0.0
94598	GN-22487	WebUI	노드관리 검색조건에 노드명 검색조건이 누락된 문제	5.0.38
94598	GN-22433	CWP	CWP 신규 사용자등록에서 파일업로드가 정상적으로 되지 않는 문제	5.0.36
94598	GN-22411	WebUI	노드 정책 생성 및 수정시 validation error가 발생하는 문제	4.0.M5, 5.0.29
94598	GN-22386	IPMGMT	IP신청시스템에서 사용자변경이 할당되지 않은 상태임에도 메뉴에 출력되는 문제	5.0.27

16.3.19 Genian NAC 5.0.40 Release Notes (2021-04-02)

Last Updated: 2021-06-01

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-22461	WebUI	Tomcat 버전 업데이트 (7.0.104 --> 7.0.107 / 8.5.55 --> 8.5.61)		5.9

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-22926	WebUI	cloud 환경에서 CWP의 remote ip 처리수정	
	GN-22620	WebUI	Excel Export시에 출력 컬럼에 대한 Formatting 기능 추가	
	GN-22408	Windows Agent	무선랜제어 플러그인 수집항목에 802.11ax 프로토콜이 표시되도록 수정	
	GN-22391	WebUI	REST API로 노드 등록할때 노드타입 유효성 검사 추가	
	GN-22380	Sensor, W10	WPA3 보안방식 무선랜 장치 탐지 지원	
	GN-22366	Center	IP 변경으로 등록된 에이전트 미설치 노드는 Agentless AD SSO 인증되지 않는 문제	
	GN-22355	Center	keepalive 동작 디버깅 기능 추가	
	GN-22351	WebUI	노드관리화면 "IP충돌보호+변경금지(지정대역)" 기능 추가	
	GN-22341	Center	휴면사용자 삭제기능 추가	
	GN-22326	Center	노드정보동기화 및 장비수명주기정보동기화시 로그에 노드정보가 포함되어있지 않는 문제 개선	
	GN-22296	CLI/gnlogin	Alias IP 설정된 인터페이스에 VLAN 설정시 오류 발생할 수 있는 문제	
	GN-22254	Center	CWP SSL 사용시 http를 통해 CWP에 접속하면 https로 리다이렉트 되도록 개선	
	GN-22240	Center	수동노드등록 기능을 통해서 등록되는 노드에 대해서도 동일한 디바이스가 있는지 검사하고 동일장비로 묶일수 있도록 옵션 제공	
	GN-22238	Center	'비활성노드정책갱신' 설정을 노드그룹별로 적용 가능하도록 개선	
	GN-22235	WebPlugin, WebUI	월드비전 웹 플러그인 이름을 아이루키로 변경	
	GN-22212	WebUI	2단계 인증 사용여부 설정의 라벨 변경	

continues on next page

Table 24 - continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-22205	Sensor	nmap 스캔시 옵션에 따라 딜레이를 줄 수 있도록 개선	
	GN-22203	WebUI	노드 등록 다이얼로그에서 노드의 추가필드 입력할 수 있도록 개선	
	GN-22202	WebUI	Secondary Sensor 트리에서 출력시 Prefix (SA-) 무조건 붙여서 출력되도록 수정	
	GN-22201	WebUI	관리화면에서 엑셀 export 할 때 2단계 인증 후 다운로드 할 수 있도록 개선	
	GN-22186	WebUI	부서 삭제 시 사용중인 부서항목 검사 중 처리완료된 사용자 신청서의 부서는 제외하도록 수정	5.0.40
	GN-22184	Windows Agent	GnBrowser 에서 html 스크립트 오류 출력되지 않도록 수정	
	GN-22176	Sensor	Wake-on-LAN (WOL) 기반 원격 PC 전원 On 기능	
	GN-22168	IPMGMT	노드 삭제시 MAC 변경금지(지정 IP대역) 정책을 삭제할 수 있도록 개선	5.0.39
	GN-22081	macOS Agent	MAC 에이전트가 가상인터페이스 정보를 전송하지 않아 중복노드가 분리되지 않는 문제	
	GN-22076	WebUI	사용자 내보내기 csv 파일을 가져오기 가능한 형태로 개선	
	GN-22075	IPMGMT	IP신청시스템 신청서추가/가져오기 버튼 출력여부 옵션 처리	
	GN-22015	WebUI	시스템 메뉴에 있던 디버그 로그 화면을 로그 메뉴로 이동 및 화면 개선	
	GN-21970	Center	에이전트 인터페이스정보를 이용해서 접속AP 정보 업데이트하도록 개선	
	GN-21940	Center	이중화 정책서버의 VIP가 미사용 IP로 등록되는 문제 개선	
	GN-21937	Windows Agent	윈도우용 에이전트 센서 기능 강화	
	GN-21832	Enforcer	접근제어 수행시 FQDN 네트워크 그룹에 대해서 TLS SNI를 통한 필터링 기능 제공	
	GN-21620	WebUI	노드관리에서 장치수명주기 관련 추가필드 출력될 수 있도록 개선	
	GN-21598	WebUI	신규 노드그룹 조건 추가 UI에 계속추가 버튼 추가	
	GN-21371	CWP	IP 및 컴퓨터이름 변경방법 help 페이지 NAC 관리콘솔과 통일성 있는 UI로 개선	
	GN-21239	Database, Enforcer	Failsafe 옵션 센서별로 설정할 수 있도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-23042	Sensor	센서 FQDN 객체 사용시 Memory Leak 문제	5.0.19
	GN-23037	Center	같은 IP를 가진 다수의 노드중 하나의 노드 삭제시 해당 IP변경금지 정책이 모두 삭제 될 수 있는 문제	4.0.143, 5.0.40
	GN-22979	WebUI	IP신청 옵션중 승인자 이메일 전달 대상이 설정된 경우 (동일부서, 관리자) 사용자 정보가 정상적으로 출력되지 않는 오류	4.0.139, 5.0.37
	GN-22973	Windows Agent	네트워크 인터페이스 UP/DOWN 변경시 failsafe 비정상 동작 수정	5.0.36
	GN-22933	CLI/gnlogin	bonding인터페이스 설정 안되는 문제	4.0.138, 4.0.143, 5.0.40
	GN-22915	Center	노드정책 > 주기적 재인증 동작 안하는 문제	4.0.1, 5.0.0
	GN-22913	Center	RADIUS Accounting FRAMEDIP 로 인해서 중복노드가 만 들어지는 문제	5.0.34
	GN-22897	Windows Agent	무선연결관리자 삭제시 기존 연결정보가 남아있는 문제	4.1.0, 5.0.0
	GN-22876	Sensor	스위치포트 차단 기능에 의해서 노드가 잘못된 정책을 적용받는 문제 재수정	5.0.28
	GN-22841	macOS Agent	CLI 명령을 통한 macOS 에이전트 디버그 로그 수집 실패 문제	5.0.33
	GN-22469	Windows Agent	변경되지 않은 운영체제 정보가 업데이트 되는 문제	5.0.0, 4.0.125
	GN-22441	macOS Agent	macOS Agent 트레이아이콘 메뉴가 영문으로 표시되는 문제	4.0.106, 5.0.14
	GN-22424	WebUI	라이선스 파일 업로드 했을때 유지보수 만료일자 등의 값이 갱신되지 않는 문제	5.0.36
	GN-22406	WebUI	노드관리 검색시에 검색항목의 이름에 사용할 수 없는 쿼리가 들어있을 경우 검색이 되지 않는 문제	5.0.38
	GN-22385	CLOUD	클라우드정책서버/센서 syscollect 동작안하는 문제	5.0.16
	GN-22383	WebUI	IP 매트릭스 뷰에서 미러센서(0.0.0.0) 아이피 클릭시 오류 화면 발생 문제	4.0.8
	GN-22345	CWP	CWP 사용자등록 가져오기시 검증 문구 메시지를 출력하지 못하는 문제	5.0.36
	GN-22327	WebUI	'MAC / IP Clone' 이 노드정책에 할당되지 않는 현상	5.0.0
	GN-22317	WebUI	노드 속성 가져오기에서 추가된 추가필드(10~20)가 입력되지 않는 문제	5.0.11
	GN-22315	Database	새시 유형 '알수없음' 조건으로 상태그룹이 포함되지 않는 문제	5.0.15
	GN-22303	CWP	CWP 사용자 정의 버튼 두줄 시 아이콘 정렬 달라지는 문제	5.0.14
	GN-22285	Windows Agent	액션수행 결과의 메시지가 일부분만 표시되는 오류	5.0.0

continues on next page

Table 25 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-22258	Windows Agent	간헐적으로 GnPMS 비정상 종료	4.0.38, 4.0.115, 5.0.12
	GN-22241	Windows Agent	윈도우즈 업데이트 Proxy 통한 검색 실패 (0x80072EE2, 시스템계정)	4.0.115, 5.0.12
	GN-22231	WebUI	[CWP] 보안질문 방식으로 비밀번호 찾기 시 비밀번호 변경 화면에 가이드 문구 미표시 수정	5.0.8
	GN-22206	Windows Agent	무선랜 제어 액션의 "무선 연결 이력 정보 수집"을 사용하면 DB에러(Duplicate) 출력	5.0.0
	GN-22171	Windows Agent	인터페이스 제어 플러그인에서 "코드인증 사용" 옵션 값 적용 안됨.	5.0.0
	GN-22169	CWP	IP관리 메시지 우선 On 일때 에이전트 사용자 인증 메뉴로 CWP 인증 시 계정으로만 인증 되는 문제	4.0.0, 5.0.0
	GN-22165	WebUI	검색필터 저장 시 입력한 "사용자입력" 검색기간으로 출력되지 않는 문제	5.0.15
	GN-22161	WebUI	CVE 현황 목록화면에서 CVE-ID로 정렬이 정상동작하지 않는 문제	5.0.24
	GN-22153	Windows Agent	복수개의 IP 설정시 네트워크정보수집플러그인으로 인해 플러그인 수집정보 전달안되는 문제	4.1.0, 5.0.0
	GN-22130	WebUI	관리자의 관리범위를 센서로 설정한 뒤 IP 신청서 결과조회 화면에서 검색이 제대로 되지 않는 문제	4.0.120, 5.0.17
	GN-22113	WebUI	사용자/IP 선택기에서 선택한 항목에 대한 출력 템플릿 설정할 수 있도록 수정	4.0.120, 5.0.17
	GN-22093	WebUI	MatrixView 출력시 선택된 센서가 관리하는 노드의 IP만 보여지도록 수정	4.0.8
	GN-22056	WebUI	신규 노드상세화면에서 사용자선택기를 통한 추가필드 값 업데이트가 설정대로 되지 않는 문제	5.0.22
	GN-22042	macOS Agent	MAC 에이전트 간헐적으로 keepalive 전송에 실패하는 문제	5.0.38
	GN-21860	Sensor	스위치를 통해서 등록되는 노드의 MAC 주소가 소문자로 등록되는 문제	5.0.14
	GN-21500	CWP, WebUI	CWP 디자인템플릿 변경 후 기존 접속된 CWP 페이지에서 템플릿 미리보기 화면으로 출력되는 문제	5.0.14

16.3.20 Genian NAC 5.0.39 Release Notes (2021-02-01)

Last Updated: 2021-04-08

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-21985	WebUI	관리콘솔 취약점 개선 (XSS 공격, 에러코드 노출)		4.3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-22737	Center	센서의 failsafe 상태를 유지할 수 있도록 하는 기능 제공	
	GN-22586	CWP	CWP 사용자등록 페이지의 동의관련 UI가 반응형으로 동작할 수 있도록 tag 개선	
	GN-22468	Database, VRRPD	DB서버 mysqld 서비스 이중화 기능 및 keepalive 서비스 이중화 기능 개선	
	GN-22467	CLI/gnlogin	CLI콘솔접속 IP 허용개수 설정 기능 추가	
	GN-22340	CWP	모바일 환경에서 CWP 보안서약서 페이지 UI 개선	
	GN-22292	WebUI	Cloud NAC 'System > Service > Port' 메뉴의 'Public IP' 를 https://checkip.amazonaws.com 을 통해 구하도록 개선	
	GN-22257	WebUI	스위치 포트 설정의 관리자 Down 및 설명이 UI에 표시 되지 않는 문제	
	GN-22136	WebUI	추가필드에 대해 필수입력 옵션 추가	
	GN-22134	Center, Database	다국어 처리시 locale 별 정의 안된 메시지가 UNKNOWN으로 출력되는 문제	
	GN-22133	Windows Agent	인증창,WCM 등에서 로고이미지 출력시 이미지 깨짐(계단)현상 안나오도록 수정 (고배율)	
	GN-22117	WebUI	네트워크 객체 설정화면의 네트워크 주소 수정 프로세스 개선	
	GN-22091	Enforcer	kernel debug 기능 추가	
	GN-22089	Windows Agent	에이전트가 PC에 설정된 기본 웹브라우저를 사용할수 있도록 옵션 추가	
	GN-22020	Windows Agent	한컴워드 SafeIdentity v5 의 SSO연동 커스텀 플러그인 개발	
	GN-22018	Center	검색필터 > Webhook 호출시 감사기록 생성	
	GN-22004	Center	에이전트 설치노드에 대한 CVE 목록 표시 및 DPI 링크 연결 추가	
	GN-21827	WebUI	CVE 관련 정보에 대한 현황화면 제공	
	GN-21782	Center, WebUI	제어정책 목록에서 EarlyRole임을 확인할 수 있도록 개선	
	GN-21269	WebUI	사용자정의 버튼을 삭제하면 업로드된 이미지도 같이 삭제되도록 개선	
	GN-20093	WebUI	노드그룹의 노드수 차트 위젯 추가	
	GN-15682	WebUI	WebUI를 통한 업그레이드시 선택적으로 백업을 수행할 수 있도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-22811	WebUI	라이선스 노드 수 초과 시 노드관리 화면 출력되지 않는 문제	5.0.38
	GN-22779	CLOUD	Cloud NAC 화면보호기파일(.scr) upload가 불가능한 문제 개선	5.0.6
	GN-22705	Authsync	SQL Escape 처리가 안되어 정보동기화 안되는 문제	3.3.5
	GN-22687	WebUI	동의페이지 약관내용에 img 태그 입력시 src가 제거되는 문제	5.0.21
	GN-22648	Center	IPv6 주소가 탐지될때 정책적용이 비정상적으로 할당되는 문제	5.0.16
	GN-22601	Windows Agent	DLL인젝션 차단 옵션을 사용할 경우 에이전트 비정상 종료 문제 수정	5.0.38
	GN-22569	CWP	CWP에서 인증제한으로 인해 인증 해제시 로그아웃 버튼을 클릭해도 로그아웃이 안되는 문제	5.0.38
	GN-22552	RADIUS	[RADIUS] MS-Chap 인증 안되는 문제	5.0.19
	GN-22549	WebUI	노드관리 검색바 노드타입 조건에서 항목에 대한 인텔리전스 툴팁이 출력되지 않는 문제	5.0.38
	GN-22546	Center	노드에 확인 플랫폼이 자동으로 설정 되는 문제	4.0.114, 5.0.11
	GN-22478	Center, CLOUD	NAT환경에서 클라우드정책서버 -> 에이전트로 이벤트 전송 안되는 문제	5.0.9
	GN-22275	CWP	사용자 계정 신청 페이지에서 SMS 문자통보가 입력되지 않는 문제	5.0.19
	GN-22182	WebUI	사용자 삭제 시 감사로그 중복으로 출력되는 문제 (BETA 버전 이후에서 발생)	4.0.37, 4.0.114, 5.0.11
	GN-22163	WebUI	시스템관리 > 운영정보데이터 > 운영체제 감지 데이터의 링크 오동작	5.0.22
	GN-22131	WebUI	IP 신청시스템에서 신규 신청시 사용위치에 지정된 노드 그룹 외 센서가 출력되는 문제	4.0.113, 5.0.10
	GN-22118	Windows Agent	SHA1 인증서에 만료에 따른 에이전트 업데이트 실패 수정	4.0.0, 5.0.0
	GN-22110	WebUI	무선랜AP의 감사로그 팝업창의 정보 출력위치 개선	5.0.11
	GN-22108	WebUI	센서 이중화 환경에서 Slave 센서가 Master로 전환되었을 때 관리 > 노드 UI의 장비명/센서명이 잘못 표시되는 문제	5.0.29
	GN-22078	WebUI	노드추가필드(문자열패턴입력)로 노드그룹 조건을 설정할 수 없는 문제	5.0.34
	GN-22062	Windows Agent	64비트 운영체제에서 백신정보 수집 플러그인을 통한 Windows Defender 상세 정보가 수집되지 않는 문제	4.0.50, 4.0.127

16.3.21 Genian NAC 5.0.38 Release Notes (2020-12-01)

Last Updated: 2021-02-04

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-21396	WebUI	노드관리 검색바에서 사용할 수 없는 sql 문법 및 시스템 변수 제한하도록 개선		4.5

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-22316	macOS Agent	macOS Agent 하드웨어 정보수집 최소비율 기능 추가	
	GN-22298	IPMGMT	IP신청페이지 관리자 계정으로 로그인 시 로그인이 느린 문제 개선	
	GN-22047	Sensor	센서 노드동작상태(up or down) 체크 기능 개선	
	GN-22034	WebUI	에이전트 알림 메시지에서 한글로 구성된 타이틀인 경우 에이전트 출력시 깨져 보이는 문제	
	GN-22019	GenianOS	Nmap 버전 업그레이드 (7.80 -> 7.91)	
	GN-21997	CLI/gnlogin	center CLI를 통해 센서 status를 확인수 있는 기능 추가	
	GN-21971	WebUI	WebSSH 버튼 출력 여부 설정 옵션 추가	
	GN-21965	CLI/gnlogin, Sensor	install wizard에서 센서 장비인 경우, NTP 서버 설정 옵션 제거하도록 개선	5.0.38
	GN-21964	Center	셸 에서 cmd 명령으로 센서 동작을 중지시킬 수 있도록 기능 추가	
	GN-21947	WebUI	설정 > 사용자관리의 검증 정규식 사용 설정이 off일때 입력된 정규식을 검증하지 않도록 개선	
	GN-21941	Windows Agent	PentaSecurity v3.0 (이상) 모듈 연동 플러그인 개발	
	GN-21935	Center, Sensor	SNMP를 이용한 Aruba Virtual Controller 관리 기능 지원	
	GN-21933	Center	REST API를 통한 외부시스템 정보동기화기능	
	GN-21924	Enforcer	[NexG NAC] 가상 mac 을 사용하면 차단동작 안되는 문제	
	GN-21896	Center	center thread 카운트 모니터링 감사로그 기능 추가	
	GN-21895	GenianOS	아파치 접속자수 모니터링 스크립트 작성	
	GN-21685	WebUI	변경정책적용 다이얼로그에서 정책의 변경된 내용 출력 될 수 있도록 개선	
	GN-21674	Center, Windows Agent	센터IP가 설정된 에이전트 MSI 패키지 다운로드 가능하도록 수정	
	GN-21605	Center	모니터링 중인 스위치/포트 정보 변경시, 로깅하도록 개선	
	GN-21529	macOS Agent	macOS 에이전트의 macOS Big Sur (11.x) 지원	
	GN-21270	WebUI	노드/로그/무선랜 리포트에 다운로드 기능 추가	
	GN-21254	WebUI	노드액션의 수행주기 변경이 있어도 변경정책적용이 활성화 되지 않는 문제	
	GN-20973	WebUI	관리콘솔에서 공인인증서(ssl.cer)를 등록 할 수 있도록 기능 개선	
	GN-20141	Windows Agent	관리UI의 에이전트 설치 파일(ZIP)을 이용한 수동 설치	
	GN-19820	CWP	노드의 사용자 재인증 설정시 CWP에서 인증 버튼 클릭시 로그아웃 버튼 나오는 문제 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-22505	Windows Agent	4.X 버전 에이전트 자동업데이트 미동작 문제 수정	4.0.141
	GN-22474	Center, RA-DIUSD	RADIUS 정책을 통해서 VLAN 할당 안되는 문제	5.0.36
	GN-22472	Center	IPv6 프로토콜을 지원하지 않는 환경에서 센터 구동 안되는 문제	5.0.36
	GN-22457	macOS Agent	macOS Agent 허용된 무선랜그룹 차단되는 문제	5.0.33
	GN-22451	Center	노드 운영체제 이름이 User Agent 정보에 의해서 잘못된 이름으로 변경되는 문제	5.0.33
	GN-22436	Windows Agent	빈번하게 네트워크 사용량이 업데이트 되는 문제	4.0.114, 5.0.11
	GN-22429	WebUI	빠른검색 수행 시 IP 정책관련 테이블 조인 예외토록 수정	5.0.38
	GN-22354	Windows Agent	UAC 활성화 환경에서 무선연결관리자에서 연결가능한 AP항목이 표시되지 않는 문제	5.0.27
	GN-22353	Sensor	센서 IP 설정 삭제후에도 센터에 다시 등록되는 문제	5.0.36
	GN-22336	Windows Agent	관리자권한이 없는 AD 환경에서 MSI로 에이전트 설치할 때 트레이 아이콘 표시 오류	5.0.0
	GN-22309	WebUI	노드 수동 등록 시 관리센서를 지정하지 않으면 허용 정책을 설정해도 센서의 신규노드정책이 적용되는 문제	4.0.M8
	GN-22307	Center	노드 수동 등록 시 관리센서를 지정하지 않으면 IP/MAC 정책이 잘못 적용되는 문제	4.1.M4, 4.0.18, 3.5.14
	GN-22287	Windows Agent	에이전트 인증창에서 SMS/이메일 인증 시 잘못된 인증코드가 통과되는 문제	5.0.25
	GN-22279	Center	4.0.1 NAC Center 데몬 초기 구동 과정에서 HA Virtual IP 노드가 활성화 되는 문제	4.0.141, 5.0.38
	GN-22260	Sensor	센서 MAC 충돌회피 기능사용시 센서 비정상 종료 문제	4.0.118, 5.0.15
	GN-22239	WebUI	관리콘솔 로그인 되지 않는 문제 (로그인 과정 중 센터 아이피 가져오는 부분의 문제)	5.0.37
	GN-22226	Center	감사기록 필터를 통한 태그 할당시 인증된 사용자 정보가 보이지 않는 문제	5.0.21
	GN-22211	CWP	인증제한수를 초과하여 인증시 CWP 사용자 현황 목록이 보이지 않는 문제	5.0.37
	GN-22209	WebUI	추가필드로 추가한 옵션을 노드그룹에 추가했을때 설정 값이 보이지 않는 문제	5.0.34
	GN-22198	macOS Agent	Mac OS 터치바 모델에서 노드가 등록될때 동일한 MAC 으로 등록될 수 있는 문제	5.0.38
	GN-22177	WebUI	REST API 노드 태그 할당 이벤트 호출 시 정책 재적용 이벤트가 적용되지 않는 문제	4.0.134, 5.0.31
	GN-22141	WebUI	노드 추가필드 생성 후 노드 속성변경에서 추가필드 설정 시 오류가 발생됨	5.0.38
	GN-22101	macOS Agent	MAC 에이전트 액션 주기적 수행이 동작하지 않는 문제	5.0.11

continues on next page

Table 26 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-22083	macOS Agent	MAC 에이전트 저장장치 정보가 중복으로 쌓이는 문제	5.0.11
	GN-22045	Center, macOS Agent, Windows Agent	에이전트 로그가 정상 수집되지 않는 문제	5.0.33
	GN-22037	Windows Agent	클라이언트에 위험인터페이스 감지로 가상 네트워크 인터페이스가 차단되지 않는 증상	5.0.16
	GN-22010	macOS Agent	MAC 에이전트 모니터 정보 수집시 중복 데이터로 인한 DB 오류가 발생하는 문제	5.0.17
	GN-22008	CLOUD, CWP	Cloud CWP에서 Timezone을 Asia/Seoul로 인식하는 문제	5.0.14
	GN-22006	WebUI	사용자 관리의 부서 트리 선택시 트리 메뉴에 오류 페이지 발생	5.0.0
	GN-21982	Center	PMS 상태값 만족함 과 만족안함 이 함께 설정되는 문제	4.0.14
	GN-21958	Windows Agent	VPN 환경에서 비밀번호 만료 페이지 표시 오류 수정	4.0.0
	GN-21943	Windows Agent	에이전트 인증창을 통한 인증완료 후 "인증 후 실행"에 등록된 실행파일이 과심오류로 수행되지 않는 문제	5.0.9
	GN-21882	WebUI	보안질문에 대한 답이 등록되고 인증이 완료된 상태에서 CWP 메시지가 변경되지 않는 문제	5.0.33

16.3.22 Genian NAC 5.0.37 Release Notes (2020-11-02)

Last Updated: 2020-12-03

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-21879	WebUI	CWP 취약점을 통한 인증권한 탈취 개선		6.2

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-22116	WebUI	관리 > 노드 > 현황&필터의 에이전트 > 소프트웨어 UI가 Slow Query 인해 정상적으로 조회되지 않는 문제	4.0.0, 5.0.0
	GN-21922	Sensor	AXGATE 장비의 업그레이드 기능 지원.	5.0.33
	GN-21911	WebUI	승인자 이메일 전달 대상이 모두전달인 경우 메일 발송 되도록 기능 추가	
	GN-21910	WebUI	다른 사용자 IP 신청시 신청자 IP/MAC 정보를 할당하지 않도록 기능 추가	
	GN-21885	Center	센서 장비 신규 등록시 DHCP가 아닌 인터페이스가 센서 대표IP로 우선 설정되도록 개선	
	GN-21878	Database, MySQL	sha256_password 플러그인을 사용하는 mysql 계정 로그인을 위한 RSA 키 생성로직 추가	
	GN-21876	Elastic-Search	CSV 파일의 로그를 logserver로 전달하는 프로그램 작성	
	GN-21870	Center, WebUI	Web 콘솔에서 에이전트 로그 수집 명령 실행 가능하도록 개선	
	GN-21869	Center	syslog 감사기록 저장 필터 개선	
	GN-21862	WebUI	IP 사용신청서 거부시 알람 가능하도록 기능 추가	
	GN-21853	Enforcer	Enforcement 모드 외부 네트워크제어 옵션 추가	
	GN-21835	GenianOS, Sensor	NexG UTM Sensor nodeinfo 정보 볼 수 있는 기능 추가	
	GN-21831	WebUI	디버그로그 메뉴에서 에이전트로그 다운가능하도록 권한 추가	
	GN-21823	WebUI	디버그로그 트리에 검색기능 추가	
	GN-21808	Center, WebUI	E1 / 보안서약서를 복수개 사용할 수 있도록 개선	
	GN-21784	WebUI	소프트웨어 버전으로 노드그룹 조건 추가	
	GN-21781	Center, Database	EarlyRole에 적용받지 않는 등록된 모든 노드가 포함될 수 있는 노드그룹 조건 추가	
	GN-21780	WebUI	제어정책의 기본정책 권한을 선택할 수 있도록 개선	
	GN-21778	WebUI	스위치 트리 출력 쿼리 개선	
	GN-21379	WebUI	IPv6 환경에서 관리콘솔 설정에 OS 별 에이전트 지원 아이콘 출력될 수 있도록 개선	
	GN-21028	Center, RADIUS	RADIUS 정책에서 User-Name에 대한 AD/LDAP Group Membership 포함여부 조건을 추가	
	GN-20192	Windows Agent	멀티운영체제 탐지를 위한 Windows 부팅설정 정보 수집 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-22190	GenianOS	백업 시 일부 저장서버에서 저장장치로 마운트 실패하는 현상	5.0.36
	GN-22179	CWP	CWP 사용자 등록 페이지의 Form Data에서 패스워드가 평문으로 보이는 문제	4.0.38, 5.0.35
	GN-22135	Center	disable 한 장치제어 정책이 에이전트로 전달되는 문제	5.0.23
	GN-22127	Windows Agent	가상장치에서 에이전트 수행시 운영체제 정보수집플러그인으로 인한 GnPlugin.exe 비정상 종료문제	5.0.37
	GN-22102	Center	글로벌미러에서 노드 업다운 정보 갱신시 센터 및 센서 모두의 관리노드를 보도록 개선	4.0.37, 4.0.114, 5.0.11
	GN-22058	Windows Agent	에이전트에 등록된 외부연동작업 정보가 사라지는 문제	5.0.0
	GN-22043	Windows Agent	플러그인을 통하여 인터넷 연결 공유 해제 후 정책제거되어도 윈도우에서 재설정 안되는 문제	4.1.0, 5.0.0
	GN-21830	Center	신규노드 등록시 플랫폼 관련 정보가 감지되면 BY=DHCP Server Scan 으로 감사기록이 남는 문제	4.0.120, 5.0.17
	GN-21819	Center, CWP	CWP 비밀번호 찾기 기능 사용 시, 관리자 정보를 요구하는 문제 수정	4.0.61, 4.0.138, 5.0.35
	GN-21815	Center	이전 정책적용이 나중에 적용되어 잘못된 정책을 가지고 있는 문제	4.0.M1
	GN-21798	CLI/gnlogin	CLI data-server access-list ip 설정 시, 구분자를 점(.)이 아닌 특수문자로 입력해도 설정되는 문제 개선	3.0_0912

16.3.23 Genian NAC 5.0.36 Release Notes (2020-10-05)

Last Updated: 2020-11-06

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-21843	Center	SQL 인젝션 검사하지 않는 예외 처리된 SOAP API 의 인자값도 escape 처리 하도록 수정		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-22027	Center	IPv6 전용노드에 대한 노드 등록을 옵션으로 동작하도록 개선	
	GN-21928	WebUI	업데이트 서버에서 유지보수 만료일자 가져오지 못하는 환경의 장비에서는 라이선스 파일 참고할 수 있도록 개선	
	GN-21802	GenianOS	백업저장 장치(CIFS) 사용시 SMB ver2 추가 및 버전 선택 사용 가능하도록 개선	5.0.36
	GN-21761	Center	gSOAP에서 SNI(Server Name Indication) 지원하도록 개선	
	GN-21748	WebUI	수동 등록된 스위치 표시 및 옵션 출력 개선	
	GN-21743	WebUI	센서설정을 REST API 로 가져올 수 있는 기능 추가	
	GN-21726	WebUI	노드관리 Having 절로 인한 성능 개선을 위해 노드 관련 검색조건은 Where 절에도 추가되도록 수정	
	GN-21725	Windows Agent	프로그램 제거 플러그인에 여러 프로그램을 설정할 수 있도록 개선	
	GN-21696	Authsync	사용자 정보동기화 인증처리 MAC/IP 복수개 처리 가능하도록 개선	
	GN-21692	Sensor	Agentless AD SSO 쿼리 실패시 부하 및 최초 적용시 인증 지연 개선	
	GN-21691	CLOUD, IP-MGMT	Cloud NAC IP신청 (ipmgmt) 포함하도록 수정	5.0.7
	GN-21685	WebUI	변경정책적용 다이얼로그에서 정책의 변경된 내용 출력될 수 있도록 개선	
	GN-21681	macOS Agent	MAC 에이전트 네트워크 정보 수집 시 DHCP 사용유무 정보도 수집되도록 개선	
	GN-21670	Center	센서 미존재 대역의 스위치 SNMP 연동을 통한 신규노드 감지 딜레이 및 부하 개선	
	GN-21530	WebUI	CWP 비밀번호 찾기기 SMS/Email 비밀번호 찾기 컴포넌트가 모두 출력되는 부분 개선	
	GN-20114	Center, Sensor	IPv6 전용노드에 대한 노드 등록기능	
	GN-18378	WebUI	유지보수 만료시 제품이미지 업그레йд 하지 못하도록 제한	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-22055	WebUI	사용자 선택기 출력값이 무조건 검색결과값으로 출력되는 문제	4.0.120, 5.0.17
	GN-22049	RADIUSD	RADIUS GTC 인증시 패스워드에 && 문자가 있는 경우 인증 실패하는 문제	5.0.19
	GN-22028	GenianOS	센서에 의한 노드 스캔 시 SMB OS 정보가 수집되지 않는 문제	5.0.26
	GN-22021	Windows Agent	디스크 정보 수집 오류에 의한 IP/MAC Clone 탐지 오탐 수정	5.0.0
	GN-22011	CLOUD, WebUI	[Cloud] 대시보드 리포트 생성시 "connection refused" 오류가 발생하면서 동작하지 않는 문제	5.0.16
	GN-21994	Center	scanraw의 NSE 정보 파싱중 centerd shutdown 문제 발생	5.0.27
	GN-21990	WebUI	모바일 앱(Genian NAC Monitor)에서 노드검색 되지 않는 문제	5.0.33
	GN-21962	Center	Segmentfault 발생 후 센터데몬 종료되지 않는 문제	5.0.26
	GN-21955	CLI/gnlogin	CLI에서 백업파일 복구 안되는 문제	5.0.34
	GN-21944	WebUI	추가필드의 사용자 선택기 옵션 수정되지 않는 문제 및 보안서약서의 사용자 선택 문제	4.1.5
	GN-21873	Windows Agent	에이전트 디버그파일이 센터에 수집되지 않는 문제	3.5.34, 4.0.136, 5.0.33, 4.0.60
	GN-21857	WebUI	리포트 현황에 출력되는 카운트와 실제 노드목록 및 스냅샷의 노드 카운트가 맞지 않는 문제	5.0.8
	GN-21787	WebUI	관리자 설정의 노드상세화면 보기제한시 설정한 탭이나 권한이 없음에도 노드정보 내용이 무조건 출력되는 문제	5.0.22
	GN-21769	WebUI	관리자 비밀번호찾기가 보안질문 설정이고 질문이 추가되어 있지 않은 경우에 관리자 비밀번호찾기 팝업에서 시스템 에러가 발생하는 문제	5.0.20
	GN-21757	Center	SNMP에 의해 감지된 노드 연결방식이 노드스캔 이후 이전 정보로 변경되는 문제	4.0.106
	GN-21754	CWP	보안질문에 대한 답이 등록되지 않은 경우 CWP 메시지가 변경되지 않는 문제	5.0.33
	GN-21746	Center	Master 서버 VC폴더내 파일이 삭제될 수 있는 문제 수정	4.0.39, 4.0.116, 5.0.13
	GN-21732	Windows Agent	수행계정 변경으로 인한 간헐적인 에이전트 미동작 현상	4.0.2, 4.1.0
	GN-21678	WebUI	사용자 일괄 등록 시 일부 컬럼 정보가 정상적으로 등록되지 않는 문제	5.0.15
	GN-21583	Windows Agent	에이전트 설치시 AD 사용자 폴더를 직접 만들어 사용하지 않도록 수정	5.0.0
	GN-20914	Center	윈도우 플랫폼 변경시 업데이트가 되지 않는 문제	4.1.M3, 4.0.17, 3.5.13

16.3.24 Genian NAC 5.0.35 Release Notes (2020-09-01)

Last Updated: 2020-10-05

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-21843	Center	SQL 인젝션 검사하지 않는 예외 처리된 SOAP API 의 인자값도 escape 처리 하도록 수정		
	GN-21647	Database	MySQL 업그레이드 (5.6.47 -> 5.6.48)		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-21721	CLOUD, Containerization, Docker	Add Policy Server AMI(s) to AWS Marketplace	
	GN-21688	CLOUD, WebUI	노드관리 트리에서 클라우드 센서 할당 기능 추가	
	GN-21676	WebUI	사용자 조회 Slow Query 발생 개선	
	GN-21660	WebUI	노드타입 이름 입력시 공백 허용되도록 수정	
	GN-21650	Windows Agent	에이전트 서비스 속성 임의 변경 감지 및 복구하는 기능	
	GN-21588	Database	메뉴명 802.1x 정책을 RADIUS 정책으로 이름변경	
	GN-21587	Database, WebUI	용어 접속장치/접속포트에 대한 일관성 개선	
	GN-21582	Sensor	dhcp request 수신시 offer하지않는 request에 대해서 NAK를 보내도록 개선	4.0.5
	GN-21579	Center, RADIUS	Cisco ASA AnyConnect VPN 접속관련 개선	
	GN-21552	macOS Agent	macOS 파일 배포 플러그인의 실행 옵션 개선 및 수행 계정 추가	
	GN-21550	Center	[RADIUS] 인증대체 기능을 사용 안하는 경우에도 RADIUS 어카운트 로그 남을수 있도록 개선	
	GN-21549	Center, RADIUS	RADIUS 정책에 Cisco-AVPair 속성 Key 추가	
	GN-21546	Windows Agent	WCM의 연결대상에 신호탐지안되는 SSID 출력하도록 개선	
	GN-21544	Center	Webhook 인증연동 설정에 데이터전송타입 옵션 추가	
	GN-21484	Center, Sensor	스위치를 통한 노드등록시 가상센서로 노드등록 할 수 있도록 개선	
	GN-21459	Windows Agent	SafePC와의 인증연동 커스텀 플러그인 개발	
	GN-21037	WebUI	스위치목록 동작상태 컬럼 추가	
	GN-20329	WebUI	스위치 SNMP Write Community 설정 바로가기 링크 추가	
	GN-20144	macOS Agent	macOS 파일 관리 플러그인의 실행 옵션 개선 및 수행 계정 추가	
	GN-20077	Center	제어정책에서 SNMP를 통한 VLAN 설정기능	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-21925	WebUI	장치그룹 생성 및 수정시 조건으로 추가된 클래스명이 잘 못입력되어 장치제어가 동작하지 않는문제	5.0.31
	GN-21915	Sensor	Nmap 7.80 간헐적으로 hang 걸리는 문제	5.0.26
	GN-21902	Center	URL Request에 대한 응답 메시지가 비어있는 경우, Center 데몬이 비정상적으로 죽는 문제 수정	4.0.137, 5.0.34
	GN-21889	WebUI	노드그룹 정책적용 현황 위젯의 카운트와 노드관리 화면의 카운트가 맞지 않는 문제	4.1.M3
	GN-21883	Windows Agent	운영체제정보 수집 플러그인 업데이트 안되는 문제	5.0.29
	GN-21881	Center, ElasticSearch	adv에서 엘라스틱 리인덱스 시 다음날 해당 인덱스가 삭제되는 문제	4.0.117, 5.0.14
	GN-21859	WebUI	노드속성가져오기로 인한 데이터 업데이트되지 않는 문제	5.0.33
	GN-21842	Windows Agent	안전모드상태에서 장치제어 안되는 문제	5.0.25
	GN-21837	macOS Agent	센터 Domain name에 하이픈(-)이 있는 경우 macOS 에이전트 설치 실패하는 문제	5.0.7
	GN-21731	CLOUD	CLOUD NAC aws를 이용한 email 전송안되는 문제	5.0.33
	GN-21707	IPMGMT	IP신청시스템 신청서처리결과와 조회범위가 신청자ID 내 조회 일경우 검색필터 동작하지 않음	5.0.18
	GN-21658	Center	호스트네임/도메인 정보 갱신시 active node의 정보만 갱신되는 문제	4.0.M8
	GN-21639	WebUI	IE 브라우저 사용시 노드상세화면에서 태그할당시 할당 시각이 설정되지 않는 문제	5.0.22
	GN-21632	Windows Agent	특정 PC에서 네트워크 정보를 수집하지 못하는 문제	4.0.0, 5.0.0
	GN-21622	Center	웹콘솔 로그인페이지에서 일반 사용자 계정의 ID/PW를 찾을 수 있는 문제 수정	3.0_0912
	GN-21612	Center, RADIUS	[RADIUS] AD Domain과 Pre-Win2k Domain 이 다른 경우에 인증 안되는 문제	4.0.3
	GN-21595	GenianOS	syscollect.sh 실행 시 old 로그를 삭제하지 않도록 개선	4.0.M1, 3.4.1, 3.3.13, 3.2.13
	GN-21592	WebUI	IP사용 신청 결과 메시지에서 처리일자가 표시되지 않는 문제	4.0.M9
	GN-21556	Windows Agent	인증페이지(CWP) 표시가 오래걸릴 경우 다량의 인증안내 메시지 표시 문제	5.0.0
	GN-20724	WebUI	RADIUS서버 클라이언트 설정에서 인증키를 수정할 수 없는 문제	5.0.15

16.3.25 Genian NAC 5.0.34 Release Notes (2020-08-03)

Last Updated: 2020-09-11

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-21766	Center	Genian Syncer 에서 센터로 업로드시 감사로그 개선		
	GN-21513	WebUI	웹 취약점으로 501 에러가 발생했을 경우 전용 에러페이지 출력되지 않는 문제 수정		0.6

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-21762	Genian Syncer	GenianSyncer 에서 센터에서 다운로드시 감사로그 추가	
	GN-21542	WebUI	매트릭스 뷰에서 브라우저의 사이즈가 작을 경우에 하단 툴팁이 잘 보이지 않는 문제 개선	
	GN-21521	Windows Agent	에이전트에서 띄우는 웹브라우저가 최상위 표시될지에 대한 옵션 추가	
	GN-21499	WebUI	노드관리 관련 용어 변경 및 노드상세화면의 태그할당시 태그할당시각 컬럼 출력에 대한 개선	
	GN-21457	CLI/gnlogin	인증서 재발급 CLI 추가	
	GN-21441	WebUI	WSUS 서버 설정 UI에서 입력예시 표기 개선	
	GN-21430	Windows Agent	설치되어있는 무선연결관리자(WCM) 삭제 기능	
	GN-21427	Center, macOS Agent, Windows Agent	macOS 호스트명 변경 플러그인 제작	
	GN-21416	RADIUS	[RADIUS] Active Directory 인증연동 시 Multi-Domain 지원	
	GN-21385	WebUI	원문을 볼 수 있는 비밀번호 컴포넌트 추가	
	GN-21364	Center	PMS 동작방식이 Offline인 경우만 WSUSSCN2.CAB 파일을 다운받도록 변경	
	GN-21359	Windows Agent	AD 정책으로 설정된 화면보호기 정보도 수집 가능하도록 개선	
	GN-20476	WebUI	변경정책적용 버튼 클릭시 정책적용이 바로 되지 않고 변경된 정책항목을 확인후 적용할 수 있도록 개선	
	GN-19322	macOS Agent	macOS 에이전트 설치 패키지 UI 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-21811	Sensor	DHCP relay 환경에서 dhcp 주소 임대시간이 잘못 설정되는 문제	4.0.123, 5.0.20
	GN-21810	WebUI	자산관리 소프트웨어 위젯에서 노드관리 이동하는 링크 클릭시 정상적인 결과 출력되지 않는 문제	5.0.32
	GN-21794	Center	제어정책 변경시 무한 blocking 으로 인해 행이 걸리는 문제	5.0.25
	GN-21788	Center	관리콘솔에서 시스템 로그 수집 수행시, 빈번하게 실패함.	5.0.33
	GN-21777	Center	네트워크정보 수집 플러그인에 의해 연결방식이 변경되어도 해당조건을 사용하는 노드그룹 재적용안되는 문제	4.0.M8
	GN-21760	Authsync, CLOUD	CLOUD/UBUNTU NAC LDAP 정보동기화 오류	5.0.33
	GN-21733	WebUI	노드상세화면 조회시 노드 변경때마다 정책현황의 내용이 반복해서 출력되는 문제	5.0.22
	GN-21702	Center	감사로그 검색필터의 Syslog over TLS 동작하지 않는 문제	4.0.117, 5.0.14
	GN-21636	Center	간헐적으로 center 데몬에서 발생하는 감사로그가 유실되는 문제 수정	4.1.3, 4.0.26
	GN-21533	Center, Sensor	https 포트 변경 시, 센서 이미지 업데이트 실패 현상 수정	4.0.114, 5.0.11
	GN-21522	macOS Agent	macOS 에이전트 UI의 html 링크가 동작하지 않는 문제	5.0.16
	GN-21512	WebUI	태그할당시 관리자의 타임존이 시스템 타임존과 다른 경우 만료시각 등 시간 설정이 잘못출력되는 문제	4.1.2
	GN-21502	WebUI	POST '201 Created' 응답에도 에러로 출력되는 현상 수정	4.0.118, 5.0.15
	GN-21481	Center	사용자 삭제시 과거 비밀번호 변경내역이 삭제되지 않는 문제	3.0_1007
	GN-21462	WebUI	비밀번호 변경 창에서 비밀번호가 입력되지 않는 것처럼 보이는 문제 (IE에서만 발생)	5.0.25
	GN-21461	Sensor	간헐적으로 gdcid가 죽는 문제	4.0.113, 5.0.10
	GN-21456	Database, macOS Agent	macOS 노드의 호스트명이 컴퓨터명으로 표시되는 문제	4.0.106, 5.0.0
	GN-21435	Center	이중화 정책서버 구성에서 파일동기화 시 정책서버포트를 고려하지 않는 문제	4.0.114, 5.0.11
	GN-21412	CLI/gnlogin	ping 테스트 과정에서 Source interface 설정시 Parameter 에러로 인한 테스트 불가 현상 수정	5.0.16
	GN-21410	Windows Agent	에이전트액션으로 프로세스 존재여부 조건체크가 간헐적으로 안되는 문제	5.0.0
	GN-21406	Center	변경금지 및 충돌보호 변경시 NL_LASTACTIVE 가 잘못된 조건에서 갱신되는 문제	4.0.36, 4.0.113, 5.0.10
	GN-21392	Center	342개 이상의 센서를 할당하여 관리자의 노드 관리범위 제한시 오류 발생	4.0.M3
	GN-21335	Windows Agent	사용자알림메시지로 고정메시지 출력대상이 아니지만 출력되는 문제	5.0.0
	GN-21287	Center	FTP 백업 하위 디렉토리 설정시 정상동작하지 않는 문제	4.0.135, 5.0.32
678	GN-21265	Center, RADIUS	[RADIUS] NAS IP 및 PORT 정보 업데이트 <small>구조 개선</small>	5.0.23
	GN-20312	WebUI	IP관리현황, MAC현황 화면에서 설정된 태그가 테이블 컬럼에 보이지 않고 태그 조건 필터가 동작하지 않는 문제	4.0.M9

16.3.26 Genian NAC 5.0.33 Release Notes (2020-07-01)

Last Updated: 2020-11-02

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-21641	macOS Agent, Windows Agent	에이전트 openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2u)		
	GN-21640	GenianOS	openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2u)		
	GN-21397	WebUI	Tomcat 버전 업그레이드 7.0.100 --> 7.0.104 / 8.5.51 --> 8.5.55		7
	GN-21386	GenianOS	Apache httpd 2.4.43 업그레이드		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-21489	Documents, macOS Agent, Windows Agent	Change Win/Mac shutdown plugin to "Control Power Options"	5.0.32
	GN-21467	Center, GenianOS, WebUI	ES 접속 호스트명을 설정할 수 있도록 개선	
	GN-21413	Containerization	Container 기반 환경에서 Ingress를 Nginx로 전환	
	GN-21377	GenianOS	httpd timeout 을 설정할 수 있도록 개선	
	GN-21348	CWP	IP 및 컴퓨터이름 변경방법 help 페이지 내용 변경	
	GN-21306	Windows Agent	Nexess SSO 연동 플러그인 로그아웃 상태까지 연동 가능하도록 기능 개선	
	GN-21305	Windows Agent	Ksign SSO 연동 플러그인 개발	
	GN-21304	Windows Agent	프로그램 제거 플러그인에서 삭제 명령이 등록되지 않은 제품 제거시 동작 방식 개선	
	GN-21299	Authsync, CLOUD	CLOUD NAC에 authsync 포함하도록 수정	
	GN-21092	Windows Agent	필수 소프트웨어 검사 플러그인의 제품 중 신규 버전이 출시된 항목 추가	
	GN-20695	Center, macOS Agent	macOS 무선랜제어 플러그인에 AP 연결 제어 기능 추가	
	GN-19701	WebUI	노드그룹 UI 개선 (중요 노드그룹 및 카테고리 컬러)	
	GN-19673	WebUI	운영체제별 버전현황을 확인할 수 있는 대시보드 위젯 추가	
	GN-19519	Center	노드정보에 운영체제, 버전 정보 추가	
	GN-13772	Center	NAC 감사기록 syslog 전송시 CEF 형식으로 전송할 수 있도록 기능추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-21680	Sensor	센서 재부팅후 차단노드의 네트워크내 통신이 가능한 문제	5.0.8, 4.0.111
	GN-21677	Center	802.1x 인증에서 등록된 노드가 0.0.0.0 IP로 남아 있는 문제	5.0.28
	GN-21642	CLOUD	Cloud에서 WEBUI를 이용해 upload 한 센서이미지로 upgrade 할수 없는 문제	5.0.33
	GN-21635	Windows Agent	간헐적으로 에이전트 업데이트 실패되는 문제	5.0.9
	GN-21631	Database	DB(mysql) 버전 업그레이드 이후 처리속도가 느려져 부하가 발생하는 문제	4.0.135, 5.0.32
	GN-21604	Windows Agent	인증창이나 인증팝업이 출력되어있는 상태에서 정책재 적용받으면 창이 사라지는 문제	4.0.56, 4.0.133, 5.0.30
	GN-21603	Center	에이전트에서 NETIF 정보 업데이트시 센터에서 연결방식이 갱신되지 않는 문제	5.0.32
	GN-21594	WebUI	스위치 상세화면의 Write Community 값이 수정되지 않는 문제	5.0.32
	GN-21581	Center	계정 비밀번호변경후에도 비밀번호강제변경을 조건으로 하는 사용자그룹에서 빠지지 않는 문제	3.3.4
	GN-21524	WebUI	K8s 사이트에서 로그인시 출발지IP가 K8s IP로 나오는 문제	4.1.M7, 4.0.21
	GN-21509	Center	플랫폼이름 (PLID) 와 trustScore 값이 일치하지 않는 문제	4.0.129, 5.0.26
	GN-21390	Windows Agent	efork 로그아웃에 대한 인증연동 안됨.	4.0.51
	GN-21351	WebUI	대시보드 탭 생성시 공유 옵션 수정 불가 및 탭 레이아웃 컬럼 수 0 입력 가능 문제 수정	5.0.31
	GN-21332	Windows Agent	디스플레이 패율변경된 환경에서 시스템종료 대화상자의 이미지가 비정상 출력되는 문제.	5.0.0
	GN-21307	macOS Agent	macOS 인증 상태에서 에이전트 인증창이 팝업되는 문제	5.0.15
	GN-21071	Windows Agent	AD로그인되어있지만 로컬로그인으로 오탐하여 AD대체 인증 안되는 문제.	4.1.5, 4.0.28, 5.0.0

16.3.27 Genian NAC 5.0.32 Release Notes (2020-06-01)

Last Updated: 2020-07-03

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-21181	Database	MySQL 업그레이드 (5.6.41 -> 5.6.47) 및 파일 권한 변경		
	GN-21084	WebUI	관리콘솔 취약점 개선		7.5

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-21252	macOS Agent, Windows Agent	파일배포 플러그인의 용어 개선	
	GN-21241	WebUI	노드관리의 태그명칭을 노드 태그로 변경	
	GN-21214	Database	제어정책 액션에 사용가능한 액션 추가	
	GN-21209	Enforcer	Enforcer TCP Response 패킷 TTL 변경	4.0.114, 5.0.11
	GN-21186	WebUI	시스템관리 상세화면의 인터페이스 정보 개선	
	GN-21082	Center, Sensor, WebUI	원격지 네트워크에 대한 노드스캔 기능 (가상센서 추가)	
	GN-21079	Center, RADIUS	[RADIUS] PAP - AD 인증연동 동작하도록 개선	
	GN-21065	Center	에이전트수행 계정을 로컬 시스템계정으로 선택시 계정 입력란 안보이게 수정	
	GN-21061	WebUI	노드관리 작업선택에서 센서의 예외처리 MAC 기능 추가	
	GN-21053	WebUI	목록 화면에서 특정 범위의 항목을 일괄 선택할 수 있도록 개선	
	GN-21029	Center, WebUI	VPN 장비와의 RADIUS SSO 및 노드관리 개선	
	GN-20978	WebUI	스위치관리 메뉴 센서기반 계층적 구조 지원	
	GN-20850	WebUI	감사 > 로그 > RADIUS 결과 컬럼 내용 추가 및 관리뷰 편집 기능 추가	
	GN-20845	WebUI	RADIUS 로그 로그필터 저장기능 추가	
	GN-20711	macOS Agent	macOS 시스템 종료 플러그인 수행 시 남은 대기 시간을 표시하도록 개선	
	GN-20515	WebUI	목록 UI에서 선택한 row를 쉽게 식별할 수 있도록 개선	
	GN-20191	Windows Agent	윈도우 보안설정 플러그인에 복구콘솔 자동 로그인 금지 설정 추가	
	GN-19822	WebUI	Web UI를 통해서 장비 SSH 접속 할 수 있도록 처리	
	GN-19375	WebUI	이메일발송 - 일일 리포트 개선	
	GN-16915	Windows Agent	Windows 업데이트 플러그인 설정 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-21547	Genian Syncer	Syncer 를 통해 업로드된 파일이 다운로드 안되는 문제	5.0.21
	GN-21519	Windows Agent	에이전트 액션 조건에서 폴더의 존재여부 체크 못하는 문제	5.0.31
	GN-21507	WebUI	센터 SSL 인증서 다운로드 실패하는 문제	5.0.31
	GN-21506	Center	SOAP queue max 로그 발생시 메모리 릭 생기는 문제	4.0.119, 5.0.16
	GN-21491	macOS Agent	센서의 비관리 IP 대역에서 macOS 에이전트 신규 설치 시 비정상동작하는 문제	5.0.13, 4.0.131
	GN-21450	Sensor	스위치포트 차단 기능에 의해서 노드가 잘못된 정책을 적용받는 문제	5.0.28
	GN-21442	macOS Agent	macOS 무선랜제어 플러그인 사용 시 GnPlugin 메모리가 과다 점유하는 문제	5.0.30
	GN-21440	Windows Agent	운영체제 정보수집 플러그인으로 인한 GnPlugin.exe 의 메모리 증가(MemoryLeak)	5.0.29
	GN-21434	Center	dhcp 노드 정보 갱신시 deadlock 이 발생할 수 있는 문제	5.0.26, 4.0.130
	GN-21429	WebUI	Genian Monitor App 에서 로그인 되지 않는 문제	5.0.27
	GN-21261	Windows Agent	복수개의 PC에서 USB 랜카드를 재사용시 사용자 인증 정보가 맞지 않는 문제	4.0.0, 4.1.0, 5.0.0
	GN-21211	Enforcer	AND 조건의 earlyrole 생성시 오동작 하는 문제	4.0.114, 5.0.11
	GN-21206	WebUI	IP 매트릭스뷰에서 미사용IP의 노드상세화면 링크에서 잘못된 노드 상세화면이 출력되는 문제	5.0.22
	GN-21202	WebUI	무선랜 접속 AP 현황 위젯 그래프가 정상적으로 표시안 되는 문제	4.1.4
	GN-21190	Authsync	AD 서버 정보 동기화 이후 AD서버에서 삭제된 사용자 정보가 남아있는 현상	5.0.1, 4.0.110
	GN-21183	WebUI	설정 > CWP 설정에서 "호스트명 변경" 설정이 출력되는 문제	5.0.14
	GN-21182	WebUI	장치그룹 생성후 노드관리에서 장치그룹 설정 대상이 아닌 노드에서 차단 툴팁이 출력되는 문제	4.0.M1, 3.4.1
	GN-21076	Database	log2migration 스크립트 DBPORT 변수 오류 수정	4.0.123, 5.0.20
	GN-21046	Center, Sensor	미러센서 단말의 UP/DOWN 상태변경시 이벤트가 전송 되지 않는 문제	4.0.37, 4.0.114, 5.0.11
	GN-20975	macOS Agent	VPN 환경에서 macOS 업데이트 플러그인이 동작하지 않는 문제	5.0.11
	GN-20899	WebUI	계정정보 수정 시 오류페이지 출력되는 문제	5.0.22

16.3.28 Genian NAC 5.0.31 Release Notes (2020-05-06)

Last Updated: 2020-06-05

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-20848	WebUI	보안 취약점 개선 - 파일업로드 확장자우회, web에서 인증없이 /disk/data/custom 폴더내 파일 접근 등		5.3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-21043	Sensor	Agentless AD 인증대체 - 센서에서 AD 서버 접속시 NTLMv2 인증 사용하도록 개선	
	GN-21036	WebUI	정책생성시 노드그룹 및 에이전트 액션 PickList에 검색기능 추가	
	GN-21021	Center	로그매크로에 JSON 인코딩한 값을 사용할 수 있도록 수정	
	GN-20992	WebUI	로그검색 IP 필터 설정시, IP패턴매칭 조건 지원	
	GN-20972	Center	SNMP TRAP 감사기록 남도록 개선	
	GN-20970	WebUI	대시보드 탭 추가시 다른 사용자가 생성한 탭 기반으로 생성할 수 있도록 개선	
	GN-20966	Center, RA-DIUSD	802.1x 정책에 인증 허용/차단 정책 생성 및 그룹조건 AND 조건 추가 개선	5.0.31
	GN-20962	Sensor	노드 이동시 스위치/포트 정보 부정확하게 설정되는 문제 개선	
	GN-20961	Center, WebUI	감사기록 이메일 알람의 MAC/IP 정책색상 및 허용처리 단순화	
	GN-20951	Center, RA-DIUSD	[RADIUS] 인증시 사용자 인증허용MAC 이 적용되도록 개선	5.0.31
	GN-20945	Center	사용자 최초 인증시 인증허용 MAC을 고정하도록 하는 기능 추가	
	GN-20929	WebUI, Windows Agent	트레이메뉴의 "에이전트 삭제"에 대한 동작 방식의 옵션 추가	
	GN-20921	Center	IP/MAC 사용시간 만료시 GENI 장비이면 노드가 삭제되지 않도록 개선	
	GN-20919	WebUI	센서그룹을 관리자의 관리범위로 지정할 수 있는 기능 추가	
	GN-20916	Windows Agent	비밀번호 검증창을 가운데 화면에 고정하는 옵션 추가.	
	GN-20900	Center	에이전트액션결과 만족상태에 따른 노드그룹에 수행전 상태값 구분	

continues on next page

Table 27 - continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-20896	Windows Agent	필수 소프트웨어 검사 플러그인 목록에 백신 정보 수집 플러그인에서 수집 가능한 제품 정보 추가	
	GN-20892	WebUI	[REST API] 사용자/노드 태그 할당 시 정책재적용(에이전트, 센터) 이벤트 호출할 수 있도록 개선	4.0.11
	GN-20885	Windows Agent	Windows 방화벽 제어 플러그인 커스텀 규칙 설정시 알림 메시지 표시기능 추가	
	GN-20856	WebUI	REST API 태그 할당 시 만료시각에 대한 기간설정 개선	
	GN-20827	macOS Agent	macOS 업데이트 액션 수행 결과에 업데이트 동작 상태를 나타내도록 개선	
	GN-20823	Windows Agent	사용자 알림메시지에서 CWP URL 미입력시에도 CWP 페이지 접속할수 있도록 개선	
	GN-20816	Sensor	스위치에 연결된 노드의 접속장치 및 접속포트가 틀린 문제	4.0.0, 3.5.4, 3.4.10
	GN-20772	Center, Sensor	Agentless AD 인증대체를 위한 서버 모니터링을 센서에서 수행하도록 개선	
	GN-20683	Center, RADIUS	RADIUS 로컬인증과 AD 인증을 함께 사용할 수 있도록 수정	
	GN-20677	macOS Agent	macOS ARP 관리 플러그인 추가	
	GN-20630	macOS Agent	macOS 에이전트 파일배포 플러그인 제작	
	GN-20552	Sensor, WebUI	Genian 장비 local.conf를 시스템정보탭을 통해 확인할 수 있도록 기능 추가	
	GN-20513	WebUI	노드그룹 등록 UI 개선	
	GN-20512	WebUI	필터 조건설정 조회 Rest Api 추가	
	GN-20511	WebUI	그룹 카테고리 관리 Rest API 추가	
	GN-20108	Linux Agent	리눅스 에이전트 OS 재시작시 재 인증 기능 추가	
	GN-19934	macOS Agent	macOS 에이전트 크롤링 방어 옵션에 따른 CWP 페이지 표시 변경	
	GN-18837	WebUI	사용자 정의 항목(쿼리 리포트)에 대해서 자동으로 메일 전송 받을 수 있도록 개선	
	GN-16845	Sensor	SSDP Multicast 패킷에 포함된 User-Agent 스트링 수집 및 플랫폼 감지 기능 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-21409	WebUI	Elasticsearch http 포트 변경시 웹 정상 동작하지 않는 문제 수정	5.0.24
	GN-21378	Sensor	비관리IP 제어 기능 동작하지 않는 문제	4.0.116, 4.0.40, 5.0.14
	GN-21373	WebUI	IE 브라우저에서 노드 상세의 정책 탭 내용이 수정되지 않는 문제	5.0.22
	GN-21370	Center	Webhook 인증시 타임아웃에 의해서 인증실패하는 문제	5.0.19
	GN-21041	Windows Agent	에이전트 인증창 화면 중앙에 표시되지 않는 문제	5.0.8
	GN-21039	Windows Agent	플러그인으로 컴퓨터명을 한글로 변경시 NAC에서 파악되는 컴퓨터명과 다르게 나타나는 문제	4.1.0, 5.0.0
	GN-21031	Windows Agent	에이전트 인증창 비활성화 상태에서도 인증버튼 기능이 동작하는 문제	5.0.14
	GN-21019	macOS Agent	macOS 에이전트 설치 시 나눔고딕 서체 다운로드가 필요한 문제	5.0.10
	GN-20996	WebUI	IP 사용신청서 메일승인대기 관리화면 출력되지 않는 문제	4.0.129, 5.0.26
	GN-20995	WebUI	액션 상세화면에서 wnac 라이선스와 일반 라이선스 권한 에러 메시지가 같이 출력되는 문제	5.0.0
	GN-20987	Center	Agentless AD 인증대체 - 도메인에 가입되지 않은 노드에서 AD 서버 로그인시 인증대체되는 문제	5.0.25
	GN-20984	WebUI	노드관리화면의 트리(센서) API 호출시 센서리스트가 출력되지 않는 문제 수정	4.1.4, 5.0.26
	GN-20980	WebUI	장치그룹 추가 시 클래스명이 직접입력일때 장치정보가 추가되지 않는 문제	5.0.25
	GN-20955	Windows Agent	제어유보시간 1분 초과 설정 방지 및 안내 메시지 출력되도록 수정	4.0.22, 4.1.0
	GN-20942	Windows Agent	PassNI SSO 인증이 간헐적으로 동작하지 않는 문제	5.0.17
	GN-20905	Windows Agent	윈도우보안설정 플러그인으로 인한 잘못된 감사로그 출력	5.0.0
	GN-20881	Linux Agent	일부 개방형OS(hamonikrOS)에서 소프트웨어정보 수집이 되지 않는 현상	4.0.133, 5.0.30
	GN-20878	WebUI	사용자 > 전체사용자 > 부서별 메뉴 클릭시 오류 발생	5.0.28
	GN-20846	WebUI	사용자관리의 인증노드수 선택 시 정상적으로 출력되지 않는 문제	5.0.26
	GN-20796	Center	노드 UPDOWN 상태 일치하지 않는 문제	NoVersion
	GN-20791	WebUI	IP사용신청서 결과조회 엑셀 다운로드 시 표시되지 않는 컬럼이 존재하는 문제	4.1.M5
	GN-20425	macOS Agent	macOS 노드가 서비스 대상 그룹에 속하지 않아도 인증 관련 트레이 메뉴가 활성화됨.	5.0.0, 4.0.108
	GN-20390	Windows Agent	허용되지 않은 Gateway 사용으로 인터페이스 차단된 이후 허용된 Gateway로 설정하지 못하는 문제	4.0.0, 5.0.0
	GN-18722	Windows Agent	플러그인 버전 업그레이드시 최초 한번 설치 실패하는 문제	4.0.0, 5.0.0

16.3.29 Genian NAC 5.0.30 Release Notes (2020-04-01)

Last Updated: 2020-05-18

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-20928	WebUI	Tomcat 버전 업그레이드 7.0.99 --> 7.0.100 / 8.0.53 --> 8.5.51		4.8
	GN-20875	WebUI	GET 방식의 크로스 사이트 스크립팅 (XSS) 취약점 개선		1.6
	GN-20874	GNOS	Bash 취약점 (shellshock) 패치	4.1.3	

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-20912	Center	인증서 발급시 EKU(ExtendedKeyUsage) 를 포함하여 발급하도록 개선	
	GN-20865	RADIUSD	[RADIUS] 어카운팅 패킷을 이용한 인증 연동시에 잘못된 인증키로 접근하는 경우 에러로그에 NAS IP 정보가 남도록 개선	
	GN-20847	WebUI	디버그로그 전체보기시 로그파일 용량 체크 후 용량이 큰 경우 메시지 출력	
	GN-20842	WebUI	노드타입 기타(Other)를 IoT/OT 로 표기되도록 수정	
	GN-20804	RADIUSD	[RADIUS] PEAP 인증 ON/OFF 기능/설정 추가	5.0.19
	GN-20794	Center	인증서 발급시 EKU(ExtendedKeyUsage) 를 포함하여 발급하도록 개선	
	GN-20775	Center	[IPAM] 라이선스에 포함된 에이전트수 제한설정에 따라서 전체 에이전트 설치 노드수 제한할수 있도록 개선	
	GN-20771	CWP	CWP 디자인 템플릿 추가	
	GN-20743	Authsync	Oracle 정보동기화 설정시 복수의 서버주소 설정 가능하도록 개선	
	GN-20694	CWP	CWP 사용자 인증 페이지에 인증정책 설정에 따라 사용자 등록 링크가 보이도록 개선	
	GN-20690	WebUI	CSV파일 업로드시 컬럼명에 대한 오타 검사 추가	5.0.27
	GN-20631	macOS Agent	macOS 무선랜 인터페이스 정보수집 플러그인 추가	
	GN-20497	Center, Database, Sensor, WebUI	센서 인터페이스 DHCP 설정여부를 UI에서 확인할수 있도록 개선	
	GN-20450	WebUI	RADIUS 기반의 인가정책 설정 UI 추가	
	GN-20449	WebUI	스위치 포트 관리 화면에 포트 속성 변경 명령 추가 및 VLAN변경 기능 추가	
	GN-20448	Center, Sensor	스위치 포트 관리기능을 통한 VLAN 변경 기능	5.0.27
	GN-20152	Enforcer, GNOS, Sensor	엑스게이트 UTM 장비에 센서 모듈 포팅	
	GN-20107	Linux Agent	리눅스 에이전트 트레이/팝업창을 통한 사용자 인증 (CWP) 개발	
	GN-20089	Center, WebUI	RADIUS 기반의 인가정책 (Authorization Policy) 추가	
	GN-19997	WebUI	WebUI를 통한 시스템로그(syscollect) 다운로드 기능	
	GN-19947	- Unknown/None-	[CC인증] CC 인증에 따른 custom script 수정	
	GN-19513	Enforcer, Sensor	엑스게이트 (AXGATE) UTM 장비에 NAC 센서 포팅	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-21284	Center	SMTP 인증연동시 인증서 검증실패로 인증실패하는 문제	5.0.19
	GN-21277	WebUI	사용자 상태별 현황 위젯에서 사용자 수 클릭시 에러페이지 발생	4.0.129, 5.0.26
	GN-21204	GNOS	crond 스크립트 정상실행 안되는 문제	5.0.10
	GN-21184	Center	센서 이중화 구성에서 포트 노드가 증가하는 문제	4.0.126, 5.0.23
	GN-21010	Center, Sensor	SNMP set 명령 community 값을 ReadCommunity 로 설정하는 오류 및 write memory 지원 검사시 실패하는 경우 snmp 정보수집 안되는 문제	5.0.30
	GN-20927	Windows Agent	VPN 사용하는 네트워크 환경에서 에이전트가 센터에 연결되고 중복노드발생	4.1.0, 5.0.0
	GN-20897	Center	dhcp relay 사용시 중복 dhcp ip를 할당하는 문제	4.0.5
	GN-20843	Windows Agent	Agent에서 특정 소프트웨어 목록을 수집하지 못하는 현상	4.0.0, 5.0.0
	GN-20831	macOS Agent	macOS 에이전트 트레이메뉴의 업데이트 확인 클릭 시 오류 발생하는 문제	5.0.9
	GN-20820	Windows Agent	센터와 통신하는 인터페이스가 변경된 노드에서 네트워크정보 즉시 보내지 않는 문제	4.0.114, 5.0.11
	GN-20789	Windows Agent	IE 보안옵션 제어 시작 페이지 설정 옵션을 제거하여도 계속 동작하는 문제	5.0.0
	GN-20769	Genian Syncer	GenianSyncer 에서 라이선스 확인 실패하여 업로드 안되는 문제	4.0.108, 5.0.5
	GN-20713	WebUI	노드의 엑셀 내보내기에서 장비소유부서가 부서코드로 출력되는 문제	4.0.1
	GN-20688	Windows Agent	호스트 인증사용시 에이전트에서 외부인증연동이 잘못된 정보를 전송하는 문제	4.0.0, 5.0.0
	GN-20687	Windows Agent	에이전트 수행계정 변경시 일부 외부인증연동 기능이 동작하지 않는 문제	5.0.0, 4.0.107, 4.0.30
	GN-20495	WebUI	노드관리 IP정책명령 사유입력을 받도록 설정하여도 노드상세에서 정책변경 시 사유입력창이 표시되지 않는 문제	5.0.22

16.3.30 Genian NAC 5.0.29 Release Notes (2020-03-04)

Last Updated: 2020-04-01

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-20737	Windows Agent	Panda Endpoint Protection 백신 정보 수집기능 추가	
	GN-20615	Windows Agent	운영체제 정보에 마지막 업데이트 날짜 정보 추가	
	GN-20502	WebUI	시스템, 센서관리의 이름 컬럼 개선	
	GN-20112	Center, macOS Agent, Windows Agent	IP 사용 만료전 에이전트 알림메시지 표시 기능 추가	
	GN-20094	WebUI	Diagram 기반 노드정보 출력기능	
	GN-20031	WebUI	정책, 그룹, 객체 최종 수정시각 표시	
	GN-19850	macOS Agent	macOS 에이전트 트레이 메뉴에 사용자정의 버튼 표시 기능 추가	
	GN-18604	WebUI	로그필터 Webhook 호출시 디폴트 JSON 데이터 포맷 지원	
	GN-18510	WebUI	nodes REST API 사용시 MAC의 다양한 포맷 지원토록 개선	
	GN-18162	WebUI	사용자정보 동기화 설정시 이름 컬럼 필수항목으로 지정	
	GN-16862	Center	노드 속성 정보 관련 매크로 추가	
	GN-14270	WebUI	위젯 설정 변경시 상세로그 표기가 코드로 표시되는 문제	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-21069	CWP	CWP 버튼을 통한 정보수집 시 gnconf_EnableAllFormElmt 정의 오류	4.0.M5
	GN-20902	WebUI	사이즈 조절이 가능한 트리에서 사이즈 조절시 현황 및 필터 항목이 Close 되는 문제	5.0.28
	GN-20893	WebUI	에이전트 버전 현황 위젯을 통해 노드관리 출력시 내용이 나오지 않는 문제	5.0.26
	GN-20883	Center	Slave 센서 등록과정에서 센터데몬 shutdown 될 수 있는 문제	4.0.0, 3.5.4
	GN-20798	Windows Agent	GTC모듈 등록 실패로 무선연결 안되는 문제	5.0.20
	GN-20431	GenianOS	[범용 OS] https로 특정 페이지 이동시 not found 에러가 뜨는 문제	5.0.23
	GN-20066	WebUI	로그아웃 이후에 감사로그 실시간 모드 팝업창의 세션이 유지되는 현상	5.0.22
	GN-18866	WebUI	다중사용자 선택기에 유효하지 않은 사용자가 출력되는 문제	5.0.5
	GN-18733	macOS Agent	macOS 계정에 비밀번호가 존재하지 않으나 설정됨으로 표시되는 문제	4.0.106, 5.0.0

16.3.31 Genian NAC 5.0.28 Release Notes (2020-02-03)

Last Updated: 2020-03-04

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-20471	Center	openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2t)		
	GN-20443	macOS Agent, Windows Agent	에이전트 openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2t)		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-20826	IPMGMT	IP신규신청 화면 로딩시 사용자 검색 UI에서 검색어가 없을 때 전체 사용자를 가져오는 문제 개선	
	GN-20807	WebUI	크롬 최신 버전 (80.0.3987.100 이상)에서 NAC 5.0 관리자 웹콘솔 접속했을 때 인증서 만료로 페이지 중지 되는 문제	

continues on next page

Table 28 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-20594	Center	MAC+IP Clone 감지 위험 이벤트에 MAC Clone 감지 옵션 추가	
	GN-20539	WebUI	로그필터 수정시 감사기록 상세내용에 SNMP Community String이 포함되지 않도록 개선	
	GN-20535	WebUI	시스템관리 IP설정 UI 개선	
	GN-20509	WebUI	노드상세 페이지 스위치(포트) 정보의 여백 변경	
	GN-20505	WebUI	ES의 PI데이터 정보를 출력 기능 추가	
	GN-20491	CWP	안드로이드폰으로 CWP 접속시 에이전트 설치버튼이 노출되는 문제	
	GN-20472	CWP, WebUI	PC 상태재검사 동작시 진행바 표시 설정 제거	
	GN-20469	Center, Genian Syncer, GeniUpdate	geniupdate를 통해 PI 데이터 업데이트되도록 개선	
	GN-20467	WebUI	시스템 관리의 작업선택 메뉴에서 센서와 관련된 메뉴 제거	
	GN-20451	Sensor	sensord에서 nmap 스캔시 OS정보 수집을 옵션으로 동작할 수 있도록 추가	
	GN-20436	WebUI	알림창출력 기능 개선	
	GN-20435	WebUI	노드그룹 조건 중 Platform Security Vulnerability 조건의 "ID contains" Operator 철자 잘못된 부분 수정	
	GN-20433	CLI/gnlogin	Global 버전 Channel Bonding 기능을 기본 기능으로 변경	
	GN-20422	Database	DPI End of Support 용어를 End of Life로 변경	
	GN-20411	Linux Agent	리눅스 에이전트에서 TmaxOS를 지원하도록 함.	
	GN-20404	WebUI	센서 동작상태 표시 개선	
	GN-20347	WebUI	DEVINFOALL 관련 조회 API 추가	
	GN-20306	GenianOS	제품설치시 네트워크 검사 개선	
	GN-20258	macOS Agent	[CC] macOS 에이전트 전자서명 검증을 OpenSSL 사용하도록 변경	
	GN-20257	Windows Agent	[CC] 에이전트 전자서명 및 인증서유효기간 검증을 OpenSSL 사용하도록 변경	
	GN-20104	Windows Agent	윈도우즈 설정 옵션 중 전원 옵션을 강제화 하는 제어기능 추가	
	GN-20090	WebUI	노드관리 동작 아이콘 유무선 구분	
	GN-20058	WebUI	RADIUS 감사기록 상세정보 조회기능	
	GN-19963	WebPlugin	[우정사업정보센터] 사용자정보동기화 API 연동 WebPlugin 작성	

continues on next page

Table 28 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19922	Windows Agent	무선연결관리자, 유선랜인증 플러그인을 통하여 "스마트 카드 또는 기타 인증서" 인증방법 제공	
	GN-19746	Database, macOS Agent	macOS 소프트웨어의 최근변경시각을 표준 날짜 형식으로 표시하도록 개선	
	GN-19466	WebUI	선택된 부서의 삭제 기능을 쉽게 인지하도록 수정	
	GN-18890	Windows Agent	윈도우 방화벽 제어를 통한 에이전트 차단 기능 강화	
	GN-18859	WebUI	페이지별 메뉴얼 링크 / 도움말 출력 기능 추가	
	GN-18125	macOS Agent	macOS 네트워크 정보 수집 플러그인의 네트워크 인터페이스 수집 정보 확대	
	GN-17682	macOS Agent	macOS 에이전트 프로세스 강제종료 플러그인 제작	
	GN-17681	macOS Agent	macOS 에이전트 파일 관리 플러그인 제작	
	GN-16453	Center, Sensor	제어정책의 스위치포트 차단 기능이 동작하지 않는 문제	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-20924	Center	정책서버에서 글로벌미러센서의 제어정책을 구할 때 Unknown field name 에러발생	5.0.28
	GN-20894	Center	Slave 센터가 Radius 서비스 관련 설정을 로드하면서 shutdown 발생	5.0.25
	GN-20849	WebUI	정책 사용중 icon 표시 안되는 문제	5.0.28
	GN-20830	WebUI	IP 매트릭스뷰에서 포커스가 있는 상태에서 툴팁이 사라지는 문제	5.0.28
	GN-20819	Windows Agent	안랩연동 모듈(GnAhnLab.exe)사용시 메모리 사용량이 계속 증가하는 문제 (메모리릭)	5.0.0
	GN-20793	RADIUS	[RADIUS] ActiveDirectory 이름포맷형식인경우에 사용자 그룹조건 동작 안하는 문제 수정 및 라디우스 로그 안남는 문제 수정	5.0.18
	GN-20773	Database	mysql 포트 변경시 dbmigration 실패하는 문제	4.0.106, 5.0.0
	GN-20767	Center	[RADIUS] RADIUS 를 통해서 노드 등록 후 관리 센서로 이동할때 노드가 삭제 되는 문제	5.0.25
	GN-20674	Linux Agent	리눅스 에이전트 업그레이드 안되는 현상	4.0.129, 5.0.26
	GN-20657	Windows Agent	인터페이스제어 플러그인에서 전체를 대상으로 인터페이스제어가 안되는 문제	5.0.22
	GN-20613	Windows Agent	무선연결관리자를 통하여 GTC 프로파일 등록 실패하는 문제	5.0.28
	GN-20585	WebUI	MAC이 없는 노드에서 MAC 정책 설정화면이 노출되는 문제	5.0.22
	GN-20582	Center	에이전트 업로드 시 /disk/data/upgrade 디렉토리 동기화되지 않는 문제	5.0.2
	GN-20568	WebUI	Dashboard Full Screen 전환후 "esc" 키 입력후 원래 화면으로 복원되지 않는 문제	5.0.24
	GN-20562	WebUI	노드 상세정보의 액션수행결과 현황 결과가 노드정책의 액션과 일치하지 않는 문제	5.0.22
	GN-20555	WebUI	HA 환경에서 Active 정책서버 파일 업로드 시 custom 디렉토리 파일 동기화 되지 않는 문제	5.0.14
	GN-20548	WebUI	노드 스냅샷에서 Excel 내보내기가 진행되지 않음	5.0.25
	GN-20489	CWP	CWP 페이지 모바일UI 지원 개선 이후 적용이 안되는 문제	5.0.23
	GN-20481	WebUI	정책에 위험감지 설정 (Malware 감지)이 없는데 노드목록에 Malware Icon이 표시되는 문제	5.0.19
	GN-20480	WebUI	추가필드관리 > 장비 수명주기 관리에서 사용하지 않는 필드를 삭제해도 노드그룹 조건에 표시되는 문제	5.0.11
	GN-20475	Windows Agent	프린터 정보수집 플러그인에서 가상프린터 수집제의 옵션 동작 안함.	5.0.0
	GN-20446	Center	커스텀 외부인증 연동시 인증방식이 누락된 문제	5.0.16
	GN-20444	WebUI	[범용OS 버전- MySQL 8] 태그 삭제시 오류가 발생하는 문제	
	GN-20439	macOS Agent	VPN 사용 시 macOS의 MAC 주소가 00:00:00:00:00:00로 탐지되는 문제	4.0.106, 5.0.0
	GN-20430	WebUI	[관리>노드]의 장치사용관리뷰에서 장치그룹ID 표시 문제	5.0.24
696			Chapter 16. Release Notes	
	GN-20428	Center, GPDB	GPDB 업데이트 시 정책 재적용을 수행하도록 개선	
	GN-20341	Windows Agent	에이전트 알림 팝업이 떠 있는 상태에서 에이전트 멈춤 현상	5.0.0

16.3.32 Genian NAC 5.0.27 Release Notes (2019-12-30)

Last Updated: 2020-02-24

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-18882	WebUI	OWASP ZAP 툴에 의해 검색된 관리콘솔 취약점 개선		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-20434	WebUI	노드그룹 업데이트 팝업 UI/UX 변경	5.0.27
	GN-20370	WebUI	시스템 센서 명령 Rest API 구현	
	GN-20337	CLOUD	Cloud NAC Syslog 서버 지원	
	GN-20334	WebUI	IP신청시스템 관리화면전환 기능 숨김처리	
	GN-20078	WebUI	노드 일괄 등록시 태그를 설정하여 자동 등록 되도록 개선	
	GN-20048	Center, Sensor	IoT 장치 플랫폼탐지 기능	
	GN-19993	Windows Agent	컴퓨터이름 변경 플러그인에 노드정책의 호스트명제한 설정값 적용	
	GN-19944	WebUI	제품에 업로드 된 에이전트에 대해서만 UI에 표시되도록 개선	
	GN-19929	Center, CWP, Windows Agent	CWP URL을 이용한 Scraping(크롤링)을 방어 가능하도록 개선	
	GN-19910	WebUI	사소한 UI Look & Feel 수정	
	GN-19906	WebUI	노드관리 목록의 제어정책 출력시 Passive/Active 구분 가능하도록 수정	
	GN-19794	Center	업그레이드시 디폴트 노드그룹 사용할 수 있도록 개선	
	GN-19739	Center	로그필터 알람전송을 SMS, EMAIL 구분하여 전송할 수 있도록 개선	
	GN-19737	macOS Agent	macOS 사용자 알림메시지 플러그인 추가	
	GN-19386	Center, Sensor, WebUI	FQDN 네트워크 객체 동작 방식 개선	
	GN-19374	WebUI	로그 리포트 목록 항목에 링크 제공	
	GN-18871	WebUI	License 파일에 유지보수 만료일이 설정되어 있을 경우 우선 적용하도록 개선	4.0.127, 5.0.24
	GN-18500	Center	리포트로 생성된 파일 주기적으로 삭제하는 기능	
	GN-17867	WebUI	노드 목록의 플랫폼 링크를 플랫폼 이름으로도 가능하도록 개선	
	GN-14643	Center	스위치 자신의 관리IP에 대해서 스위치정보가 표시되지 않는문제	
	GN-12430	GenianOS	원격 센서 디버그를 관리콘솔에서 확인할 수 있도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-20870	macOS Agent	macOS Catalina에서 에이전트 업데이트가 수행되지 않는 문제	5.0.27
	GN-20577	Center	정책서버 HA 이중화 환경에서 파일 동기화 수행되지 않는 문제	4.0.39, 4.0.116, 5.0.13
	GN-20537	GenianOS	제품 설치직후 IPv6 Link Local 주소가 인터페이스에 설정되지 않는 문제	5.0.27
	GN-20507	Center	CRAM-MD5 인증방식으로 메일이 전송되지 않는 문제	5.0.16
	GN-20506	WebUI	동의페이지 > 보안서약에서 수집정보 할당 시 추가 버튼을 눌러도 반응이 없는 문제	5.0.27
	GN-20498	WebUI	관리 > 노드 > 현황&필터 > 에이전트 > 액션별 수행결과 선택 시 시스템 에러 페이지 발생	5.0.27
	GN-20437	WebUI	IP사용신청서 관리뷰 편집의 초기화 기능이 동작하지 않는 문제	5.0.22
	GN-20380	WebUI	Windows 업데이트 상세 현황의 테이블 필터가 이전 필터 결과(승인)에 영향을 받는 문제	4.0.M8
	GN-20368	WebUI	로그인한 관리자가 아닌 관리자의 타임존 수정시 로그인한 관리자의 타임존이 변경되는 문제	4.1.M4
	GN-20330	WebUI	신규등록 사용자신청서 임시계정 승인시 사용기간 날짜 포맷이 yyyy-MM-dd가 아니면 오류발생 문제	5.0.0, 4.0.107
	GN-20326	WebUI	무선랜 대시보드 정보 조회에서 이전 조건이 포함되어 결과를 잘못 표시하는 문제	4.0.M8
	GN-20311	WebUI	신규등록 사용자 신청서 목록 화면 용도 다국어 표시 및 승인/거부 사유 입력시 UI 깨짐 문제	5.0.24
	GN-20304	macOS Agent	macOS 프린터 정보가 삭제되었으나 정보를 갱신하지 못하는 문제	5.0.16
	GN-20289	IPMGMT	승인대기 중인 IP신청서/장비변경신청서 수정과 사용자 변경이 되지 않는 문제	5.0.13
	GN-20197	WebUI	CWP 지원언어 설정에 따라 CWP 사용자 정의버튼 생성시 이름을 입력해도 "이름을 입력해주세요" 문구가 표시되는 문제	4.1.M5
	GN-20111	WebUI	무선랜 관련 위젯명이 모호한 부분 및 카운터 맞지 않는 문제 수정	4.0.M8
	GN-19918	WebUI	Windows 업데이트 모음 일괄작업 취소 버튼이 동작하지 않는 문제	4.0.0
	GN-17968	Windows Agent	5G 탐지가 되는 무선랜카드가 있어도 2.4G AP 정보만 수집 될 수 있는 문제	4.0.0, 4.1.0, 5.0.0
	GN-17723	Enforcer	SS64버전의 MAC당 최대등록 옵션이 센서 인터페이스별로 적용되지 않는 문제	4.1.M8

16.3.33 Genian NAC 5.0.26 Release Notes (2019-12-02)

Last Updated: 2020-01-06

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-20576	Windows Agent	에이전트의 AD인증대체 기능이 Azure AD 환경에서도 동작하도록 수정	
	GN-20523	Center	Agentless AD 인증대체 - Windows Server 2008 지원	5.0.25
	GN-20385	WebUI	IP 신청서 관리화면 쿼리 개선 및 노드그룹 관리화면의 예외노드그룹 사용처 체크 로직 개선	
	GN-20328	Sensor	IPv6 감사기록이 과다하게 남는문제	
	GN-20296	Sensor	기본 ARP Poisoning 주기를 1초로 변경	
	GN-20098	WebUI	감사로그 타임라인차트의 차트타입 변경 및 anomaly 색상 변경	
	GN-20062	CWP	CWP 사용자정의 버튼을 통해 파일 다운로드 시 VC 경로의 파일 일 경우 정상적으로 다운로드 되지 않는 문제	
	GN-20010	WebUI	이메일 발송리포트 자동생성된 항목을 수동으로 다운받을 수 있도록 수정	5.0.24
	GN-20008	GenianOS	NMAP 최신버전 업그레이드	
	GN-19975	WebUI	시스템관리 센서 최근 갱신시각 컬럼 추가	
	GN-19955	WebUI	무선랜 관리 SSID 검색시 대소문자 구분하지 않도록 개선	
	GN-19928	Windows Agent	에이전트 Failsafe 기능을 에이전트 액션별로 설정가능하도록 개선	
	GN-19860	macOS Agent	macOS 원격 에이전트 삭제 코드 재발급할 수 있도록 개선	
	GN-19852	WebUI	'이미 작업이 완료되었습니다.' 라는 메시지가 간헐적으로 발생하는 문제	
	GN-19849	macOS Agent	macOS 에이전트의 macOS Catalina 지원	
	GN-19766	Center	원격 에이전트 삭제시 에이전트설치노드그룹에서 포함되지 않도록 개선	
	GN-19765	WebUI	목록 UI에서 표시된 정보가 잘리는 문제 개선	
	GN-19753	WebUI	플랫폼 현황 목록에 해당하는 CVE 수 표시	
	GN-19702	WebUI	노드관리 링크 검색조건이 검색창에 표시되도록 개선	
	GN-19373	WebUI	노드 스냅샷 그룹항목 출력 개선	
	GN-19107	Windows Agent	에이전트 인증창 전체화면 잠금 기능 사용시 웹페이지를 자체 윈도우에서 표시하도록 개선	
	GN-18475	Linux Agent	리눅스 에이전트의 DB(sqlite3)에 보안성 강화	4.0.119, 5.0.16

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-20596	Windows Agent	네트워크정보수집 플러그인으로 연결된 AP 정보 얻을 때 SSID 깨지는 문제	4.0.0, 4.1.0, 5.0.0
	GN-20584	Windows Agent	액션을 통하여 프로세스 강제종료 후 감사로그 남지 않는 문제.	5.0.25
	GN-20581	macOS Agent	macOS 에이전트 액션 수행 결과가 갱신되지 않는 문제	5.0.11
	GN-20551	WebUI	제어정책 > 센서운영모드 현황 위젯에서 Active 한 노드 상태의 센서만 출력되는 문제	4.0.106
	GN-20545	Windows Agent	플러그인의 리부팅 옵션 관련 알림메시지 표시 오류	5.0.0
	GN-20536	Sensor	노드 SNMPv3 검사시 센서데몬 비정상 종료	5.0.17
	GN-20521	WebUI	ES 6.8에서 로그리포트 항목을 읽어오지 못하는 오류	5.0.24
	GN-20517	CWP	사용자동의 페이지에서 동의 체크박스를 체크하지 않고 동의 시 새로고침되면서 약관내용이 표시되지 않는 문제	5.0.22
	GN-20510	Center	사용자 인증 실패시 에러메시지 누락	5.0.20
	GN-20508	WebUI	노드 현황&필터에서 플랫폼 정보가 출력되지 않는 문제	5.0.26
	GN-20488	Windows Agent	에이전트 커스텀 아이콘 동작하지 않는 증상 수정	5.0.0
	GN-20485	Windows Agent	장치제어 예외설정이 동작하지 않는 문제	4.0.20, 5.0.0
	GN-20482	Windows Agent	통합에이전트 사용시 GPI 메뉴 연동 오류 수정	5.0.19
	GN-20454	WebUI	정책 사용중 icon 이미지 표시가 브라우저에 따라 정상적으로 표시되지 않는 문제	5.0.16
	GN-20440	WebUI	사용자 > 전체사용자 > 부서별 메뉴 클릭시 오류 발생	5.0.26
	GN-20426	WebUI	제어정책에서 사용중인 제어액션을 삭제할 수 있는 문제	4.0.M8
	GN-20420	Center	관리자 email, 휴대폰번호 여러개 설정시 로그필터 알람, 알람테스트 실패하는 문제	4.0.M4
	GN-20402	Windows Agent	위험정책 위반으로 에이전트에서 인터페이스 차단 후 5분 후에 네트워크를 계속 사용할수있는 문제	3.5.0, 4.0.0, 4.1.0, 5.0.0
	GN-20378	Linux Agent	리눅스 최신 배포판에서 리눅스 에이전트 설치 실패함.	4.0.128, 5.0.25
	GN-20335	WebUI	호스트 인증된 노드가 현황&필터에서 인증안됨 상태로 분류되는 현상	5.0.20
	GN-20308	WebUI	오류페이지에 bundle messageid 가 출력되는 현상	5.0.26
	GN-20291	Linux Agent	Linux Agent 설치 안되는 문제	4.0.128, 5.0.25
	GN-20235	macOS Agent	NAC를 통한 연결로 macOS 업데이트를 설정한 경우 업데이트가 동작하지 않는 문제	5.0.11

continues on next page

Table 29 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-20199	CWP	호스트인증일때 CWP에서 비밀번호 인증창이 보이는 문제	5.0.14
	GN-20188	WebUI	사용자 현황&필터에서 연동구분 Tree를 펼치면 위의 직급 리스트가 정상적으로 표시되지 않는 문제	4.0.M6
	GN-20181	WebUI	사용자> 현황&필터> 연동구분의 위젯에서 "연동계정" 이름이 중복 표시되는 문제	4.1.M4, 4.0.18
	GN-19983	Elastic-Search	메모리 4GB인 장비에서 로그서버 단독구성 시 Elastic-Search 구동되지 않는 문제	4.1.1
	GN-19769	WebUI	컴플라이언스정책 생성/삭제 동작에 따라 "변경정책 적용" 버튼이 다르게 동작하는 문제	4.1.M6
	GN-19678	- Unknown/None	장비 라이선스가 정상적임에도 라이선스 경고창이 계속 해서 뜨는 문제	4.0.15
	GN-19455	GenianOS	정책서버 점검 스크립트(sysinspect)에 LOG서버(Elastic-search) 포트변경에 대한 고려가 되지 않은 문제	4.0.117, 5.0.14
	GN-18864	WebUI	센서 alias 에 대한 부분이 매트릭스뷰에 적용되어 있지 않은 문제	4.0.116, 5.0.13

16.3.34 Genian NAC 5.0.25 Release Notes (2019-11-04)

Last Updated: 2019-12-13

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-20386	CWP	CWP Alert 메시지를 브라우저 기본 Alert을 사용하지 않고 메시지를 보여주도록 개선	
	GN-20305	GenianOS	Intel NUC7 wireless interface not support	
	GN-19998	WebUI	무선랜정책 Air-Sentry 필요 알림 메시지 추가	
	GN-19995	Database	Grammarly를 이용한 영문 오타자 문법오류 수정	
	GN-19984	Windows Agent	노드상세정보의 인터페이스정보 링크 값을 UP/DOWN으로 표시	
	GN-19956	Center	무선랜 BSSID(MAC) 유사성 검색 개선	
	GN-19946	WebUI	[GS인증]사용자 ID 생성시 사용할 수 없는 ID에 대한 검증 기능 추가	
	GN-19917	WebUI	권한의 조건설정 중 네트워크 객체에 노드그룹을 할당 할 수 있도록 기능 추가	
	GN-19916	WebUI	사용자관리 목록에 누락된 컬럼 추가	
	GN-19914	macOS Agent	[CC] macOS 에이전트 프로그램 정보의 제품명을 Genian NAC Suite v5.0으로 변경	

continues on next page

Table 30 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19913	GenianOS	syscollect에 정보수집 추가	
	GN-19912	WebUI	노드그룹 리스트 목록의 설정정보 중 중복된 에이전트 필요여부 아이콘 표시 개선	
	GN-19909	Center	윈도우 디펜더와 일반 백신이 동시에 설치되어 있는 PC 들은 백신관련 노드그룹이 정상 동작하지 않는 문제	
	GN-19907	CWP	SAML을 통한 인증 후 에이전트에서 "사용자 인증 정보" 클릭시 나오는 UI 개선	
	GN-19903	Authsync	부서동기화시 부서 생성/삭제에 대한 감사기록 생성	
	GN-19899	Database	Google G Suite 정보 동기화 예제추가	
	GN-19898	Windows Agent	PC전원제어 플러그인에서 즉시실행 버튼 클릭시 다시 한번 확인는 메시지창(YES/NO)이 팝업되도록 개선	
	GN-19889	WebUI	WebUI에서 감사로그 처리 로직 개선	
	GN-19886	Center	노드그룹 3단계 이상의 다중 중첩 그룹 지원	
	GN-19882	WebUI	시스템 관리 > 작업선택 > 센서 생성 메뉴 추가	
	GN-19881	CLI/gnlogin	CLI Interface VLAN 추가 및 수정 시 사용자 실수 방지를 위한 확인 절차 추가	
	GN-19856	Windows Agent	라톤테크 SSO 연동 Custom Plugin 개발	
	GN-19842	Hardware	ipmicfg 구동시 발생하는 경고 메시지 제거	
	GN-19831	RADIUS	[범용 OS] RADIUS 기능 동작하도록 개선	
	GN-19827	Center, RADIUS	노드의 상태 변경(노드그룹 포함 및 사용자 그룹 포함 여부)에 따라서 VLAN을 재할당 받도록 한다	
	GN-19826	Center, RADIUS	802.1X 감사기록 강화	
	GN-19825	Center, RADIUS	802.1X Radius 인증처리를 통한 신규노드 등록	
	GN-19823	WebUI	Active 센서가 없을때 제어정책 상단에 알림창 출력	
	GN-19804	WebUI	노드그룹 내보내기 가져오기 기능 추가	
	GN-19792	Center	CVE데이터 관련 노드그룹 조건 추가	
	GN-19786	Genian Syncer	GnSyncer 업데이트 유무 확인기능	
	GN-19785	WebUI	Genian Syncer 제품 설치 패키지 내에 포함	
	GN-19775	GPDB	GPDB 업데이트 시 연결방식 필드도 비교 대상에 포함하도록 개선	
	GN-19762	WebUI	정책 생성시 정책 기본설정의 설명이 감사 로그에 남도록 개선	

continues on next page

Table 30 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19750	Center	Elasticsearch 6.x 버전 업데이트 후에도 정책서버 정상 동작할 수 있도록 개선	
	GN-19744	RADIUS, WebUI	RADIUS shared secret 다중으로 설정가능하도록 개선	
	GN-19743	WebUI	노드그룹 조건 연산자 설명 및 리스트 표시 개선	
	GN-19738	WebUI	CLOUD NAC Web Install Wizard에서 SMS 국가코드 선택 UI 추가	
	GN-19703	GenianOS	GNAC 설치 스크립트에서 최소 디스크 크기 검사하도록 개선	
	GN-19623	Authsync	노드정보 동기화시에 인증사용자의 부서/직급정보가 있으면 업데이트하도록 개선	5.0.1, 4.0.108
	GN-19542	Center	비밀번호 찾기 SMS 인증시 인증 코드의 유효시간 설정을 추가	3.0_0912
	GN-19385	WebUI	WebUI_SiteMap 테이블 구조 개선 / 페이지 설정(기존화면 / 신규화면) 기능 추가	
	GN-19274	Center, Sensor	Agentless AD 인증대체 및 시스템정보 수집	
	GN-18858	WebUI	모든관리자에게 시스템 제공 리포트 email 전달기능 및 관리화면 개선	
	GN-18679	GenianOS	제품 패키지에 MSI 설치파일 추가 및 관리콘솔을 통한 다운로드 기능	
	GN-17138	WebUI, Windows Agent	장치제어 사용편의성 강화	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-20398	Center	호스트인증시 CWP 접속노드의 인증상태 확인이 정상적으로 되지 않는 문제	5.0.16
	GN-20377	Elastic-Search	Elasticsearch 프로세스가 template 설정 파일이 적용되지 않은채로 시작될 수 있는 문제	4.0.17
	GN-20366	WebUI	디버그로그 화면에서 권한 없는 기능에 대한 메시지 출력 등 오류사항 및 정렬 및 파일 예외처리 기능 추가	5.0.25
	GN-20360	Elastic-Search	로그 검색필터 변경시 percolator 쿼리가 변경되지 않는 문제	5.0.24
	GN-20345	Sensor	플랫폼 정보가 지속적으로 변경되는 문제	5.0.24
	GN-20340	WebUI	관리-사용자-전체관리자-(사용자클릭)-이력관리 CSV 파일 내보내기 시 오류	5.0.24
	GN-20338	Authsync	사용자정보 동기화로 사용자 생성/삭제시 감사기록의 사용자ID 컬럼에 사용자ID 표시되지 않는 문제	4.0.119, 5.0.17
	GN-20332	WebUI	설치 후 기본 생성된 일일리포트의 이메일폼 항목이 빈값으로 표시되는 문제	5.0.24

continues on next page

Table 31 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-20309	GPDB	노드관리 화면에서 플랫폼 링크가 잘못 걸리는 문제	5.0.0
	GN-20282	GenianOS	UEFI 시스템에서 제품이 설치되지 않는 문제	5.0.9
	GN-20274	WebUI	REST API apiKey로 호출시 한번 인증을 성공하면 계속 호출이 가능한 문제	5.0.23
	GN-20266	Windows Agent	비밀번호인증과 AD인증대체를 같이 사용할 경우 인증대체 실패시 인증알림메시지 미표시 문제	3.4.5, 4.0.0, 5.0.0
	GN-20246	Center, Sensor	AD 서버주소를 도메인으로 설정시 Agentless 인증대체 기능이 동작하지 않는 문제	5.0.25
	GN-20225	Windows Agent	Dissolvable Agent 사용시 일정기간 센터 미접속시 에이전트 삭제 기능 동작안함.	5.0.17
	GN-20206	WebUI	관리자 비밀번호 찾기지 SMS 인증코드 유효시간이 만료됐으나 인증되는 문제	5.0.25
	GN-20205	Center	관리자 비밀번호 찾기지 SMS 인증코드 유효시간이 만료됐으나 인증되는 문제	5.0.25
	GN-20100	Center	Agentless AD 인증대체 - 도메인에 가입되지 않은 상태에서 로그인 수행시 인증대체 처리되는 문제	5.0.25
	GN-19982	Center	비밀번호 저장방식이 HMAC-SHA256 임에도 동일한 비밀번호에 대해 동일한 해쉬가 나오는 문제	4.0.13
	GN-19979	WebUI	'NIC벤더별 MAC 수 현황' 위젯에서 보여지는 수량과 NIC 벤더 노드리스트 갯수가 일치하지 않는 문제	4.0.M7
	GN-19971	Database	SAML 관련 default DB 값이 dbmigration시 duplicate 오류 발생 문제	5.0.19
	GN-19966	WebUI	이메일 발송 리포트 자동생성에 성공했으나 실패 감사로그가 남는 문제	5.0.23
	GN-19884	CWP	CWP > 사용자 등록> 가져오기 페이지에서 '파일선택'으로 가져오기가 되지 않는 문제	5.0.0
	GN-19868	macOS Agent	macOS 화면보호기 제어 시 동작/동작해제가 반복되는 문제	5.0.15
	GN-19861	macOS Agent	macOS 네트워크 인터페이스 변경 시 에이전트 동작안함 상태로 표시되는 문제	5.0.13
	GN-19855	Center	과거비밀번호 기억 개수를 줄여도 예전 비밀번호가 남아 있는 문제	3.0_1007
	GN-19841	CWP	[범용 OS] CWP 페이지가 제대로 표시되지 않는 문제	5.0.23
	GN-19763	GPDB	WebBrowser 정보가 수집되었으나 오탐보고 버튼이 출력되지 않음	4.0.124, 5.0.21
	GN-19758	GenianOS	[범용 OS] 센터/센서 재구동 명령(systemctl restart)이 간헐적으로 비정상 동작하는 문제	5.0.23
	GN-19757	GenianOS	[범용 OS] 시스템 재부팅시 각 데몬들이 elasticsearch에 접근하지 못하는 문제	5.0.23
	GN-19740	Authsync	[범용 OS] 정보 동기화가 정상 동작하지 않는 문제	5.0.23
	GN-19713	WebUI	[범용 OS] 웹 콘솔에서 파일업로드 기능이 동작하지 않는 문제	5.0.23
	GN-19708	Database	[범용 OS] mysql 쿼리시 정책서버가 비정상 동작하는 문제	5.0.23

continues on next page

Table 31 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19669	VRRPD	HA no-virtual-mac 사용시 nopreempt 설정이 정상동작하지 않는 문제	4.1.M3
	GN-19469	CWP	보안질문 답변이 비어있으나 답변입력 화면이 출력되지 않는 문제와 보안질문과 관련된 사용성 부분 개선	5.0.20
	GN-18862	WebUI	지니안 모니터에서 감사기록(위험) 카운트 클릭시 로그 인페이지로 이동되는 문제	4.0.112, 5.0.9

16.3.35 Genian NAC 5.0.24 Release Notes (2019-10-04)

Last Updated: 2019-11-14

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-20041	Center, Enforcer, Sensor	미러센서 차단방식 옵션으로 동작하도록 개선	
	GN-20022	WebUI	동의페이지 약관명 입력가능 글자수 늘림 및 줄바꿈 가능하게 개선	
	GN-19879	WebUI	정책, 설정, 시스템 메뉴에 서브메뉴 추가	
	GN-19840	Windows Agent	Symantec Endpoint Protection 제품 버전정보 수집 기능 추가	
	GN-19816	Hardware	C10 SYSDEV 변경	
	GN-19790	WebUI	센서 Active 모드관련 설정 위치변경	
	GN-19782	Sensor	센서 예외처리 MAC 설정시 커널모듈(enforcer)에도 해당 노드가 등록되지 않도록 수정	
	GN-19749	CWP	CWP 사용자 등록페이지(Guest)의 비밀번호 필드의 설명문 추가 가능하도록 개선	
	GN-19747	WebUI	노드 > 일괄작업 > 장비속성변경 기능 추가	
	GN-19735	Sensor	Redundant Power 상태 감사기록 추가	
	GN-19734	WebUI	IP Matrix View DHCP Pool 표시색상 변경	
	GN-19732	GenianOS	부팅시 발생하는 불필요한 오류메시지 제거	
	GN-19727	Center	글로벌버전에서 SMS를 이용한 2단계인증 추가	
	GN-19721	WebUI	Cloud NAC 라이선스에 region 정보와 Cloud site의 공인IP를 표시하도록 개선	5.0.23
	GN-19711	WebUI	Web Browser URL에 정책서버 IP 입력 시 웹페이지 Title 정보에 Genian NAC가 표시되는 문제	

continues on next page

Table 32 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19695	Center	4.1 버전에 백업파일 ftp/sftp 전송시 포트설정 기능 추가	
	GN-19688	Windows Agent	PassNI SSO 연동 플러그인 로그아웃 처리 기능 추가	
	GN-19682	Windows Agent	Windows 10 1809 이후 버전 부터 Windows Defender 버전 정보 수집 안되는 문제	
	GN-19671	Center	플랫폼을 분류하지 못한 경우 NIC Vendor 를 플랫폼정보로 사용하도록 개선	
	GN-19670	WebUI	"New detections since last login" 위젯에 Device 개수 추가	
	GN-19668	Windows Agent	백신정보 플러그인에 CylancePROTECT 정보 수집 기능 추가	
	GN-19618	Authsync	사용자정보 동기화에서 인증처리 MAC/IP 옵션 사용시 노드리스트, 장비리스트의 부서/직급 정보 업데이트되지 않는 문제	4.0.M3, 3.4.3
	GN-19594	Center	성능개선을 위한 CVE데이터 Elasticsearch에 저장	
	GN-19590	WebUI	시스템 관리의 상세 페이지 뷰에서 돌아가기 기능이 없어 목록보기 상태로 이동하기 불편한 문제	
	GN-19550	Center, WebUI	Elasticsearch version과는 관계없이 정책서버 동작하도록 개선	
	GN-19520	WebUI	CONF Engine의 addRemove component의 동작구조 개선	
	GN-19435	Center, ElasticSearch, WebUI	CVE 데이터 ES로 사용하도록 개선	
	GN-18691	WebUI	영문 UI OS구분에 따른 소프트웨어목록의 타이틀 개선	
	GN-18404	WebUI	사용자 신청서 관리화면에서 파일업로드 한 파일 다운로드 가능하도록 개선	
	GN-17739	Windows Agent	[McAfee] Total Protection VirusScan, Endpoint Security 백신 제품 정보 수집 기능 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-20273	WebUI	관리자 사용자관리범위 제한' 추가(하위포함)'이 동작하지 않음	5.0.24
	GN-20260	WebUI	대체인증 사용시 노드 목록에서 엑셀 내보내기 기능이 인증사용자 정보가 없어서 오류 발생 문제	4.0.127, 5.0.24
	GN-20245	WebUI	노드상세화면에서 추가필드가 잘못출력되는 문제	5.0.21
	GN-20232	WebUI	노드그룹 카테고리 생성시 설정한 상위 카테고리로 적용되지 않는 문제	5.0.23
	GN-20203	Windows Agent	WCM에서 MsChapV2 인증방법사용되는 AP에 연결안되는 문제	5.0.0

continues on next page

Table 33 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-20196	Windows Agent	모양 및 개인설정 플러그인이 정책에서 제외될 경우 Gn-Plugin hang 문제	4.0.124, 5.0.21
	GN-20195	WebUI	CWP 사용자 신청서에 추가한 조직명/부서명 등의 사용자 정보가 관리콘솔 페이지에서 보이지 않는 문제	4.0.127, 5.0.24
	GN-20187	macOS Agent	신규 macOS 설치 시 Unknown으로 표시되는 문제	4.0.122, 5.0.19
	GN-20185	WebUI	노드상세화면에서 MAC 허용 변경금지(모든 IP 대역) 설정시 MAC 차단되는 문제	5.0.22
	GN-20082	WebUI	로그리포트 즉시수행 시 설정한 '감사로그필터' 가 아닌 모든 로그가 출력되는 오류	5.0.24
	GN-20071	Center	센터에서 정보업데이트 시에 Unknown 컬럼 처리 오류에 따른 (데이터베이스 오류. ERRMSG='Duplicate entry') 로그 발생	4.1.0, 4.0.23
	GN-20055	Center	IP신청서 거부처리 기능 사용시 부하가 발생할 수 있는 문제	4.1.2, 4.0.25
	GN-20004	Database	영문버전 설치시 Windows Update Action의 패치모음이 설정되지 않는 문제	4.0.106
	GN-19992	Center	이미지 업그레이드 시 확인된 노드타입 및 확인된 플랫폼 정보가 갱신될 수 있는 문제	4.0.114, 5.0.11
	GN-19981	WebUI	노드스냅샷에서 검색어 입력 시 검색이 되지 않는 문제	5.0.24
	GN-19968	Center	CVE데이터 출력되지 않는 문제	5.0.24
	GN-19932	Sensor	DHCP로 할당된 IP가 노드 삭제시 Expire 처리가 안되고 계속 사용중이 되는 문제	4.0.5
	GN-19923	Hardware	NAC5.0 복구이미지 에서 C50_R1 설치시 DBDEV 영역 설정 되는 문제 발생	5.0.21
	GN-19921	WebUI	Radius 서버 설정에서 새로운 CA 인증서 업로드 시 업로드한 CA 인증서 정보로 업데이트 되지 않는 문제	5.0.21
	GN-19908	Windows Agent	백신정보 수집 플러그인 Windows Defender 미설치 상태에서도 백신 이름 정보가 전송되는 문제	4.0.14, 5.0.0
	GN-19883	WebUI	제품 업그레이드 이후 관리자 Web Console 최초 로그인 시 "라이선스 경고" 메시지 출력되는 문제	5.0.19
	GN-19878	WebUI	리포트 생성시 오류 발생하면 INFO로 감사로그가 남는 문제	4.0.M5
	GN-19853	Windows Agent	스크립트 수행 플러그인 실행시 cmd 창이 팝업 되는 문제	4.0.3, 5.0.0
	GN-19835	macOS Agent	macOS 수행조건만 검사로 인증상태 검사 시 액션수행 결과가 다르게 표시되는 문제	5.0.21
	GN-19817	WebUI	라이선스 초과 메시지 출력 오류	5.0.21
	GN-19799	Center	노드정책의 에이전트 사용여부에 의해 삭제시 장기간다운에 의한 정보삭제로 감사기록 남는 문제	3.3.2.1010
	GN-19796	IPMGMT	IP신청시스템 Secondary 대역 IP신청 승인시 결과조회 화면의 사용위치항목이 Primary 센서로 출력되는 문제	4.0.113, 5.0.10
	GN-19788	macOS Agent	macOS 에이전트 만료 전 알림 기능이 동작하지 않는 문제	5.0.13

continues on next page

Table 33 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19773	macOS Agent	macOS 노드에 대해 에이전트 업데이트 수행 후 에이전트가 동작하지 않는 문제	5.0.18
	GN-19772	Sensor	2.4G AP의 프로토콜정보를 표시하지 못하는 문제	4.1.2
	GN-19764	WebUI	Android 및 iPhone 모바일 OS에 대한 Google OTP 앱 다운로드 주소 변경	4.0.48, 4.0.125, 5.0.22
	GN-19759	Windows Agent	무선랜제어 플러그인을 통하여 5G 무선AP의 프로토콜 잘못 수집되는 문제	4.1.2, 5.0.0
	GN-19755	macOS Agent	macOS의 네트워크 서비스를 삭제할 경우 에이전트 로그가 반복해서 출력되는 문제	5.0.14
	GN-19728	WebUI	관리 > 노드의 엑셀 내보내기시 UI에 표시된 인증사용자명이 출력안되는 문제	4.0.7
	GN-19725	macOS Agent	이벤트 포트 변경 시 macOS 에이전트 동작이 멈추는 문제	5.0.11
	GN-19709	WebUI	IE에서 SMS 인증화면 UI 및 신청결과조회 input 컬럼 한 줄로 나오는 오류 개선	5.0.23
	GN-19696	Center	비밀번호 변경 시 설정된 비밀번호 암호화 알고리즘 저장방식으로 변경되도록 수정	4.0.M6, 3.5.0, 3.4.6
	GN-19602	GenianOS	에이전트 정보 삭제 시간 체크가 정상적으로 동작하지 못하는 문제	5.0.8, 4.0.111, 4.0.34
	GN-19556	RADIUS	RADIUS 서버설정의 TLS사용시 CA인증서 등록후 다운로드 클릭하면 오류페이지 발생하는 문제.	5.0.19
	GN-19289	macOS Agent	macOS의 시스템 정보가 IE에서 한글이 분리되어 표시되는 문제	5.0.14

16.3.36 Genian NAC 5.0.23 Release Notes (2019-09-03)

Last Updated: 2019-10-04

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-19953	WebUI	소프트웨어 업데이트 화면을 통한 업데이트 동작시 메시지 출력 방식 개선	
	GN-19945	WebUI	Basic / Pro Edition에서 Notification 사용할 수 있도록 처리	
	GN-19905	Database	Tag 기반 디폴트 노드그룹 추가	
	GN-19900	Database	AD 사용자 정보 동기화 예제추가	
	GN-19880	WebUI	노드그룹 생성 시 정책그룹 / 상태그룹 메뉴표기 및 출력 아이콘 표기 개선	
	GN-19800	Center	에이전트 수집한 정보에 대한 기본 노드 그룹 추가	

continues on next page

Table 34 - continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19731	WebUI	노드관리 목록에 스위치 인터페이스 정보 컬럼 추가	
	GN-19693	WebUI	네트워크 객체 생성시 FQDN 설정의 경우 입력값에 대해서 validation 강화	
	GN-19690	WebUI	노드 > 현황&필터 > 에이전트에 Windows 제품 Key 현황 UI 추가	
	GN-19666	WebUI	관리콘솔의 노드에서 CSV를 이용한 등록 시 센서 '자동선택' 및 MAC, 시간에 대한 자동 입력 기능, 오류 메시지 개선	4.0.125, 5.0.22
	GN-19649	Sensor	Invalid DHCP DNS 감사기록 개선	
	GN-19631	Center	에이전트 액션 플러그인 업로드 및 삭제 시 감사기록 개선	
	GN-19614	CLI/gnlogin	CLI에서 인터페이스 IP 설정 시 Network 및 Broadcast IP 가 사용되지 않도록 개선	
	GN-19609	Center	정책적용 동시 수행 최소화	
	GN-19596	WebUI	제어정책 생성시 권한할당이 없을 경우 권한객체 컬럼의 값에 PERM-DENY가 출력되어 사용자가 인지할 수 있도록 적용	
	GN-19589	WebUI	Web 관리콘솔 타이틀 문구에 대한 글자수 제한 개선	
	GN-19558	WebUI	CWP2 아이디, 비밀번호찾기 미 설정시 block 엘리먼트 남아있는 오류 및 알림 메시지 가로 크기 수정	
	GN-19545	WebPlugin	[스타벅스 웹플러그인] 기존 작업된 부분에서 IP 신청 연동시 IP변경 금지 로직 제거	
	GN-19515	Center	RADIUS MAC인증(MAB(MAC Authentication Bypass)) 에서 인증실패시 감사기록 남기도록 개선	
	GN-19506	GenianOS	사용자가 로그인한 최근로그인 IP 를 출력하도록 개선	
	GN-19488	WebUI	관리콘솔의 관리>스위치>스위치관리 화면의 테이블을 편집가능하도록 개선	5.0.21
	GN-19485	Center, Database, Sensor	스위치 관리에 스위치 소프트웨어 버전정보 추가	
	GN-19483	Linux Agent	리눅스 에이전트의 운영로그에 대해서 주기적으로 삭제하도록 기능 개선.	4.0.125, 5.0.22
	GN-19472	WebUI	WebUI 설정 > 관리콘솔의 노드관리 기본대상/관점/뷰 옵션 제거	
	GN-19460	WebUI	시스템 카탈리나 로그에 Error 발생시 Error발생 경로를 표시하도록 개선	5.0.22
	GN-19431	WebUI	대체인증 사용시 에이전트에서 사용자정보보기를 할 수 없는 문제	
	GN-19423	Linux Agent	리눅스 에이전트의 동일 로그에 대해서 중복 방지 기능 구현 함.	4.0.112, 5.0.9
	GN-19403	WebUI	[REST API] 네트워크 객체 관리 API 추가	
	GN-19359	Linux Agent	리눅스 에이전트의 신규 리눅스 배포판 지원	4.0.124, 5.0.21

continues on next page

Table 34 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19337	macOS Agent	macOS 에이전트 프로그램 정보 창 오류보고 버튼 디자인 개선	
	GN-19272	CWP	CWP 페이지 모바일UI 지원	
	GN-19162	WebUI	신규 사용자 신청 승인시 인증제한 설정이 사용자용도 별로 자동 적용되도록 하는 기능	
	GN-19016	Center	에이전트 업/다운시 한번에 많은 정책적용이 발생하는 문제	
	GN-18839	GNOS	[범용 OS] NAC 범용OS에 설치할 수 있도록 패키징	
	GN-15960	WebUI	관리 UI에 에이전트 업로드 실패시 표시되는 메시지 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-20056	WebUI	[Cloud] 동일한 계정으로 다른 PC에서 로그인 시 기존 로그인 된 단말에서 로그아웃 없이 계속 사용할 수 있는 문제	5.0.6
	GN-20054	Center	글로벌버전에서 사용자패스워드 저장방식 초기 값이 NTHASH 로 설정되지 않는 문제	5.0.21
	GN-20016	WebUI	주기적 수행 웹플러그인 설치시 cwp 화면 출력 안되는 오류	4.0.116, 5.0.13
	GN-20013	Center	수동등록한 노드의 관리센서 변경 시 CUSTOM 값이 초기화되는 문제	4.0.114, 5.0.11
	GN-20006	CLOUD	Cloud NAC 알람메일의 정책서버 링크 포트번호가 8443으로 설정되어 접속이 안되는 문제	5.0.19
	GN-19980	Windows Agent	ARP관리 플러그인적용 중 관리 MAC에 대한 차단이 되지 않는 문제	4.0.39, 4.0.116, 5.0.13
	GN-19972	Center	센터 구동시 초기화 과정에서 DB 접속에 실패하는 경우 keepalive 처리 쓰레드 구동안되는 문제	4.0.117, 5.0.15
	GN-19970	WebUI	노드액션에 라벨을 추가하면 노드그룹 조건 중 에이전트 액션 > 특정 액션을 만족하면/안하면 조건의 아이콘 표시가 정상적으로 안되는 문제	5.0.20
	GN-19969	WebUI	센서 일괄 설정 시 센서의 옵션 중 수행시간 리스트 박스가 활성화 되지 않는 문제	5.0.9
	GN-19948	Windows Agent	사용자 전환 후 에이전트 동작하지 않는 문제	4.0.27, 5.0.0
	GN-19925	WebUI	스위치관리의 snmp 일괄수정 다이얼로그에서 snmp version 항목이 출력되지 않는 문제	5.0.17
	GN-19895	CWP	SAML 로그인 버튼 디자인이 깨지는 문제	5.0.23
	GN-19784	WebUI	macOS에서 차단이후 CWP에서 에이전트 다운로드시에 다른 브라우저가 열리는 현상	5.0.14
	GN-19723	Database	노드 리스트에서 연결방식 마우스 오버 시 by null로 표기되는 문제	4.0.0, 4.0.106

continues on next page

Table 35 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19661	Windows Agent	윈도우 Product Key가 정상적으로 수집안됨.	5.0.0
	GN-19653	Database	DB서버의 불필요한 계정 삭제되지 않는 문제	4.0.112, 5.0.9
	GN-19652	Center	정책서버에 센서가 등록되지 않는 상태에서 Global DHCP 모드 동작하지 않는 문제	4.0.5
	GN-19621	WebUI	Windows 업데이트 모음별 현황 위젯 카운트 불일치	4.1.0
	GN-19613	macOS Agent	macOS 인증 코드 입력 없이 에이전트 삭제 버튼 클릭 시 비정상 종료하는 문제	5.0.15
	GN-19612	WebUI	REST API를 통해 MAC 태그 할당되지 않는 문제	5.0.21
	GN-19607	Linux Agent	일부 리눅스 배포판(우분투 12.04)에서 자동 업그레이드 실패함.	4.0.125, 5.0.22
	GN-19601	macOS Agent	macOS 주기적 재인증 설정 시 에이전트가 비정상 동작하는 문제	5.0.19
	GN-19591	WebUI	사용자 추가필드 리소스변들 누락 및 파일 업로드 개선	5.0.0
	GN-19575	WebUI	CWP2 등록페이지에서 국제전화번호 select 창 레이어 위치가 버튼에 가려져서 보이지 않는 문제 개선	5.0.19
	GN-19574	Windows Agent	노드의 정책현황 화면에서 스크립트수행 플러그인 스크립트 결과 메시지가 표시되지 않는 문제	4.0.119, 5.0.16
	GN-19573	CLOUD	CLOUD 버전에서 파일검색실패 따른 배포기능이 동작하지 않는 문제	5.0.6
	GN-19572	WebUI	다중그룹생성 다이얼로그의 취소 버튼이 동작하지 않는 문제	5.0.22
	GN-19571	CLI/gnlogin	글로벌 버전은 gnlogin 에서 ssh 포트 변경 설정을 하여도 포트가 변경되지 않는 문제	4.1.5
	GN-19570	Windows Agent	에이전트가 로컬시스템 계정으로 동작할 때 (%UserDir%)에 대한 검사조건 동작 오류	5.0.0
	GN-19566	macOS Agent	macOS 업데이트를 지정한 시간대에 검사/설치하지 않는 문제	5.0.11
	GN-19565	Authsync	노드정보 동기화 사용시 사용자 인증 처리 후 에이전트로 이벤트 전송 안하는 문제 수정	
	GN-19563	macOS Agent	macOS 에이전트 '운영체제 시작시 재인증' 설정했으나 로그아웃에 실패하는 문제	5.0.0, 4.0.108
	GN-19561	WebUI	CWP2 동의페이지에서 수집정보 table-cell 크기 오류 수정	5.0.16
	GN-19560	Windows Agent	일부PC의 디스크 시리얼 정보에 깨진 문자가 표시되는 오류	5.0.0
	GN-19546	macOS Agent	macOS 호스트인증 시 트레이아이콘이 미인증으로 표시되는 문제	5.0.7
	GN-19544	Windows Agent	장치제어 플러그인에서 장치 차단 항목이 다른 장치제어 예외항목에 의하여 차단되지 않는 문제	4.0.0, 4.1.0, 5.0.0
	GN-19528	macOS Agent	OS X Mavericks에서 에이전트 동작하지 않는 문제	5.0.0

continues on next page

Table 35 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19527	Center	Database 오류 현황 감사기록 타입이 에러로 기록되는 문제	4.0.M4, 3.4.4
	GN-19526	Center	센서 장비 교체 시 가상IP 및 세컨더리IP 노드의 MAC 주소가 갱신되지 않음	4.0.M8
	GN-19514	WebUI	클라우드 환경에서 센터 주소가 사용자에게 노출되는 문제	5.0.20
	GN-19482	Windows Agent	WCM에서 사용중인 무선 프로파일 항목이 제거되었지만 정책에 반영되지 않는 문제	5.0.0
	GN-19459	macOS Agent	로그온 사용자가 다수일 때 에이전트 업데이트 되지 않는 문제	5.0.7
	GN-19339	macOS Agent	macOS 프로그램 정보 창에 설치된 플러그인 정보가 표시되지 않는 문제	5.0.16
	GN-19278	Linux Agent	리눅스 에이전트 업그레이드 시 기존 로그가 삭제되는 문제	4.0.112, 5.0.9
	GN-18907	macOS Agent	macOS Agent 프로세스가 비정상 종료되는 문제	4.0.108, 5.0.4
	GN-16751	Center	인증된 노드에 사용자재인증실정시 실제 인증정보가 있음에도 미인증 그룹에 속하는 문제	4.0.0

16.3.37 Genian NAC 5.0.22 Release Notes (2019-08-07)

Last Updated: 2019-09-03

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-19719	WebUI	InfoColumn 의 Disp 및 rendered 조건을 el 표현식으로 작성하여 ui 에 출력될 수 있도록 개선	
	GN-19650	Center	[Anomaly] Unregistered Node detected 감사기록 개선	
	GN-19645	Packaging	제품 이미지 생성시 동일버전의 센서 및 에이전트만 포함되도록 개선	
	GN-19644	Database	디폴트로 제공되는 노드관리뷰에서 등록시각을 가장 마지막 컬럼으로 순서조정	
	GN-19634	Authsync	Google G Suite 사용자 정보 동기화시 부서ID 동기화 가능하도록 개선	
	GN-19524	WebUI	UI Label Cleanup (EN)	5.0.21
	GN-19473	WebUI	UI Improvements to Control Wireless Connection Manager and Control WLAN Agent Plugins	5.0.21
	GN-19465	Center	백업파일 ftp/sftp 전송시 포트설정 기능 추가	
	GN-19461	WebUI	사용자 추가필드 중 파일업로드 타입을 필수입력 설정 가능하도록 개선	
	GN-19450	Center, Design, WebUI	이메일 Template 설정으로 변경 가능하도록 개선	

continues on next page

Table 36 - continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19443	Windows Agent	공유폴더 제어플러그인에서 프린터관리공유에 대한 예외옵션 추가.	
	GN-19430	Sensor	센서가 센터로 정책 요청시 연속적으로 실패할때 정책요청 soap에 딜레이를 주도록 개선	
	GN-19420	CWP	사용자 인증완료전 알림 팝업을 클릭하여 CWP페이지로 이동 시 로그인창이 보이도록 개선	
	GN-19394	WebUI	페이지 소스별로 중복정의된 항목 정리 / 공통 사용 함수 정리	
	GN-19390	WebUI	[CWP] 사용자 등록 동의페이지 스타일(글자크기, 색깔, 굵기 등) 변경 가능하게 개선	
	GN-19376	WebUI	이메일 발송 항목 개선	
	GN-19366	GenianOS	syscollect.sh 에 lsof 정보 수집기능 추가	
	GN-19363	Center	SMS/Email 전송 실패 감사기록 개선	
	GN-19356	Linux Agent, macOS Agent, Windows Agent	운영체제의 특정 버전별로 노드 그룹을 생성할 수 있는 기능 추가	
	GN-19355	Center, RA-DIUSD	RADIUS VLAN 할당 조건에 "Calling(Called)-Station-Id(MAC) 이 노드그룹에 포함되면" 조건 추가	
	GN-19294	WebUI	노드관리 목록의 컬럼을 부별 제한없이 사용가능하게 하고 카테고리로 구분하여 관리	
	GN-19276	WebUI	노드목록 출력시 설정된 Width값으로 출력되도록 개선	
	GN-19228	Linux Agent	리눅스 에이전트 일부 패키지의 무결성 검사 실패시, 전체 에이전트 패키지 재 설치하도록 개선 함.	4.0.112, 5.0.9
	GN-19226	Genian Syncer	GenianSyncer로 NAC운영데이터 업로드 방법 개선	
	GN-19182	Center	FQDN Lookup 결과 확인할 수 있도록 개선	
	GN-19152	WebUI	장비 수명주기 관리 (Device Lifecycle Management) 에서 파일(CSV)을 통한 일괄입력 기능 추가	
	GN-19114	WebUI	시스템 > 시스템관리에서 센서만 검색시 DB, LOG, RA-DIUSD 서버는 포함되지 않도록 개선	5.0.18
	GN-18855	WebUI	감사로그 UI 개선	
	GN-18854	WebUI	사용자와 관리자 생성 및 수정 UI개선	
	GN-18541	Windows Agent	프로그램 제거 플러그인에서 특정 문자열이 포함되는 프로그램을 제거할 수 있도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-19911	Center	미러센서에 NODEADDED 이벤트시 전체 노드정보가 추가되는 문제	4.0.106
	GN-19869	Windows Agent	백신정보 수집 플러그인 사용시 GnPlugin이 비정상 종료되는 문제	5.0.0
	GN-19867	CLI/gnlogin	replica enable CLI 입력시 mysql 쿼리 오류 발생	4.0.122, 5.0.19
	GN-19833	WebUI	신규 감사로그화면에서 검색필터 수정시 태그를 할당하면 조건이 정상 저장되지 않는 문제 등의 오류 수정	5.0.22
	GN-19832	Windows Agent	위험감지-허용되지 않은 IP를 가진 인터페이스 차단 정책 사용시 허용된 IP를 사용하는데도 차단되는 문제	5.0.0
	GN-19819	CWP	[CWP] 사용자재인증 후에도 재인증창이 표시되는 문제	5.0.22
	GN-19802	CLI/gnlogin	replica enable CLI 입력시 mysql 쿼리 오류 발생	4.0.122, 5.0.19
	GN-19791	CLOUD	Cloud NAC 에서 Web UI를 통한 센서 이미지 업그레이드 실패하는 문제	5.0.22
	GN-19787	Center	주기적 재인증 옵션을 매달로 설정할 경우 남아있는 인증 유효시간이 정상적으로 계산되지 않는 문제	4.0.106
	GN-19754	Center	RADIUS 인증연동을 로컬 RADIUS서버와 연동할때 인증 요청이 반복되는 문제 수정	5.0.21
	GN-19736	WebUI	노드관리 목록의 컬럼 카테고리별 출력시 영문에서 정렬 안되는 오류	5.0.22
	GN-19724	WebUI	Front-end 로 전환된 페이지에 콘솔 새로그침 기능 추가	5.0.22
	GN-19683	Center	인증연동 > SMTP 가 설정되어 있을 경우, 패스워드에 관계없이 관리자 ID만 맞으면 무조건 로그인 성공 되는 문제	5.0.19
	GN-19633	WebUI	이메일 승인/거부 처리 URL 이 잘못(8443포트 누락)된 부분 수정	5.0.19
	GN-19577	WebUI	신규노드상세 링크 누락 및 기능 오동작 문제 수정	5.0.21
	GN-19512	GenianOS	Windows 10 PMS 수행시 0x80072EE2 오류 패치검색실패하는 문제	3.5.33, 4.0.38, 4.0.115, 5.0.12
	GN-19500	WebUI	노드정책 수정시 XSS 공격에 관련한 로그가 남는 문제	4.0.123, 4.0.47, 5.0.21
	GN-19442	Center	인증한 계정 현황 기록 중 DB연결이 끊어진 경우 센터데몬이 비정상 종료되는 문제	ALDER
	GN-19434	macOS Agent	macOS 에이전트 업데이트 후 팝업 메시지 타이틀이 GENIANS, INC.로 잘못 표시됨	5.0.9
	GN-19426	Sensor	미러센서 사용시 노드 정책이 변경될때마다 early role을 받아오는 문제	4.0.1
	GN-19405	macOS Agent	macOS 에이전트가 무결성 검사에 실패했으나 재설치하지 않는 문제	5.0.9
	GN-19397	WebUI	사용자 신청 등록 자동승인 API 오류	5.0.7, 4.0.110

continues on next page

Table 37 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19395	Authsync	Google G Suite 정보 동기화시 사용자정보 외에는 동기화 실패하는 문제	5.0.17
	GN-19372	macOS Agent	macOS 에이전트 오류 보고 버튼 클릭 시 저장에 실패함.	4.0.108, 5.0.4
	GN-19371	Center	센터데몬의 정상적인 종료 시에도 간헐적으로 coredump 발생하는 문제	ALDER
	GN-19360	Enforcer	enforcer 모듈에서 DHCP AutoIP 제외 옵션이 off일 경우에러 디버그 발생하는 문제	4.1.M8
	GN-19351	Linux Agent	동일한 액션 ID에 대해서 에이전트 액션 결과가 다수 발생하는 문제	4.0.112, 5.0.9
	GN-19336	Linux Agent	일부 리눅스 배포판에서 리눅스 에이전트의 소프트웨어 정보 수집 플러그인이 실패함.	4.0.122, 5.0.19
	GN-19257	macOS Agent	macOS Agent GnPlugin이 간헐적으로 중복 실행되는 문제	5.0.11
	GN-19216	Linux Agent	네트워크 카드가 다수인 일부 노드중 리눅스 노드의 동작 표시가 "DOWN"으로 표시됨.	4.0.112, 5.0.9
	GN-19181	macOS Agent	macOS 에이전트 인증창에 한글 입력되지 않는 문제	5.0.15
	GN-19143	WebUI	사용자관리화면에서 하위부서포함 옵션을 해제했지만 하위부서 사용자가 출력되는 문제	4.0.37, 4.0.114, 5.0.11

16.3.38 Genian NAC 5.0.21 Release Notes (2019-07-02)

Last Updated: 2019-08-21

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-19317	GenianOS	opensshd 취약점으로 인한 버전 패치	5.0.8, 4.0.111, 4.0.34	

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-19704	RADIUSD	RADIUSD 감사기록 저장 경로 변경	
	GN-19672	RADIUSD	글로벌버전에서 사용자 관리>비밀번호 저장방식 초기 설정값을 HMAC-SHA256 에서 NTHASH로 변경	
	GN-19616	WebUI	Revise node preference menu	
	GN-19610	Sensor	vlan 인터페이스가 많은 센서가 센터와 접속이 끊어진 후 재연결시 한번에 다량의 정책요청 SOAP을 호출하는 문제	
	GN-19508	WebUI	로그인 요청 후 응답 데이터에 패스워드가 평문으로 노출되는 문제	
	GN-19474	Center	시스템 셧다운/재구동 감사기록이 에러로 남는 문제개선	
	GN-19419	WebUI	변경관리 화면에 IPv6 아이콘이 줄바꿈 되는 문제	
	GN-19409	Database	기본정책 용어변경 Denied by IPAM -> Unauthorized Device	
	GN-19368	WSOS	[W10] Static IP 설정 프로세스 개선	
	GN-19354	Center	Webhook 실패 감사로그 메시지에 검색필터 이름 추가	
	GN-19349	Database	DB 초기화시에도 Fixup 이 수행되는 문제	
	GN-19345	WebUI	CWP 및 관리콘솔의 언어 우선순위 변경	
	GN-19307	Authsync	mssql로 정보 동기화시 TDS version을 선택하지 않아도 동기화 할 수 있도록 개선	
	GN-19288	macOS Agent	macOS 운영체제 정보 수집 시 사용자 계정 정보가 빈번하게 전송되지 않도록 개선	5.0.11
	GN-19260	CWP, IPMGMT	SAML 인증연동 개선	
	GN-19241	Center	장비 내용연수 만료 상태를 확인할 수 있는 노드그룹 조건 추가	
	GN-19205	GeniUpdate	CVE 데이터 전체 업데이트 조건 추가	5.0.19
	GN-19176	Sensor	수동오탐보고 시 오탐보고할 내용이 없을 때 오탐보고 UI를 출력하지 않도록 개선	
	GN-19160	Linux Agent	센터와 통신이 안되는 환경에서 에이전트 액션이 동작하지 않는 증상 개선	4.0.112, 5.0.9
	GN-19157	WebUI	XSS 관련 개선 작업	
	GN-19144	WebUI	노드타입 이미지 업로드 다이얼로그 개선	
	GN-19099	Linux Agent	리눅스 에이전트의 SOAP 통신시 HTTPS 사용하도록 개선함.	4.0.112, 5.0.9
	GN-19090	Windows Agent	SHA1 인증서 발급중단에 따른 윈도우 7 이하에서 에이전트 설치 문제 개선	
	GN-19079	Center	GenianSyncer를 통한 NAC운영데이터 업로드 개선	
	GN-19069	CWP,	보안질문 설정 화면 및 CWP 출력 개선	
718	19069	WebUI		Chapter 16. Release Notes
	GN-18834	WebUI	라이선스 초과 시 제한기능 변경	
	GN-18804	Center	태그의 시작시간 기능 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-19756	Sensor	SS64 미러모드 트래픽어카운트 정보 업데이트시 centerd 죽는 문제	4.0.114, 5.0.11
	GN-19752	Center	에이전트 플러그인이 수집한 정보 수신시 간헐적으로 센터데몬 비정상종료되는 문제	4.1.0, 4.0.23
	GN-19730	CWP	Global SMS 발송되지 않는 문제	5.0.19
	GN-19715	Packaging	Global NAC Software Update의 Release Notes 링크 오류 수정.	5.0.20
	GN-19687	WebUI	노드그룹 조건 중 에이전트 정보에 대한 설정시 지원OS 아이콘이 정상출력 안되는 문제	5.0.15
	GN-19681	Center, Genian Mobile	등록되지 않은 푸시토큰을 유지하는 문제	5.0.18
	GN-19680	WebUI	관리 > 사용자 > 전체사용자에서 CSV 파일 저장시 목록에 표시된 데이터의 일부만 저장되는 문제	5.0.15
	GN-19654	Center	2단계인증으로 OTP 사용시 1단계 인증결과 메시지가 다 국어로 리턴되지 않는 문제	5.0.20
	GN-19640	WebUI	GNAC 소프트웨어 > 업데이트 링크 클릭 시 정상 동작하지 않는 문제	5.0.4
	GN-19625	Database	영문버전에서 위험감지 기본 설정값이 적용되지 않는 문제	5.0.16
	GN-19603	Windows Agent	컴퓨터이름 변경 플러그인을 별도수행계정으로 이름변경 시 적용실패 및 GnPlugin 비정상 종료되는 문제	5.0.0
	GN-19595	Windows Agent	Windows 7이하에서 바탕화면 제어 / 이미지 위치가 플러그인 정책과 다르게 강제화되는 문제	4.0.2, 3.5.5, 5.0.0
	GN-19536	Windows Agent	[5.0] 에이전트 트레이아이콘 표시 안되는 문제.	5.0.0
	GN-19535	GenianOS	snmp trap을 통해 위험감지 시 정상동작하지 못하는 문제	5.0.16
	GN-19530	macOS Agent	v5.0 macOS 에이전트에서 플러그인 수집정보를 전송하지 못하는 문제	5.0.15
	GN-19529	Center	센서 센터간 통신실패시 센서의 IPv6 변경정보 누적되는 문제	5.0.16
	GN-19523	Center	CLOUD버전 감사기록이 표시기한전에 close되는 문제	5.0.7
	GN-19509	Center	메일서버 SMTP 사용시 인증사용자 아이디로 인증을하지 않아서 메일 전송이 안되는 문제 및 서버설정 변경시 메일 발송 안되는 문제	5.0.16
	GN-19463	macOS Agent	macOS 도메인사용자가 로컬사용자로 표시되는 문제	4.0.108, 5.0.5
	GN-19445	Center	이메일 전송시 한글이 깨져서 표시 되는 문제	5.0.16
	GN-19421	macOS Agent	macOS AD 대체인증 기능이 동작하지 않는 문제	4.0.108, 5.0.5
	GN-19400	WebUI	로그 검색필터 생성시 태그가 할당되어 있는 검색필터가 생성되지 않는 문제	4.0.124, 5.0.21
	GN-19369	WebUI	[Cloud] LogFilter 리포트가 동작하지 않는 문제	5.0.8

continues on next page

Table 38 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19330	Windows Agent	5.0 에이전트가 일부PC에서 디스크 시리얼 체크 오류로 인한 비정상 종료 문제	5.0.0
	GN-19273	Linux Agent	Linux Agent 인터페이스 정보중 IP/NETMASK 정보가 수집되지 않음.	4.0.122, 5.0.19
	GN-19267	Windows Agent	사용자계정정보에서 도메인사용자의 최근비밀번호변경 시각이 잘못 출력되는 문제	5.0.0
	GN-19251	CWP	노드 상세정보의 '접속인증페이지 (CWP)' 접속시 공지사항의 디자인이 적용 안되는 문제	5.0.20
	GN-19200	Linux Agent	리눅스 에이전트가 실행중이지만, "에이전트 동작 상태"가 "에이전트 동작 안함" 으로 표시됨.	4.0.118, 5.0.15
	GN-19194	macOS Agent	macOS Agent의 업데이트 확인 클릭 시 업데이트가 진행되지 않는 문제	5.0.16
	GN-19159	macOS Agent	macOS PC전원 제어 플러그인에서 변경된 종료 대기시간이 적용되지 않는 문제	5.0.17
	GN-19121	Center	사용자인증>사용자관리>과거비밀번호 저장시 DUPLICATE 에러 발생문제	3.0_1007

16.3.39 Genian NAC 5.0.19 Release Notes (2019-05-02)

Last Updated: 2019-06-07

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-19203	Center, WebUI	Apache httpd 2.4.39 업그레이드		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-19343	macOS Agent	macOS 에이전트 '수행 조건만 검사' 플러그인이 멀티 플러그인으로 동작할 수 있도록 개선	
	GN-19319	WebUI	시스템 > 센서관리 기본정보 탭에 NAT IP 정보 추가	
	GN-19304	WebUI	사용자 신규 생성시에 관리역할 할당하면 Email 항목 필수 입력하도록 개선	4.0.M9
	GN-19244	Center, CLI/gnlogin	디자인 템플릿도 백업에 포함되도록 개선	
	GN-19138	Center, RADIUS	[RADIUS] VLAN 할당 목록 조건 User-Name 를 선택한 경우만 사용자 조건 나오도록 개선	
	GN-19109	macOS Agent	macOS 에이전트에 SAML 인증 연동 기능 추가	
	GN-19067	WebUI	Update Labels For Syslog Options (receiving events)	5.0.19
	GN-18979	Linux Agent	구름 OS 1.2 지원	
	GN-18976	GenianOS	reset-database 수행 이후 제품 구동시 에이전트 등록 과정이 수행되도록 개선	
	GN-18952	Center, RADIUS	RADIUS 서버 GTC 인증을 센터데몬으로 통합	5.0.19
	GN-18943	WebUI	로그인 이후 신규로 발생한 에러로그 표시기능	
	GN-18922	Database, macOS Agent	신규 macOS에 대해 에이전트 액션을 수행할 수 있도록 개선	
	GN-18911	WebUI	위험감지 위험도 아이콘 개선	
	GN-18902	WebUI	Elasticsearch 서비스의 문제가 있을 경우 WebUI Top 메뉴 출력이 지연되는 문제	
	GN-18893	Center	SMTP 메일서버 MSA/STARTTLS (tcp/587) 방식 지원	
	GN-18870	Center	노드의 Platform에 대한 CVE 정보 확인 기능	
	GN-18842	Database, Linux Agent	신규 리눅스 배포판에 대해 에이전트 액션을 수행할 수 있도록 개선	
	GN-18819	Windows Agent	윈도우 에이전트가 웹페이지 표시할 때 사용하는 웹브라우저 설정 가능하도록 개선	
	GN-18753	WebUI	Web 관리콘솔 별도의 포트(8443)로 바인딩 하도록 변경	
	GN-18675	Center	네트워크그룹에서 FQDN 지원	
	GN-18614	RADIUS	RADIUS 서버 EAP-TLS 지원	
	GN-18446	Center	SAML(Security Assertion Markup Language) 인증 연동 지원	
	GN-18246	Enforcer	Passive 기반의 플랫폼 분류 기능 추가	5.0.19
	GN-18017	Center, Database, Windows Agent	에이전트 설치 단말에 대한 Malware Detection 기능	
16.3. Previous Versions				721
	GN-17987	GeniUpdate	Global 버전 SMS 전송기능 추가	5.0.14
	GN-17372	macOS Agent	macOS 에이전트 디버그 로그 영문화	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-19370	macOS Agent	macOS AVG Antivirus 패턴 버전, 날짜가 잘못 수집되는 문제	5.0.11
	GN-19361	Center	업데이트서버에 제품 라이선스 정보 잘못 전송하는 문제	5.0.16
	GN-19341	Center	휴대폰 번호가 비어있으나 SMS 전송하는 문제	5.0.19
	GN-19338	Windows Agent	불특정상황에서 에이전트 Failsafe 기능이 동작안함.	4.0.0, 5.0.0
	GN-19326	Center	SNMP 포트 차단 기능 동작하지 않는 문제	4.0.121, 5.0.18
	GN-19318	Elastic-Search, RADIUS	RADIUS 로그가 생성되지 않는 문제	5.0.18
	GN-19275	macOS Agent	macOS 소프트웨어 목록 삭제 감지됨으로 처리되는 문제	4.0.114, 5.0.11
	GN-19269	Authsync	사용자정보 동기화 시 인증 된 사용자 정보가 업데이트 되면 직급 또는 부서 정보가 리스트 정보에서 사라지는 문제	4.0.119, 5.0.17
	GN-19266	macOS Agent	유/무선 동시에 사용 시 macOS 에이전트 설치된 노드가 NAT로 잘못 탐지되는 문제	4.0.106, 5.0.0
	GN-19264	Database, MySQL	DB포트시 replica port를 변경하지 못하는 문제	4.0.106
	GN-19232	IPMGMT	IP신청시스템 신청서 결과목록에 미사용IP신청서가 출력 안되는 오류	4.0.118, 5.0.15
	GN-19229	Windows Agent	에이전트 업데이트가 정상적으로 되지 않음 (GnAccount.exe 파일 치환 실패)	4.0.0, 4.1.0, 5.0.0
	GN-19227	macOS Agent	macOS 에이전트가 무결성 검증 실패로 인해 무한 재설치 되는 문제	5.0.8
	GN-19218	RADIUS	[RADIUS] RADIUS서버와 센터 통신시 soap 요청 버퍼사이즈 문제로 인해 soap 요청이 실패하는 문제	5.0.19
	GN-19217	RADIUS	[RADIUS] EAP-TLS 환경에서 ca 인증서의 확장자 .cer 도 업로드될 수 있도록함	5.0.19
	GN-19153	Windows Agent	안전모드용 장치제어 서비스가 동작하지 않는 문제	4.1.5, 4.0.28, 5.0.0
	GN-19082	Windows Agent	정책변경후에도 에이전트 고정 알림메시지가 계속 표시 되는 문제	5.0.0
	GN-18990	WebUI	쿼리리포트 > 즉시조회 시 컬럼명에 HTML tag ID 속성값으로 사용할 수 없는 문자열이 포함될 경우 에러 발생	4.0.8
	GN-18970	Elastic-Search	do restore에서 log 복원 정상동작하지 않는 문제	5.0.14
	GN-18944	WebUI	IP 관리센서 목록과 Export된 Excel의 내용이 맞지 않는 문제	4.0.16
	GN-18942	Windows Agent	프로세스 강제종료 플러그인 2개이상 적용 시 하나만 제어되는 문제	5.0.0
	GN-18941	Sensor	WebUI에서 CLI 비밀번호 변경시 Slave 장비에는 반영되지 않는 문제	4.1.2, 4.0.25
	GN-18936	macOS Agent	macOS 에이전트 서비스 중지 후 서비스 시작 실행 시 동작하지 않는 문제	5.0.11
	GN-18928	Windows Agent	Offline 환경의 윈도우즈10에서 GnPMS로 윈도우 업데이트 설치가 안되는 문제	4.0.109, 5.0.6, 4.0.43
16.3. Previous Versions	GN-18927	macOS Agent	macOS 에이전트 인증 성공 후 내부 오류 메시지가 창으로 출력되는 문제	5.0.15
	GN-18906	WebUI	직급관리 CSV 내보내기(Export) 한 파일로 가져오기(Import)를 할 수 없는 문제	5.0.15
	GN-18905	Windows Agent	유연케이블 정보 수집 프로그램이 에러 드래인 정보 변경까지	4.1.0

16.3.40 Genian NAC 5.0.20 Release Notes (2019-06-07)

Last Updated: 2019-07-08

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-19499	Center	NAC 모바일 노드탐지 푸시 알람 기본적으로 사용하게 변경	
	GN-19379	Center	업데이트되는 NAC 운영데이터 백업하지 않도록 하여 백업용량 감소	
	GN-19367	Center	centerd 최대 file descriptor 수 증가	
	GN-19295	WebUI	superAdmin 역할로 제한된 기능을 operator 역할에도 사용하도록 개선	
	GN-19230	Database	Gnlogin에서 각종 비밀번호 설정시 영문 대, 소문자와 특수문자를 반드시 포함해야 설정될 수 있도록 개선	
	GN-19202	RADIUS	RADIUS 서버 EAP-TLS 인증서 등록 후에 인증서 정보 표시 및 RADIUS 서버 재구동하도록 함	5.0.19
	GN-19112	CLI/gnlogin	bonding parameters CLI 입력시 조건 검사 추가	
	GN-19102	WebUI	태그 관리에 시스템 태그 기능 추가	
	GN-19100	Center	DB/LOG/RADIUS 서버 추가시 센서초기설정 따르지 않도록 개선	5.0.7
	GN-19032	Center	정보 동기화시 원본 암호화 알고리즘에 플러그인 지원하도록 개선	
	GN-19028	WebUI	장치사용신청서의 결과조회 화면 엑셀 내보내기 기능 추가	
	GN-18986	WebUI	지니안 장비에 할당된 태그가 없을 경우 시스템 항목의 검색 기능에서 장비 태그가 비어있는 문제 개선	
	GN-18946	Windows Agent	무선연결 관리자를 통하여 무선인증시 인증 실패시 메시지 표시	4.0.0, 4.1.0, 5.0.7
	GN-18853	WebUI	top메뉴 네비게이션 개선	
	GN-18752	Center	Active Directory 사용자정보 동기화시 사용자의 그룹정보 (memberOf)를 동기화할 수 있도록 개선	
	GN-18657	CWP	CWP 접근허용 IP 설정기능	
	GN-18001	WebUI	노드액션 메뉴 트리에 설정된 라벨을 표시하도록 개선	
	GN-17994	WebUI	노드 스냅샷기능 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-19516	Center	인증연동으로 인증한 경우에 비밀번호만료를 체크하여 인증에 실패하는 문제	5.0.20
	GN-19511	Center	외부인증 연동을 사용하지만 Local DB를 참고하여 인증에 실패하는 문제	5.0.16
	GN-19507	WebUI	파일 해쉬값 변경 오류로 인하여 무결성 검사에 실패하여 에이전트에서 파일 다운로드를 계속 시도하는 문제	5.0.20
	GN-19480	Database	ja 리소스번들에 잘못추가된 리소스번들 제거	5.0.20
	GN-19479	Database, GenianOS	최초 설치시 센서정보가 잘못 등록되어 센서설정 화면에 에러페이지 출력되는 문제	5.0.20
	GN-19478	GenianOS	Install wizard에서 nameserver 설정안되는 문제	4.0.120, 5.0.17
	GN-19475	GenianOS	CSV를 통한 장비수명주기정보 동기화가 안되는 현상	5.0.11
	GN-19458	GenianOS	procmond에서 udprelay 실행문구 오류	4.0.M3, 3.4.3
	GN-19454	Center	에이전트를 통해 노드등록 도중에 실패할 경우, 이후에 에이전트가 다시 노드등록을 시도해도 실패하는 문제	4.0.117, 5.0.14
	GN-19453	WebUI	신규 사용자 추가시 보안질문의 답변으로 0 값이 디폴트 값으로 설정된 문제	4.0.M6
	GN-19446	Sensor	센서가 하나의 노드에서 DHCP DISCOVER 패킷을 동시에 받은 경우 다른 IP를 OFFER 하는 문제	4.0.123, 5.0.20
	GN-19444	CWP	사용자가 생성한 디자인템플릿으로 CWP 페이지 출력시 디자인 적용 누락 문제	5.0.14
	GN-19440	Center	호스트인증 + 인증대체정보 사용시 에이전트가 무한 재인증 시도하는 문제	5.0.16
	GN-19427	WebUI	정책서버 관리자 Web Console port를 443을 설정 시 관리포트로 접속하지 못하는 문제	5.0.19
	GN-19422	Linux Agent	일부 리눅스 배포판(SuSE)에서 리눅스 에이전트 설치 오류가 발생함.	4.0.119, 5.0.16
	GN-19416	Sensor	센서가 정책을 받아가는데 실패해도 재시도 하지 않는 문제	4.0.1
	GN-19408	Center	'사용자인증 적용 - 사용자제한 기능' 사용시 인증된 노드가 미인증 노드 그룹에 포함되는 문제	4.0.0
	GN-19399	Windows Agent	동일한 복수의 WMI 수집정보를 한번에 전송하여 정책서버 부하발생	4.1.2, 4.0.25, 3.5.21, 5.0.0
	GN-19398	Center	fd(file descriptor) open 에 실패했을때 노드 동작상태 이력 저장시 센터가 shutdown 될 수 있는 문제	4.0.17
	GN-19382	Sensor	글로벌 DHCP 서비스 사용시 센서의 IP가 할당되는 오류 수정	4.0.110
	GN-19380	Windows Agent	에이전트 인증창 종료 금지 기능 사용시 비밀번호 변경수행이 불편한 문제	5.0.0
	GN-19352	Windows Agent	스크립트 수행 플러그인 액션을 다중으로 사용할 경우 일부 액션만 수행되는 문제	4.0.119, 5.0.16
	GN-19347	Database	정책서버 및 DB서버 분리구성에서 DB포트 변경 상황에서 관리콘솔로 접속하지 못함	4.0.106

continues on next page

Table 39 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-19344	WebUI	스위치 관리화면 트리 편집시 스위치 항목이 없어지는 문제	5.0.10
	GN-19335	Center, RA-DIUSD	제어정책 > RADIUS CoA 제어 옵션이 RADIUS 서버 격리 VLAN 설정을 ON 한 경우에만 동작하는 문제 개선	5.0.19
	GN-19287	Authsync	mssql 동기화시 DB 접속 실패 또는 한글 문자열이 비정상 표기될 수 있는 문제	4.0.119, 5.0.16
	GN-19255	Sensor	SS64버전에서 DHCP 서버에 설정된 가상IP가 사용자에게 부여되는 문제	4.1.M8
	GN-19225	Windows Agent	일부 PC에서 mfc140u.dll 파일 미존재로 발생하는 에이전트 설치 실패 문제 수정	5.0.0
	GN-19164	WebUI	Genian 소프트웨어 목록 출력시에 사용불가능한 소프트웨어 버전항목이 출력되는 오류	5.0.2
	GN-19158	IPMGMT	관리자 계정에 노드 관리범위를 정책그룹으로 제한시 IP 신청서가 보이지 않는 문제	4.0.120, 5.0.18
	GN-19083	CWP	노드상세정보의 '접속인증페이지 (CWP) 조회' 페이지의 조작이 가능한 문제	5.0.17
	GN-19081	Windows Agent	IE 웹브라우저 크기 최대화 옵션이 정상동작안함.	3.5.1, 4.0.0, 5.0.0
	GN-19066	macOS Agent	macOS Agent 비밀번호 만료 전 알림 메시지가 표시되지 않는 문제	5.0.11
	GN-18995	WebUI	설정된 임시비밀번호 패턴과 문자로 수신되는 비밀번호가 상이한 문제	4.1.2, 5.0.17
	GN-18987	Windows Agent	에이전트 인증창에서 인증시 비밀번호가 특정 길이 이상일 경우 인증되지 않는 문제	5.0.11
	GN-18937	Linux Agent	리눅스 에이전트 액션 정책중 일부만 "액션 수행결과 현황"에 표시됨.	4.0.112, 5.0.9
	GN-18915	Sensor	허용에서 차단정책으로 변경시 ARP Poisoning 동작하지 않음	5.0.0, 4.0.107
	GN-18897	macOS Agent	macOS 에이전트 액션정책의 재시도 시간/횟수 옵션이 동작안함.	5.0.11
	GN-18783	Center	2단계 인증과 비밀번호 변경권유/강제를 설정할시 CWP/에이전트에서 2단계 인증이 정상적으로 동작하지 않음	5.0.16

16.3.41 Genian NAC 5.0.18 Release Notes (2019-04-05)

Last Updated: 2019-04-30

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-18861	WebUI	ES 초기화 시 LOGBACKUP REPOSITORY 자동설정기능 추가	
	GN-18847	WebUI	REST API 권한 Url pattern 허용시 전체 url의 pattern을 확인하는것이 아닌 context로만 확인하는 문제 개선	
	GN-18827	WebUI	노드의 기본정보 UI에 커스텀 필드 정보들을 2열로 표시 되도록 개선	
	GN-18806	WebUI	CWP 2단계 인증 완료 후 인증 허용 개수가 초과되었을 경우 로그아웃 페이지가 출력되도록 개선	
	GN-18800	Windows Agent	화면보호기 없이 대기시간 경과 후 Windows 로그인 화면 표시할 수 있는 기능 추가	
	GN-18720	Windows Agent	전원제어플러그인에 대한 플러그인 정책이 변경되면 종료대기시간을 다시 적용되도록 수정.	
	GN-18709	macOS Agent	macOS 에이전트 업데이트 이후 에이전트 버전 정보 갱신 되지 않음.	
	GN-18696	Center	Rogue DHCP Server 위험감지 추가	
	GN-18687	WebUI	센서맵 출력되지 않는 문제	
	GN-18685	Center	사용자 최초 인증시 인증허용 IP 자동 설정 기능	
	GN-18624	Linux Agent	리눅스 에이전트 정보 수집 항목중 미구현 기능 구현함.	4.0.112, 5.0.9
	GN-18511	macOS Agent	macOS 에이전트 인증창 도움말을 플러그인 설정으로 변경	
	GN-18509	Windows Agent	에이전트 인증창 도움말을 플러그인 옵션으로 변경	
	GN-18485	WebUI	Swagger에 apiKey 사용안내 문구 추가	
	GN-18481	WebUI	모바일 Push를 위한 PushToken을 관리자별로 관리하도록 개선	
	GN-18431	GenianOS	Docker 기반 네트워크 센서	
	GN-18027	RADIUSD	RADIUS Attribute 매치조건을 통한 Dynamic VLAN 할당	
	GN-17788	macOS Agent	macOS Agent Downgrade 기능 추가	
	GN-17501	GenianOS	SECUI MF2 장비에 NAC 포팅	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-19224	Authsync	LDAP "사용자정보동기화" 최초 실행시, SQL 함수가 그대로 데이터로 들어가는 문제	4.0.119, 5.0.17
	GN-19213	Windows Agent	위험감지-허용되지 않은 IP를 가진 인터페이스 차단 정책 사용시 PC 과부하 문제	5.0.0
	GN-19212	Center	IP가 같으면의 or 조건으로 earlyrole 생성시 ip가 바뀌어 전달되는 현상	5.0.14
	GN-19199	CWP	CWP 사용자 정보 수정 페이지 접속시 로그인 페이지에서 ~가 포함된 비밀번호를 사용할 경우 로그인 안되는 문제	5.0.14
	GN-19198	WebUI	관리 > 사용자에서 특정 사용자 검색 후 검색어를 제거하고 검색해도 이전 검색어가 사라지지 않는 문제	4.0.M7
	GN-19186	Center	노드그룹 조건 중 "에이전트 상태 버전" (보다높으면, 보다낮으면) 비교 조건이 동작하지 않음	4.0.119, 5.0.16
	GN-19166	IPMGMT	임시사용신청으로 IP 신청시 신청서처리결과 목록에 바로 보여지는 문제	4.0.120, 5.0.17
	GN-19131	WebUI	제품 업그레이드시에 관리역할의 적용모드가 초기화 되는 오류	4.0.10
	GN-19129	WebUI	관리 > 노드 > 현황&필터에서 태그의 목록이 출력되지 않는 문제	5.0.16
	GN-19117	GenianOS	이미지 업그레이드 이후 인증서 문제로 httpd 구동되지 않는 문제	4.0.119, 5.0.16
	GN-19111	Windows Agent	일부 PC 에서 GnAgent MSI 설치패키지로 에이전트 설치 안되는 문제	5.0.16
	GN-19106	CWP	IP인증제한이 설정된 경우 Agent에서 인증해제 버튼 클릭시 팝업된 브라우저에서 한글이 깨지는 문제	5.0.0
	GN-19094	Center	에이전트로부터 동일한 mac 주소를 가진 복수의 인터페이스정보를 받은 경우 NAT장치로 감지될 수 있는 문제	4.0.M8
	GN-19023	WebUI	노드 트리 메뉴에서 센서그룹 생성시 생성한 그룹명 설정 및 Drag&Drop 이동 등이 정상적으로 되지 않는 문제	5.0.0
	GN-18991	Authsync	사용자 정보 동기화에서 패스워드 변경시각 동기화되지 않는 문제	4.0.119, 5.0.17
	GN-18938	WebUI	PushToken 수정/추가시 앱이 설치된 단말로 Push가 전송되지 않는 문제	5.0.18
	GN-18929	WebUI	보안질문 설정시 항목이 존재하지 않음에도 데이터가 설정되는 오류	4.0.112, 5.0.9
	GN-18865	Center	정상적인 CIDR IP패턴을 유효하지 않다고 디버그남기는 문제	4.0.14
	GN-18830	CWP, WebUI	CWP 확인버튼의 URL 설정이 적용되지 않는 문제	5.0.14
	GN-18822	Genian Syncer	Genian Syncer로 운영정보 데이터(GenianData)만 업로드하면 운영정보 데이터 갱신안되는 문제	4.0.113, 5.0.10
	GN-18809	Windows Agent	비밀번호 검증했지만 다시 미검증으로 처리되어 팝업되는 문제.	4.0.106, 4.0.29, 5.0.0
	GN-18801	Center	인증허용 MAC/IP 개수를 초과할경우 인증허용대역이 아닌곳에서도 노드인증을 해제시킬수 있는 문제	3.2.3
	GN-18796	WebUI	사용자정의 IP용도로 IP 신규신청시 IP 소유자 갱신이 되지 않는 문제	4.1.2

continues on next page

Table 40 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-18764	WebUI	장치사용관리화면에서 검색기능이 동작하지 않는 문제	4.0.37, 4.0.114, 5.0.11
	GN-18725	Center	감사로그 검색필터를 통한 메시지 전송시 {_SENSORIP} 매크로 사용할 수 없는 문제	4.0.M8
	GN-18724	Center	플러그인 업로드로 인한 에이전트액션 자동생성시 액션 설정에 특정문자가 누락되는 문제	4.0.2
	GN-18708	Linux Agent	에이전트 액션 즉시 적용해도 최초에는 액션 수행 안하는 문제.	4.0.112, 5.0.9
	GN-18699	WebUI	플러그인 업로드할때 파일명에 공백이 있을 경우 업로드가 되지 않는 문제	4.0.M8
	GN-18676	WebUI	장치신청서 상세화면에서 승인이 되지 않는 문제	5.0.7, 4.0.110
	GN-18616	WebUI	노드그룹 분류 트리 하위에 값이 없음에도 펼침 아이콘이 출력됨.	4.0.106

16.3.42 Genian NAC 5.0.17 Release Notes (2019-02-25)

Last Updated: 2019-04-01

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
	GN-19044	GenianOS	openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2r)		
	GN-18607	WebUI	tomcat-connectors 버전 업그레이드		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-19000	Elastic-Search	elasticsearch publish_host 설정 기능 추가	
	GN-18898	WebUI	라이센스 갱신시 Cached Data 초기화 하도록 개선	
	GN-18761	WebUI	CWP 메타데이터에 인증사용자부서명 추가	
	GN-18635	Sensor	센서 배포 서버 사용시 다운로드중 중단시 다시 다운로드 받지 않는 문제	
	GN-18629	Windows Agent	PC전원제어 플러그인에서 PC가동시간에 전원제어대화 상자 보여지도록 수정	
	GN-18621	WebUI	유지보수 만료일자 출력 개선	

continues on next page

Table 41 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-18540	Windows Agent	ESET 백신 정보 수집 제품군 확대	
	GN-18496	macOS Agent	macOS 전원 제어 플러그인 제작	
	GN-18482	WebUI	IP소유부서 설정시 부서설정 화면 개선	
	GN-18480	macOS Agent	macOS 백신정보수집 플러그인에 Sophos Antivirus 정보 추가	
	GN-18459	Authsync, WebUI	정보동기화 목록화면에 최근 동기화 상태정보 표시	
	GN-18454	Windows Agent	무선랜제어 플러그인으로 Win10 모바일 핫스팟기능 제어	5.0.0
	GN-18444	WebUI	ElasticSearch 관리 화면 추가	
	GN-18430	macOS Agent	macOS 모니터 정보 수집 플러그인 제작	
	GN-18429	GPDB	GPDB 수동 업그레이드 기능 추가	
	GN-18402	Center	장비 MAC 태그 해제시 기간 만료 로그 기록 개선 (BY 정보 추가)	
	GN-18399	WebUI	메시지 관리 관리화면 개선	
	GN-18394	IPMGMT	신청서처리결과화면에서 변경사용자 컬럼 추가 요청	
	GN-18390	IPMGMT, WebUI	Email 승인 환경에서 다중신청 및 일괄신청시 전체 승인 및 거부 위치 변경	
	GN-18388	IPMGMT, WebUI	엑셀을 통한 일괄 신청시 폼에 맞지 않은 엑셀 업로드시에 경고 출력 개선 요청	
	GN-18387	IPMGMT, WebUI	Email을 통한 승인자 선택시 승인자 이름 출력되도록 개선 요청	
	GN-18361	Windows Agent	Window 에이전트 인증창 웹 플러그인을 통한 OTP 인증 기능 추가	
	GN-18349	macOS Agent	macOS 에이전트 인증창에 OTP 인증 기능 추가	
	GN-18303	Sensor	미러 모드 사용시, 차단 방법 개선	
	GN-18145	RADIUSD	RADIUS CoA(Change of Authorization) 메시지를 이용한 단말 접속제어	
	GN-18128	WebUI	에이전트 운영체제별 위젯 개선	
	GN-17833	Sensor	SNMP 정보수집/포트차단시 Version 3 지원	
	GN-17756	Center	Switch Port 셧다운 방지 문자열 설정기능	
	GN-17354	Center	사용자정보 동기화 Google G Suite 지원 (OAuth2)	
	GN-17136	Windows Agent	Dissolvable Agent 패키지 개발	

continues on next page

Table 41 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-11614	Windows Agent	유선랜 802.1x 접속관리자 Plugin 개발	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-19058	Center	비활성노드정책갱신 설정사용시 제어되지 않는 문제	3.4.M6
	GN-19054	Hardware	efibootmgr (UEFI 부트 매니저) 실행 안되는 문제	5.0.7
	GN-19051	WebUI	IP 신청시스템에서 해당 노드의 센서로 선택되지 않는 문제	4.1.4
	GN-19047	Enforcer	미러센서 - 비관리 노드에서 관리노드로 통신하는 단말이 제대로 차단 안되는 문제	4.0.114, 5.0.11
	GN-19039	Sensor	IP변경금지 위반 이후 IP원복 시 원복된 기존IP에 대해서 차단 되는 문제	4.0.117, 5.0.14
	GN-19011	Center	여러 IP를 사용하는 에이전트 설치 노드의 플랫폼이 'Unknown Platform'으로 변경되는 문제	4.0.6
	GN-18994	GNOS	Install wizard를 통해 복수개의 nameserver 입력하면 DNS lookup 동작하지 않는 문제	4.1.3
	GN-18982	WebUI	노드 그룹 조건에 설정메모가 추가되면 삭제 버튼이 동작하지 않는 문제	5.0.16
	GN-18977	Elastic-Search, WebUI	로그필터 생성시 IP 검색을 CIDR로 수행하는 경우 로그필터가 정상 동작하지 않음	5.0.0, 4.0.107, 4.0.30
	GN-18962	GNOS	Windows 10에서 패포서버를 통한 PMS proxy 동작하지 않는 문제	5.0.15
	GN-18924	macOS Agent	정책에서 macOS PC전원 제어 액션을 제거해도 동작하는 문제	5.0.17
	GN-18908	WebUI	부서관리 전체사용자 하위의 부서별을 클릭하면 부서코드뷰가 출력되는 문제	5.0.0
	GN-18901	WebUI	미사용노드 인증유효시간 설정이 설명과는 다르게 설정되는 오류	5.0.0, 4.0.107
	GN-18697	Center	개별 플러그인 업로드시 설정값들이 에이전트에 전송되지 않는 문제	3.3.1.1009
	GN-18662	Center	소프트웨어정보 변경시 감사기록의 로그 ID가 시스템정보로 남는 문제 수정	4.0.1
	GN-18653	WebUI	관리 > 노드 목록 엑셀 export시 화면에 설정된 컬럼 중 누락되는 컬럼이 발생하는 문제	4.0.106
	GN-18648	macOS Agent	macOS 소프트웨어 정보 수집 시 추가, 삭제가 반복되는 문제	4.0.106, 5.0.0
	GN-18631	Center	eth0 인터페이스를 사용하지 않는 장비의 시리얼이 업데이트되지 않는 문제	4.0.106
	GN-18608	Windows Agent	네트워크 인터페이스 장치명이 비정상 수집되는 문제	5.0.0

continues on next page

Table 42 – continued from previous page

Revision	Key	Components	Description	Affects Versions
	GN-18588	macOS Agent	macOS 에이전트에서 전송한 NIC 정보에 의해 NAT 장비로 오탐되는 문제	4.0.106, 5.0.0
	GN-18571	Windows Agent	무선랜제어 플러그인으로 AP정보 수집 시 일부 SSID 값 깨지는 문제	5.0.0
	GN-18544	macOS Agent	macOS 에이전트 인증창을 사용하고 있으나 인증 안내 메시지도 표시됨	5.0.15
	GN-18543	WebUI	리포트 생성시 이름에 슬래시 (/)가 있을경우 파일이 생성되지 않는 문제	4.0.6
	GN-18521	WebUI	IP Matrix view 에서 IP/MAC 사용시작 설정시 아이콘이 잘못출력되는 문제	4.0.8
	GN-18502	Center	HA 파일 동기화 수행을 위한 파일목록 다운로드 실패시 해당 경로의 파일이 모두 삭제되는 문제	4.0.39, 4.0.116, 5.0.13
	GN-18486	IPMGMT, WebUI	IP사용신청서 승인시 호스트명 직접입력인 경우 승인 오류	
	GN-18479	RADIUSD	RADIUS MAC 인증시 MAC format으로 인한 인증오류	4.0.12
	GN-18396	Authsync, Center	사용자 정보 동기화시 사용자 생성/삭제 처리가 정상적으로 수행되지 않는 문제	4.0.6
	GN-18256	Authsync, Center	정보 동기화의 기존인증노드 인증해제 설정이 정상동작하지 않는 문제	3.0_0910
	GN-17683	Authsync	정보 동기화의 인증처리MAC/IP 설정이 정상동작하지 않는 문제	3.0_0910
	GN-17461	Windows Agent	에이전트 인증창 이미지 다운로드가 계속 수행되는 문제	5.0.17

16.3.43 Genian NAC 5.0.16 Release Notes (2018-12-18)

Last Updated: 2019-02-22

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
	GN-18810	Windows Agent	신규 Insights E 에이전트에 관련된 트레이 메뉴 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
	GN-18939	Windows Agent	네트워크정보수집 플러그인을 통하여 열린포트 정보 수집시 메모리 증가현상	5.0.0
	GN-18925	Windows Agent	네트워크정보 수집플러그인으로 정보가 갱신되지 않는 문제	5.0.0
	GN-18923	WebUI	CWP 인증시 암호 중간에 ~표시가 있는 경우 인증안되는 오류	5.0.14
	GN-18914	WebUI	쿼리 리포트 파일 생성 후 웹에 생성된 파일 안보이는 현상	4.0.119, 5.0.16
	GN-18895	Database, macOS Agent, Windows Agent	에이전트 노드그룹 조건이 실시간 반영되지 않음.	5.0.12
	GN-18891	Windows Agent	에이전트 액션정책의 재시도 시간/횟수 옵션이 동작안함.	5.0.0
	GN-18884	WebUI	수신된 감사로그 필터 알람메일에 IP/MAC 링크 클릭시 에러페이지 출력하는 문제	5.0.16
	GN-18876	Center	인증사용자 계정이 휴먼계정으로 처리되는 문제	NoVersion
	GN-18851	Windows Agent	가상 환경에서 Windows Update 이후 에이전트의 평균 CPU 사용률이 증가하는 문제	4.0.0, 4.0.1
	GN-18788	Database	4.0.x 버전에서 5.0.14 버전으로 업그레이드 시 Log2Migration이 정상동작하지 않는 문제	5.0.14
	GN-18217	macOS Agent	macOS 에이전트에서 플러그인 수집정보를 전송하지 못하는 문제	5.0.11

16.4 Security Advisories

16.4.1 Genian NAC Security Advisories

Last Updated: 2024-03-04

Security Vulnerability

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.60, 5.0.56 (50 LTS), 5.0.55 (LTS)	GN-27242	WebUI	NAC 5.0에서 사용자 검색 화면을 통해서 sql injection이 가능한 취약점	5.0.15	4.8

continues on next page

Table 43 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.60, 5.0.56 (50 LTS), 5.0.55 (LTS)	GN-27107	WebUI	권한 없는 관리자로 인한 Tomcat 재구동 명령 수행으로 서비스 무력화	5.0.41	2.7
5.0.58, 5.0.56 (50 LTS), 5.0.55 (LTS)	GN-26393	WebUI	접근 권한 없는 페이지에 직접 URL을 입력하여 정보 수정이 가능한 취약점		3.1
5.0.58, 5.0.56 (50 LTS), 5.0.55 (LTS)	GN-26390	WebUI	감사로그 REST API를 통한 권한 없는 관리자의 파일 내보내기 권한 우회 취약점		3.1
5.0.57, 5.0.56 (50 LTS), 5.0.55 (LTS), 5.0.42 (LTS)	GN-26315	WebUI	2단계 인증에서 인증코드 입력값 횡수제한, 시간제한하도록 개선		4.3
5.0.57, 5.0.56 (50 LTS), 5.0.55 (LTS)	GN-27492	WebUI	Tomcat Version Upgrade (8.5.94 -> 8.5.96 / 9.0.81 -> 9.0.83)		7.5
5.0.57, 5.0.56 (50 LTS), 5.0.55 (LTS)	GN-27278	WebUI	Tomcat Version Upgrade (8.5.94 / 9.0.81)		7.5
5.0.57, 5.0.56 (50 LTS), 5.0.42 (LTS)	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

continues on next page

Table 43 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.56 (50 LTS), 5.0.55 (LTS), 5.0.53, 5.0.42 (LTS)	GN-26814	Center	Bufferoverflow 에 대한 코드 개선		2
5.0.56 (50 LTS), 5.0.55 (LTS), 5.0.42 (LTS)	GN-26865	WebUI	대시보드 위젯 설정에서 XSS 입력 취약점		1.2
5.0.56 (50 LTS), 5.0.55 (LTS), 5.0.42 (LTS)	GN-26835	Center	데이터 업데이트에 사용되는 SQL을 통한 Command Injection 취약점		6.6
5.0.56 (50 LTS), 5.0.55 (LTS), 5.0.42 (LTS)	GN-26833	Sensor	센서의 NMDB 업데이트 과정에서 nmap 스크립트 변조 취약점		4.1
5.0.56 (50 LTS), 5.0.55 (LTS), 5.0.42 (LTS)	GN-26725	Linux Agent, macOS Agent, Windows Agent	[Agent] 센터 및 센서에서 전송된 이벤트에 대한 유효성 검사 추가		6.3
5.0.56 (50 LTS), 5.0.55 (LTS), 5.0.42 (LTS)	GN-26696	Sensor	센서의 수신 이벤트에 대한 검증 미흡		6.3

continues on next page

Table 43 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.56 (50 LTS), 5.0.55 (LTS), 5.0.42 (LTS)	GN-26694	Center	다운로드 URL 검증 미흡으로 인한 Parameter Injection 취약점		6.6
5.0.56 (50 LTS), 5.0.55 (LTS), 5.0.42 (LTS)	GN-26383	WebUI	html/script 코드 주입 가능한 취약점		5.3
5.0.56 (50 LTS), 5.0.55 (LTS)	GN-26935	WebUI	부서명으로 출력된 html tag가 tree에서 실행되는 취약점	5.0.0	1.2
5.0.55 (LTS)	GN-26222	WebUI	관리콘솔 내 페이지 이동시 사용하는 returnUrl 파라미터를 변조하여 리다이렉트 할 수 있는 문제		1.9
5.0.54, 5.0.53, 5.0.50, 5.0.42 (LTS)	GN-26460	Windows Agent	에이전트를 통해 일반 사용자가 PC 관리자 권한을 획득할 수 있는 취약점	5.0.0, 6.0.0	4.6
5.0.54, 5.0.53, 5.0.50, 5.0.42 (LTS)	GN-26392	WebUI	권한 없는 관리자가 디버그 로그 다운로드 가능한 취약점		2.9
5.0.54, 5.0.53, 5.0.50, 5.0.42 (LTS)	GN-26368	WebUI	관리자의 API 키가 다른 관리자에게 노출되는 취약점		5.3
5.0.54	GN-26391	WebUI	권한 없는 관리자가 디버그로그 실시간 보기 가능한 취약점	5.0.0, 6.0.0	2.9
5.0.53, 5.0.50, 5.0.42 (LTS)	GN-26286	WebUI	Google OTP 2단계 인증에서 보안키를 신규로 발급받아 2단계 인증을 통과할 수 있는 문제		6.5
5.0.53, 5.0.50, 5.0.42 (LTS)	GN-26205	Database	mysql 버전 업그레이드 5.7.40 -> 5.7.41		

continues on next page

Table 43 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.53, 5.0.50, 5.0.42 (LTS)	GN-26062	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 1.1.1t 업데이트 - 임의 포인터를 memcmp 호출에 전달하여 메모리 내용을 읽거나 서비스 거부를 유발할 수 있음		7.4
5.0.53, 5.0.50	GN-26150	WebUI	Tomcat version upgrade (9.0.68 -> 9.0.72, 8.5.78 -> 8.5.86)		
5.0.53, 5.0.50	GN-25869	CWP	IP관리 메시지 우선 On 일때 에이전트 사용자 인증 메뉴로 CWP 인증 시 계정 (ID)으로만 인증 되는 문제	6.0.3, 5.0.46	3.4
5.0.51, 5.0.50, 5.0.42 (LTS)	GN-26000	MySQL	mysql 버전 업데이트 5.7.33 -> 5.7.40		
5.0.50, 5.0.42 (LTS)	GN-26051	WebUI	5.0 WebUI lib 취약점 항목 점검		
5.0.50, 5.0.42 (LTS)	GN-25982	WebUI	WebUI Response Header에 CSP, HSTS Header 추가		
5.0.50, 5.0.42 (LTS)	GN-25925	IPMGMT, WebUI	IP 신청시스템 > IP 신청 화면 XSS 가능한 문제		5.4
5.0.50, 5.0.42 (LTS)	GN-25875	Windows Agent	에이전트가 웹브라우저 실행할 때 High권한 가지는 문제	4.0.0, 5.0.0, 6.0.0	3.3
5.0.50, 5.0.42 (LTS)	GN-25847	WebUI	CWP 화면에서 사용자 정보 수정 페이지 접근시 재인증 절차 추가		4.2
5.0.50, 5.0.42 (LTS)	GN-25740	WebUI	감사 > 로그 > 로그검색바에서 XSS가 가능한 문제		5.6
5.0.50	GN-25811	IPMGMT	IP 신청시스템에서 frontpage를 통해 사용자ID만으로 로그인 가능한 문제		4.9
5.0.50	GN-25250	WebUI	HTML Tag 문자열 뒤에 /를 붙이는 경우 XSS가 가능한 문제		4.9
5.0.50	GN-23677	Center, Sensor	센서 정책서버 등록시 보안성 강화를 위한 관리자 승인 시스템		7.9
5.0.49, 5.0.42 (LTS)	GN-25753	WebUI	CWP 에서 PAGEFW 파라미터를 통한 불법 경로로 리다이렉트 하지 않도록 개선		4.2
5.0.49, 5.0.42 (LTS)	GN-25561	WebUI	노드검색바 Blind SQL Injection 취약점		5.3
5.0.49, 5.0.42 (LTS)	GN-25184	Sensor	DNS Cache Poisoning 공격방어를 위해서 Dns-masq 에서 쿼리 결과를 캐쉬하지 않도록 수정		3.7

continues on next page

Table 43 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.49, 5.0.42 (LTS)	GN-25119	macOS Agent	macOS Agent, OpenVPN(2.5.7) 및 OpenSSL(1.1.1q) 최신 버전으로 업그레이드		5.3
5.0.49	GN-25193	WebUI	[범용 OS Ubuntu] 관리콘솔 > CWP Design Template 목록 페이지 'X-Frame-Options' Header 가 allowall로 표시되는 문제		6.5
5.0.48, 5.0.42 (LTS)	GN-25438	Center, Sensor	_filelist.html 파일을 센터마다 다르게 생성하도록 개선		3
5.0.48, 5.0.42 (LTS)	GN-25306	WebUI	사용하지 않는 HTTP-Method를 통해 사용가능 method 정보가 출력되는 문제		5.3
5.0.47, 5.0.42 (LTS)	GN-25104	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1q)		5.3
5.0.47, 5.0.42 (LTS)	GN-25064	WebUI	웹서비스 취약점 Apache WAS 정보를 노출하지 않도록 개선	4.0.119, 5.0.16	2.5
5.0.47	GN-23947	Windows Agent	윈도우 에이전트 시큐어코딩 점검결과 취약점 패치	5.0.0, 6.0.0	
5.0.46, 5.0.42 (LTS)	GN-24917	Center, macOS Agent, Sensor, Windows Agent	OpenSSL 최신버전으로 업그레이드 (OpenSSL 1.1.1o)		9.8
5.0.46, 5.0.42 (LTS)	GN-24908	WebUI	Tomcat version upgrade (8.5.78)		8.6
5.0.46, 5.0.42 (LTS)	GN-24851	Center	Apache HTTP Server 2.4.53 업그레이드		9.8
5.0.45, 5.0.42 (LTS)	GN-24689	WebUI	감사 > 로그 > 로그검색에서 XSS가 가능한 문제		4.3
5.0.45, 5.0.42 (LTS)	GN-24687	WebUI	디버그로그 화면에서 상대경로로 파일 접근 가능한 문제		3.83
5.0.45, 5.0.42 (LTS)	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
5.0.45, 5.0.42 (LTS)	GN-24535	WebUI	logstash 제거		5.9

continues on next page

Table 43 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.44, 5.0.42 (LTS)	GN-24305	GNOS	Apache 취약점 조치를 위한 2.4.52 버전 업데이트		9.8
5.0.44, 5.0.42 (LTS)	GN-24253	WebUI	log4j 취약점 개선		9.8
5.0.42 (LTS)	GN-24030	GNOS	제품에 포함된 netcat(nc) 명령에서 reverse shell 기능 제거		
5.0.42 (LTS)	GN-24014	Center	HTTP로 호출가능한 SOAP/REST 제한		2.5
5.0.42 (LTS)	GN-23981	macOS Agent, Windows Agent	에이전트에 UDP 이벤트의 패킷 조작을 통한 비정상 종료 문제		3.4
5.0.42 (LTS)	GN-23977	macOS Agent, Windows Agent	에이전트에서 인스턴트 메시지 표시할 때 존재하는 XSS 취약점 수정		6.8
5.0.42 (LTS)	GN-23972	Center, Sensor	UDP event 패킷처리시 데몬 비정상 종료 가능한 문제	5.0.36	6.4
5.0.42 (LTS)	GN-23970	WebUI	모바일 앱을 이용한 관리자 로그인 우회 취약점		6.1
5.0.42 (LTS)	GN-23967	WebUI	REST API Command Injection		6.7
5.0.42 (LTS)	GN-23966	WebUI	CWP 사용자 신청시 Excel 파일로 신청되는 경우 XSS 공격 가능 취약점		6.8
5.0.42 (LTS)	GN-23965	WebUI	Agent Download 페이지에서 상대경로를 통한 내부 파일 다운로드 취약점	5.0.37	5.2
5.0.42 (LTS)	GN-23794	WebUI	REST API 호출시 유효한 인증 토큰이 존재하지 않아도 호출 가능한 문제		4.9
5.0.42 (LTS)	GN-23743	Center	API를 통한 서비스 거부 공격(DoS, Denial of Service) 취약점 개선		6.4
5.0.42 (LTS)	GN-23714	Center	인증처리가 미비한 에이전트관련 API 보완		4.6
5.0.42 (LTS)	GN-23708	Center	인증처리가 미비한 센서관련 API 보완		4.6
5.0.42 (LTS)	GN-23706	Center	내부적으로 사용되는 SOAP API가 RPC를 통해 외부로 노출된 취약점		
5.0.42 (LTS)	GN-23705	WebUI	(KVE-2021-1062) Conf Engine 에서 파일 업로드 컴포넌트의 이름 유효성 체크 강화		6.7
5.0.42 (LTS)	GN-23702	WebUI	(KVE-2021-1062) CWP Design Template 에서 SSTI 취약점		
5.0.42 (LTS)	GN-23701	Windows Agent	(KVE-2021-1062) Agent 파일 생성시 상대경로를 사용할 수 있는 취약점		6.1
5.0.42 (LTS)	GN-23700	Center	(KVE-2021-1061) 노드에 인증된 사용자가 아닌데도 비밀번호를 변경할 수 있는 취약점		8.7
5.0.42 (LTS)	GN-23699	Center, Sensor	(KVE-2021-1061) 센서정보 없이 모든 노드의 정보를 얻을 수 있는 취약점		

continues on next page

Table 43 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.42 (LTS)	GN-23663	macOS Agent, Windows Agent	에이전트 OpenSSL 1.1.11 업데이트		9.8
5.0.42 (LTS)	GN-23662	GNOS	openssl 버전 1.1.11 로 업그레이드	4.0.146, 5.0.44, 6.0.1	9.8
5.0.42 (LTS)	GN-23578	WebUI	REST API 취약점 개선		6.8
5.0.42 (LTS)	GN-23563	Center	Command injection 공격 방어를 위한 수정		8
5.0.42 (LTS)	GN-23533	Center	사용불가 플러그인이 에이전트로 전달되지 않도록 개선		7.6
5.0.42 (LTS)	GN-23500	Center	SQL Injection 방어 처리방법 개선		8.7
5.0.42 (LTS)	GN-23499	GNOS	GNOS 내부 취약한 LD_LIBRARY_PATH 환경 변수 제거		
5.0.42 (LTS)	GN-23488	WebUI	[SaaS] SaaS 보안인증 WAS(Tomcat) 취약점 개선		7.5
5.0.42 (LTS)	GN-23446	gnlogin, WebUI	비밀번호에 특정단어를 사용할 수 없도록 처리		8.7
5.0.42 (LTS)	GN-23377	GNOS	openssh 버전 8.6p1 으로 업그레이드		
5.0.42 (LTS)	GN-23358	WebUI	[CC] Web 취약성 점검결과 보안		6.5
5.0.42 (LTS)	GN-23237	GenianOS	Apache httpd(2.4.48) / tomcat(8.5.63) 업그레이드		7.5
5.0.42 (LTS)	GN-23233	Elastic-Search	[CC] elasticsearch 5.6.16 버전으로 업그레이드		8.8
5.0.42 (LTS)	GN-23055	WebUI	시큐어코딩 점검 결과 취약점 패치 - javascript	5.0.42 (LTS)	
5.0.42 (LTS)	GN-22473	Center	시큐어코딩점검결과 개선 - 불충분한 랜덤 값 사용		7.5
5.0.41	GN-22872	- Unknown/None-	openssl 1.1.1k 패치		7.4
5.0.41	GN-22747	Database	GNOS MySQL 5.7 업그레이드		
5.0.41	GN-22558	- Unknown/None-	DNSMASQ 취약점 수정을 위한 버전 업그레이드		8.1
5.0.41	GN-22551	WebUI	시큐어코딩 점검 결과 취약점 패치 - 자바 코드		9.3
5.0.41	GN-22475	Center	시큐어코딩점검결과 개선 - 조치없이 오류 조건 감지		1.8
5.0.41	GN-21728	- Unknown/None-	OpenSSL 업그레이드 (1.0.2u -> 1.1.1j)		9.8

continues on next page

Table 43 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.40	GN-22461	WebUI	Tomcat 버전 업그레이드 (7.0.104 --> 7.0.107 / 8.5.55 --> 8.5.61)		5.9
5.0.39	GN-21985	WebUI	관리콘솔 취약점 개선 (XSS 공격, 에러코드 노출)		4.3
5.0.38	GN-21396	WebUI	노드관리 검색바에서 사용할 수 없는 sql 문법 및 시스템 변수 제한하도록 개선		4.5
5.0.37	GN-21879	WebUI	CWP 취약점을 통한 인증권한 탈취 개선		6.2
5.0.36, 5.0.35	GN-21843	Center	SQL 인젝션 검사하지 않는 예외 처리된 SOAP API 의 인자값도 escape 처리 하도록 수정		
5.0.35	GN-21647	Database	MySQL 업그레이드 (5.6.47 -> 5.6.48)		
5.0.34	GN-21766	Center	Genian Syncer 에서 센터로 업로드시 감사로그 개선		
5.0.34	GN-21513	WebUI	웹 취약점으로 501 에러가 발생했을 경우 전용 에러페이지 출력되지 않는 문제 수정		0.6
5.0.33	GN-21641	macOS Agent, Windows Agent	에이전트 openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2u)		
5.0.33	GN-21640	GenianOS	openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2u)		
5.0.33	GN-21397	WebUI	Tomcat 버전 업그레이드 7.0.100 --> 7.0.104 / 8.5.51 --> 8.5.55		7
5.0.33	GN-21386	GenianOS	Apache httpd 2.4.43 업그레이드		
5.0.32	GN-21181	Database	MySQL 업그레이드 (5.6.41 -> 5.6.47) 및 파일권한 변경		
5.0.32	GN-21084	WebUI	관리콘솔 취약점 개선		7.5
5.0.31	GN-20848	WebUI	보안 취약점 개선 - 파일업로드 확장자우회, web 에서 인증없이 /disk/data/custom폴더내 파일접근 등		5.3
5.0.30	GN-20928	WebUI	Tomcat 버전 업그레이드 7.0.99 --> 7.0.100 / 8.0.53 --> 8.5.51		4.8
5.0.30	GN-20875	WebUI	GET 방식의 크로스 사이트 스크립팅 (XSS) 취약점 개선		1.6
5.0.30	GN-20874	GNOS	Bash 취약점 (shellshock) 패치	4.1.3	
5.0.28	GN-20471	Center	openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2t)		
5.0.28	GN-20443	macOS Agent, Windows Agent	에이전트 openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2t)		
5.0.27	GN-18882	WebUI	OWASP ZAP 틀에 의해 검색된 관리콘솔 취약점 개선		

continues on next page

Table 43 – continued from previous page

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
5.0.21	GN-19317	GenianOS	opensshd 취약점으로 인한 버전 패치	5.0.8, 4.0.111, 4.0.34	
5.0.19	GN-19203	Center, WebUI	Apache httpd 2.4.39 업그레이드		
5.0.17	GN-19044	GenianOS	openssl 최신버전으로 업그레이드 (OpenSSL 1.0.2r)		
5.0.17	GN-18607	WebUI	tomcat-connectors 버전 업그레이드		

SECURITY ADVISORIES

17.1 GN-SA-2024-001: Genian NAC - 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

지니안 NAC 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 NAC SQL 인젝션

17.1.5 영향 버전

- Genian NAC 5.0.60 이하
- Genian NAC 5.0.55 LTS(Revision 125558 이하)
- Genian NAC 5.0.56 LTS(Revision 125560 이하)

17.1.6 해결 방법

이 권고 사항에 포함된 취약점은 아래 버전으로 업데이트하여 해결할 수 있습니다.

- Genian NAC 5.0.61 이상
- Genian NAC 5.0.55 LTS(Revision 125559 이상)
- Genian NAC 5.0.56 LTS(Revision 125561 이상)

17.1.7 임시 조치 방법

- 없음

17.2 GN-SA-2023-001: Genian NAC - 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 NAC 4.0.155 이하
- Genian NAC 5.0.42 LTS (Revision 117460 이하)
- Genian NAC 5.0.54 이하

17.2.5 해결 방법

이 권고 사항에 포함된 취약점은 아래 버전으로 업데이트하여 해결할 수 있습니다.

- Genian NAC 4.0.156 이상
- Genian NAC 5.0.42 LTS (Revision 117461 이상)
- Genian NAC 5.0.55 이상

17.2.6 임시 조치 방법

- 평문노출 취약점은 이벤트 포트 변경을 통해 임시조치 가능합니다.

GN-SA-2023-001 임시 조치 방법 가이드

GN-SA-2023-001 취약점 관련하여 제조사에서는 취약점 조치가 완료된 버전으로 패치를 권고 하고 있습니다.

본 임시 조치 방법 가이드는 네가지 취약점 중 비인가 설정(네트워크센서 비밀번호) 변경 취약점 에 한한 임시 조치 가이드입니다.

준비 사항

1. 정책서버 SSH 접속을 위한 준비(접속계정, 패스워드)

정책서버 설정 변경은 CLI를 통해서 진행합니다.

정책서버 설정 변경 시 주요 서비스가 재구동 됩니다.

2. 네트워크센서 재부팅을 위한 SSH 접속 준비(접속계정, 패스워드)

정책서버 포트 변경 후 네트워크센서에 변경사항 적용을 위해서는 장비 재부팅이 필요합니다.

3. 에이전트 미동작 정책 OFF

정책서버 설정 변경 후 에이전트 정상통신을 위해서는 PC재부팅이 필요하며 PC재부팅이 되지 않은 PC는 에이전트 미동작 차단 정책으로 차단 될 수 있습니다.

4. 방화벽 허용 정책 추가

변경된 이벤트 포트에 대한 방화벽 허용 정책의 추가가 사전에 필요합니다.

변경된 이벤트포트에 대해 정책서버 <> 네트워크센서IP, 정책서버 <> PC 허용 정책 추가가 필요합니다.

주의 사항

- DB서버 LOG서버가 분리 구성된 환경에서는, 정책서버 이벤트 포트 변경 작업 후, DB서버와 Log서버 재부팅이 필요합니다.
- 정책서버 이벤트 포트 변경 작업 후, 네트워크센서, Agent 재부팅 전까지는 정책서버와 이벤트 전송이 불가능합니다. 따라서 네트워크센서, Agent 동작 상태가 다운 상태로 표시됩니다.

설정 및 확인 사항

설정 방법은 범용OS 버전과 GNOS 버전의 접속 방법을 제외한 모든사항은 동일합니다.

정책서버 접속

범용OS인 경우 아래와 같이 진행합니다.

1. 터미널 프로그램을 이용하여 SSH에 연결합니다. (접속 포트 번호: 3910)

```
ID/PASSWORD 입력하여 SSH 접속
genian@ubuntu:~$
genian@ubuntu:~$ sudo su          <-- root 권한 획득
[sudo] password for genian:       <-- 패스워드 한번 더 입력
root@ubuntu:/home/genian#
root@ubuntu:/home/genian# gnlogin <-- genian shell 진입
genian>
genian> enable                    <-- enable 모드 진입
Password:                         <-- enable password 입력
genian#
```

2. 프롬프트가 genian# 으로 변경되면 이벤트포트 변경 항목으로 이동합니다.

GNOS인 경우 아래와 같이 진행합니다.

1. 터미널 프로그램을 이용하여 SSH에 연결합니다. (접속 포트 번호: 3910)

```
Username:          <-- CLI 접속 계정 입력
Password:          <-- 패스워드 입력
genian> enable     <-- enable 모드 진입
Password:          <-- enable 패스워드 입력
genian#
```

2. 프롬프트가 genian# 으로 변경되면 이벤트포트 변경 섹션으로 이동합니다.

이벤트 포트 변경 설정

1. 상단 준비 사항 에 작성된 내용에 대해 확인하고 조치합니다.
2. 정책서버 SSH 접속했다면 설정 모드로 진입합니다.

```
genian# config terminal
genian(config) #
```

3. 정책서버와 Client(네트워크센서, 에이전트)에서 이벤트 송수신에 사용하는 포트를 변경합니다.

```
genian(config) # node-server event-port {변경할 포트번호 default 3870}
Stopping Service...done
Starting Service...done
genian(config) # sensor event-port {변경할 포트번호 default 3871}
Stopping Service...done
Starting Service...done
```

4. 정책서버 이벤트 포트 변경 사항 체크

```
genian(config) # exit
genian# @shell
genians$ netstat -an | grep -E "3870|3871" <-- 기존 사용하던 포트가 명령 결과에
표시되지 않아야합니다.
genians$ netstat -an | grep -E "변경한포트|변경한포트" <-- 새로 변경한 포트가 명령
결과에 표시되어야합니다.
```

5. 네트워크센서 SSH에 접속해서 장비를 재구동합니다.

```
genian# reboot
Are you sure to reboot system (y/N): y
```

6. 정책서버에 센서에서 발송하는 Keepalive 패킷이 변경한 포트로 인입되는지 확인합니다.

```
genians$ tcpdump -ni {interface명} host {네트워크센서 IP} and port {변경한 포트}
e.g. genians$ tcpdump -ni eth0 host 1.1.1.1 and port 5870
※ 네트워크센서 Keepalive는 네트워크센서에서 출발하며 10초 간격으로 양방향 UDP 통신이
발생합니다.
```

7. Web콘솔에 접속하여 네트워크센서 상태가 정상적으로 표시되는지 확인합니다.

8. 에이전트가 설치된 PC를 재부팅합니다.

9. 정책서버에 에이전트에서 발송하는 Keepalive 패킷이 변경한 포트로 인입되는지 확인합니다.

```
genians$ tcpdump -ni {인터페이스명} host {재부팅한 PC IP} and port {변경한 포트}
e.g. genians$ tcpdump -ni eth0 host 2.2.2.2 and port 5870
```

10. Web콘솔에 접속하여 재부팅한 PC 노드의 에이전트 동작 상태를 확인합니다.

Note: 취약점 관련 사항을 해결하기 위해서는 정책서버, 네트워크센서, 에이전트를 업그레이드 해야 합니다.

17.3 GN-SA-2022-001: Genian NAC - Multiple Vulnerabilities

17.3.1 날짜

- 2022년 10월 7일

17.3.2 영향도

- 높음

17.3.3 내용

지니언스는 아래 나열된 네 가지 중요한 취약점을 해결한 업데이트와 함께 제품 보안성 강화를 위한 보안 업데이트를 발표했습니다. 해당 버전을 사용하는 이용자들은 최신 버전으로 업데이트를 권고합니다.

- 서버에 불법적인 파일을 업로드 할 수 있는 취약점
- 서버 내 다운로드 가능한 파일 목록에서의 정보노출 취약점
- REST API 에서 관리자 권한 우회 취약점
- IP 신청시스템에서 관리자 전환 가능 취약점

17.3.4 영향 버전

- Genian NAC v5.0.48 이하
- Genian NAC v5.0.42(LTS) (Revision 108297 미만)
- Genian NAC v4.0.151 이하 (Revision 108063 미만)

17.3.5 해결 방법

이 권고 사항에 포함된 취약점은 아래 버전으로 업데이트하여 해결할 수 있습니다.

- Genian NAC v5.0.49 이상
- Genian NAC v5.0.42(LTS) (Revision 108297 이상)
- Genian NAC v4.0.151 (Revision 108063 이상)

Important: 취약점 관련 사항을 해결하기 위해서는 정책서버, 네트워크센서 를 업그레이드 해야 합니다.

17.3.6 임시 조치 방법

- 없음

17.4 GN-SA-2021-003: Genian NAC - Apache Log4j 2 remote code execution Vulnerability.

17.4.1 날짜

- 2021년 12월 20일

17.4.2 영향도

- 높음

17.4.3 내용

최근 Java 기반의 모든 어플리케이션에서 무료로 사용할 수 있는 오픈소스 프로그램인 Apache Log4j 2 서비스에 보안취약점이 발견되었습니다. 관련 취약점을 공격자가 악용할 경우 악성코드 감염 등 피해를 발생시킬 수 있으므로 신속하게 업데이트 할 것을 권고드립니다.

- [KISA Apache Log4j 보안 업데이트 권고](#)

17.4.4 영향 버전

- Genian NAC V5.0.42(LTS) (Revision 101319 이하)
- Genian NAC V5.0.44 (Revision 101317 이하)

17.4.5 해결 방법

이 권고 사항에 포함된 취약점은 아래 버전으로 업데이트하여 해결할 수 있습니다.

- Genian NAC V5.0.42(LTS) (Revision 101422 이상)
- Genian NAC V5.0.44 (Revision 101696 이상)

17.4.6 임시 조치 방법

- 없음

17.5 GN-SA-2021-002: Genian NAC - Multiple Vulnerabilities

17.5.1 날짜

- 2021년 11월 5일

17.5.2 영향도

- 높음

17.5.3 내용

지니언스는 아래 나열된 두 가지 중요한 취약점을 해결한 업데이트와 함께 제품 보안성 강화를 위한 보안 업데이트를 발표했습니다. 해당 버전을 사용하는 이용자들은 최신 버전으로 업데이트를 권고합니다.

- 네트워크 센서가 호출하는 특정 API에서 시스템 셸 command injection 취약점 존재하는 문제.
- 에이전트에서 인증된 사용자의 비밀번호를 변경할 때 다른 사용자의 비밀번호를 변경할 수 있는 문제.

17.5.4 영향 버전

- Genian NAC v5.0.41 이하
- Genian NAC v5.0.42(LTS) (Revision 100181 이하)
- Genian NAC v4.0.145 이하

17.5.5 해결 방법

이 권고 사항에 포함된 취약점은 아래 버전으로 업데이트하여 해결할 수 있습니다.

- Genian NAC v5.0.43 이상
- Genian NAC v5.0.42(LTS) (Revision 100182 이상)
- Genian NAC v4.0.146 이상

Important: 취약점 관련 사항을 해결하기 위해서는 정책서버, 네트워크센서, 에이전트를 업그레이드 해야 합니다.

17.5.6 임시 조치 방법

- 없음

17.6 GN-SA-2021-001: Genian NAC - SQL Injection Vulnerability

17.6.1 날짜

- 2021년 8월 9일

17.6.2 영향도

- 높음

17.6.3 내용

지니언스는 SQL 쿼리 이스케이프 처리의 보안 취약점을 해결한 정책서버에 대한 업데이트를 발표했습니다. 해당 보안 취약점으로 인해 공격자는 데이터베이스에 대한 SQL Injection 공격이 가능합니다. 공격자는 시스템내 데이터를 검색하거나 수정, 추가, 삭제할 수 있으며 또한 관리자 계정을 생성할 수 있으므로 해당 버전을 사용하는 이용자들은 최신 버전으로 업데이트를 권고합니다.

17.6.4 영향 버전

- Genian NAC v5.0.41 이하
- Genian NAC v4.0.144 이하

17.6.5 해결 방법

이 권고 사항에 포함된 취약점은 아래 정책서버 버전으로 업데이트하여 해결할 수 있습니다.

- Genian NAC v5.0.42 (LTS)
- Genian NAC v4.0.145

17.6.6 임시 조치 방법

- 없음