

NAC (네트워크 접근제어 시스템)

운영자 메뉴얼



CONTENTS

I . NAC Console 접속 방법

II. 메뉴 바(Menu Bar) 설명

III. 노드 관리 방법

IV. 정책 관리 방법

V. 백업 관리 방법

VI. 차단센서 관리 방법

1. 시리얼 콘솔 접속 방법

시리얼 접속 방법

Port : PC의 시리얼 포트로 설정

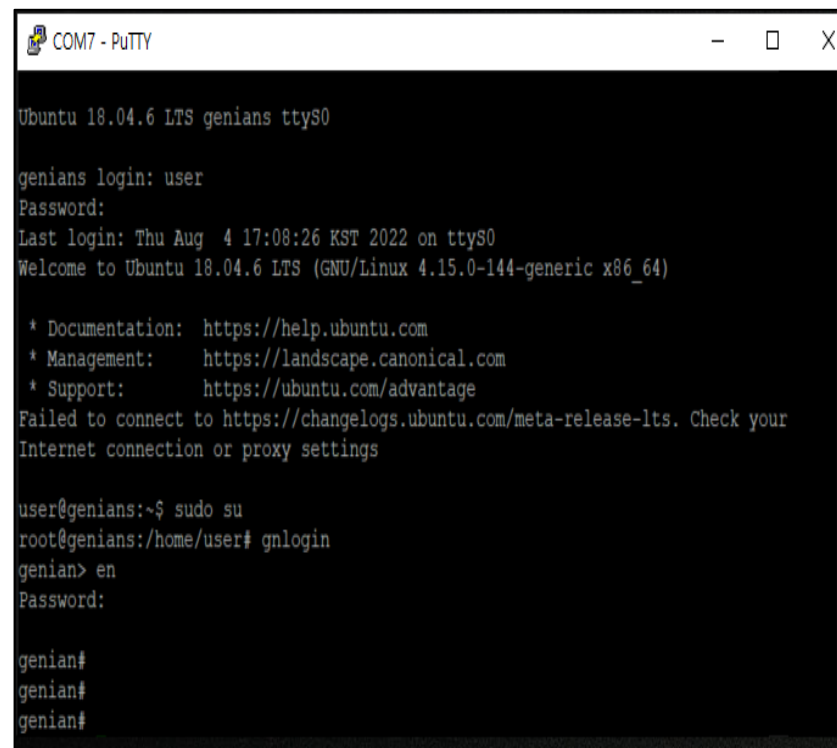
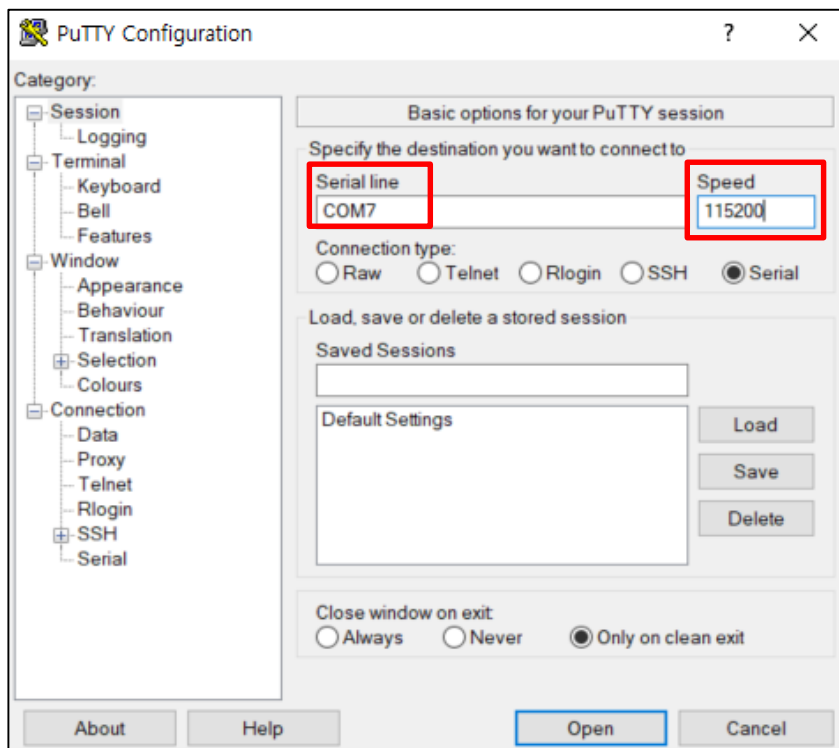
Baud rate : 115200 입력

ID / Password : user/admin123!

Root 권한 획득 : sudo su

Privilege mode 전환 : gnlogin

Enable mode 전환 : enable (en) / pw : admin123!



1. SSH 접속 방법

SSH 접속 방법

Port : 3910

ID / Password : user/admin123!

Root 권한 획득 : sudo su

Privilege mode 전환 : gnlogin

Enable mode 전환 : enable (en) / pw : admin123!

Quick Connect

Protocol: SSH2

Hostname: xxx.xxx.xxx.xxx

Port: 3910

Firewall: None

Username:

Authentication

☒ Password
 ☒ PublicKey
 ☒ Keyboard Interactive
 ☒ GSSAPI

Properties...

☐ Show quick connect on startup
 ☒ Save session
 ☐ Open in a tab

Connect

Cancel

COM7 - PuTTY

```

Ubuntu 18.04.6 LTS geniens ttyS0

geniens login: user
Password:
Last login: Thu Aug  4 17:08:26 KST 2022 on ttyS0
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-144-generic x86_64)

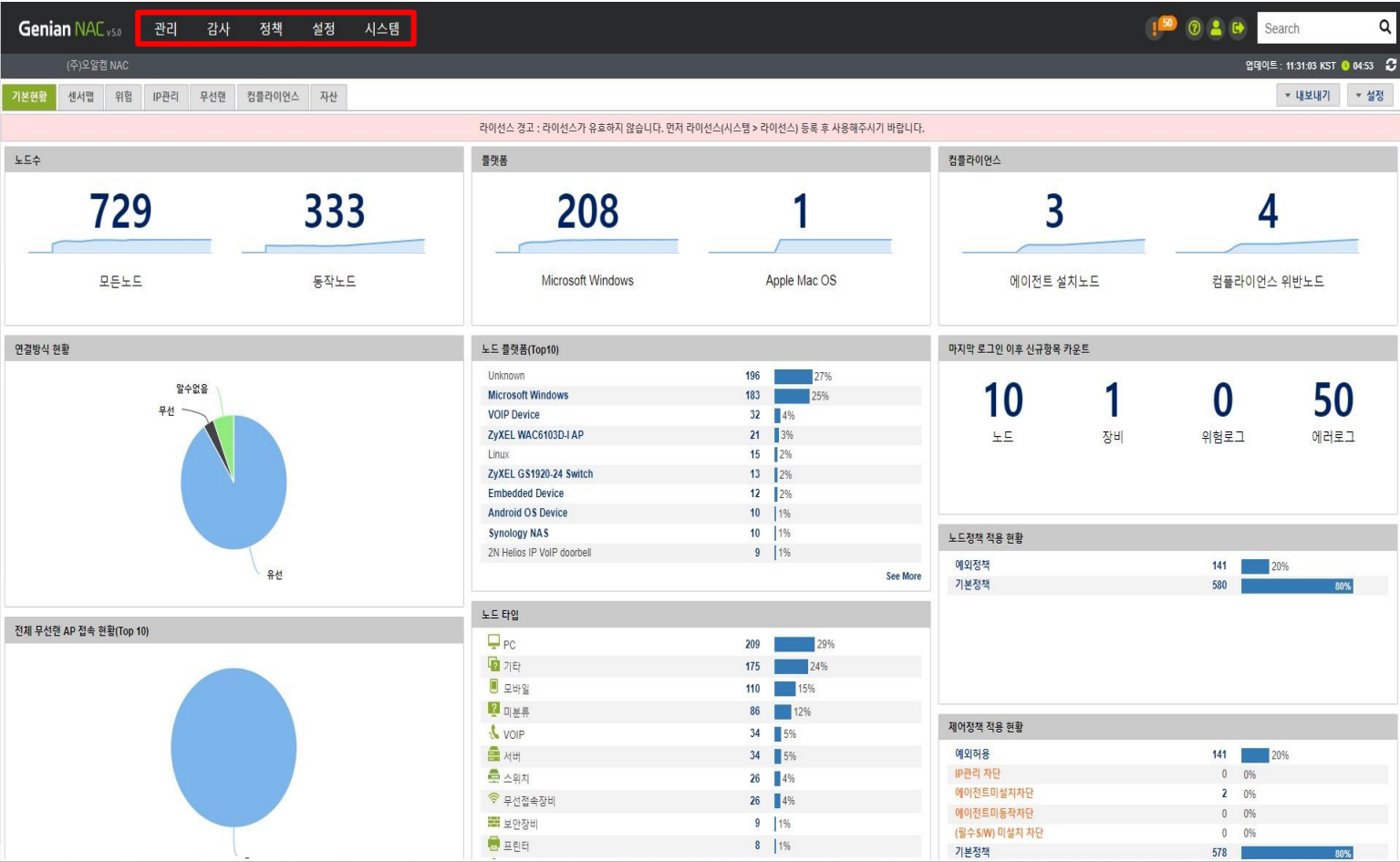
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

user@geniens:~$ sudo su
root@geniens:/home/user# gnlogin
genian> en
Password:

genian#
genian#
genian#
  
```

1. 메뉴바 소개

- Genian 위젯을 통한 전체 현황 조회
- 관리 노드(IP/MAC), 유지 관리
- 감사 로그, 리포트 조회
- 정책 노드/제어 정책 수립
- 설정 기본적인 환경설정
- 시스템 시스템 동작상태 및 환경 설정



- 신규 MAC/IP 차단

- 차단 노드 MAC/IP 클릭하여 노드상세페이지로 이동
- [정책] - [IP허용-충돌보호해제], [MAC허용-변경금지(모든IP대역)] 선택
- [MAC허용-변경금지(모든IP대역)] 메뉴에서 IP 선택 후 [추가] 버튼 클릭하여 하단에 IP가 추가 됐는지 확인후 상단 [수정] 버튼 클릭

Genians NAC (네트워크 접근제어) 운영자 매뉴얼

2. MAC 차단

• 신규 MAC 차단

<input type="checkbox"/>	NT AG SS	위험	동작	동작상태차트	IP주소 ↑	MAC주소	정책	제어정책
<input type="checkbox"/>					172.23.104.121	00-04-2E-52-2A-04		IP관리 차단 ⓘ

- MAC 차단 대상 노드 체크박스 체크
- [작업선택] - [IP/MAC정책] - [MAC 허용 - 변경금지해제] 선택

The screenshot displays the Genian NAC v5.0 web interface. On the left, there's a sidebar with navigation options like '전체 노드 (540)', '노드바구니 (0)', and '노드 그룹 (0)'. The main area shows a table of nodes with columns for IP address, MAC address, and policy. A context menu is open over the table, showing various actions. The 'MAC 허용 - 변경금지해제' option is highlighted in red. The table lists nodes with their respective IP and MAC addresses, and the policy applied to them.

3. MAC변경금지 위반

• MAC변경금지(고정)

<input type="checkbox"/>	NT AG SS	위험	동작	동작상태차트	IP주소	MAC주소	정책	제어정책
<input type="checkbox"/>					192.168.1.188	00:E0:4C:63:F7:8A		기본정책
<input type="checkbox"/>					192.168.1.188	5C:6F:69:31:1F:A8	IP변경금지 - 단일 IP 위반됨	기본정책

- MAC변경금지가 적용된 노드가 IP변경이 필요한 경우
 - MAC변경금지 위반 노드의 노드상세페이지로 이동하여 **[MAC허용-변경금지]**에 변경할 IP를 추가하여 조치 가능
- MAC변경금지가 적용된 노드 IP변경이 필요하고 더 이상 MAC변경금지를 적용시키지 않을 경우
 - MAC변경금지 위반 노드 체크박스 체크 후 **[작업선택] - [IP/MAC 정책] - [MAC허용-변경금지 해제]**로 조치 가능

172.23.104.121 00:01:2E:52:2A:01

CDCOM40-131210 Microsoft Windows 10 Enterprise x64

노드정보 장비정보 시스템정보 네트워크정보 소프트웨어정보 운영체제 및 이프 정보 정책 정책현황 Malware 이학관리

정책

IP 정책: 유선 설정안됨, 무선 설정안됨, 유선부서 설정안됨

정책: IP제한, IP허용, 유선보조해제, IP허용, 유선보조(지정 IP대역)

IP사용 시작:

IP사용 종료:

IP사용 신규노드정책: 설정안됨

MAC 정책: 유선 설정안됨, 무선부서 설정안됨

정책: MAC제한, MAC허용, 변경금지(지정 IP대역), **MAC허용, 변경금지 (모든 IP대역)**

172.23.104.121

172.23.104.121 삭제

MAC사용 시작:

MAC사용 종료:

노드(IP+MAC) 정책

사용자인증정책: 사용자인증 노드정책준수, 사용자인증 적용, 모은사용자, 사용자인증 적용, 사용자제한

IP사용 포트명 제한:

제한감시기능: ☐

노드에 허용되지 않은 네트워크 접근행위(대역)에 감시(포함)합니다

노드정보 검사: ☒

노드의 불적응(알림포함) 정보 검사 사용여부를 선택합니다

노드삭제 금지: ☐

노드를 영구적으로 유지합니다

전체노드 (전체)

작업선택

IP/MAC 정책

노드 및 장비

노드 사용자

노드 대상 명령

빠른 실행 명령 편집...

IP 차단

IP 허용 - 충돌보조 해제

IP 허용 - 충돌보조 (지정 MAC)

IP 사용 포트명제한 설정

IP 사용 포트명제한 해제

IP 사용시간 제한/해제 설정

IP 사용 신규노드정책 설정

IP 충돌설정

MAC 차단

MAC 허용 - 변경금지 해제

MAC 허용 - 변경금지(지정 IP대역)

MAC 허용 - 변경금지(모든 IP대역)

MAC 사용시간 제한/해제 설정

IP 및 MAC 차단

IP 및 MAC 허용

IP 충돌보조 및 변경금지

IP 충돌보조 및 변경금지(지정대역)

172.23.31.167 VS 00:E0:4C:3D:51

172.23.31.168 8C:EC:4B:D7:8E

4. 노드타입 변경

- 노드타입변경 대상 노드 상세페이지로 이동
- [노드정보] - [노드타입] - [지정] 체크박스 체크
- 원하는 [노드타입] 선택 후 상단 [수정] 버튼 클릭

The screenshot displays the Genian NAC v5.0 interface. On the left, a sidebar shows a tree view of nodes. The main area shows the details for a node with IP 172.23.104.121. The 'Node Information' (노드정보) tab is active. In the 'Node Type' (노드타입) dropdown menu, 'PC' is selected, and the 'Specify' (지정) checkbox is checked. The 'Edit' (수정) button is highlighted in the top right corner. Below the node information, there is a table of CVEs (CVE-2022-34728, CVE-2022-34729, CVE-2022-34730) with their respective severity levels (CRITICAL, MEDIUM, HIGH).

1. 그룹 생성 [1/2]

노드 그룹 생성 방법

1. [정책] - [그룹] - [노드]로 이동
2. [작업선택] - [생성(상태그룹)]/[생성(노드정책 전용)] 생성 선택
 - 노드정책 또는 제어정책에서 사용 가능한 정책그룹 상세 설정을 할 수 있습니다.
 - [생성(노드정책 전용)]은 노드정책과 제어정책에서 모두 사용 가능하지만 [생성(상태그룹)]은 제어정책에서만 사용 가능합니다.

The screenshot shows the Genian NAC v5.0 web interface. The 'Policy' (정책) menu is active, and the 'Group' (그룹) sub-menu is selected. The 'Create (Node Policy Dedicated)' (생성 (노드정책 전용)) option is highlighted in the 'Job Selection' (작업선택) dropdown. Below this, a table lists existing node groups with columns for group name, count, and policy rules.

그룹명	노드수	정책	생성일
생성 (노드정책 전용)	30	백신정보/최신업데이트/보안오래됨/1주, 백신명=AhniLab V3 Internet Security 9.0	2022-08-22 14:43:10
삭제	6	시스템/비밀번호 미변경 사용자계정/90일	2022-08-22 14:43:10
노드그룹 내보내기	29	시스템사용자계정/비밀번호없는 계정 존재	2022-08-22 14:43:10
노드그룹 가져오기	8	시스템사용자계정/비밀번호없는 로그인된 계정 존재/비밀번호없는 로그인된 계정 존재	2022-08-22 14:43:10
노드	221	노드그룹/속하지 않으면/신뢰 노드	2022-08-22 14:43:10
업데이트 (9)	37	태그/존재하면/TRUSTED	2022-08-22 14:43:10
카테고리 생성	11	에이전트상태/설치상태/설치됨	2022-08-22 14:43:10
카테고리 삭제	127	에이전트상태/동작상태/Down	2022-08-22 14:43:10
카테고리 할당	25	노드그룹/속하면/PC	2022-08-22 14:43:10
노드그룹 생성결과	12	에이전트상태/설치상태/설치안됨	2022-08-22 14:43:10
운영체제 업데이트 미설치	25	운영체제 업데이트/통정시간내에 업데이트 설치되지 않은/1개월	2022-08-22 14:43:10
운영체제 업데이트 상태 한쪽	6	운영체제 업데이트/업데이트 상태/한쪽만	2022-08-22 14:43:10
운영체제 업데이트 상태 한쪽	25	운영체제 업데이트/업데이트 상태/한쪽만	2022-08-22 14:43:10
원격데스크톱 사용	1	시스템/원격데스크톱/허용됨	2022-08-22 14:43:10
원격데스크톱 사용	73	원격데스크톱/노드에 설치된 원격/감지되면	2022-08-22 14:43:10
원격데스크톱 사용	50	원격데스크톱/원격데스크톱을 사용하는 원격이 있는/존재하면	2022-08-22 14:43:10
원격데스크톱 사용	1	원격데스크톱/원격데스크톱을 사용하는 원격이 있는/존재하면	2022-08-22 14:43:10
원격데스크톱 사용	35	원격데스크톱/원격데스크톱을 사용하는 원격이 있는/존재하면	2022-08-22 14:43:10

1.그룹 생성 [2/2]

노드그룹 : 특정 액티노드

가변된 조건설정 내를 사용할 수 있습니다. 실행실에서 활성화해 보세요 설정

기본정보

다항 노드리스트

기본정보

카테고리

2 분류

검색

생성

ID

특정 액티노드

타입

상위그룹

설명

경신시간

2022-09-22 12:42:52

CWP메시지

ko en zh ja

1000000 입력 가능합니다.

적용모드

사용할

감사로그

Off

필요

Off

노드관리 기본뷰

노드뷰

해제유보

설정

노드그룹에 포함되어 있던 노드가 상위변경에 따라 노드그룹에서 해제될 경우 설정한 기간동안 해제되는것을 유보합니다.

그룹조건

조건연산

(OR) 아래의 조건 중 하나를 만족하면

조건설정

추가

1-44/44

50

번호	항목	조건	설정	설명	작업
1	MAC주소	MAC이 같으면	00:E0:AC:62:A8:C4	관리하원/호외명	삭제
2	IP주소	IP가 같으면	172.23.104.100	ICT시스템팀/전산실/업무서버	삭제
3	IP주소	IP가 같으면	172.23.104.101	뉴미디어연구실/이강욱(OA)	삭제
4	IP주소	IP가 같으면	172.23.104.123	ICT시스템팀/MRTG(DMC구간)	삭제
5	IP주소	IP가 같으면	172.23.104.136	ICT서일본부장/원다범	삭제

- 1.ID : 노드그룹 ID 설정
- 2.타입 : 노드그룹 타입 표시
- 3.설명 : 해당 노드그룹 설명 기입 부분
- 4.CWP메시지 : 접속인증페이지에 표시 될 메시지
- 5.적용모드 : 노드그룹 사용 여부 선택
- 6.감사로그 : 감사로그 설정 여부 선택
- 7.노드관리 기본뷰 : 노드그룹의 기본뷰 설정
- 8.조건연산 : AND, OR 조건연산 설정
- 9.조건 : 아이템의 세부적인 조건 설정
- 10.생성 : 설정한 조건설정 내용으로 신규 정책그룹을 생성

Genians NAC (네트워크 접근제어) 운영자 매뉴얼

- 11 -

SM Information
(주)에스엠인포메이션

2. 에이전트 액션

에이전트액션 생성방법

1. [정책] - [노드정책] - [노드액션]으로 이동
2. [작업선택] - [생성] 클릭으로 노드액션 생성페이지로 이동하여 생성

Genian NAC v5.0 관리 감사 정책 설정 시스템

(주)오일컴 NAC 업데이트: 18:00:14 KST 09:21

정책

- 노드 정책
 - 노드 액션

노드액션 관리

라이선스 경고 : 라이선스가 유효하지 않습니다. 먼저 라이선스(시스템 > 라이선스) 등록 후 사용해주시기 바랍니다.

작업선택 운영체제 플러그인 타입 검색

1 - 50 / 58 50

생성	액션명 ↑	플러그인명	설명
삭제	(필수 S/W) 문서중앙화 설치유무 검사	수행조건만 검사	필수 S/W
	(필수 S/W) EPP 설치유무 검사	수행조건만 검사	필수 S/W
	ARP 관리	ARP 관리	사용자 PC의 ARP 테이블에 대한 관리 작업을 수행합니다.
	ARP 관리	ARP 관리	사용자 PC의 ARP 테이블에 대한 관리 작업을 수행합니다.
	DNS 제어	DNS 제어	DNS 관련 로컬설정을 제어합니다.
	macOS 업데이트	macOS 업데이트	macOS의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.
	Malware Detector	Malware Detector	Insights ECO 시스템과 연동하여 단말에서 발생하는 악성코드를 감지합니다.
	TCP세션검사	TCP세션검사	주기적으로 TCP 세션수를 수집하여 일계치이상되는 세션수가 발견되면 네트워크 인터페이스를 차단합니다.
	Windows 방화벽 제어	Windows 방화벽 제어	Windows 방화벽을 사용하여 사용자 네트워크를 제어합니다.
	Windows 보안설정	Windows 보안설정	시스템에 설정된 Windows 방화벽, 원격 데스크톱, 자동 실행의 동작을 제어합니다.
	Windows 업데이트	Windows 업데이트	Windows의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.
	WMI정보수집	WMI정보수집	WMI를 통하여 시스템 정보를 수집합니다.
	공유프로그램 미존재	수행조건만 검사	P2P와 같은 사내에서 사용이 적합하지 않은 공유프로그램
	네트워크 공유폴더	네트워크 공유폴더	네트워크에 공유된 폴더정보를 수집하여 일정 시간 이상 공유되는 폴더를 제어합니다.
	네트워크 공유폴더	네트워크 공유폴더	네트워크에 공유된 폴더정보를 수집하여 일정 시간 이상 공유되는 폴더를 제어합니다.
	네트워크 트래픽 제어	네트워크 트래픽 제어	주기적으로 네트워크 사용량을 수집하여 설정된 수치 이상일 경우 네트워크 인터페이스를 차단합니다.
	네트워크정보 수집	네트워크정보 수집	네트워크 인터페이스 정보와 할당된 포트정보를 수집하여 노드정보에 표시합니다.
	네트워크정보 수집	네트워크정보 수집	네트워크 인터페이스 정보와 할당된 포트정보를 수집하여 노드정보에 표시합니다.
	매신저프로그램 미존재	수행조건만 검사	사내에서 필요에 따라 제어되어야 할 메신저프로그램
	모니터정보 수집	모니터정보 수집	로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다.
	모니터정보 수집	모니터정보 수집	로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다.
	모양 및 개인설정	모양 및 개인설정	Windows 바탕화면, 화면 보호기에 대한 설정 정보를 수집 및 제어합니다.
	모양 및 개인설정	모양 및 개인설정	바탕화면, 화면보호기에 대한 설정 정보를 수집 및 제어합니다.
	무선 연결 관리자	무선 연결 관리자	Wireless Connection Manager 프로그램에 대한 옵션 및 동작을 제어합니다.

2. 에이전트 액션

기본설정

액션명

설명

ko en zh ja

CWP메시지

4095자 입력 가능합니다.
* CWP메시지는 정책적응여부에 따라 접속인증페이지에 표시됩니다. HTML을 사용하여 입력창을 더블클릭하면 미리보기 가능합니다.

라벨

액션 수행설정

OS 종류

Windows

조건연산

(AND) 아래의 모든 조건을 만족하면

추가

조건설정

항목	조건	설정	설정메모
설정된 조건없음			

조건설정

항목

프로세스

조건

동작하면

설정

설정메모

반드시 실행되어야 할 필수 프로세스를 설정합니다.

추가

계속 추가

취소

1. **액션명** : 에이전트액션 이름 지정
2. **설명** : 해당 에이전트액션에 대한 설명 기입 부분
3. **CWP메시지** : 차단페이지에 출력될 CWP메시지 설정
4. **조건연산** : AND, OR 조건 설정(설정된 복수의 조건 설정값을 AND또는 OR연산으로 적용을 할 것인지 설정하는 부분입니다.)
5. **항목** : 프로세스, 파일 디렉토리 등 액션 검사를 수행해야 할 아이টে를 설정
6. **설정** : 각 아이টে의 세부 항목 설정
7. **설정메모** : 해당 에이전트액션에 대한 간략한 메모 기입 부분

2.에이전트 액션

플러그인선택

수행조건만 검사

플러그인설정

별도의 설정이 필요 없는 플러그인 입니다.

주기적 수행

수행주기

24 시간

설정된 주기마다 액션을 수행합니다.

수행시간대

@ANYTIME

액션을 수행할 시간대를 선택합니다.

재시도 시간

0 분

액션수행 실패시 재시도를 수행할 최대 시간을 설정합니다.(0: 재시도 안함)

재시도 횟수

0

액션수행 실패시 재시도 시간내에 수행할 재시도 횟수를 설정합니다.

1. 플러그인선택 : 액션 조건 검사에 대한 수행할 플러그인 선택
2. 수행주기 : 에이전트 액션의 수행 주기를 설정 (한번만 수행, 주기적 수행, 윈도우 시작 시 한번 수행,지정시각 수행, 항상수행)
3. 수행주기 : 주기적 수행 선택 시 에이전트 액션을 수행 할 기준 선택
4. 수행시간대 : 액션을 수행할 시간대를 선택(정책 > 객체 > 시간그룹에 설정되어있는 그룹 선택)
5. 재시도 시간 : 액션수행 실패시 재시도를 수행할 최대 시간을 설정
6. 재시도 횟수 : 액션수행 실패시 재시도 시간내에 수행할 재시도 횟수를 설정

ex) 재시도 시간 : 10, 재시도 횟수 : 3 으로 설정되어있을 경우 액션수행 실패시 10분동안 3회 재시도

적용언어

☒ 전체
☒ Korean
☒ English
☒ Chinese
☒ Japanese
☒ Other

적용OS

☒ 전체

☒ Microsoft Windows XP
☒ Microsoft Windows Server 2003
☒ Microsoft Windows Vista
☒ Microsoft Windows 7
☒ Microsoft Windows Server 2008
☒ Microsoft Windows 8
☒ Microsoft Windows Server 2012
☒ Microsoft Windows 8.1
☒ Microsoft Windows 10
☒ Microsoft Windows Server 2016
☒ Microsoft Windows Server 2019
☒ Microsoft Windows 11

☒ Microsoft Windows XP x64
☒ Microsoft Windows Server 2003 x64
☒ Microsoft Windows Vista x64
☒ Microsoft Windows 7 x64
☒ Microsoft Windows Server 2008 x64
☒ Microsoft Windows 8 x64
☒ Microsoft Windows Server 2012 x64
☒ Microsoft Windows 8.1 x64
☒ Microsoft Windows 10 x64
☒ Microsoft Windows Server 2016 x64
☒ Microsoft Windows Server 2019 x64
☒ Microsoft Windows 11 x64

1. 적용 언어
- 에이전트액션 적용언어 설정
2. 적용 OS
- 에이전트액션이 수행 될 OS 설정(32bit/64bit 구분 가능)

3. 노드 정책 [1/11]

노드 정책 설정 방법

[정책] - [노드정책] - [작업선택] - [생성] 선택

- 그림과 같이 팝업 형식으로 출력 되는지 확인

The screenshot displays the Genian NAC v5.0 management interface. At the top, the '정책' (Policy) menu is highlighted. On the left sidebar, the '노드정책' (Node Policy) section is expanded, showing a list of sub-items including '노드정책', '노드액션', '제어정책', '제어액션', '무선랜정책', 'AP 프로파일', 'Client 프로파일', 'Windows 업데이트 정책', '장치제어 정책', '장치그룹', '컴플라이언스정책', '그룹', '노드', '무선랜', '사용자', and '객체'. The '노드' section is further expanded, showing a list of nodes with columns for ID, Name, and Status. The '작업선택' (Job Selection) dropdown menu is open, showing '생성' (Create) as the selected option. The main panel shows a list of policies with columns for ID, Name, and Status. A modal window titled '노드정책 방법사' (Node Policy Method) is open, displaying options for '정책 선택' (Policy Selection) and '정책 기본설정' (Policy Basic Settings). The '정책 선택' tab is active, showing a list of policies with columns for ID, Name, and Status. The '정책 기본설정' tab is also visible, showing a list of policies with columns for ID, Name, and Status.

3. 노드 정책 [2/11]

노드 정책 설정 방법 (단계 1 : 정책 선택)

노드정책 마법사

정책 선택

정책 기본설정

노드그룹 설정

정책 세부설정

노드액션 설정

위험감지 설정

1

기존 정책을 선택하면 해당 정책에 대한 설정이 자동으로 설정됩니다.

신규생성

신규로 정책을 생성합니다.

기존 정책 기반으로 생성

선택한 정책의 설정을 기준으로 신규 정책을 생성합니다.

예외정책

취소

→ 다음

1. 정책 선택 탭
- 정책 신규생성 또는 기존 정책 기반 생성 중 선택 가능
2. 신규생성
- 신규로 정책을 생성
3. 기존 정책 기반으로 생성
- 미리 설정되어있는 기존 정책 기반으로 정책 생성
4. 정책선택
- 생성된 정책 선택
5. 다음 버튼
- 다음 버튼을 통해 2단계 설정 가능

3. 노드 정책 [3/11]

노드 정책 설정 방법 (단계 2 : 정책 기본 설정)

정책 관련 기본설정을 하는 단계로 ID, 설명, 순서, 적용모드를 설정할 수 있습니다.

노드정책 마법사

정책 선택 **정책 기본설정** 노드그룹 설정 정책 세부설정 노드액션 설정 위험감지 설정

1

 정책 관련 기본설정을 합니다.

ID

설명

순서

1

적용모드

사용함

→

사용함

사용안함

사용함

← 이전

취소

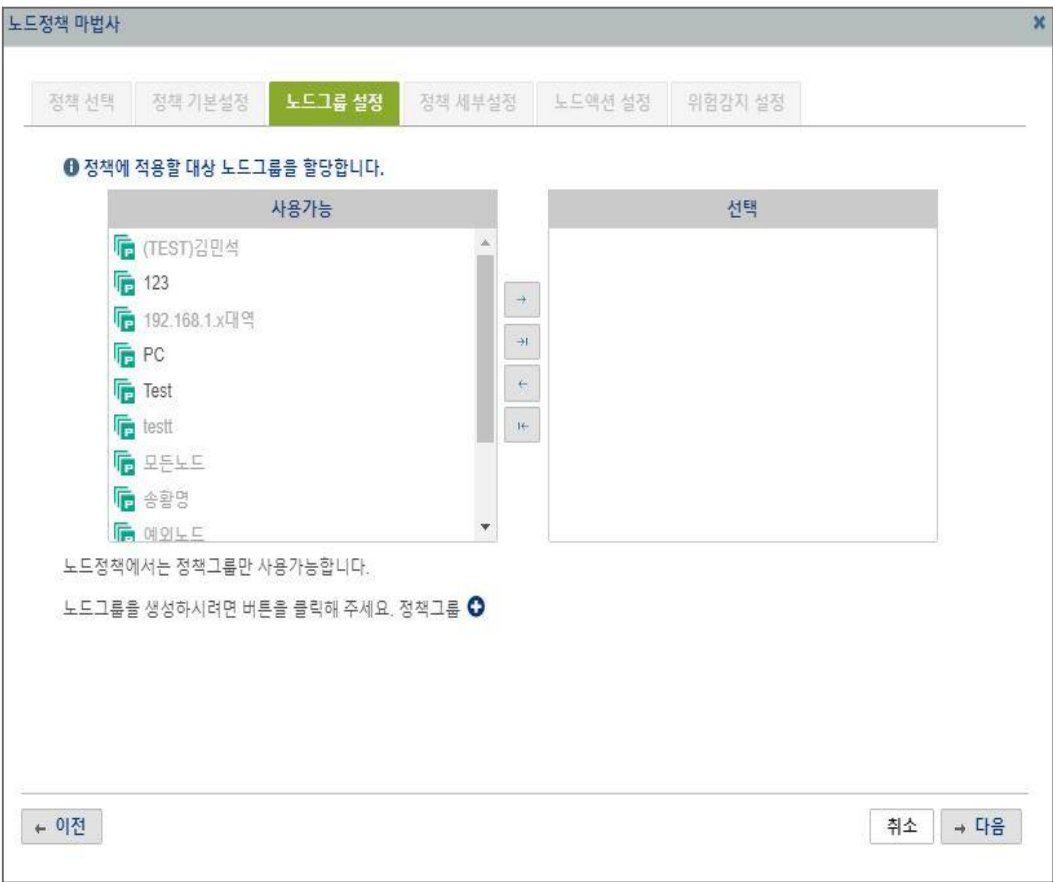
→ 다음

1. ID
- 정책의 ID(이름) 을 설정
2. 설명
- 정책의 상세 설명 입력
3. 순서
- 정책의 우선순위 설정(숫자가 낮을 수록 우선순위가 높음)
4. 적용모드
- 정책 사용 여부 선택

3. 노드 정책 [4/11]

노드 정책 설정 방법 (단계 3 : 노드 그룹 설정)

정책에 적용할 대상 노드 그룹을 선택 가능합니다. 원하는 노드 그룹이 없을 경우 생성 버튼으로 생성이 가능합니다.



- 1. 사용가능**
바로 사용가능한 노드그룹 목록
- 2. 선택**
적용될 노드그룹 목록
- 3. →**
선택한 노드그룹 [선택]란으로 이동
(현재 생성중인 정책에 적용될 노드 그룹)
- 4. →|**
[사용가능]란의 노드그룹 [선택]란으로 일괄 이동
- 5. ←**
선택한 노드그룹 [사용가능] 란으로 이동
- 6. |←**
[선택] 란의 노드그룹 [사용가능] 란으로 일괄 이동
- 7. +add**
정책그룹 생성
- 8. ← 이전**
이전 단계로 이동

3. 노드 정책 [5/11]

노드 정책 설정 방법 (단계 4 : 정책 세부 설정) - 계속

노드 정책에서 에이전트가 수행할 인증 정책과 에이전트 정책의 세부사항을 설정할 수 있습니다.

노드정책 마법사

정책 선택

정책 기본설정

노드그룹 설정

정책 세부설정

노드액션 설정

위험감지 설정

1

에이전트가 수행할 인증정책과 에이전트 정책의 세부사항을 설정합니다.

인증정책

인증방법

비밀번호인증

사용자인증 수행방법을 선택합니다.

인증방식

Local DB

RADIUS

LDAP (ActiveDirectory)

POP3

IMAP

SMTP

할당

인증서버 요청 순서를 설정합니다. 사용자인증에 실패시 설정된 순서대로 다음 인증서버에 시도합니다.

2단계 인증

사용안함

2단계 인증 방법을 선택합니다.

인증대체정보

사용안함

에이전트에서 읽어들이 사용자정보를 인증정보로 대체하기 위한 방식을 선택합니다.

인증 사용자그룹

USER-ALL

← 이전

취소

→ 다음

- 인증방법**
 사용자인증 수행방법 설정
 (귀사에서는 사용자 인증을 사용하지 않기 때문에 **호스트인증으로 설정 필수 및 인증정책 관련 부분 수정을 안하는 것을 권장**)
- 인증방식**
 인증할 방식을 선택
- 인증대체정보**
 에이전트에서 읽어들이 사용자정보를 인증정보로 대체하기 위한 방식을 선택
- 인증 사용자 그룹**
 사용자인증이 가능한 사용자그룹을 선택

3. 노드 정책 [6/11]

노드 정책 설정 방법 (단계 4 : 정책 세부 설정) - 계속

노드 정책에서 에이전트가 수행할 인증 정책과 에이전트 정책의 세부사항을 설정할 수 있습니다.

노드정책 마법사

정책 선택 | 정책 기본설정 | 노드그룹 설정 | **정책 세부설정** | 노드액션 설정 | 위험감지 설정

주기적 재인증 : 사용안함 ▼
지정된 주기마다 사용자인증을 해제하여 사용자가 재인증을 받도록 하기위한 방법을 선택합니다.

인증만료전알림 : 10 분 ▼
인증만료전 사용자에게 알람을 보낼 시간을 설정합니다. (1분 - 1년)

사용자인증페이지 :
사용자인증 페이지의 URL을 설정합니다. (미입력시 시스템에 정의된 기본 사용자인증페이지가 사용됩니다.)

운영체제 시작시 재인증 : Off ▼
시스템 재부팅 또는 절전모드 해제시 자동 로그아웃되고 재인증을 받을지 여부를 선택합니다.
절전모드는 '설정 > 환경설정 > 에이전트 > 절전모드 재시작 시간' 옵션에 따라 자동 로그아웃이 수행됩니다.
단, 인증 대체 정보를 사용할 경우 동작하지 않습니다.

사용자명 출력이름 : ko en zh ja
아이디
445자 입력 가능합니다.
사용자명 입력장에 출력할 이름을 설정합니다. (예:사번)

비밀번호 출력이름 : ko en zh ja

사용자등록 페이지 : Off ▼
사용자등록 페이지 링크를 사용자에게 보여줄지 여부를 선택합니다.

1. 주기적 재인증

지정된 주기마다 사용자인증을 해제하여 사용자가 재인증을 받도록 하기위한 방법을 선택

2. 윈도우 시작시 재인증

시스템 재부팅시 자동 로그아웃되고 재인증을 받을지 여부를 선택

3. 사용자명 출력이름

사용자명 입력장에 출력할 이름을 설정(예:사번)

4. 비밀번호 출력이름

비밀번호 입력장에 출력할 이름을 설정

5. 사용자등록 페이지

사용자등록 페이지 링크를 사용자에게 보여줄지 여부를 선택

3. 노드 정책 [7/11]

노드 정책 설정 방법 (단계 4 : 정책 세부 설정) - 계속

노드 정책에서 에이전트가 수행할 인증 정책과 에이전트 정책의 세부사항을 설정할 수 있습니다.

노드정책 마법사

정책 선택

정책 기본설정

노드그룹 설정

정책 세부설정

노드액션 설정

위험감지 설정

1

사용여부

On

노드에 에이전트를 사용할지 여부를 선택합니다. Delete를 선택한 경우에는 에이전트를 삭제합니다.

에이전트삭제시간

30

일

에이전트가 센터로 접속이 되지 않는 시간이 설정된 시간 이상이 되면 에이전트를 삭제합니다. (0: 사용안함, 1시간 - 1년)

Dissolvable Agent

Off

Dissolvable Agent 사용여부를 선택합니다.

기본 에이전트는 PC 구동할 때 항상 실행되며 시스템 정보 수집 및 제어 기능을 수행합니다.

Dissolvable Agent는 사용자가 시스템에 로그인할 때 실행되며 시스템 정보를 수집하고 수집이 완료되면 프로세스가 종료됩니다.

2

Agent FailSafe 사용

Off

에이전트가 센터로 접속이 되지 않을 경우 에이전트 동작중지

3

트레이아이콘표시

On

트레이아이콘 표시 여부를 선택합니다.

수행 계정

PC에 로그인된 계정

에이전트 실행시 기본계정을 설정합니다. 로그인 계정의 권한이 제한되어있다면 별도의 수행계정 또

이전

취소

다음

1. 사용여부
- 에이전트 사용여부 설정
2. Agent FailSafe 사용
- 에이전트가 센터로 접속이 되지 않을 경우 에이전트 동작중지
3. 트레이아이콘표시
- 트레이아이콘 표시 여부 선택
- (CWP 페이지에서 표시되는 트레이 아이콘)

3. 노드 정책 [8/11]

노드 정책 설정 방법 (단계 4 : 정책 세부 설정) - 계속

노드 정책에서 에이전트가 수행할 인증 정책과 에이전트 정책의 세부사항을 설정할 수 있습니다.

노드정책 마법사

정책 선택

정책 기본설정

노드그룹 설정

정책 세부설정

노드액션 설정

위험감지 설정

수행 계정

PC에 로그인된 계정

에이전트 실행 시 기본계정을 설정합니다. 로그인 계정의 권한이 제한되어있다면 별도의 수행계정 또는 로컬 시스템 계정으로 동작하도록 설정해야 합니다.

단, UAC가 동작중인 경우 별도의 수행계정으로 설정시 정상동작하지 않습니다.

정책변경검사주기

4

시간

설정된 주기에 따라서 에이전트 정책 변경 여부를 센터에 확인합니다. (1시간 - 4시간)

에이전트정보삭제

30

일

설정된 기간이상 업데이트되지 않는 에이전트정보 삭제함. (0:사용안함, 1시간 - 1년)

- 수행계정**
 에이전트 실행 시 기본계정 설정.
 수행계정 미설정 시 로그인 계정으로 수행
- 정책변경검사주기**
 설정된 주기에 따라서 에이전트 정책 변경 여부를 센터에서 확인
- 에이전트정보삭제**
 설정된 기간 이상 업데이트되지 않는 정보 삭제

Genians NAC (네트워크 접근제어) 운영자 매뉴얼
- 23 -

SM(주)에스엠인포메이션

3. 노드 정책 [9/11]

노드 정책 설정 방법 (단계 4 : 정책 세부 설정) - 계속

노드 정책에서 에이전트가 수행할 인증 정책과 에이전트 정책의 세부사항을 설정할 수 있습니다.



1. **사용가능**
바로 사용가능한 액션정의 목록
2. **선택**
적용될 액션정의 목록
3. →
선택한 액션정의[선택]란으로 이동
(현재 생성중인 정책에 적용될 액션정의)
4. →|
[사용가능]란의 액션정의 [선택]란으로 일괄 이동
5. <
선택한 액션정의 [사용가능] 란으로 이동
6. |<
[선택] 란의 액션정의 [사용가능] 란으로 일괄 이동
7. **+add**
액션정의 생성

3. 노드 정책 [10/11]

노드 정책 설정 방법 (단계 4 : 정책 세부 설정) - 계속

노드 정책에서 에이전트가 수행할 인증 정책과 에이전트 정책의 세부사항을 설정할 수 있습니다.



1. **사용가능**
바로 사용가능한 위험정의 목록
2. **선택**
적용될 위험정의 목록
3. **→**
선택한 위험정의[선택]란으로 이동
(현재 생성중인 정책에 적용될 위험정의)
4. **→|**
[사용가능]란의 위험정의 [선택]란으로 일괄 이동
5. **←**
선택한 위험정의 [사용가능] 란으로 이동
6. **|←**
[선택] 란의 위험정의 [사용가능] 란으로 일괄 이동
7. **+add**
위험정의 생성
8. **완료**
완료 버튼 클릭 시 정책 생성 완료

3. 노드 정책 [11/11]

노드 정책 설정 방법

생성된 시스템 정책은 정책 > 정책 > 노드정책 에서 확인 할 수 있습니다.

Genian NAC v5.0 관리 감사 **정책** 설정 시스템

에스엠인포메이션

변경정책적용 업데이트: 17:05:41 KST 09:41

정책

노드정책

라이선스 경고 : 라이선스가 유효하지 않습니다. 먼저 라이선스(시스템 > 라이선스) 등록 후 사용해주시기 바랍니다.

작업선택 1-9/9 50

정책	순서	ID	노드수	사용	노드그룹	노드액션	위험감지	설명	재정렬
노드정책	1	POC 테스트 정책		☑	123	소프트웨어정보 수집			↕
	2	예외정책	104	☑	예외노드				↕

정책 생성이 완료되면 위의 화면이 출력되며 화면 상단에 [√ 변경정책적용] 을 클릭하면 변경된 정책이 적용됩니다.

4. 제어 정책 [1/12]

제어정책 설정 방법

1. 정책선택
2. 제어정책 선택
3. 작업 선택 선택
4. 생성 클릭

생성을 클릭하면 정책 설정 화면이 출력됩니다.

Genian NAC v5.0
관리
감사
정책
설정
시스템

▼ 정책

- ▼ 노드정책
 - 노드액션
 - 위험감지
- ▼ 제어정책
 - 제어액션
- ▼ 무선랜정책
 - AP 프로파일
 - Client 프로파일

▼ 작업선택

생 성

삭 제

	노드수	사용	노드그룹	권한객체	제어액션	설명
1	123	<input checked="" type="checkbox"/>	예외노드	PERM-ALL		
2		<input checked="" type="checkbox"/>	예외허용	PERM-ALL		서버,스위치,라우터 등 네트워크 차단을 받지 말아야 하는 노드들
3	7	<input checked="" type="checkbox"/>	IP관리 차단노드	PERM-ALL		노드의 IP/MAC이 인가되지 않은 노드를 차단하는 정책
4		<input checked="" type="checkbox"/>	미인증차단	PERM-DNS		인증을 수행하지 않는 노드들을 네트워크 차단을 통해 인증수행 하
5		<input checked="" type="checkbox"/>	가동	PERM-ALL	전원제어	
6		<input checked="" type="checkbox"/>	에이전트미설치차단	PERM-DNS		신규로 네트워크 연결을 하거나 에이전트 정보가 서버에서 삭제된
7		<input checked="" type="checkbox"/>	에이전트미동작차단	PERM-DNS		에이전트가 동작되지 않는 노드들을 네트워크 차단을 통해 재설치
8		<input checked="" type="checkbox"/>	운영체제업데이트불만족차단	PERM-DNS		운영체제 업데이트 상태가 만족이 아닌 노드를 네트워크 차단을 통

4. 제어 정책 [2/12]

제어정책 설정 방법 (단계1 : 정책 선택)

제어정책 마법사

정책 선택

정책 기본설정

노드그룹 할당

권한 할당

제어옵션 설정

제어액션 설정

1

1

기존 정책을 선택하면 해당 정책에 대한 설정이 자동으로 설정됩니다.

2

기존 정책 기반으로 생성

신규생성

신규로 정책을 생성합니다.

선택한 정책의 설정을 기준으로 신규 정책을 생성합니다.

TEST


취소

→ 다음

1. 신규 생성
신규로 제어 정책을 생성할 시 선택
2. 기존 정책 기반으로 생성
기존 제어 정책을 기반으로 생성 시 선택

Genians NAC (네트워크 접근제어) 운영자 매뉴얼

- 28 -


SM Information
(주)에스엠인포메이션

4. 제어 정책 [3/12]

제어정책 설정 방법 (단계2 : 노드그룹 할당)

정책 기본 설정 작업이 모두 끝난 후 다음 클릭

제어정책 마법사

정책 선택
정책 기본설정
노드그룹 할당
권한 할당
제어옵션 설정
제어액션 설정

1 정책 관련 기본설정을 합니다.

ID

설명

순서

적용모드

사용함 ▼

← 이전

취소
→ 다음

1. ID
제어정책의 이름 설정
2. 설명
정책에 대한 설명
3. 순서
정책을 할당 할 순서 설정
4. 적용모드
정책 사용 유/무 설정

4. 제어 정책 [4/12]

제어정책 설정 방법 (단계3 : 노드그룹 할당)

제어 정책을 할당 할 노드 그룹 선택 후 다음

제어정책 마법사

정책 선택
정책 기본설정
노드그룹 할당
권한 할당
제어옵션 설정
제어액션 설정

① 제어정책을 적용할 대상 노드그룹을 할당합니다.

사용가능

(TEST)김민석

123

192.168.1.x대역

PC

Test

testt

모든노드

송활명

예외노드

이동일_TEST

장재명_TEST

차재석_TEST

→
→
←
←

선택

노드그룹을 생성하시려면 버튼을 클릭해 주세요. 정책그룹 + 상태그룹 +

← 이전

취소

→ 다음

4. 제어 정책 [5/12]

제어정책 설정 방법 (단계3 : 네트워크 권한 할당)

사용자에게 허용할 권한을 설정합니다. 원하는 권한이 없을 시 add 버튼을 눌러 권한을 생성 합니다.

- 선택없이 다음으로 넘어갈 경우 **PERM-DENY**으로 자동 설정(**네트워크 차단 및 CWP리다이렉션**)

제어정책 마법사

정책 선택

정책 기본설정

노드그룹 할당

권한 할당

제어옵션 설정

제어액션 설정

① 할당된 노드그룹에 허용할 네트워크 권한을 할당합니다.

사용가능

DENY_445
PERM-ALL
PERM-DNS
필수 백신 미사용 (TEST)

→

→

←

←

선택

권한을 생성하시려면 버튼을 클릭해주세요. +

← 이전

취소

→ 다음

Genians NAC (네트워크 접근제어) 운영자 매뉴얼

- 31 -

SM

SM Information

(주)에스엠인포메이션

4. 제어 정책 [6/12]

제어정책 설정 방법 (단계3 : 네트워크 권한 할당)

추가 버튼 클릭 시 아래의 그림과 같은 팝업 창이 출력 됩니다.

권한객체 : 신규 객체 생성

기본설정

ID

설명

조건설정

네트워크객체

+

③LOCAL

▼

예 속하지 않는

서비스객체

+

③ALL

▼

예 속하지 않는

시간객체

+

③ANYTIME

▼

예 속하지 않는

생성

1. 권한ID : 신규 네트워크 권한 ID 설정
2. 네트워크객체 : 노드가 접근하게 될 목적지 네트워크 그룹 지정
3. 서비스객체 : 목적지 네트워크에 접근했을 때 노드가 부여받는 서비스(포트)를 지정
4. 시간객체 : 노드가 해당 네트워크 권한을 적용받는 시간을 설정

4. 제어 정책 [7/12]

제어정책 설정 방법 (단계3 : 네트워크 권한 할당)

네트워크 권한 추가 방법 (계속)

네트워크정책 : 신규 객체 생성

기본설정

ID

설명

포함그룹

사용가능

①LOCAL

②MANAGED

필수 백신 미사용 (TEST)

선택

→ ← ↶ ↷

네트워크주소

IP/Netmask / 32 (255.255.255.255) 추가 CSV 가져오기

0 - 0 / 0 50 ▼

TYPE	설정
설정된 조건없음	

1 2 3 4

생성

권한정책 : 신규 객체 생성

기본설정

ID

설명

조건설정

네트워크정책 + ①LOCAL ▼ ☐에 속하지 않는

서버스캐체 + ②ALL ▼ ☐에 속하지 않는

시간정책 + ③ANYTIME ▼ ☐에 속하지 않는

생성

추가 클릭 → 포함그룹에서 기존에 생성된 네트워크 그룹 선택 → Add 클릭

기존에 생성된 네트워크 그룹을 포함시킬 수 있습니다.

(포함그룹은 필수 선택 사항은 아닙니다. 상황에 따라 유동적으로 적용할 수 있습니다.)

4. 제어 정책 [8/12]

제어정책 설정 방법 (단계3 : 네트워크 권한 할당)

네트워크 권한 추가 방법 (계속)

네트워크정책 : 신규 객체 생성

기본설정

ID

설명

포함그룹

사용가능

@LOCAL

@MANAGED

필수 백신 미사용 (TEST)

→

←

↔

↔

선택

네트워크주소

IP/Netmask / 32 (255.255.255.255)

0 - 0 / 0 50 ▼

TYPE	설정
설정된 조건없음	

1개 2개 3개 4개

IP 해당 노드나 넷 마스크 설정을 통한 그룹지정 방법

1. IP 설정
2. Netmask 설정
3. 설정한 IP/Netmask를 추가
4. 생성 버튼을 클릭하여 그룹을 생성합니다.

4. 제어 정책 [9/12]

제어정책 설정 방법 (단계3 : 네트워크 권한 할당)

네트워크 권한 추가 방법 (계속)

기본설정

ID

설명

조건설정

네트워크객체

+

③LOCAL

▼

에 속하지 않는

☐

서비스객체

+

③LOCAL

③MANAGED

③NET-ALL

필수 백신 미사용 (TEST)

에 속하지 않는

☐

시간객체

+

에 속하지 않는

☐

생성

네트워크 그룹 설정을 완료하면 상단 그림과 같이 생성한 네트워크 그룹을 확인할 수 있습니다.

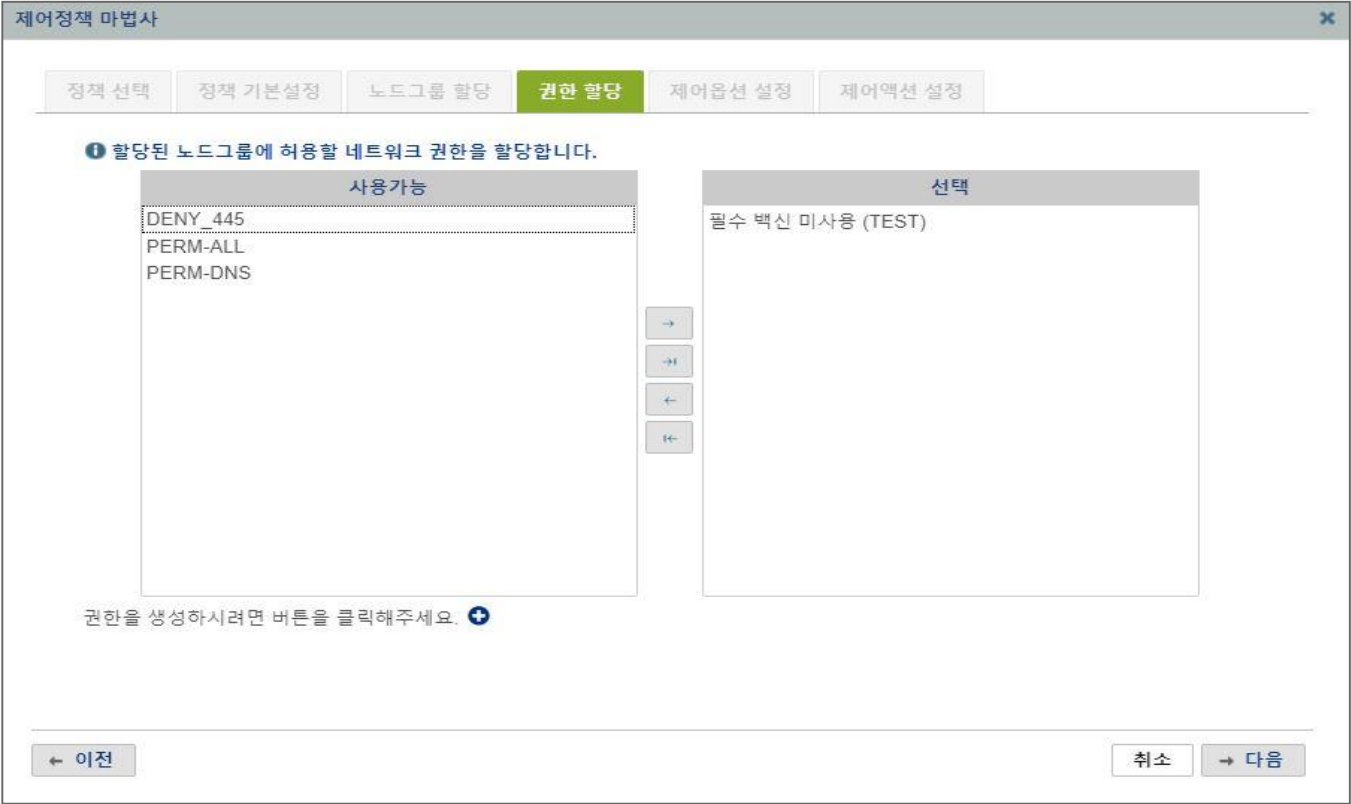
그룹 설정이 완료되면 생성 버튼을 클릭하여 네트워크 권한을 생성할 수 있습니다.

서비스그룹과 시간그룹도 **네트워크그룹과 같은 방법으로 추가**가 가능합니다.

4. 제어 정책 [10/12]

제어정책 설정 방법 (단계3 : 네트워크 권한 할당)

네트워크 권한 추가 방법 (계속)



신규 네트워크 권한 생성이 완료되면 좌측 그림과 같이 권한이 생성된 것을 확인할 수 있습니다.
 추가할 권한을 선택 → 클릭 → 할당 클릭을 통해 위 그림처럼 네트워크 권한 할당을 후 다음 클릭 합니다.

4. 제어 정책 [11/12]

제어정책 설정 방법 (단계4 : 제어옵션 설정)

제어정책 마법사

정책 선택
정책 기본설정
노드그룹 할당
권한 할당
제어옵션 설정
제어액션 설정

제어정책 관련 제어옵션을 설정합니다.

Captive Web Portal

CWP 페이지

표준 CWP 페이지
자단된 웹 접속에 대해서 리다이렉션 시키는 대상 페이지를 선택합니다.

사용자 메시지

ko en zh ja

19999자 입력 가능합니다.
제어정책 적용시 사용자에게 표시할 메시지를 설정합니다. (HTML사용)

스위치포트 차단

포트차단 수행

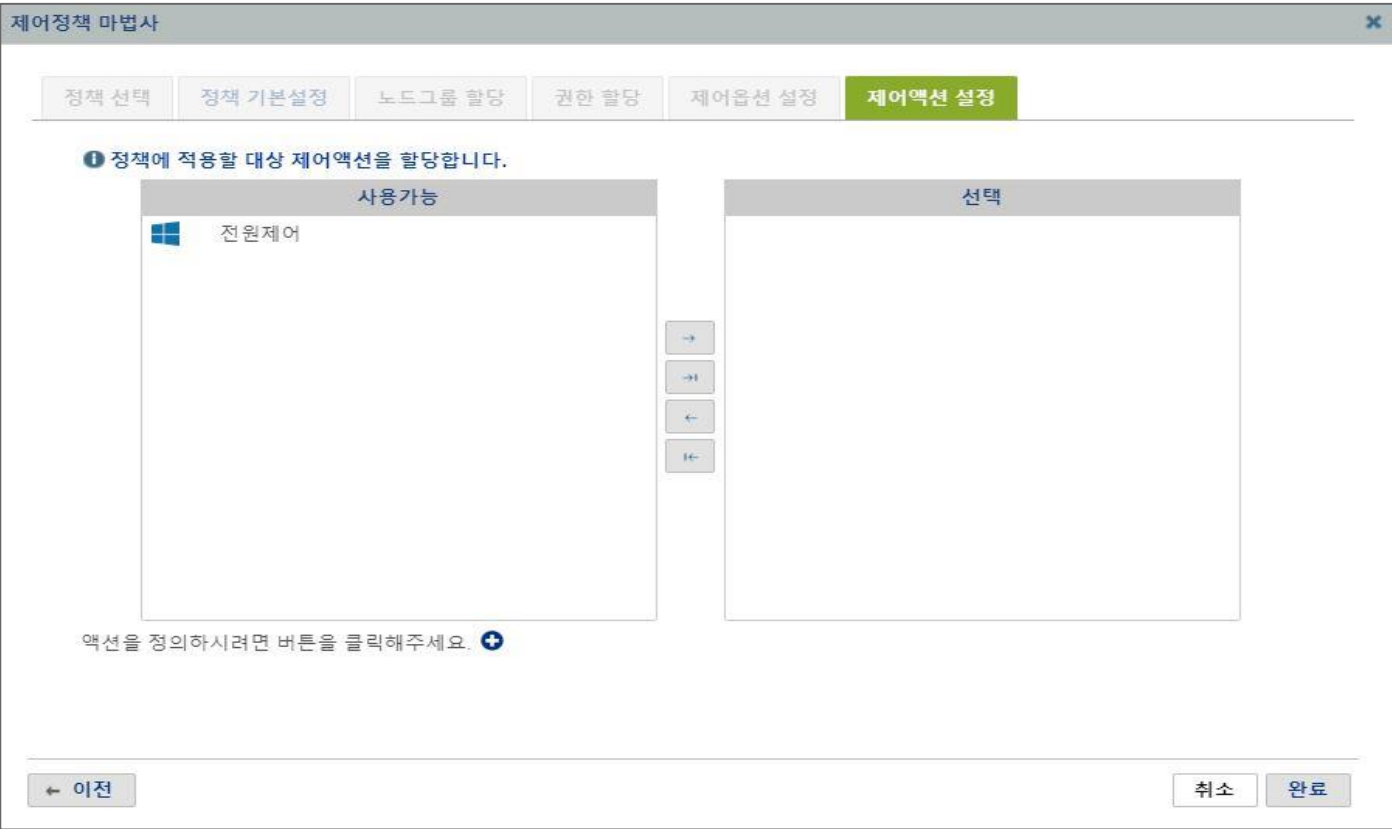
Off
노드가 연결된 스위치포트를 SNMP를 통하여 차단할지 여부를 선택합니다.

이전
취소
다음

1. CWP 페이지 : 메시지의 CWP 출력여부를 선택
2. 사용자 메시지 : 제어정책 적용 시 사용자에게 표시할 메시지를 설정

4. 제어 정책 [12/12]

제어정책 설정 방법 (단계5 : 제어액션 설정)



설정이 모두 완료되면 확인 버튼을 클릭하여 네트워크 정책 설정을 완료할 수 있습니다.
 생성 후 우측 상단에 있는 변경정책 적용을 클릭하여 생성을 완료합니다

5. 정책 수정

정책 수정 방법

정책 ID를 클릭하여 수정가능

- 순서, 적용모드
- 할당 그룹, 할당 권한
- 제어 옵션 (CWP에서 출력되는 메시지)
- 정책에 노드 그룹 추가 및 삭제



Genian NAC v3.0.0 관리 감사 정책 설정 시스템

(주)오일엔 NAC

정책

노드 정책

노드 액션

위험 감지

RADIUS 정책

제어 정책

제어 액션

무선랜 정책

AP 프로파일

Client 프로파일

Windows 업데이트 정책

장치 제어 정책

장치 그룹

협동라이선스 정책

그룹

노드

1. 식별

2. 분류

3. 규제 준수

카테고리 미지정

무선랜

사용자

각제

권한

네트워크

서비스

시간

정책 목록

ID	순서	노드수	사용	노드그룹
1	임시예외허용	3	<input checked="" type="checkbox"/>	임시예외 노드그룹
2	예외허용	133	<input checked="" type="checkbox"/>	예외노드
3	IP관리 차단		<input checked="" type="checkbox"/>	IP관리 차단노드
4	모바일 차단		<input checked="" type="checkbox"/>	모바일장치
5	에이전트미설치차단		<input checked="" type="checkbox"/>	에이전트미설치노드
6	(필수S/W) 미설치 차단		<input checked="" type="checkbox"/>	(필수S/W) EPP 미설치 노드 (필수S/W) 문서중요파일 미설치
7	기본정책	396	<input checked="" type="checkbox"/>	모든노드

정책 설정

제어정책

작업선택

센서 운영모드 전환

자단 활성 센서 (Enforcement) ☒ 자단 비활성 센서 ☐



제어정책 : 예외허용

라이선스 경고 : 라이선스가 유효하지 않습니다. 먼저 라이선스(시스템 > 라이선스) 등록 후 사용해주시기 바랍니다.

기본설정

ID: 예외허용

설명: 서비스위치 라우터 등 네트워크 자단을 방지 할아야 하는 노드들에 대한 예외처리 정책

순서: 2

적용모드: 사용함

경신시각: 2022-10-24 17:37:12

노드그룹 할당

노드그룹	연산	설정	설명	삭제
예외노드	OR	노드타입 / 감지된 노드타입이 같으면 / VOIP 노드타입 / 감지된 노드타입이 같으면 / 네트워크장비 노드타입 / 감지된 노드타입이 같으면 / 라우터 노드타입 / 감지된 노드타입이 같으면 / 무선접속장치 노드타입 / 감지된 노드타입이 같으면 / 보안장치	정책에서 예외되어야 하는 노드들의 그룹	삭제

See More

관련 설정 할당

관련정책	네트워크정책	서비스정책	시간정책	설명	삭제
PERM-ALL	@NET-ALL	@ALL	@ANYTIME	모든 네트워크, 모든 서비스 허용	삭제

제어 옵션

Captive Web Portal

CWP 페이지: 표준 CWP 페이지

자단된 웹 접속에 대해서 리다이렉션 시키는 대상 페이지를 선택합니다.

사용자 메시지: ko en zh ja

1. 백업 설정 방법

백업 관리 방법

아래 사진이 기본설정

- 오전 4시 백업 자동 수행
- 정책서버 디스크 여유공간이 30% 이하일때 오래된 백업파일 자동 삭제



백업파일 자동 삭제 여유공간 기준 %단위로 수정가능 (최소 10%)

[지금시작] 버튼으로 즉시 수행가능

저장경로 변경가능

[백업목록]에서 현재까지 수행된 백업파일 리스트 확인가능 및 팝업창에서 파일 클릭하여 **현재 사용PC에 다운로드 가능**

2. 백업 파일 내용

ALDER-107423-20220926-040000.tar.gz - 반디집 (스탠더드)

파일(F) 편집(E) 찾기(I) 설정(S) 보기(V) 도구(T) 도움말(A)

열기

풀기

새로 압축

파일 추가

파일 삭제

테스트

스캔

칼럼 설정

코드페이지

이름	압축 크기	원본 크기	파일 종류	수정한 날짜
ALDER-107423-20220926-040000				
agent				2022-09-26 오전 4:00:...
conf				2022-09-26 오전 4:00:...
custom				2022-09-26 오전 4:00:...
design				2022-09-26 오전 4:00:...
devicon				2022-09-26 오전 4:00:...
plugins				2022-09-26 오전 4:00:...
ALDER_DATA-20220926-040000.sql	384,619,975		SQL-Script	2022-09-26 오전 4:03:...

- 파일리스트
- 장비 Config 내용
 - 관리자 웹페이지 설정 값
(정책, 액션, 그룹 포함)
 - 에이전트 파일
(플러그인 포함)
 - 웹페이지 DB 값

1. 대역별 운영모드 변경

[시스템] - [센서관리]에서 변경대상 대역센서 [센서설정] 클릭하여 설정페이지 접속

Genian NAC v5.0

관리

감사

정책

설정

시스템

(주)오알렘 NAC

업데이트 : 17:48:48 KST 09:48

시스템 관리

시스템

센서 관리

시스템 초기설정

세션 관리

라이선스

업데이트 관리

소프트웨어

에이전트 플러그인

정책서버 플러그인

운영정보 데이터

서비스 관리

서비스 제어

접속 포트

시스템 목록

라이선스 경고 : 라이선스가 유효하지 않습니다. 먼저 라이선스(시스템 > 라이선스) 등록 후 사용해주시기 바랍니다.

작업선택

노드유형

장비 태그

운영모드

백문검색

검색

1 - 6 / 6 50

	NT	관리노드	KA	FS	IP주소 ↓	MAC주소	인터페이스명	센서명	설명	장비명	플랫폼	동작모드	운영모드	센서설정
<input type="checkbox"/>		17 / 19			79.14.179.57	68:ED:A4:4D:25:0E	eth0	S.구미공장_유...		S-79.14.179.57	S10_R2	Host	Enforcement	센서설정
<input type="checkbox"/>		9 / 19			79.14.100.57	68:ED:A4:4D:25:0E	eth0.2			S-79.14.100.57	S10_R2	Host	Monitoring	센서설정
<input type="checkbox"/>		0 / 0			19.14.190.57	68:ED:A4:47:C8:B1	eth0.4			S-19.14.190.57	S20H_R1	Host	Monitoring	센서설정
<input type="checkbox"/>		124 / 142			19.14.179.57	68:ED:A4:47:C8:B1	eth0	S.본사_유선(19....		S-19.14.179.57	S20H_R1	Host	Enforcement	센서설정
<input type="checkbox"/>		10 / 30			19.14.110.57	68:ED:A4:47:C8:B1	eth0.3			S-19.14.110.57	S20H_R1	Host	Monitoring	센서설정
<input type="checkbox"/>		166 / 322			19.14.100.57	68:ED:A4:47:C8:B1	eth0.2			S-19.14.100.57	S20H_R1	Host	Enforcement	센서설정

1. 대역별 운영모드 변경

- 상단에서 변경대상 대역이 맞는지 확인
- [센서 운영모드]에서 모드 변경 (Monitoring-모니터링, Enforcement-차단모드)
 - 차단모드 선택 후 하단에 출력되는 옵션값은 변경 필요없음
- 페이지 최하단에서 [수정] 버튼 클릭

Genian NAC v5.0 관리 감사 정책 설정 시스템

(주)오알렘 NAC

시스템 관리

시스템 : 19.14.179.57

라이선스 경고 : 라이선스가 유효하지 않습니다. 먼저 라이선스(시스템 > 라이선스) 등록 후 사용해주시기 바랍니다.

기본정보 시스템정보 **센서설정** 환경설정 제어

최근갱신시각 : 2022-09-28 10:53:59

인터페이스 추가

인터페이스	IP	MAC	센서 이름	서브넷마스크	게이트웨이	동작모드	운영모드	가상IP	가상IP(자동)	설정
eth0	19.14.179.57/255.255.255.0	68:ED:A4:47:C8:B1	S.본사_유선(19.14.179.0/24)	255.255.255.0	19.14.179.254	Host (자단방법 : HTTP Redirection + Drop)	Enforcement (Active 동작시간 : @ANYTIME)	ON	ON	센서설정 / IP설정
eth0.2	19.14.100.57/255.255.255.0	68:ED:A4:47:C8:B1		255.255.255.0	19.14.100.254	Host (자단방법 : HTTP Redirection + Drop)	Enforcement (Active 동작시간 : @ANYTIME)	ON	ON	센서설정 / IP설정
eth0.3	19.14.110.57/255.255.255.0	68:ED:A4:47:C8:B1		255.255.255.0	19.14.110.254	Host	Monitoring	ON	ON	센서설정 / IP설정
eth0.4	19.14.190.57/255.255.255.0	68:ED:A4:47:C8:B1		255.255.255.0	19.14.190.254	Host	Monitoring	ON	ON	센서설정 / IP설정
eth1		68:ED:A4:47:C8:B2				Inactive	Monitoring	ON	ON	센서설정 / IP설정
eth2		68:ED:A4:47:C8:B3				Inactive	Monitoring	ON	ON	센서설정 / IP설정
eth3		68:ED:A4:47:C8:B4				Inactive	Monitoring	ON	ON	센서설정 / IP설정

센서설정 - 인터페이스 : eth0.4

센서동작

센서 동작모드: Host
센서의 동작모드를 선택합니다.

스캔 및 Health 체크: On
스캔 및 Health 체크를 수행합니다.
Off - 스캔 및 health 체크를 위한 패킷이 노드로 전송되지 않습니다. (노드정보 검사, 네트워크 스캔, 노드상태 검사, 서버넷 노드스캔 이 동작하지 않습니다.)

센서 운영모드: Monitoring
센서의 운영모드를 선택합니다.

비관리IP 제어: Off
비관리대역 IP 감지시 Poisoning여부를 선택합니다.
운영모드가 Enforcement인 Host 센서에서 동작합니다.

트래픽 모니터링 (Local Mirror 모드에서만 적용됨)

수집주기: 0 초
트래픽 수집을 수행할 주기를 설정합니다. (0: 사용안함, 10초 - 1월)

1. 대역별 운영모드 변경

- [관리] - [노드]페이지 왼쪽 사이드메뉴에서 [센서IP] 좌측 아이콘이 푸른색에서 붉은색으로 변경되거나
- [시스템] - [센서관리] 페이지에서 [운영모드] 컬럼이 Enforcement로 변경됨으로 정상 적용 확인가능

※주의

최초 차단모드로 변경전 제어정책 적용대상 존재 확인필요(예외허용, 기본적책 제외)



	NT	관리노드	KA	FS	IP주소 ↓	MAC주소	인터페이스명	센서명	설명	장비명	플랫폼	동작모드	운영모드	센서설정
<input type="checkbox"/>		17 / 19			79.14.179.57	68 ED A4 4D 25 0E	eth0	S.구미공장_유...	S-79.14.179.57	S10_R2	Host	Enforcement	센서설정	
<input type="checkbox"/>		9 / 19			79.14.100.57	68 ED A4 4D 25 0E	eth0.2		S-79.14.100.57	S10_R2	Host	Monitoring	센서설정	
<input type="checkbox"/>		0 / 0			19.14.190.57	68 ED A4 47 C8 B1	eth0.4		S-19.14.190.57	S20H_R1	Host	Monitoring	센서설정	
<input type="checkbox"/>		124 / 142			19.14.179.57	68 ED A4 47 C8 B1	eth0	S.본사_유선(19...	S-19.14.179.57	S20H_R1	Host	Enforcement	센서설정	
<input type="checkbox"/>		10 / 30			19.14.110.57	68 ED A4 47 C8 B1	eth0.3		S-19.14.110.57	S20H_R1	Host	Monitoring	센서설정	
<input type="checkbox"/>		166 / 322			19.14.100.57	68 ED A4 47 C8 B1	eth0.2		S-19.14.100.57	S20H_R1	Host	Enforcement	센서설정	

2. 일괄(다중선택) 운영모드 변경

[시스템] - [센서관리]에서 변경 대상 대역센서 [체크박스] 다중 선택
[작업선택] - [센서 운영모드 일괄 설정] 클릭하여 운영모드 일괄 설정 페이지 접속

Genian NAC v5.0

관리감사정책설정시스템

51

Search

(주)오알렘 NAC

업데이트 : 17:53:30 KST 09:47

시스템 관리

시스템 목록

시스템

센서 관리

시스템 초기설정

센서 관리

라이선스

업데이트 관리

소프트웨어

에이전트 플러그인

정책서버 플러그인

운영정보 데이터

서비스 관리

서비스 제어

접속 포트

라이선스 경고 : 라이선스가 유효하지 않습니다. 먼저 라이선스(시스템 > 라이선스) 등록 후 사용해주시기 바랍니다.

작업선택

노드유형

장비 태그

운영모드

빠른검색

검색

1 - 6 / 650

	MAC주소	인터페이스명	센서명	설명	장비명	플랫폼	동작모드	운영모드	센서설정
<input checked="" type="checkbox"/>	179.57	68:ED:A4:4D:25:0E	eth0	S.구미공장_유...	S-79.14.179.57	S10_R2	Host	Enforcement	센서설정
<input checked="" type="checkbox"/>	100.57	68:ED:A4:4D:25:0E	eth0.2		S-79.14.100.57	S10_R2	Host	Monitoring	센서설정
<input checked="" type="checkbox"/>	190.57	68:ED:A4:47:C8:B1	eth0.4		S-19.14.190.57	S20H_R1	Host	Monitoring	센서설정
<input checked="" type="checkbox"/>	179.57	68:ED:A4:47:C8:B1	eth0	S.본사_유선(19...	S-19.14.179.57	S20H_R1	Host	Enforcement	센서설정
<input checked="" type="checkbox"/>	110.57	68:ED:A4:47:C8:B1	eth0.3		S-19.14.110.57	S20H_R1	Host	Monitoring	센서설정
<input checked="" type="checkbox"/>	100.57	68:ED:A4:47:C8:B1	eth0.2		S-19.14.100.57	S20H_R1	Host	Enforcement	센서설정

2. 일괄(다중선택) 운영모드 변경

- **[Enforcement]** 체크박스 클릭 후 **[실행]** 버튼 클릭 (Monitoring-모니터링, Enforcement-차단모드)
 - 차단모드 선택 후 하단에 출력되는 옵션값은 변경 필요없음

The screenshot displays the Genian NAC v5.0 web interface. The top navigation bar includes '관리' (Management), '감사' (Audit), '정책' (Policy), '설정' (Settings), and '시스템' (System). The left sidebar shows a tree view with '시스템 관리' (System Management) expanded, containing '시스템 관리', '센서 관리' (Sensor Management), '시스템 초기설정' (System Initial Setup), '센서 관리' (Sensor Management), and '라이선스' (License). The main content area is titled '일괄작업' (Batch Operation) and shows a message: '6개 센서가 선택되었습니다.' (6 sensors selected). Below this, the '센서 운영모드 일괄 설정' (Sensor Operation Mode Batch Setting) section is visible, showing two radio buttons: 'Monitoring' and 'Enforcement'. The 'Enforcement' option is selected and highlighted with a red box. At the bottom right, there are two buttons: '실행' (Execute) and '취소' (Cancel), with '실행' also highlighted by a red box.

2. 일괄(다중선택) 운영모드 변경

- [관리] - [노드]페이지 왼쪽 사이드메뉴에서 [센서IP] 좌측 아이콘이 푸른색에서 붉은색으로 변경되거나
- [시스템] - [센서관리] 페이지에서 [운영모드] 컬럼이 Enforcement로 변경됨으로 정상 적용 확인가능

※주의

최초 차단모드로 변경전 제어정책 적용대상 존재 확인필요(예외허용, 기본적책 제외)



	NT	관리노드	KA	FS	IP주소 ↓	MAC주소	인터페이스명	센서명	설명	장비명	플랫폼	동작모드	운영모드	센서설정
<input type="checkbox"/>		17 / 19			79.14.179.57	68 ED A4 4D 25 0E	eth0	S.구미공장_유...	S-79.14.179.57	S10_R2	Host	Enforcement	센서설정	
<input type="checkbox"/>		9 / 19			79.14.100.57	68 ED A4 4D 25 0E	eth0.2		S-79.14.100.57	S10_R2	Host	Monitoring	센서설정	
<input type="checkbox"/>		0 / 0			19.14.190.57	68 ED A4 47 C8 B1	eth0.4		S-19.14.190.57	S20H_R1	Host	Monitoring	센서설정	
<input type="checkbox"/>		124 / 142			19.14.179.57	68 ED A4 47 C8 B1	eth0	S.본사_유선(19...	S-19.14.179.57	S20H_R1	Host	Enforcement	센서설정	
<input type="checkbox"/>		10 / 30			19.14.110.57	68 ED A4 47 C8 B1	eth0.3		S-19.14.110.57	S20H_R1	Host	Monitoring	센서설정	
<input type="checkbox"/>		166 / 322			19.14.100.57	68 ED A4 47 C8 B1	eth0.2		S-19.14.100.57	S20H_R1	Host	Enforcement	센서설정	



Thank You

