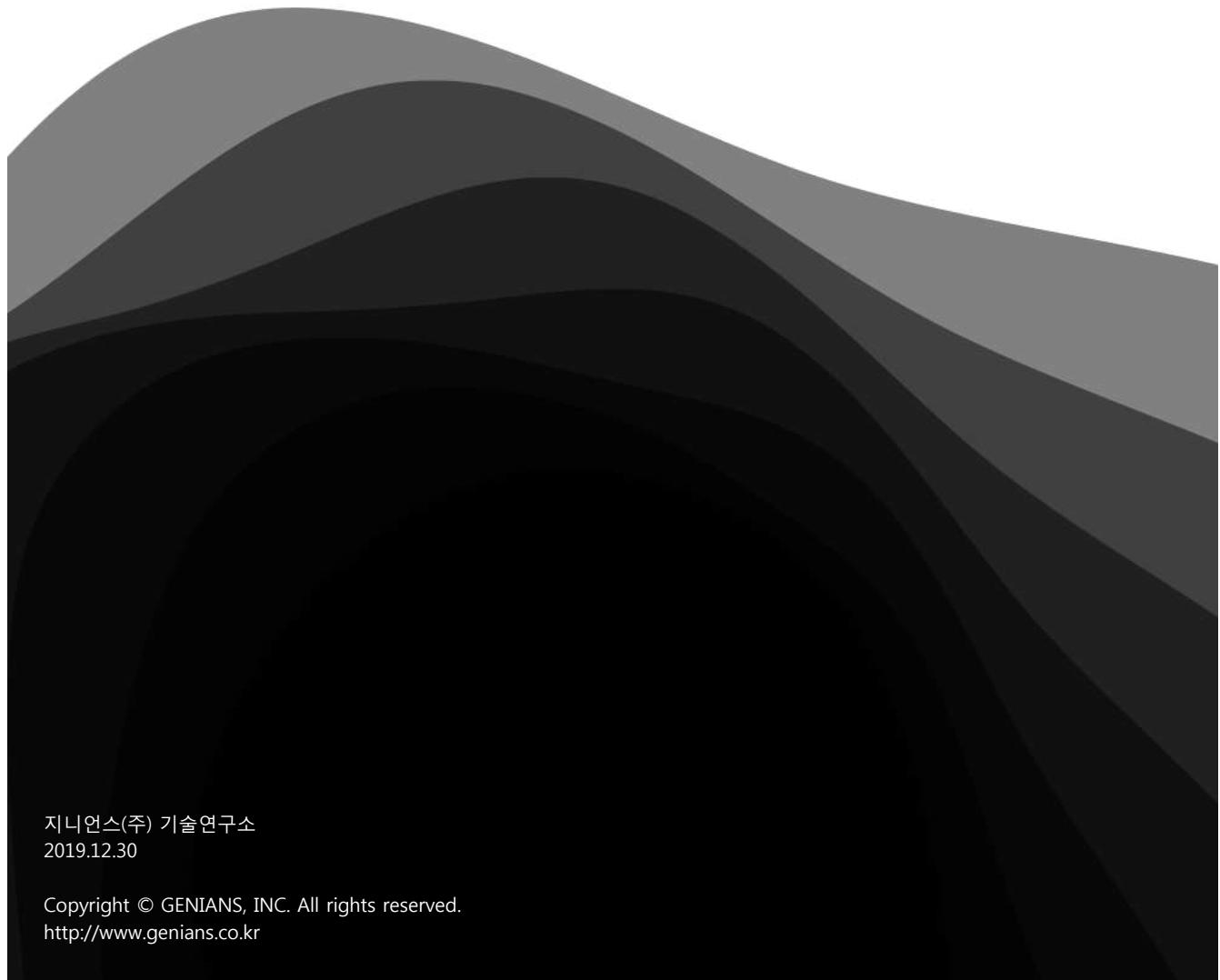


Genian NAC

관리자매뉴얼 V1.19



지니언스(주) 기술연구소
2019.12.30

Copyright © GENIANS, INC. All rights reserved.
<http://www.genians.co.kr>

1. 관리자 매뉴얼	6
1.1 배경지식	13
1.2 기본항목	14
1.2.1 제품구성환경	15
1.2.2 제품 콘솔 접속	16
1.2.3 유의사항	19
1.2.4 운영환경	20
1.2.5 에러 메시지	20
1.2.6 UI 기본 관리기능	21
1.2.6.1 관리뷰 편집	22
1.2.6.2 내보내기&가져오기	24
1.2.6.3 다국어 메시지 입력	25
1.2.6.4 변경정책적용 버튼	27
1.2.6.5 빠른실행 명령 편집	28
1.2.6.6 생성, 추가, 등록 시 기본정보 설정	30
1.2.6.7 설정 값 수정	31
1.2.6.8 전체항목 선택	32
1.2.6.9 정렬 기능	33
1.2.6.10 정책복사	34
1.2.6.11 정책 사용, 사용안함	35
1.2.6.12 정책의 순서 변경	36
1.2.6.13 펼침 닫힘	38
1.2.6.14 항목 삭제	39
1.2.6.15 항목의 생성, 추가	40
1.2.6.16 노드바구니에 담기	41
1.2.7 보안대책	43
1.3 관리	44
1.3.1 노드	45
1.3.1.1 IP관리	60
1.3.1.1.1 IP차단	61
1.3.1.1.2 IP허용 - 충돌보호해제	62
1.3.1.1.3 IP허용 - 충돌보호(지정MAC)	63
1.3.1.1.4 MAC차단	64
1.3.1.1.5 MAC허용 - 변경금지해제	65
1.3.1.1.6 MAC허용 - 변경금지(지정 IP대역)	66
1.3.1.1.7 MAC허용 - 변경금지(모든 IP대역)	68
1.3.1.1.8 IP 및 MAC 차단	70
1.3.1.1.9 IP 및 MAC 허용	71
1.3.1.1.10 IP 충돌보호 및 변경금지 설정	72
1.3.1.1.11 IP사용 신규노드정책 설정	73
1.3.1.1.12 IP사용 현재사용자인증제한 설정	75
1.3.1.1.13 IP사용 현재사용자인증제한 해제	77
1.3.1.1.14 IP사용 호스트명제한 설정	78
1.3.1.1.15 IP사용 호스트명제한 해제	80
1.3.1.1.16 IP 사용시간 제한&해제 설정	81
1.3.1.1.17 MAC 사용시간 제한&해제 설정	83
1.3.1.1.18 MAC 태그 설정	85
1.3.1.1.19 IP 소유자&소유부서 설정	87
1.3.1.1.20 IP용도설정	89
1.3.1.2 노드 장비 관리	91
1.3.1.2.1 노드등록	92
1.3.1.2.2 노드일괄등록	94
1.3.1.2.3 노드삭제	98
1.3.1.2.4 노드 태그 설정	101
1.3.1.2.5 사용자인증해제	103

1.3.1.2.6 사용자 재인증 설정&해제	105
1.3.1.2.7 노드위험해제	107
1.3.1.2.8 관리센서변경	108
1.3.1.2.9 노드속성 가져오기	110
1.3.1.2.10 장비속성 가져오기	113
1.3.1.2.11 장비 소유자설정	115
1.3.1.2.12 장비 소유부서설정	116
1.3.1.3 일괄작업	117
1.3.1.3.1 노드그룹 지정&해제	118
1.3.1.3.2 노드속성변경	121
1.3.1.3.3 노드관리설정	123
1.3.1.3.4 노드대상 작업지시	124
1.3.1.3.5 에이전트액션 수행	126
1.3.1.3.6 인스턴트메시지 전송	127
1.3.1.3.7 이메일 전송	129
1.3.1.3.8 센서대상 작업지시	130
1.3.1.3.9 센서환경설정	131
1.3.1.3.10 무결성 검증	133
1.3.1.4 노드 - 노드 상세 정보	135
1.3.1.4.1 노드 상세 - 기본정보	136
1.3.1.4.2 노드 상세 - 장비정보	139
1.3.1.4.3 노드 상세 - 시스템정보	140
1.3.1.4.4 노드 상세 - 네트워크정보	141
1.3.1.4.5 노드 상세 - 소프트웨어정보	142
1.3.1.4.6 노드 상세 - 패치정보	143
1.3.1.4.7 노드 상세 - 이력관리	144
1.3.1.4.8 노드 상세 - IP 관리	145
1.3.1.4.9 노드 상세 - 정책	147
1.3.1.4.10 노드 상세 - 정책현황	148
1.3.2 IP주소	149
1.3.2.1 IP주소 - IP Matrix View	153
1.3.2.1.1 IP Matrix View - 작업선택	156
1.3.3 스위치	157
1.3.3.1 네트워크 - 스위치 상세 정보	161
1.3.3.2 네트워크 - 포트 상세 정보	162
1.3.4 무선랜	164
1.3.4.1 무선랜 - 무선랜 상세 정보	171
1.3.4.1.1 무선랜 상세 - 기본정보	172
1.3.4.1.2 무선랜 상세 - 위치정보	173
1.3.4.1.3 무선랜 상세 - 접속정보	174
1.3.4.1.4 무선랜 상세 - 이력관리	175
1.3.5 사용자	176
1.3.5.1 사용자 - 작업선택	184
1.3.5.1.1 사용자 등록&삭제	185
1.3.5.1.2 사용자 태그 설정	191
1.3.5.1.3 사용자그룹 지정&해제	192
1.3.5.1.4 사용자용도 설정	193
1.3.5.1.5 인증제한 설정	194
1.3.5.1.6 정상 상태로 변경	195
1.3.5.1.7 사용중지 상태로 변경	196
1.3.5.1.8 비밀번호변경 강제화 설정	197
1.3.5.1.9 비밀번호변경 강제화 설정(임시비밀번호 발급)	198
1.3.5.1.10 사용자만료시각 변경	200
1.3.6 신청	202
1.3.6.1 사용자신청서	204
1.3.6.2 IP 사용신청서	208

1.3.6.3 장치사용신청서	216
1.3.6.4 에이전트 인증코드	219
1.4 정책	221
1.4.1 정책	222
1.4.1.1 노드정책	224
1.4.1.1.1 노드액션	232
1.4.1.1.2 위험감지	235
1.4.1.2 제어정책	238
1.4.1.2.1 제어액션	244
1.4.1.3 무선랜정책	247
1.4.1.3.1 AP프로파일	249
1.4.1.3.2 Client 프로파일	251
1.4.1.4 Windows 업데이트 정책	253
1.4.1.5 장치제어 정책	257
1.4.1.5.1 장치그룹	261
1.4.1.5.2 장치설정	264
1.4.2 그룹	266
1.4.2.1 노드	268
1.4.2.2 무선랜	272
1.4.2.3 사용자	276
1.4.3 객체	279
1.4.3.1 권한	281
1.4.3.2 네트워크	283
1.4.3.3 서비스	285
1.4.3.4 시간	287
1.5 설정	289
1.5.1 속성관리	290
1.5.1.1 노드타입 관리	292
1.5.1.2 태그 관리	294
1.5.1.3 추가필드관리	296
1.5.1.4 용도관리	302
1.5.1.4.1 사용자용도	303
1.5.1.4.2 IP용도	307
1.5.1.4.3 용도별 정의 수정	323
1.5.2 접속인증페이지(CWP)	325
1.5.2.1 디자인 템플릿	327
1.5.2.2 공지사항	332
1.5.2.3 메시지관리	335
1.5.2.4 동의페이지	337
1.5.2.4.1 사용자정보	338
1.5.2.4.2 보안서약	341
1.5.2.5 사용자정의 버튼	343
1.5.2.6 CWP설정	345
1.5.3 서비스	351
1.5.3.1 RADIUS 서버	352
1.5.4 사용자인증	356
1.5.4.1 사용자관리	358
1.5.4.2 사용자인증	362
1.5.4.3 인증연동	364
1.5.4.4 정보 동기화	368
1.5.4.5 관리역할	378
1.5.5 환경 설정	379
1.5.5.1 노드관리	383
1.5.5.1.1 포트스캔	386
1.5.5.2 IP 관리	388
1.5.5.2.1 IP신청시스템공지사항	394

1.5.5.3 무선랜관리	396
1.5.5.4 감사기록	397
1.5.5.5 관리콘솔	398
1.5.5.5.1 SSL 인증서	410
1.5.5.6 백업	412
1.5.5.7 에이전트	414
1.5.5.7.1 운영체제 업데이트	416
1.5.5.8 기타설정	418
1.6 시스템	421
1.6.1 시스템	422
1.6.1.1 시스템관리	424
1.6.1.2 센서관리	444
1.6.1.3 시스템초기 설정	448
1.6.1.3.1 환경설정	449
1.6.1.3.2 센서설정	449
1.6.1.3.3 무선센서 환경설정	449
1.6.1.4 세션 관리	449
1.6.1.5 라이센스	450
1.6.2 업데이트 관리	452
1.6.2.1 소프트웨어	453
1.6.2.1.1 플러그인	454
1.6.2.2 운영정보 데이터	487
1.6.3 서비스 관리	488
1.6.3.1 서비스 제어	489
1.6.3.2 접속포트	490
1.7 감사	491
1.7.1 로그	492
1.7.2 리포트	507
1.7.2.1 쿼리 리포트	509
1.7.2.2 노드 리포트	512
1.7.2.3 로그 리포트	516
1.7.2.4 대시보드 리포트	519
1.7.2.5 자동 리포트	522
1.8 CLI	525
1.8.1 시스템 명령	526
1.8.2 장비 환경설정	543
1.9 대시보드	544
1.9.1 위젯	545

관리자 매뉴얼

본 문서는 관리자가 Genian NAC를 보다 효율적으로 사용하기 위해서 제품에서 사용하는 기능을 설명해 놓았습니다.

배경지식

기본항목

- 제품구성환경
- 제품 콘솔 접속
- 유의사항
- 운영환경
- 에러 메시지
- UI 기본 관리기능
 - 관리뷰 편집
 - 내보내기&가져오기
 - 다국어 메시지 입력
 - 변경정책적용 버튼
 - 빠른실행 명령 편집
 - 생성, 추가, 등록 시 기본정보 설정
 - 설정 값 수정
 - 전체항목 선택
 - 정렬 기능
 - 정책복사
 - 정책 사용, 사용안함
 - 정책의 순서 변경
 - 펼침 닫힘
 - 항목 삭제
 - 항목의 생성, 추가

관 리

- 노 드
 - IP관리
 - IP차단

- IP허용 - 충돌보호해제
 - IP허용 - 충돌보호(지정MAC)
 - MAC차단
 - MAC허용 - 변경금지해제
 - MAC허용 - 변경금지(지정 IP대역)
 - MAC허용 - 변경금지(모든 IP대역)
 - IP 및 MAC 차단
 - IP 및 MAC 허용
 - IP 충돌보호 및 변경금지 설정
 - IP사용 신규노드정책 설정
 - IP사용 현재사용자인증제한 설정
 - IP사용 현재사용자인증제한 해제
 - IP사용 호스트명제한 설정
 - IP사용 호스트명제한 해제
 - IP 사용시간 제한&해제 설정
 - MAC 사용시간 제한&해제 설정
 - MAC 태그 설정
 - IP 소유자&소유부서 설정
 - IP용도설정
- 노드 장비 관리
 - 노드등록
 - 노드일괄등록
 - 노드삭제
 - 노드 태그 설정
 - 사용자인증해제
 - 사용자 재인증 설정&해제
 - 노드위험해제
 - 관리센서변경
 - 노드속성 가져오기
 - 장비속성 가져오기
 - 장비 소유자설정

- 장비 소유부서설정
- 노드바구니에 담기
- 일괄작업
 - 노드그룹 지정&해제
 - 노드속성변경
 - 노드관리설정
 - 노드대상 작업지시
 - 에이전트액션 수행
 - 인스턴트메시지 전송
 - 이메일 전송
 - 센서대상 작업지시
 - 센서환경설정
- 노드 - 노드 상세 정보
 - 노드 상세 - 기본정보
 - 노드 상세 - 장비정보
 - 노드 상세 - 시스템정보
 - 노드 상세 - 네트워크정보
 - 노드 상세 - 소프트웨어정보
 - 노드 상세 - 패치정보
 - 노드 상세 - 이력관리
 - 노드 상세 - IP 관리
 - 노드 상세 - 정책
 - 노드 상세 - 정책현황
- IP주소
 - IP주소 - IP Matrix View
 - IP Matrix View - 작업선택
- 스위치
 - 네트워크 - 스위치 상세 정보
 - 네트워크 - 포트 상세 정보
- 무선랜
 - 무선랜 - 무선랜 상세 정보

- 무선랜 상세 - 기본정보
- 무선랜 상세 - 위치정보
- 무선랜 상세 - 접속정보
- 무선랜 상세 - 이력관리
- 사용자
 - 사용자 - 작업선택
 - 사용자 등록&삭제
 - 사용자 태그 설정
 - 사용자그룹 지정&해제
 - 사용자용도 설정
 - 인증제한 설정
 - 정상 상태로 변경
 - 사용중지 상태로 변경
 - 비밀번호변경 강제화 설정
 - 비밀번호변경 강제화 설정(임시비밀번호 발급)

신청

- 사용자신청서
- IP 사용신청서
- 장치사용신청서
- 에이전트 인증코드

CLI

- 시스템 명령
- 장비 환경설정

정책

- 정책
 - 노드정책
 - 노드액션
 - Windows 업데이트 정책
 - 장치제어 정책
 - 위험감지

- 제어정책
 - 제어액션
- 무선랜정책
 - AP프로파일
 - Client 프로파일
- 컴플라이언스정책

• 그룹

- 노드
- 무선랜
- 사용자
- 장치그룹

• 객체

- 권한
- 네트워크
- 서비스
- 시간

설정

• 속성관리

- 노드타입 관리
- 태그 관리
- 추가필드관리
- 용도관리
 - 사용자용도
 - IP신규
 - 용도별 정의 수정

• 접속인증페이지(CWP)

- 공지사항
- 페이지구성
- 메시지관리
- 동의페이지
 - 사용자정보

- 보안서약
- 사용자정의 버튼
- CWP설정
- 환경 설정
 - 노드관리
 - IP 관리
 - IP신청시스템공지사항
 - 무선랜관리
 - 사용자관리
 - 사용자인증
 - 인증연동
 - 감사기록
 - 운영체제 업데이트
- DHCP 서버
- RADIUS 서버
- 관리콘솔
- 백업
- 에이전트
- 정보 동기화
- 기타설정
- 관리역할
- 포트스캔

시스템

- 시스템
 - 시스템관리
 - 시스템초기 설정
 - 환경설정
 - 센서설정
 - 무선센서 환경설정
 - 세션 관리
 - 라이센스

- 업데이트 관리

- 시스템 OS
 - 소프트 웨어
 - 플러그인
 - 운영정보 데이터
- 서비스 관리
- 서비스 제어

감사

- 로그
- 리포트
 - 노드 리포트
 - 쿼리 리포트

대시보드

- 위젯

배경지식

목적

- 본 관리자설명서 가이드는 제품에 대한 내용을 보다 쉽게 이해할 수 있도록 필요한 페이지입니다.

배경지식

- NAC(Network Access Control)란?
 - 사용자 PC 및 네트워크 단말기가 네트워크에 접근하기 전에 보안 정책을 준수했는지 여부를 검사해 네트워크 접속을 통제하는 기술입니다.
- Genian NAC란?
 - Genian NAC는 별도의 관리서버, 배포서버, 모니터링서버 없이 하나의 장비에서 자동 패치 관리, PC 자산 및 네트워크 자산 관리, 네트워크 사용 통제 기능을 수행하는 네트워크 허가 통제 S/W입니다.
 - Genian NAC를 통해 내부 네트워크의 자원을 관리하고 네트워크 내 장애 및 사고 원인을 예방, 탐지, 제거함으로써 안정적인 네트워크 운영 관리가 가능하도록 합니다.
 - 제품을 효과적으로 사용하기 위해서는 제품의 전체적 시스템 구성을 이해해야 합니다.
- Genian NAC 운영환경
 - Genian NAC의 제품 패키지는 크게 Policy Center와 Network Sensor 및 Windows 시스템을 대상으로 패치 및 자산 관리를 위한 Agent 모듈로 구성됩니다.
 - Genian NAC(Network Access Control)은 비인가자에 대한 네트워크 허가 통제를 목적으로 사용되는 제품으로, Policy Center와 Network Sensor로 구성되며 Policy Center는 내부 네트워크에 존재하는 모든 센서 시스템과 에이전트 시스템을 관리하고 관리자는 관리 인터페이스를 통해 PMS 정책 설정 및 네트워크 사용 통제를 위한 보안 정책 수립이 가능합니다.
 - Network Sensor는 전용운영체제(GENOS)하에서 세그먼트에서의 정보 수집, 사용자 인증 대행, 비인가 시스템 차단 등의 서비스를 제공합니다.

장비 사용전 알아두어야 할 사항

- 관리자는 반드시 Genian 장비를 물리적으로 안전한 곳에 위치시키고 사용하여야 합니다.
- 네트워크 제어기능이 제대로 동작하지 않는다면 센서 운영모드가 Active모드가 맞는지 확인하여 주십시오.
- 장비 라이센스를 반드시 등록시켜 주십시오.

기본항목

기본항목

관리자는 제품 구성 환경, 제품 콘솔 설정, 유의사항, 제품 구동을 위해 반드시 알아야 할 항목을 확인할 수 있습니다.

- 제품구성환경
- 제품 콘솔 접속
- 유의사항
- 운영환경
- 에러 메시지
- UI 기본 관리기능
- 보안대책

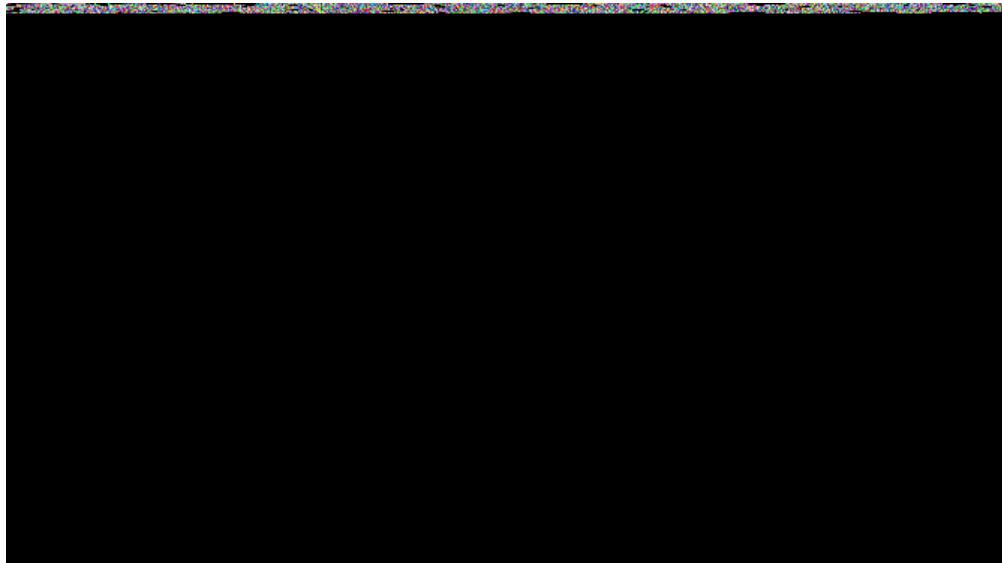
제품구성환경

필요성

제품의 구성을 알면 제품에 대한 이해도와 동작하는 원리를 알게 되어 여러 기능들을 원활히 사용뿐만 아니라 응용하여 제품의 기능을 100% 활용할 수 있습니다.

제품 구성

Genian NAC제품 구성은 크게 4가지로 Policy Center, Net-Sentry, Air-Sentry, Agent를 동작하여 노드에 대해 관리 및 제어를 합니다.



- Policy Center : 정보를 분류하고, 정책을 생성하는 기능을 합니다.
- Net-Sentry : 해당 네트워크 대역에 있는 노드에 대한 정보를 수집하고, 정책을 수행(제어)하는 기능을 합니다.
- Air-Sentry : 범위 안에 있는 AP(무선네트워크)를 탐지하고 탐지한 AP를 사용중인 노드를 탐지합니다, Air-Sentry에서 AP 기능을 지원하며 Air-Sentry AP를 사용하는 노드의 정보를 수집하여 제어할 수 있도록 합니다.
- Agent : Agent가 설치된 노드의 내부 정보를 수집하고, 노드의 내부 관련 정책을 수행할 수 있도록 하는 기능을 합니다.
※정책 : 노드를 어떻게 제어할 것인가를 관리자가 설정한 것을 정책이라 합니다.
※내부 정보 : 에이전트가 설치되어 있는 노드의 하드웨어, 인터페이스, 장비, 보안업데이트, OS 등의 정보를 수집 합니다.

동작원리

유선 노드와 무선 노드를 제어하고 정책을 세우기 위해, 노드에 대한 정보를 Net-sentry와 Air-sentry를 통해 수집을 합니다, 그에 대한 정보를 policy center에게 전송하여 Policy center는 sentry에게 받은 정보를 데이터베이스에 분류합니다.

분류한 정보는 UI에 접속하여 확인할 수 있고, UI에서 제어를 할 수 있도록 정책을 생성할 수 있습니다. 정책을 생성하면, Policy center가 생성된 정책에 대한 정보를 Net-Sentry에게 전송합니다.

Net-Sentry는 Policy center에게 받은 정책에 대한 정보를 토대로 노드를 제어합니다.

- Agent가 설치된 경우

노드에 있는 Agent는 해당 노드에 대한 상세한 내부 정보를 수집하여 플러그인으로 정의하여 Policy center에 전송합니다. 전송한 내부 정보를 이용하여 Policy center는 노드에 내부 관련에 제어할 수 있는 정책을 생성 합니다.
정책을 생성하면, 생성된 정책을 Agent에게 정책 정보를 전송합니다, Agent는 전송 받은 정책에 대한 정보를 수집하여 정책을 수행 합니다.

제품 콘솔 접속

시리얼로 접속하는 방법

시리얼 케이블로 장비에 연결을 한 후에 콘솔 접속 프로그램(하이퍼 터미널 등)을 이용해서 접속합니다.
하이퍼터미널은 더 이상 Windows viasta 이상부터는 포함되어 있지 않습니다. 이전에 하이퍼터미널을 사용하여 직렬 장치를 제어한 경우 개인용으로 무료로 제공되는 하이퍼터미널을 인터넷에서 다운로드할 수 있습니다.

1. WindowsXP에서 제어판 > 시스템 > 장치 관리자 > 통신포트를 확인합니다.
2. 콘솔 접속 프로그램을 실행하여 Quick Connect를 실행합니다.
콘솔 접속 프로그램의 설정은 다음 예와 같이 설정합니다.
(예)

Port : COM1 - 1번에서 확인한 값을 입력합니다.
Baud rate : 115200

3. connect를 실행하고 다음 아이디와 비밀번호를 입력하여 접속합니다.

user name : admin
password : genian123

 예시에 사용된 superadmin ID와 Password는 사용하지 마시고, 비밀번호 정책에 맞게 적용하여 사용하시기 바랍니다.



SecureCRT 프로그램을 사용할 경우 한글이 깨지는 현상이 발생할 경우 다음과 같이 설정을 합니다.
Options > Session Options > Appearance > Character에서 UTF-8를 선택합니다.



WebUI로 접속하는 방법

web browser를 이용해서 접속합니다.
web browser를 실행하여 정책서버 IP를 입력합니다.

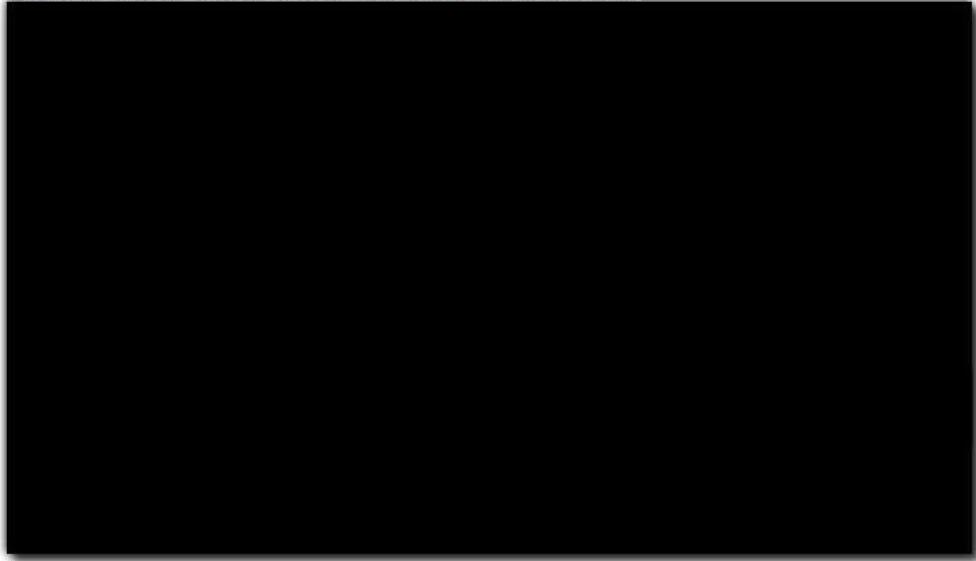
1. web browser를 실행하여 아래와 같이 접속 후 관리자 ID와 Password를 입력하여 로그인 합니다.
(예)

<https://정책서버IP/mc2>

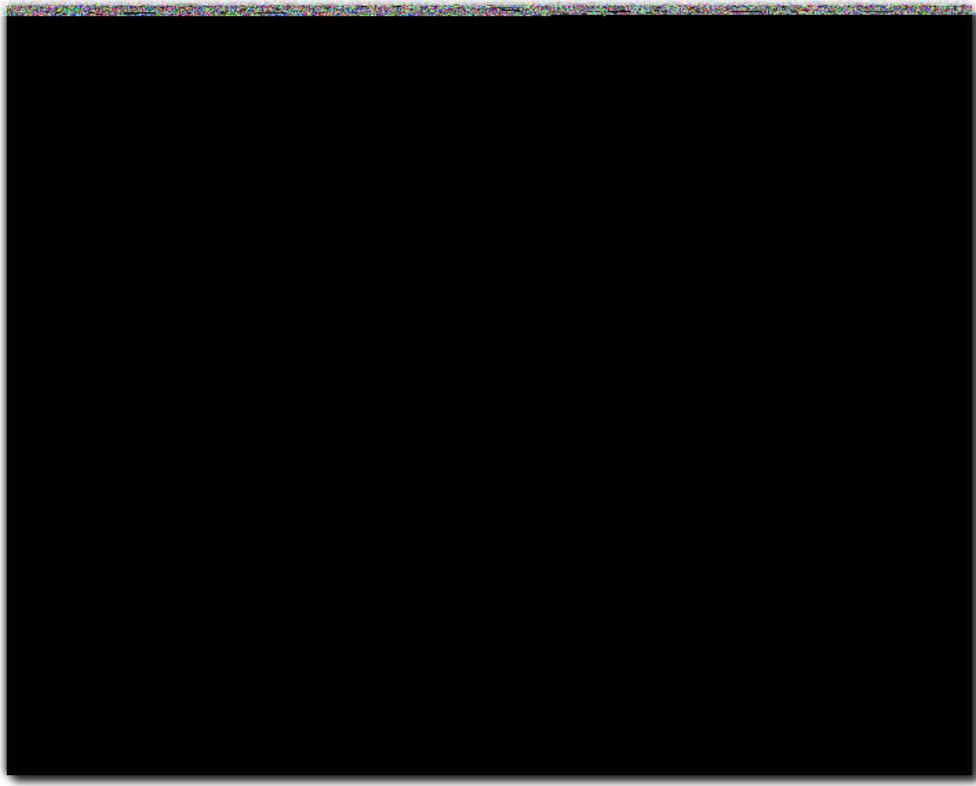
TLS 설정 방법

본 제품은 TLS v1.2를 제공합니다.
제품의 관리 페이지가 표시되지 않을 경우 Internet Explorer에서 TLS v1.2를 설정합니다.
최신 버전 Chrome으로 업그레이드할 시 TLS v1.2를 지원합니다.

1. TLS 설정이 되어 있지 않을 시 NAC WebUI에 접속할 수 없습니다. TLS 설정을 위해 설정 변경 버튼을 클릭합니다.



2. 스크롤을 아래로 내리다 보면 TLS 설정 항목이 있습니다. TLS 설정 항목에서 SSL 3.0, TLS 1.0, TLS 1.2 항목에 체크를 한 후 확인 버튼을 클릭합니다.



-
3. NAC WebUI에 접속할 시 아래의 그림과 같이 페이지가 출력되며, "이 웹 사이트를 계속 탐색합니다(권장하지 않음)."을 클릭합니다.



4. NAC WebUI에 정상적으로 접속할 시 아래의 그림과 같습니다.



항목	옵션	설명
언어선택	Korean, English	WebUI 언어를 선택합니다.

유의사항

제품 내용물

설치 전에 받은 제품에 대한 다음과 같은 확인이 필요합니다.

1. Genian NAC 제품명, 구성품, 수량 확인(일체형 하드웨어 + 사용자 설명서 CD)
(구성품에 Security Tape의 부착 여부를 확인)
2. 라이센스 확인서(사용자 설명서 CD와 동봉)
3. 설치를 담당할 보안 엔지니어

유의사항

Genian NAC 설치 전 아래와 같은 운영환경이 되도록 하여야 합니다.

1. 물리적으로 안전한 장소에 설치되어야 합니다.
2. 외부망으로부터 방화벽 등으로 보호되고 있는 안전한 내부망 네트워크에 설치되어야 합니다.
3. Genian NAC의 운영을 위해서는 Dynamic ARP로 운영되는 이더넷 스위칭 환경에 설치 운영되어야 합니다.
4. Genian NAC 의 정상적인 운영을 위해서는 구성부분 간의 통신과 운영환경에서 제공하는 서버들 간의 통신은 손실, 훼손, 변조되지 않도록 네트워크 환경을 유지해야 합니다.
5. 제품과 연동되는 모든 서버는 안전한 환경에서 운영되어야 합니다.
6. Genian NAC 와 연동되는 NTP 서버는 신뢰된 시간을 제공하여야 합니다.
7. Genian NAC가 운영 시에 사용되는 MYSQL Database 에 저장되어 있는 정보의 인가되지 않은 변경, 삭제로부터 안전하게 보호되어야 합니다.
8. 관리자는 운영에 필요한 적절한 교육을 받아야 합니다.
9. 설치 후 관리자의 지속적인 관리를 통해 의도된 보안정책이 유지되도록 하여야 합니다.
10. 관리자는 모든 기능에 접근이 가능하기 때문에 보안정책을 수립하거나 강제화를 할 경우에는 적절한 테스트를 거쳐서 확인 한 후 기능을 적용하시기 바랍니다.
11. 관리자는 개인의 사리사욕을 위해서 제품을 악용하는 일이 없도록 해야 하며 해당사항이 확인될시 형사고발 될 수 있음을 알려드립니다.

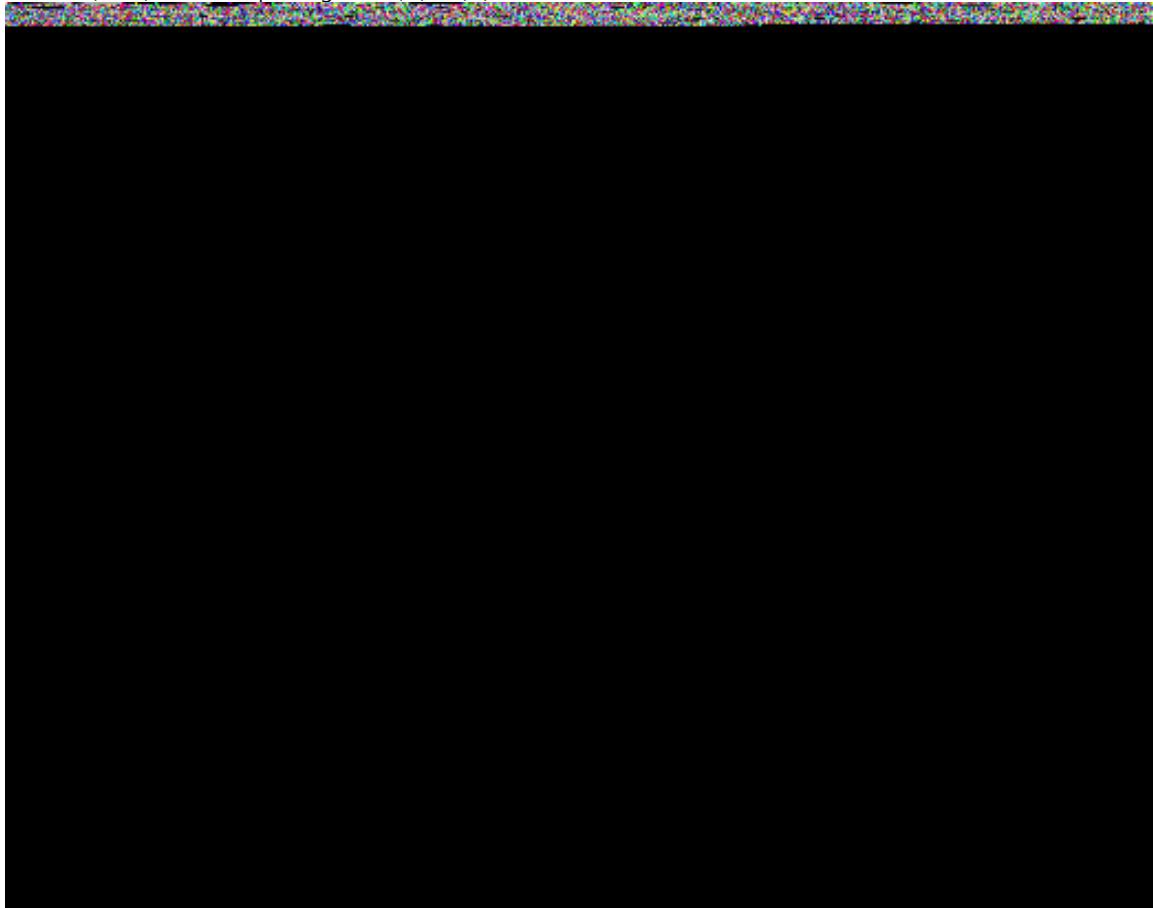
운영환경

목적

- 본 제품은 Host로 구성하여 운영할 수 있습니다.

Host

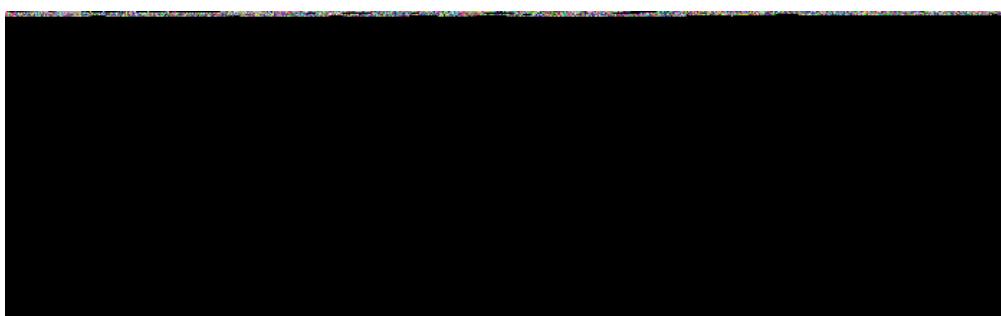
- NAC에서 가장 기본이 되는 환경입니다.
- Host 센서를 이용한 ARP Spoofing으로 제어합니다.



에러 메시지

에러 메시지

IE에서 500, 404, 403 에러가 발생할 경우 에러 메시지를 출력합니다.



UI 기본 관리기능

UI 기본 관리기능

Genian NAC를 설정하는데 있어, 공통적인 부분의 작업 수행을 설명하는 페이지들입니다.
제품을 사용하는데 있어 많은 부분을 차지 하오니 반드시 먼저 숙지하시고 제품 설명서를 이용하시기 바랍니다.

- 관리뷰 편집
- 내보내기&가져오기
- 다국어 메시지 입력
- 변경정책적용 버튼
- 빠른실행 명령 편집
- 생성, 추가, 등록 시 기본정보 설정
- 설정 값 수정
- 전체항목 선택
- 정렬 기능
- 정책복사
- 정책 사용, 사용안함
- 정책의 순서 변경
- 펼침 닫힘
- 항목 삭제
- 항목의 생성, 추가
- 노드바구니에 담기

관리뷰 편집

관리뷰 편집 기능

관리자는 관리뷰 편집 기능을 이용하여 관리뷰의 항목을 원하는 위치에 배치할 수 있습니다.

1. 관리뷰 편집

관리뷰 편집 기능은 관리 뷰가 있는 UI의 작업 선택 또는 관리뷰 옵션 메뉴에서 확인할 수 있습니다.



2. 관리뷰 편집 방법



내보내기&가져오기

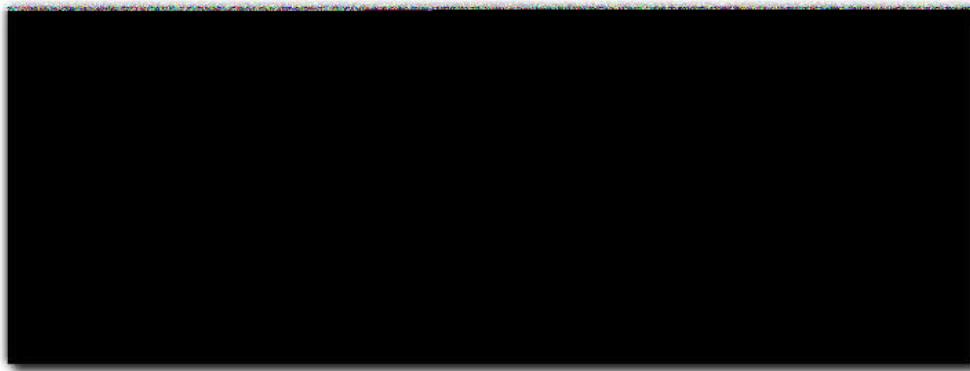
내보내기/가져오기란?

내보내기는 수집한 정보들을 테이블 형태로 정리하여 엑셀, CSV 형식으로의 문서 변환하는 기능입니다. 가져오는 CSV 파일을 가져와 NAC에 등록하는 기능입니다.

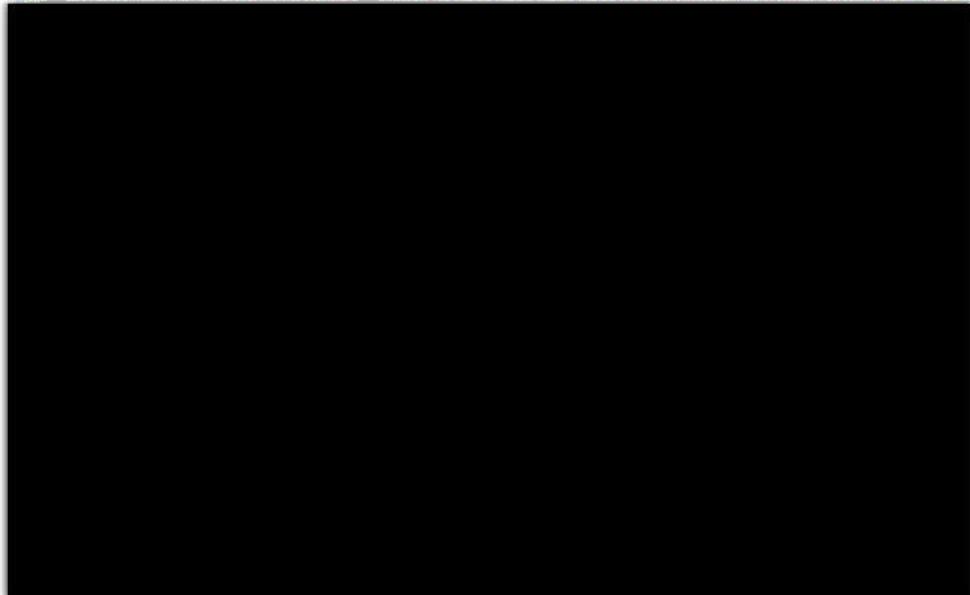
- 아래 그림과 같이 디스켓 모양의 아이콘을 누르면 xls 또는xlsx형태의 문서를 다운로드 할 수 있습니다. default로 xls로 생성되며, xlsx 형태로 문서를 다운로드하고 싶을 경우 [관리콘솔](#)에서 내보내기 엑셀 파일 형식 옵션을 참고 바랍니다.



- 내보내기 파일을 클릭할 시 아래와 같이 노드 관련 정보를 엑셀 파일로 확인할 수 있습니다.



- ,(콤마)로 구분된 CSV파일을 가져오기 시 CSV파일 데이터가 NAC에 등록됩니다.



다국어 메시지 입력

다국어 메시지 입력

사용자에게 보여지는 메시지들은 메시지 입력란 상단에 ko, en이 있습니다.
ko은 cwp 페이지의 Language 설정이 한국어일 때 보이는 메시지이고, en은 Language 설정이 English일 때 보이는 메시지입니다. en의 경우 한글이 번역되어 보이는 것이 아닙니다, 영문으로 입력하여야 합니다.

다국어 메시지 입력 방법

1. 아래 그림과 같이 CWP 페이지에서 보이는 메시지들은 모두 ko, en이라는 입력 버튼이 있으며, 각 버튼별로 메시지 입력 창이 있으며 입력한 문구들은, CWP 페이지의 Language 설정에 따라 메시지를 보이게 하는 기능을 하고 있습니다.



2. ko에 CWP 페이지의 Language가 한국어 일 때 보일 메시지를 입력하고, en에는 CWP 페이지의 Language가 English일 때 보일 메시지를 입력합니다.
예로 ko에는 "사용자 인증을 위반하여 네트워크를 사용할 수 없습니다. 사용자 인증을 수행바랍니다."을 입력하고, en에는 "You can not use the network in violation of user authentication, please perform user authentication." 입력였습니다.



-
3. 아래의 그림과 같이 CWP 페이지의 Language설정에 따라 메시지가 달라집니다.



변경정책적용 버튼

정책적용버튼

정책적용버튼은 정책 메뉴에서 각종 설정값을 변경하였을 때, 변경된 내용을 적용을 시켜주는 버튼입니다.

정책 적용 버튼은 아래 그림과 같이 로그인 정보 옆에 위치하며, 정책, 그룹, 객체의 수정이나 생성 등 작업 수행 시 발생되는 이벤트입니다. 정책, 그룹, 객체의 생성이나 수정 시 해당 정책이 바로 적용되는 것이 아닙니다. 정책적용버튼을 눌러야만 정책이 적용됩니다.

어떠한 설정을 변경하거나 생성/삭제시에 정책 적용 버튼이 표시된다면 설정을 한번 더 확인 후 눌러주십시오.



빠른실행 명령 편집

빠른실행 명령 편집

관리자는 자주 사용하는 기능을 맨 위로 올려서 보다 빠르고 쉽게 사용할 수 있게 해주는 기능입니다.

1. 빠른실행 명령 편집

관리 > 노드 > 작업선택 > 빠른실행 명령 편집 을 클릭합니다.



2. 작업선택 메뉴편집팝업

"사용 가능"에 있는 기능들을 더블클릭, 드래그, 화살표를 이용하여서 "선택" 부분으로 옮길 수 있습니다.



3. 빠른실행 명령 편집 설정

아래 그림과 같이 선택 부분으로 옮겨진 기능들은 작업 선택의 상단에 등록됩니다.



생성, 추가, 등록 시 기본정보 설정

생성/추가/등록 시 기본정보 설정

정책, 그룹, 객체 등 항목들을 생성/추가/등록 시 기본정보를 설정합니다.

- **기본정보**

정책, 그룹, 객체 등 항목을 생성하고 싶을 경우 작업선택 > 생성 을 클릭합니다.



- 기본정보는 대부분 항목을 식별할 ID, 항목의 부가 설명을 해주는 설명, 사용 유무(적용모드)으로 이루어져 있습니다. 그룹 생성 시 필요한 기본정보 중 어려운 부분인 조건 연산에 대해서는 추가적으로 아래에 작성하였습니다.



- 적용모드는 사용함/사용 안 함 옵션이 있고, 사용함 옵션 선택 시 정책을 생성하면서 사용 항목에 체크되어 생성됩니다. 생성 후 바로 적용되지 않으며 적용하려면 반드시 변경정책적용 아이콘을 눌러주어야 합니다.
- 조건 연산 AND : 두 개 이상의 조건을 사용할 때, 조건을 모두 만족시켜야 그룹에 포함됩니다.
조건 연산 OR : 두 개 이상의 조건을 사용할 때, 많은 조건들 중 하나만 만족시켜도 그룹에 포함됩니다.

예)



위 그림과 같이 조건이 두 개이고 플러그인이 인터페이스 제어라면,
조건 연산자 AND 라면 터치 메신저와 마이피플 메신저 둘 다 존재해야 인터페이스 제어가 수행되고,
조건 연산자 OR 라면 터치 메신저와 마이피플 메신저 둘 중 하나의 메신저만 존재해도 인터페이스 제어가 수행됩니다.

설정 값 수정

각종 설정 값 수정

생성된 정책 및 다른 기능들의 설정을 수정하고 싶을 경우 항목의 ID를 클릭하여 각종 설정값을 수정하고 아래쪽에 있는 수정 버튼을 클릭하여 수정할 수 있습니다.

1. 수정을 원하는 항목의 ID를 클릭합니다



2. 수정할 내용을 수정하고 수정 버튼을 클릭하여 수정을 완료합니다.



전체항목 선택

전체항목 선택

한 페이지 이상의 노드가 등록되었을 때 전체 항목을 클릭할 경우, 모든 페이지에 있는 노드를 선택할 수 있습니다.
단, 전체 노드 페이지에서는 해당 기능이 동작하지 않습니다.

1. 작업할 센서를 클릭합니다



2. 전체항목을 클릭합니다.



3. 우측에 표시되는 메시지에 체크할 시 모든 페이지에 있는 노드가 선택되고, 체크하지 않을 시 해당 페이지의 노드만 선택됩니다.

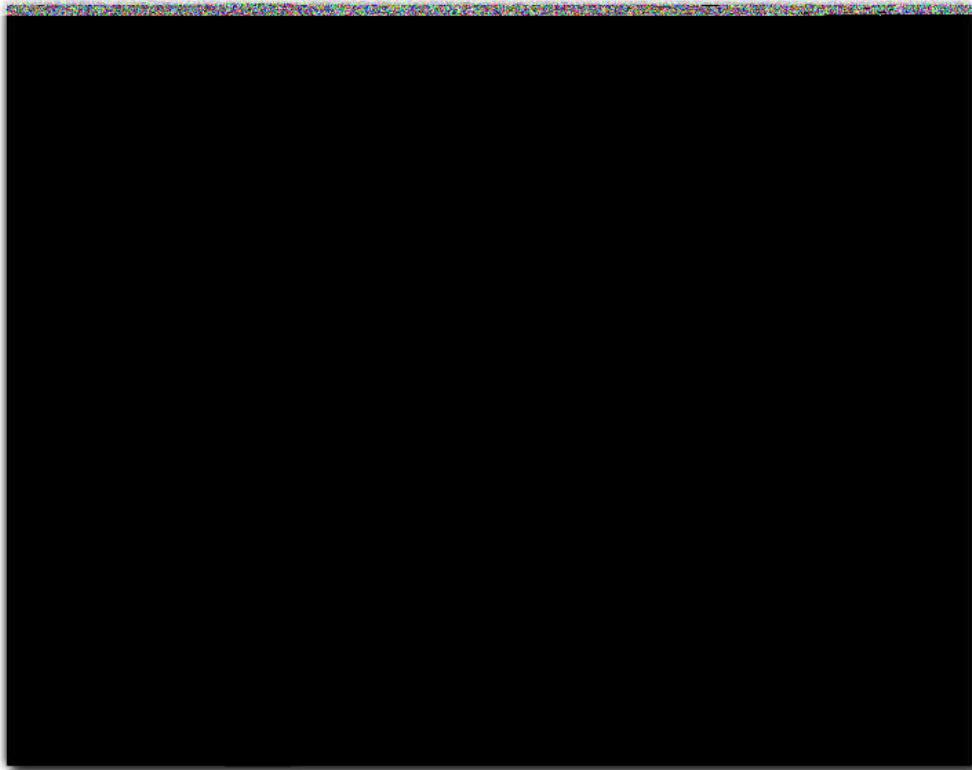


정렬 기능

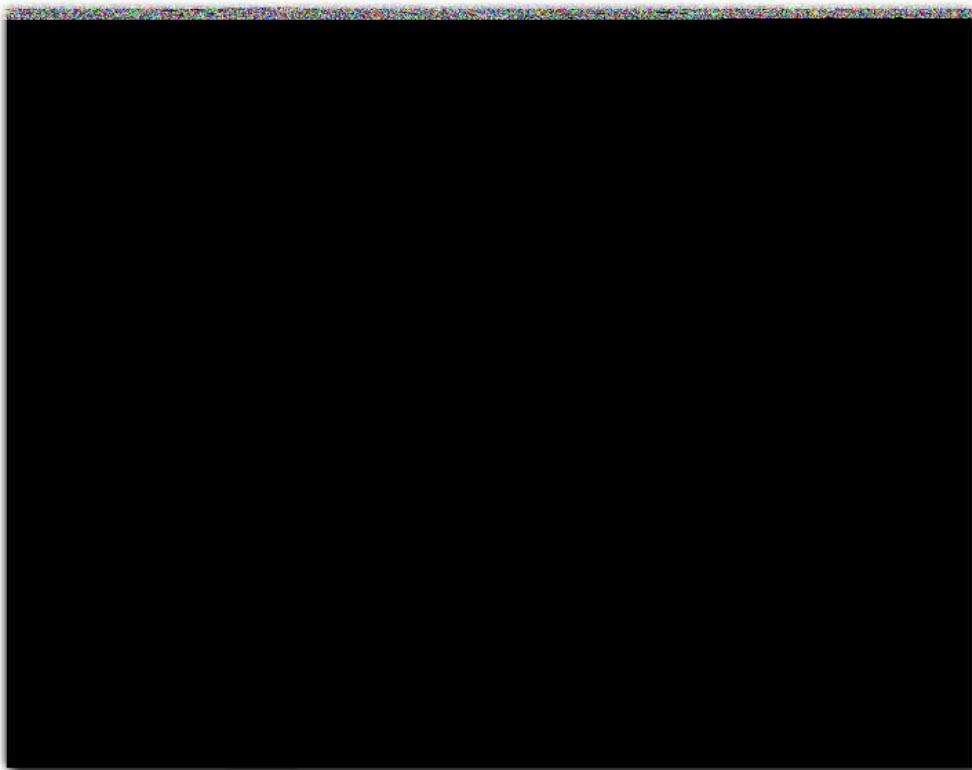
정렬 기능

관리자는 항목을 클릭하여 해당 항목이 나타내는 정보를 오름차순 및 내림차순으로 정렬할 수 있습니다.
정렬 기능을 사용할 시 항목 우측에 화살표가 나타나며 화살표가 ↑일 경우 오름차순이고 ↓일 경우 내림차순입니다.

- 정렬 전



- 정렬 후



정책복사

정책복사

관리자는 정책복사를 통하여 똑같은 내용의 정책, 그룹, 노드액션을 ID 만 바꿔 복사하여 사용할 수 있습니다.

1. 정책복사

복사할 정책, 또는 그룹의 ID를 클릭합니다.



①의 정책복사를 누르면 복사 ID를 입력하는 팝업창이 뜹니다.

복사할 ID를 넣고 ②의 정책복사를 누르게 되면 복사된 정책 / 그룹이 생성됩니다.

Geninetwokrs라는 무선랜 그룹을 정책복사를 통해 손쉽게 geni라는 또 하나의 그룹으로 만든 현황을 확인할 수 있습니다.



복사정책 / 그룹의 조건, 세부 설정, 할당 등은 복사된 정책 / 그룹의 수정 페이지에서 수정을 해야 합니다.

정책 사용, 사용안함

정책 사용 / 사용안함

정책의 사용 유무를 설정할 수 있는 기능입니다.

정책 사용 유무 설정 방법

- 정책 사용 유무를 설정하고 싶은 정책을 선택합니다.



- 해당 정책을 사용하고 싶지 않을 경우 사용안함을 선택하고, 사용하고 싶을 경우 사용함으로 선택합니다. 선택 후 하단에 있는 수정 버튼을 클릭합니다.



- 변경정책적용 버튼을 클릭합니다.



정책의 순서 변경

노드정책 / 제어정책 순서 변경

정책을 세울 때 하나의 노드가 두 개 이상의 그룹에 속하여 여러 정책을 동시에 받는 상황이 올 수 있습니다.
동시에 여러 정책을 받는 노드는 관리자가 설정한 순서를 통하여 우선순위가 제일 높은 순서의 정책 한 가지만 받게 됩니다.

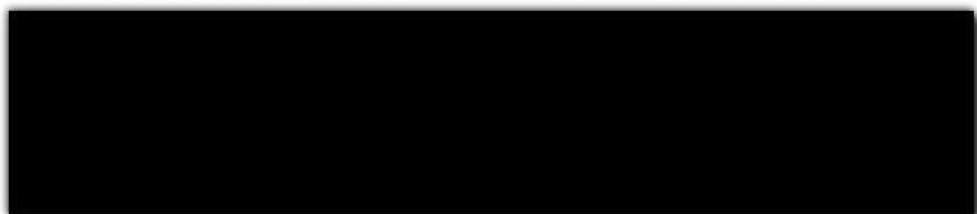
방법 1

- 정책의 수정을 이용하여 정책 순서 변경
 - 순서를 변경할 정책의 ID를 선택합니다.



- 수정 페이지에 순서 항목을 원하는 순서로 기입합니다.

다른 정책이 선점하고 있는 순서1을 현재 정책의 순서로 할당하게 되면 선점하고 있던 정책의 순서는 뒤로 밀려 순서 2가 됩니다.
예를 들어, 순서 3 과 4 사이에 현재 정책의 순서를 넣고 싶다면, 순서 4를 기입하면 됩니다.
이렇게 하면 현재 정책의 순서는 4가 되고 순서 4를 가지고 있던 정책은 순서 5가 됩니다.



- 수정 버튼을 클릭합니다.



방법 2

- 이동 항목의 화살표 아이콘을 이용하여 정책 순서 변경
 1. 순서를 변경할 정책의 이동 항목에 있는 화살표 아이콘을 클릭합니다. 아래쪽 화살표를 클릭할 시 순서1에서 순서2로 이동되며, 위쪽 화살표를 클릭할 시 순서2에서 순서 1로 이동됩니다.
정책이 위쪽이나 아래쪽으로 이동할 수 없을 경우, 화살표 아이콘이 비활성화됩니다.



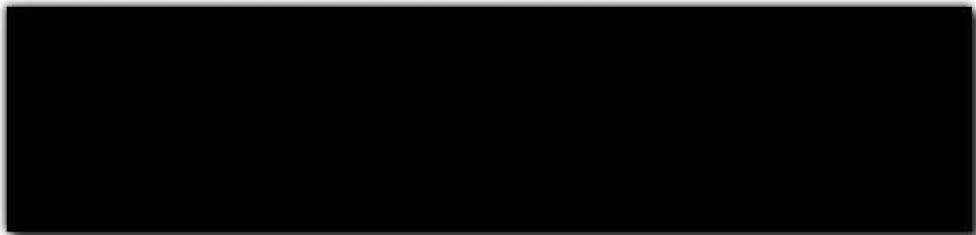
펼침 닫힘

펼침/닫힘

트리 뷰에서 하위 트리가 있는 상위 트리를 선택하여 펼침/닫힘 기능을 사용할 시 상위 트리에 속해 있는 하위 트리가 모두 펼쳐지고, 하위트리가 펼쳐져있는 상위트리에 펼침/닫힘 기능을 사용할 시 하위트리가 모두 닫혀집니다.

1. 상위 트리 선택

관리자가 원하는 상위 트리를 선택하고 펼침/닫힘 버튼을 클릭합니다.



2. 펼치기

아래의 그림과 같이 선택한 상위 트리에 속해 있는 하위 트리를 모두 볼 수 있습니다.



항목 삭제

삭제

불필요한 정책, 그룹, 설정 등을 삭제할 수 있습니다.

1. 삭제하고자 하는 항목 ID의 맨 앞 체크 박스에 체크 표시를 합니다.



2. 작업선택 > 삭제 를 클릭합니다.



정책, 그룹, 설정 등을 삭제할 경우 복구할 수 없으며 정책, 그룹, 설정을 적용받고 있는 노드가 정상적으로 동작하지 않을 수 있으니 주의하시기 바랍니다.

- 사용 중인 그룹, 객체 삭제 방법

정책에 사용되고 있는 그룹이나, 객체 등은 삭제 명령을 내렸을 때 아래 메시지를 띄우며 삭제가 되지 않습니다.



그럴 땐 아래 그림처럼, ID 옆의 아이콘에 마우스를 올려 어떤 정책에서 사용 중인지 확인합니다.



어떤 정책에서 사용 중인지 확인했다면, 그 정책 수정 페이지에서 할당되어있는 그룹 또는 객체를 삭제하여 준 후에 다시 삭제를 시도합니다.



항목의 생성, 추가

각종 항목의 생성/추가

각종 항목을 생성/추가하는 방법입니다.

작업선택 > 생성/추가버튼 을 클릭합니다.



노드바구니에 담기

노드바구니에 담기

노드바구니에 담기 기능은 관리자가 특정 노드들을 관리하거나 일련의 작업을 수행할 때 노드들을 노드 바구니에 담기 기능을 이용하면 쉽게 할 수 있습니다.

노드바구니에 담은 노드들은 관리 > 노드 > 트리 뷰 > 센서 탭 > 노드바구니에서 확인할 수 있습니다.

1. 노드바구니에 담기 선택

노드바구니에 담을 노드들을 선택 후, 작업선택 > 노드장비관리 > 노드바구니에 담기를 클릭합니다.
각각 바구니에 담기는 대상은 다음과 같습니다.

항목	대상
관리 > 노드	선택한 노드
관리 > 스위치	선택한 스위치에 접속한 노드, 관리 뷰의 노드 항목을 통해 확인할 수 있습니다.
관리 > 무선랜	선택한 무선랜에 접속한 노드, 관리 뷰의 접속(내부) 항목을 통해 확인할 수 있습니다.
감사 > 로그	검색된 로그의 IP 정보, 관리 뷰의 IP 항목을 통해 확인할 수 있습니다.



2. 노드바구니에 담기 확인

관리 > 노드 > 트리 뷰 > 센서 탭 > 노드바구니 클릭하여 확인할 수 있습니다.



선택 노드바구니 비우기

1. 선택 노드바구니 비우기 선택

노드바구니에서 제외하고 싶은 노드가 있을 시 제외할 노드 선택 후 선택 노드바구니 비우기 버튼을 클릭합니다.



2. 선택 노드바구니 비우기 확인

아래의 그림과 같이 노드바구니에서 제외됩니다.



전체 노드바구니 비우기

1. 전체 노드바구니 비우기 선택

노드바구니에 있는 모든 노드를 제외하고 싶을 경우 전체노드바구니 비우기 버튼을 클릭합니다.



2. 전체 노드 바구니 비우기 확인

아래의 그림과 같이 모든 노드가 노드바구니에서 제외됩니다.



보안대책

- 보안목적에 적합한 보안대책

보안목적	보안대책
감사	보안과 관련된 행동의 책임추적이 가능하도록 보안관련 사건을 기록 및 유지한다. 기록된 데이터를 검토할 수 있는 수단을 제공한다. 또한 감사 데이터가 포화 상태에 도달했을 때 대응기능을 제공 한다.
관리	인가된 관리자가 NAC를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제공 한다.
식별및인증	사용자를 유일하게 식별하며, NAC의 관리 및 객체에 대한 접근을 허용하기 전에 사용자의 신원을 인증 한다.
역할	사용자 역할을 구분하여 역할에 따른 보안정책 및 보안기능을 제공한다.
안전한 상태유지	장애가 발생한 경우 안전한 상태를 유지한다.
NAC정보흐름통제	노드의 내부망 접근을 제어하여 보안정책을 준수 한다. 또한 위험이벤트를 발생하는 노드의 내부망 접근을 차단 한다

관 리

관리

관리 탭은 노드, IP 주소, 네트워크, 무선랜, 사용자, 신청 총 6 개의 탭으로 구성되어 있습니다.

- 노 드 : 노드를 확인하고 노드들의 각종 정보들을 확인할 수 있으며 여러 가지 기능들을 이용하여 노드를 관리할 수 있는 탭입니다.
 - IP 주소 : 센서의 정보를 한눈에 확인할 수 있으며 Matix view를 통하여 노드 탭과는 다른 관점으로 IP를 관리하고, IP의 현황을 알 수 있는 탭입니다.
 - 스위치 : 센서와 연결되어 있는 스위치의 포트 사용우무, 접속 사용자, 포트 이름 등 센서에 연결되어 있는 스위치의 정보를 확인 할 수 있는 탭입니다.
 - 무선랜 : Air-Sentry를 통하여 수집된 AP들의 각종 정보를 확인할 수 있으며 수집된 AP에게 태그 및 그룹 지정을 할 수 있는 탭입니다.
 - 사용자 : 사용자 등록/삭제, 태그 부여, 비밀번호 강제화 등의 작업을 수행할 수 있으며, 관리자를 생성할 수 있는 탭입니다.
 - 신 청 : 신규 사용자가 IP, 사용자 등록, 장비 사용을 위해 제출하는 신청서를 관리할 수 있는 탭입니다.
- 노 드
 - IP주소
 - 스 위 치
 - 무 선 랜
 - 사 용 자
 - 신 청

노드

노드 관리

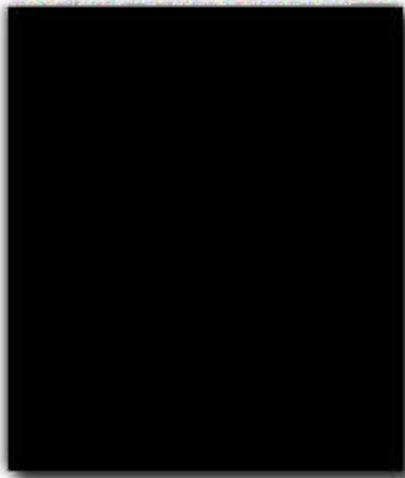
관리자는 관리 > 노드 메뉴를 통하여 노드들의 각종 상태, 현황, 상세정보를 한눈에 확인할 수 있고, 필터를 사용하여 원하는 정보만을 추출할 수 있습니다.

노드란 IP와 MAC을 가지고 있는 단말을 말합니다.

노드 관리 뷰는 아래와 같이 트리 뷰, 현황&필터 뷰, 관리 뷰로 구성됩니다.

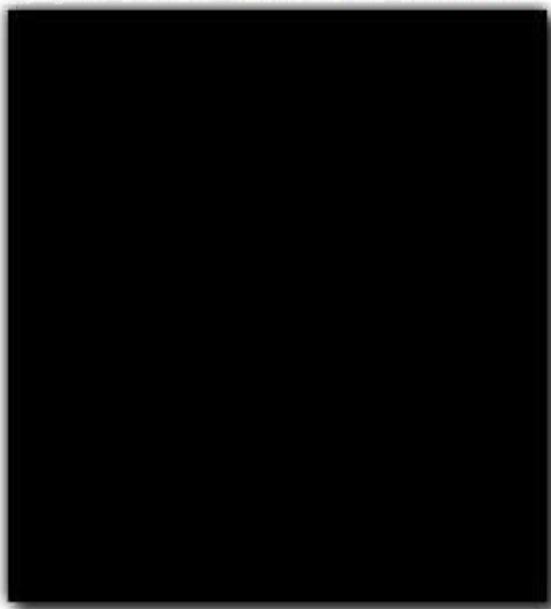
- **트리 뷰**

노드를 그룹별로 나누어 센서그룹별 / 그룹별로 볼 수 있습니다.
연필 모양을 선택하면 트리 뷰를 편집할 수 있는 편집모드가 됩니다.



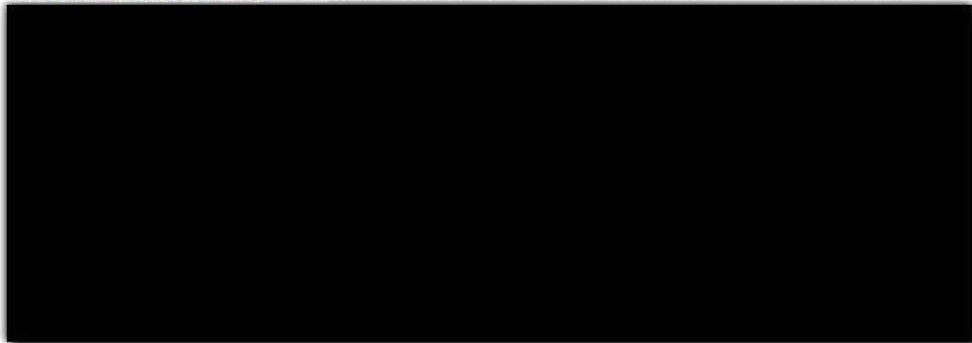
- **현황&필터 뷰**

위 트리뷰에서 선택된 노드를 바탕으로, 노드의 현황별 내용을 요약하여 보여주고, 필터를 통하여 원하는 조건에 맞는 노드들만 추출할 수 있습니다. 연필 모양을 선택하면 필터 트리를 편집할 수 있습니다.



- 관리 뷰

수집한 노드들의 정보를 테이블 형식으로 출력합니다.
내보내기 기능과 작업선택버튼을 통한 노드 관리기능, 빠른 검색 기능이 있습니다.
또한, 노드 뷰만이 아닌 위험 뷰, IP 관리 뷰 등을 통한 조건 뷰를 지원하고,
노드 관점과 장비 관점을 통하여 하나의 MAC에 여러 개의 IP를 가진 노드를 확인할 수 있습니다.

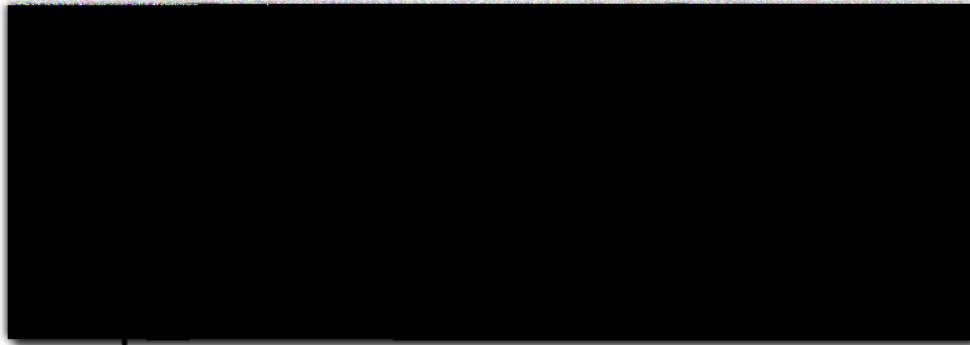


트리 뷰

관리자는 트리 뷰를 통하여 그룹별, 센서그룹별로 노드들을 분류하여 볼 수 있습니다.

- **센서그룹별**

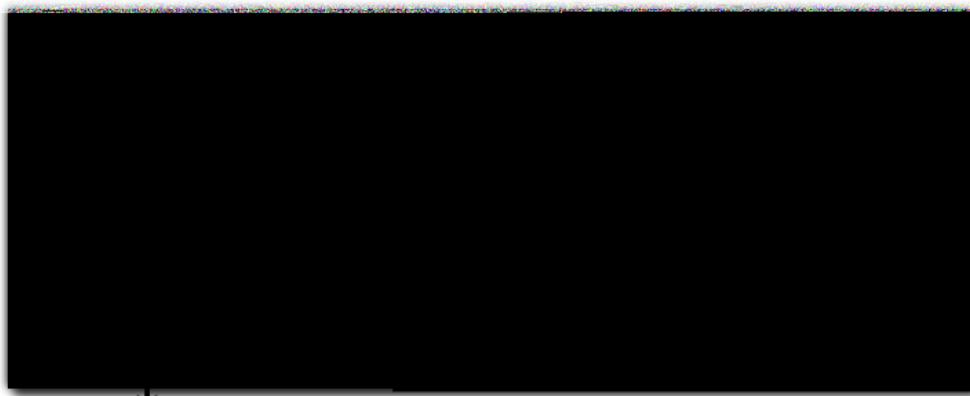
센서별을 선택하면 해당 센서가 관리하는 노드만을 출력합니다.



해당 센서는 총 76개의 노드를 관리하고 있습니다.
센서를 클릭 시 관리 뷰에 해당 센서가 관리하는 노드를 확인할 수 있습니다.

- **그룹별**

정책그룹을 선택하면 정책그룹에 포함되어 있는 노드를 출력합니다.



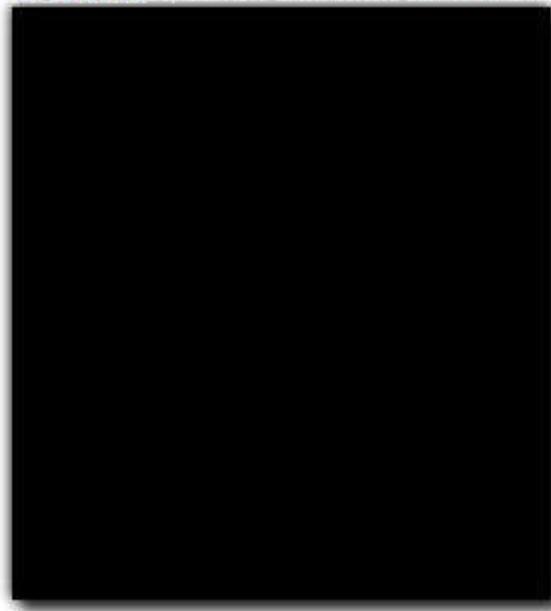
편집모드를 이용하여 센터에 카테고리, 노드그룹, 센서를 추가할 수 있습니다.
추가한 노드그룹, 센서를 클릭 시 포함되어 있는 노드를 확인할 수 있습니다.
또한, 센서에 추가한 카테고리는 정책 > 그룹 > 노드 하위에 표시되며 카테고리에 할당된 노드그룹을 확인할 수 있습니다.

- 편집모드

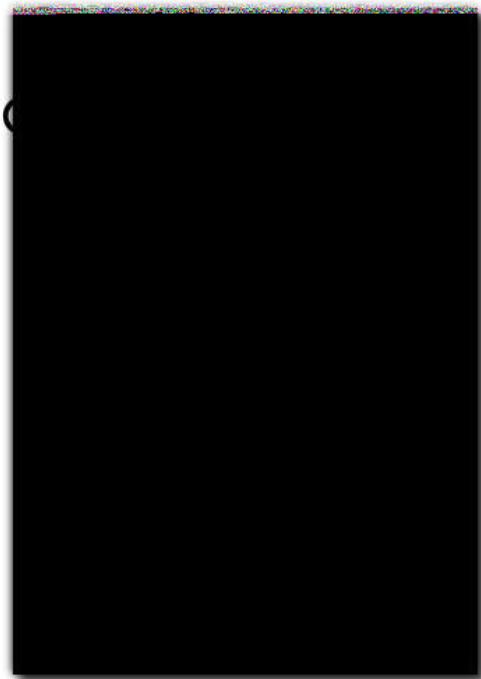
관리자는 트리 뷰의 편집모드를 이용하여 그룹을 생성하고 해당 그룹에 센서그룹 및 정책그룹을 할당할 수 있습니다.

- 그룹 할당

1. 연필 모양의 트리 편집기를 클릭하여 편집모드로 변경 후, 그룹을 할당하고 싶은 센터에서 우 클릭 후 할당을 클릭합니다.



2. 그룹을 할당할 수 있는 팝업이 생성되면, 센서나 정책그룹을 할당할 수 있습니다. 아래 예에선 정책그룹의 PC를 할당(할당한 그룹에 속해있는 노드만 관리 뷰에 보입니다.)해 보았습니다.



-
3. 연필 모양의 트리 편집 아이콘을 다시 눌러 편집모드를 해제한 후, 할당한 정책그룹을 선택하여 관리 뷰를 보게 되면 정책그룹에 포함된 노드가 보이는 걸 볼 수 있습니다.



- **다중그룹생성**

1-1 다중그룹생성하는 방법은 CSV 파일을 이용하여 그룹을 생성하는(CSV가져오기) 방법과 부서정보기반으로 생성하는 방법이 있으며, CSV 가져오기를 사용할 경우 아래의 그림과 같은 형식으로 CSV 파일을 생성합니다. Key = 그룹의 번호 ParentKey = 상위그룹 GroupTitle = 그룹 명



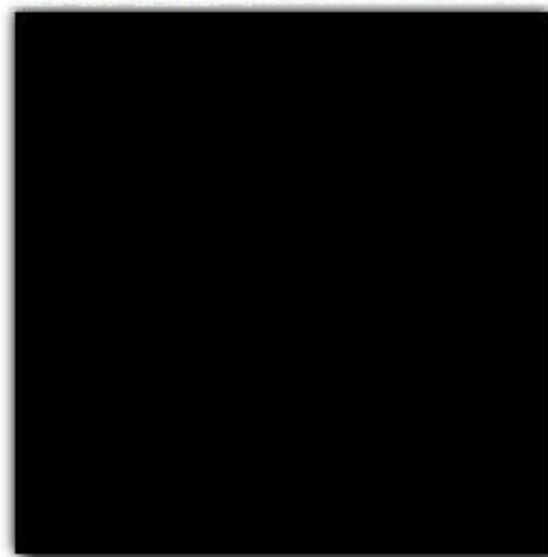
1-2 연필 모양의 트리 편집기를 클릭하여 편집모드로 변경 후, 다수의 그룹을 생성하고 싶은 센터를 선택 후 다중그룹생성을 클릭합니다.



1-3 파일선택 버튼을 클릭하여 CSV 파일을 불러온 후 가져오기 버튼을 클릭합니다.



1-4 아래의 그림과 같이 그룹이 생성되며, 연필 모양의 트리 편집기를 클릭하여 편집모드를 종료합니다.
편집모드를 종료하였을 시 그룹에 센서그룹 및 정책그룹이 할당되어 있지 않을 경우 그룹이 보이지 않으니 주의 바랍니다.



- 다중그룹생성 부서정보기반

2-1 부서정보기반으로 생성할 경우 관리 > 사용자 > 부서관리에서 부서를 생성합니다. 부서 생성 방법은 [사용자](#)에서 부서 추가 항목을 참고 바랍니다.



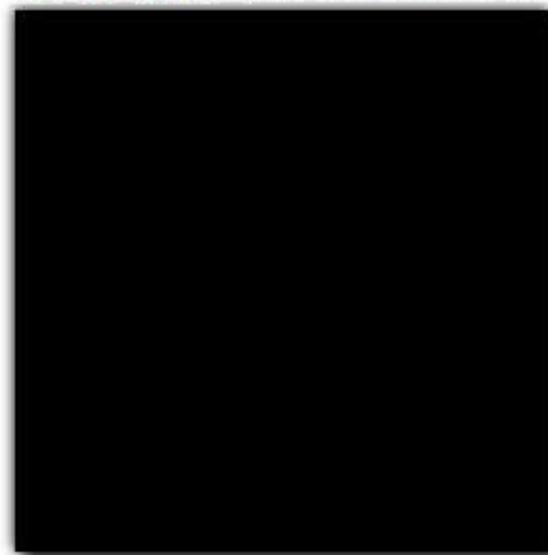
2-2 연필 모양의 트리 편집기를 클릭하여 편집모드로 변경 후, 다수의 그룹을 생성하고 싶은 센터를 선택 후 다중그룹생성을 클릭합니다.



2-3 부서정보기반생성 버튼을 클릭합니다.



2-4 아래의 그림과 같이 그룹이 생성되며, 연필 모양의 트리 편집기를 클릭하여 편집모드를 종료합니다.
편집모드를 종료하였을 시 그룹에 센서그룹 및 정책그룹이 할당되어 있지 않을 경우 그룹이 보이지 않으니 주의 바랍니다.



현황 & 필터 뷰

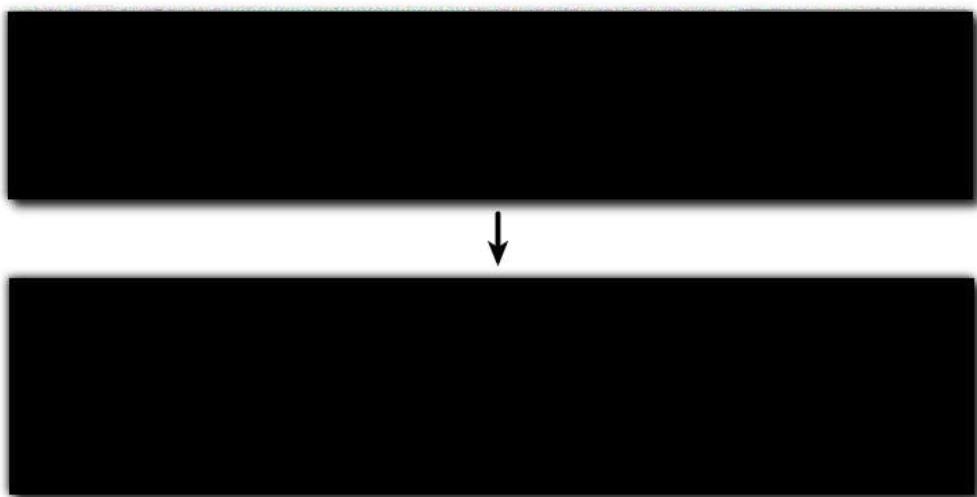
관리자는 현황 & 필터를 사용하여 트리 뷰에서 선택된 노드를 바탕으로, 원하는 항목의 정보를 손쉽게 얻을 수 있습니다.

- Genian NAC는 현황 & 필터를 이용하여 관리자가 원하는 현황에 대하여 한눈에 알아보기 쉽게 수치, 도표, 그래프 등을 이용하여 나타냅니다.

아래 그림은 트리 뷰에서 전체 노드 선택 후, 타입별 현황을 선택한 모습입니다. 타입별 노드 현황을 그래프로 나타내어 알아보기 쉽습니다.



또한, 해당 현황&필터 결과에서 제공하는 링크를 선택하면, 관리 뷰로 바로 이동합니다.



- 연필 모양의 필터 트리 편집 버튼을 선택하여 생성되는 팝업에서 원하는 현황&필터 목록만 보이게 할 수 있습니다.



현황 & 필터의 모든 항목은 다음과 같습니다.

항 목 이 름

노드정책, 제어정책, 노드그룹, 위험감지, 위험노드, 네트워크그룹, 서비스, 부서(노드그룹), 부서(인증 사용자), 인증사용자, 노드타입, 노드상태, OpenPort, 플랫폼, IP관리, 에이전트, 트래픽, 태그, 컴플라이언스정책, 연결방식, 등록일자

관리 뷰

- 항목

노드 관리 뷰에 다양한 항목이 있으며, 항목을 이용하여 노드에 대한 정보를 확인할 수 있습니다.
항목은 뷰 메뉴에서 편집할 수 있습니다. 뷰마다 항목은 다릅니다.



항목에 대한 내용은 아래의 표와 같습니다.

항목	내용
NT AG SS(장비구분)	노드 탑재과 동작 상태, 센서 동작 상태를 나타냅니다. NT 클릭 시 노드타입별 정렬 AG 클릭 시 에이전트상태별 정렬 SS 클릭 시 센서상태별 정렬 됩니다.
위험	위험이 감지될 경우 해당 항목에 위험 아이콘이 나타납니다.
동작	해당 노드가 동작할 경우 파란색으로 표시되며, 노드가 동작하지 않을 경우 회색으로 표시됩니다.
IP주소	해당 노드의 IP 주소를 나타냅니다. IPv6를 지원하는 노드일 경우 IPv6 아이콘이 표시됩니다.
MAC주소	해당 노드의 MAC주소를 나타냅니다.
NIC벤더	해당 노드의 NIC의 벤더를 나타냅니다.
서비스	해당 노드에 필요한 각종 서비스를 아이콘으로 표시하며, 아이콘을 클릭 시 해당 서비스를 이용할 수 있습니다.
정책	해당 노드가 정책을 위반할 시 위반 정책에 맞는 아이콘이 나타납니다.
노드정책	해당 노드가 현재 적용받고 있는 노드 정책의 ID를 표시합니다.
제어정책	해당 노드가 현재 적용받고 있는 제어 정책의 ID를 표시합니다. 적용받고 있는 제어 정책이 차단 정책일 경우 제어 정책 ID가 주황색으로 표시됩니다.
이름	해당 노드에 관리자가 설정한 이름을 표시합니다. 설정 방법은 노드 상세 - 기본정보를 참고 바랍니다.
호스트명	해당 노드의 호스트명이 표시됩니다.
호스트명(이름)	해당 노드의 호스트명과 관리자가 설정한 이름이 같이 표시됩니다. (예 호스트명(이름) = Genian(기술연구소 PC))
호스트명제한정책	해당 노드의 호스트명제한 정책 유무를 표시합니다. 호스트명제한 정책은 노드 상세 - 정책을 참고 바랍니다.
설명	해당 노드에 관리자가 설정한 설명이 표시됩니다. 설정 방법은 노드 상세 - 기본정보를 참고 바랍니다.
장비명	해당 노드에 관리자가 설정한 장비의 이름이 표시됩니다. 설정 방법은 노드 상세 - 장비정보를 참고 바랍니다.
포트	해당 노드와 연결된 스위치 포트를 나타냅니다. 둘보기 아이콘을 클릭 시 동일한 포트에 연결된 노드를 검색합니다.
스위치	해당 노드와 연결되어 있는 스위치의 이름을 나타냅니다. 둘보기 아이콘을 클릭 시 동일한 스위치에 연결된 노드를 검색합니다.
동작상태차트	해당 노드의 1주간의 Up/Down 동작상태를 차트로 나타냅니다. 차트를 출력하기 위해 설정 > 환경설정 > 감사기록 > 노드 동작상태 이력 저장 옵션이 On으로 설정되어 있어야합니다.
장비설명	해당 노드의 관리자가 설정한 장비의 설명이 표시됩니다. 설정 방법은 노드 상세 - 장비정보를 참고 바랍니다.
도메인	해당 노드의 도메인 및 작업 그룹을 표시합니다.
플랫폼	해당 노드의 기본적인 환경(운영체제, 모델명)이 표시됩니다.
인증사용자ID	해당 노드가 현재 인증받은 ID 나타냅니다.
인증사용자	해당 노드가 현재 인증받은 ID에 설정된 이름이 표시됩니다.
최근 사용자인증	해당 노드가 최근에 사용자 인증을 받은 시각을 표시합니다.

사용자인증정책	해당 노드가 받고 있는 사용자 인증 정책을 표시합니다. 사용자 인증 정책은 노드 상세 - 정책을 참고 바랍니다.
사용자설명	해당 노드가 인증받은 인증사용자의 설명을 표시합니다.
등록시각	해당 노드가 관리 뷰에 등록된 시각이 표시됩니다.
마지막 동작시각	해당 노드의 동작 상태가 DOWN으로 표시되었을 때의 시각이 표시됩니다.
위치	해당 노드가 어느 센서, 센터에 연결되어 있는지 표시됩니다. 둘보기 아이콘을 클릭 시 동일한 위치의 노드를 검색합니다.
연결방식	해당 노드가 유선 LAN 인지 무선 LAN 인지 표시됩니다.
접속AP	해당 노드가 어떤 AP에 접속하였는지 표시됩니다. 둘보기 아이콘을 클릭 시 동일한 AP에 접속한 노드를 검색합니다.
트래픽전체	미러 모드일 경우에 표시되며, 해당 노드의 전체 트래픽이 표시됩니다.
트래픽 OUT	미러 모드일 경우 표시되며, 해당 노드의 OUT 트래픽이 표시됩니다.
트래픽IN	미러 모드일 경우 표시되며, 해당 노드의 IN 트래픽이 표시됩니다.
태그	관리자가 해당 노드에 설정한 태그가 표시됩니다. 태그 설정 방법은 노드 태그 설정을 참고 바랍니다.
MAC 태그	관리자가 해당 노드에 설정한 MAC 태그가 표시됩니다. 태그 설정 방법은 노드 태그 설정을 참고 바랍니다.
NAT IP	해당 노드가 NAT 장비를 사용할 경우 NAT IP가 표시됩니다.
장비소유부서	노드 > 작업선택 > 장비 소유부서설정 으로 설정한 부서를 나타냅니다.
장비소유자	노드 > 작업선택 > 장비 소유자설정 으로 설정한 소유자를 나타냅니다.
IP소유부서	노드 > 작업선택 > IP 소유부서설정 으로 설정한 부서를 나타냅니다.
IP소유자	노드 > 작업선택 > IP소유자설정 으로 설정한 소유자를 나타냅니다.
장치제어	장치제어의 적용 유무를 나타냅니다.
만족안함	해당 노드가 받고 있는 에이전트 액션의 수행 결과가 만족하지 않은 에이전트 액션의 개수를 나타냅니다.
만족	해당 노드가 받고 있는 에이전트 액션의 수행 결과가 만족한 에이전트 액션의 개수를 나타냅니다.
수행전	해당 노드가 받고 있는 에이전트 액션을 아직 수행하고 있지 않는 에이전트 액션의 개수를 나타냅니다.
정보수신	SNMP를 통하여 하드웨어 관련 정보를 수신한 시각을 나타냅니다.
정보수신시각	최근에 패치 관련 정보를 수신한 시각을 나타냅니다.
열린포트	열린 포트의 개수를 나타냅니다.
CPU	해당 노드의 CPU 명을 나타냅니다. 단 해당 노드에 하드웨어 정보 수집 액션이 적용되어 있어야 CPU 명이 표시됩니다.
인터페이스	해당 노드의 인터페이스 개수를 나타냅니다.
메모리	해당 노드의 메모리(RAM)의 용량을 나타냅니다.
저장장치	해당 노드의 하드디스크 용량을 나타냅니다.
마더보드	해당 노드의 마더보드 제조사를 나타냅니다.
패치만족여부	적용받은 패치모음을 만족하였을 경우 O으로 표현되고, 패치를 하지 않아 만족하지 못할 경우 X로 표현됩니다.
위험감지	탐지된 위험이 어떤 위험인지 나타냅니다.
위험탐지	위험이 탐지된 시각을 나타냅니다.
확인된 노드타입	관리자가 해당 노드를 확인 후 설정한 노드타입을 나타냅니다.
확인된 플랫폼	관리자가 해당 노드를 확인 후 설정한 플랫폼을 나타냅니다.
OS 유형	해당 노드의 운영체제 유형을 나타냅니다.
확인된 OS 유형	관리자가 해당 노드를 확인 후 확인한 운영체제 유형을 나타냅니다.

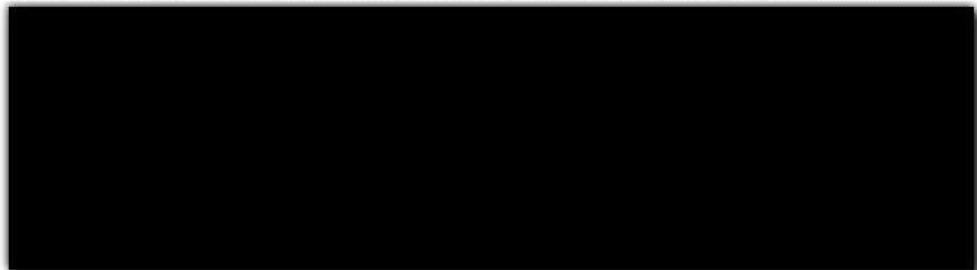
- 작업선택

작업선택 버튼을 통하여 IP관리, 노드관리, 일괄작업을 수행할 수 있습니다.
각 작업별 자세한 내용은 IP관리, 노드 장비 관리, 일괄작업 페이지를 참조해 주시기 바랍니다.



- 빠른실행 명령 편집

빠른실행 명령 편집은 위의 IP관리, 노드관리, 일괄작업의 작업들 중 자주 사용하는 작업을 미리 등록시켜 빠르게 해당 작업을 수행할 수 있도록 합니다.

- 관리 > 노드 > 작업선택 > 빠른실행 명령 편집 선택
- 

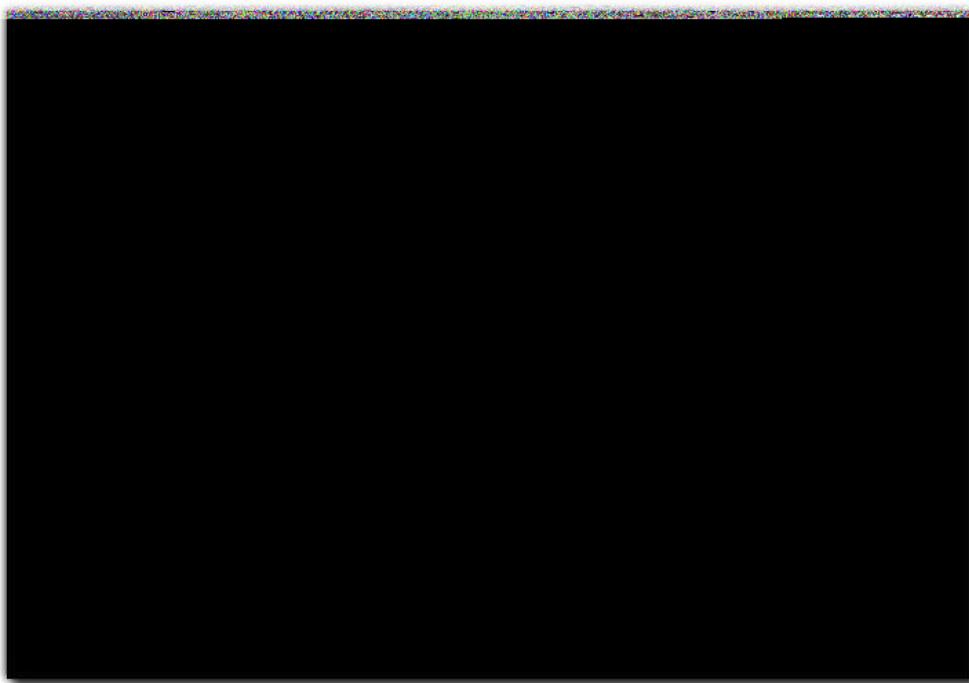
- 원하는 작업 선택 후 수정
- 

3. 작업선택 버튼의 맨 윗줄에 선택한 작업이 등록되어 있는 것을 확인할 수 있습니다.



- 뷰 선택

관리자의 관심에 맞게 여러 가지 뷰를 제공합니다. 뷰를 선택하면 해당 뷰에 맞는 항목들이 자동으로 선택되어 보입니다.

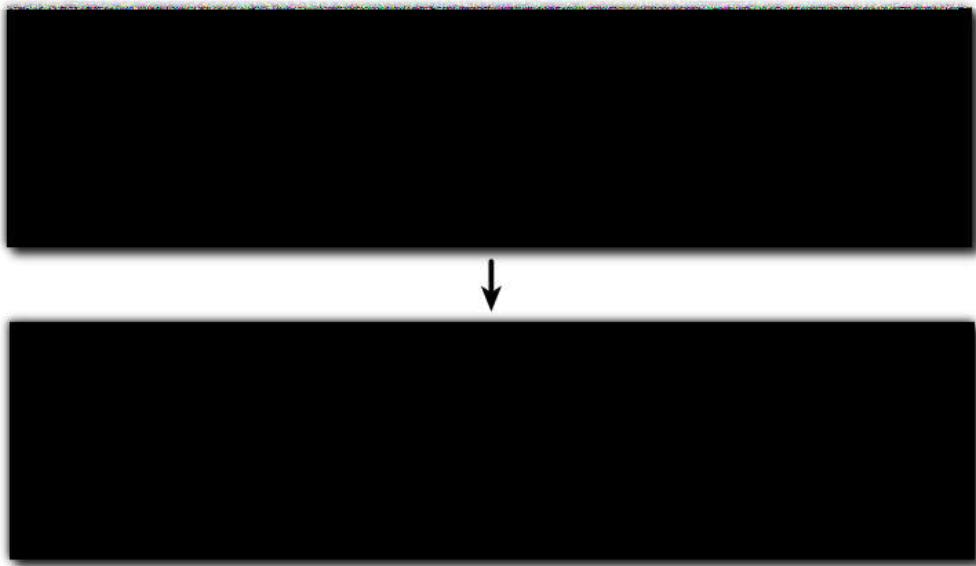


아래표는 뷰와 그 뷰에 기본값으로 설정되어 있는 항목들입니다.

뷰 이름	기본 항목
요약 뷰	장비구분, 위험, 동작, IP주소, MAC주소, 위치
노드 뷰	장비구분, 위험, 동작, IP 주소, MAC주소, 정책, 제어정책, 위치, 호스트명(이름), 플랫폼, 인증사용자
IP 관리 뷰	장비구분, 위험, 동작, IP주소, MAC주소, 정책, 인증사용자, IP용도, IP소유자, IP소유부서, IP만료시각, 장비소유자, 장비소유부서, 위치
위험 뷰	장비구분, 위험, IP주소, MAC주소, 호스트명(이름), 플랫폼, 위험탐지, 위험감지, 위치
패치관리 뷰	장비구분, 위험, IP주소, MAC주소, 호스트명(이름), 플랫폼, 패치모음, 정보수신시각, 패치만족여부, 위치
자산관리 뷰	장비구분, 위험, IP주소, MAC주소, 호스트명(이름), 플랫폼, 정보수신, CPU, 메모리, 저장장치, 인터페이스, 열린포트, 위치
에이전트 액션 뷰	장비구분, 위험, IP주소, MAC주소, 호스트명(이름), 플랫폼, 만족함, 노드정책, 수행전, 만족안함, 위치
인증 사용자 뷰	장비구분, 위험, 동작, IP주소, MAC주소, 정책, 호스트명(이름), 플랫폼, 인증사용자, 최근 사용자인증, 위치
매체사용 관리 뷰	장비구분, 위험, 동작, IP주소, MAC주소, 정책, 호스트명(이름), 플랫폼, 인증사용자ID, 인증사용자, 장치제어

- 관점

노드관점(IP+MAC 기준)과 장비관점(MAC 기준)을 두어 보다 쉽게 장비를 관리할 수 있습니다.



항목	설명
노드관점	IP와 MAC이 존재하는 모든 노드를 보입니다. MAC이 같아도 IP가 다르면 다른 노드로 등록됩니다.
장비관점	MAC 정보를 가진 노드를 모두 보입니다. MAC 주소가 같고 IP 주소는 다를 경우, 하나의 장비로 확인하여 동작 상태가 on인 1개의 노드로 등록됩니다. 하지만 하나의 장비가 각각 다른 IP와 MAC을 가지고 있을 경우, 즉, 여러 인터페이스를 가진 장비일 경우 에이전트가 갈린 MAC과 IP를 기준으로 합쳐집니다.

IP관리

IP관리

관리자는 노드 > 작업선택에서 IP 관리를 통하여 각 노드의 IP와 MAC에 대한 설정을 수행할 수 있습니다.
IP관리의 세부 항목은 다음과 같습니다.



- IP차단
- IP허용 - 총돌보호해제
- IP허용 - 총돌보호(지정MAC)
- MAC차단
- MAC허용 - 변경금지해제
- MAC허용 - 변경금지(지정 IP대역)
- MAC허용 - 변경금지(모든 IP대역)
- IP 및 MAC 차단
- IP 및 MAC 허용
- IP 총돌보호 및 변경금지 설정
- IP사용 신규노드정책 설정
- IP사용 현재사용자인증제한 설정
- IP사용 현재사용자인증제한 해제
- IP사용 호스트명제한 설정
- IP사용 호스트명제한 해제
- IP 사용시간 제한&해제 설정
- MAC 사용시간 제한&해제 설정
- MAC 태그 설정
- IP 소유자&소유부서 설정
- IP용도설정

IP차단

IP차단

관리자는 IP차단 기능을 통하여 IP 기준으로 노드의 네트워크 접속을 차단할 수 있습니다.

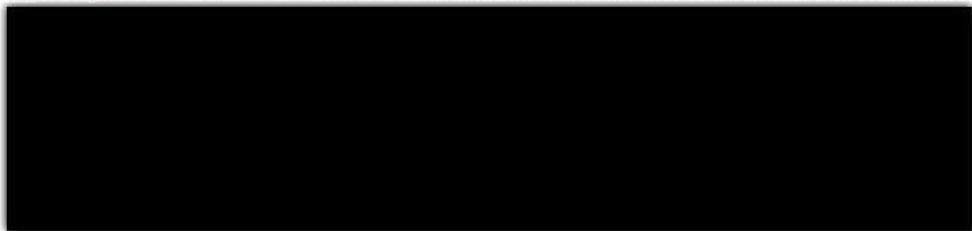
1. IP차단 선택

IP를 차단하고 싶은 노드를 선택 후, 작업선택 > IP관리 > IP차단 을 선택하여 IP를 차단합니다.



2. IP차단 확인

관리 뷰에서 노드IP가 차단되어 있는 모습을 확인할 수 있습니다.



IP차단 수행 시, 반드시 시스템관리 > 센서설정 페이지의 설정항목 중 센서 운영모드가 Active여야 하고, 제어정책의 IP관리 차단 정책이 활성화 되어 있어야 정상적인 차단이 수행됩니다.
IP차단 수행 후에도, 해당 노드의 네트워크가 제어가 되지 않는다면, 위 설정을 확인해 주시기 바랍니다.
센서설정은 [센서관리](#)를 참조해 주시기 바랍니다.

IP허용 - 충돌보호해제

IP허용 - 충돌보호해제

관리자는 노드에 적용되어 있는 IP차단, IP 충돌보호 정책을 IP 허용 기능을 이용하여 해제할 수 있습니다.

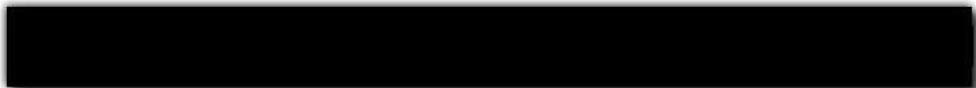
1. IP 허용 선택

IP차단, IP 충돌보호 적용 중인 노드를 선택 후, 작업선택 > IP관리 > IP허용 - 충돌보호해제 를 선택합니다.



2. IP 허용 확인

아래 그림과 같이 IP차단이 해제됩니다.



IP허용 - 충돌보호(지정MAC)

IP허용 - 충돌보호(지정MAC)

관리자는 IP허용 - 충돌보호(지정MAC) 항목 즉, IP 선점 기능을 통하여 해당 노드가 가지고 있는 IP에 해당 노드의 MAC 주소를 매핑합니다. IP는 해당 노드의 MAC만을 허용하기 때문에, 다른 노드에서 해당 IP로 IP 변경을 시도하여 충돌 발생의 위험이 있을 시, 충돌보호설정 되어 있는 쪽의 노드를 보호하고 IP를 변경하여 충돌을 유발한 노드를 차단하고 충돌보호된 노드가 해당 IP를 사용하지 않아도 다른 노드는 충돌보호설정이 된 IP를 사용할 수 없게 하여 보다 안전한 네트워크 환경을 보장합니다. 이는, 공격자가 게이트웨이 등 중요 노드들의 IP를 악의적으로 충돌시켜 내부 네트워크 환경에 악영향을 끼치는 행위를 미연에 방지할 수 있는 기능입니다.(중요노드에 충돌보호설정을 했다고 가정)
작업선택 > IP관리 > IP허용 기능을 이용하여 IP허용 - 충돌보호(지정MAC) 정책을 해제 할 수 있습니다.

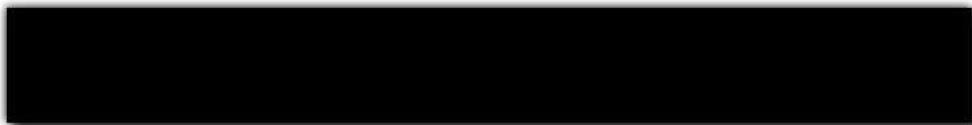
1. IP허용 - 충돌보호(지정MAC) 선택

IP허용 - 충돌보호(지정MAC) 정책을 적용할 노드를 선택 후, 작업선택 > IP관리 > IP허용 - 충돌보호(지정MAC) 를 클릭합니다.



2. IP허용 - 충돌보호(지정MAC) 확인

IP허용 - 충돌보호(지정MAC) 설정 후, 관리뷰에서 확인할 수 있습니다.



3. 충돌보호 위반

MAC 주소 D0:27:88:D5:93:0A를 가지고 있는 노드가 충돌보호 정책이 적용된 IP(172.29.56.25)로 변경할 시 아래의 그림과 같이 D0:27:88:D5:93:0A MAC 주소를 가진 노드는 충돌보호 위반 정책을 적용받게 됩니다.



IP허용 - 충돌보호(지정MAC) 수행 시, 반드시 시스템관리 > 센서설정 페이지의 설정항목 중 센서 운영모드가 Active여야 하고, 제어정책의 IP관리 차단 정책이 활성화되어 있어야 정상적인 차단이 수행됩니다.
충돌위반 정책을 적용받은 후에도, 해당 노드의 네트워크가 제어가 되지 않는다면, 위 설정을 확인해 주시기 바랍니다.
센서설정은 [센서관리](#)를 참조해 주시기 바랍니다.

MAC차단

MAC차단

관리자는 차단하고 싶은 노드의 MAC을 차단하여, 해당 노드의 네트워크를 제어합니다.
MAC 자체를 차단함으로써, IP를 바꾸어도 네트워크 제어가 계속해서 이루어집니다.

1. MAC차단 선택

MAC을 차단하고 싶은 노드를 선택 후, 작업선택 > IP관리 > MAC차단 을 선택하여 해당 노드의 MAC을 차단 설정합니다.



2. MAC차단 관리뷰 확인

선택한 노드가 관리 뷰에서 차단되어 있는 모습을 확인할 수 있습니다.



아래 그림과 같이 172.29.56.15 노드의 IP를 172.29.56.17로 IP 변경 후에도 차단이 풀리지 않는 것을 볼 수 있습니다.



MAC차단 수행 시, 반드시 시스템관리 > 센서설정 페이지의 설정항목 중 센서 운영모드가 Active여야 하고,
제어정책의 IP관리 차단 정책이 활성화 되어 있어야 정상적인 차단이 수행됩니다.
MAC차단 수행 후에도, 해당 노드의 네트워크가 제어가 되지 않는다면, 위 설정을 확인해 주시기 바랍니다.
센서설정은 [센서관리](#)를 참조해 주시기 바랍니다.

MAC허용 - 변경금지해제

MAC허용 - 변경금지해제

관리자는 노드에 적용되어 있는 MAC 차단, IP변경금지 정책을 MAC허용 - 변경금지해제 기능을 이용하여 해제할 수 있습니다.

1. MAC 허용 선택

MAC 차단, IP 변경금지정책을 적용받고 있는 노드를 선택 후, 작업선택 > IP관리 > MAC허용 - 변경금지해제 을 클릭합니다.



2. MAC 허용 확인

MAC 허용 작업 진행 후 관리 뷰에 해당 노드의 MAC 차단이 해제된 것을 볼 수 있습니다.



MAC허용 - 변경금지(지정 IP대역)

MAC허용 - 변경금지(지정 IP대역)

MAC허용 - IP변경금지 기능은 노드의 MAC과 현재 IP를 매핑하여 노드가 IP를 변경할 시 매핑된 IP와 다르므로 IP변경금지 위반 정책을 받게 됩니다.

"MAC허용 - IP변경금지(지정 IP대역)" 기능은 하나의 센터에 여러개의 센서가 존재할 시 즉, 센터가 다수의 네트워크 대역을 관리할 시 이용되는 기능입니다.

노드가 MAC허용 - 변경금지(지정 IP대역) 적용 받을 시 자신의 네트워크 대역의 IP로 IP를 변경할 시 IP변경금지 위반 정책을 적용 받습니다. 다른 네트워크 대역 즉 다른 센서가 관리하는 네트워크 대역의 IP로 IP를 변경할 시 IP변경금지 정책을 적용 받지 않습니다.

IP변경금지 위반 정책을 적용 받을 시 제어정책의 IP관리 차단 정책을 적용받게 되어 네트워크가 차단 됩니다.

NAC DHCP서버에서 IP할당 시 변경금지된 IP를 우선적으로 할당합니다.

작업선택 > IP관리 > MAC허용 기능을 이용하여 MAC허용 - 변경금지(지정 IP대역) 정책을 해제 할 수 있습니다.

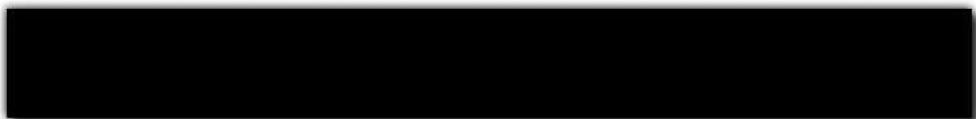
1. MAC허용 - 변경금지(지정 IP대역) 선택

MAC허용 - 변경금지(지정 IP대역)을 적용할 노드를 선택 후, 작업선택 > IP관리 > MAC허용 - 변경금지(지정 IP대역) 을 클릭 합니다.



2. MAC허용 - 변경금지(지정 IP대역) 확인

MAC허용 - 변경금지(지정 IP대역) 설정 후, 관리 뷰에서 확인할 수 있습니다.



3. 자신의 네트워크 대역의 IP로 IP 변경

172.29.56.15 에서 172.29.56.17 로 변경 시 아래 그림과 같이 IP변경금지 위반 정책을 적용받습니다.



4. 다른 네트워크 대역의 IP로 IP 변경

172.29.56.51 에서 172.29.65.51 로 변경 시 아래 그림과 같이 IP변경금지 위반 정책을 적용받지 않습니다.



MAC허용 - 변경금지(지정 IP대역) 수행 시, 반드시 시스템관리 > 센서설정 페이지의 설정항목 중 센서 운영모드가 Active여야 하고, 제어정책의 IP관리 차단 정책이 활성화 되어 있어야 정상적인 차단이 수행됩니다. 자신의 네트워크 IP로 IP변경하여 IP변경 위반 정책을 적용받은 후에도, 해당 노드의 네트워크가 제어가 되지 않는다면, 위 설정을 확인해 주시기 바랍니다.

센서설정은 [센서관리](#)를 참조해 주시기 바랍니다.

MAC허용 - 변경금지(모든 IP대역)

MAC허용 - 변경금지(모든 IP대역)

MAC허용 - IP변경금지 기능은 노드의 MAC과 현재 IP를 매핑하여 노드가 IP를 변경할 시 매핑된 IP와 다르므로 IP변경금지 위반 정책을 받게 됩니다.

"MAC허용 - 변경금지(지정 IP대역)" 기능과의 차이점은 "MAC허용 - 변경금지(모든 IP대역)" 적용된 노드는 다른 네트워크의 IP로 IP를 변경할 시 IP변경금지 위반 정책이 적용됩니다.

IP변경금지 위반 정책을 적용 받을 시 제어정책의 IP관리 차단 정책을 적용받게 되어 네트워크가 차단 됩니다.

NAC DHCP서버에서 IP 할당 시 변경금지된 IP를 우선적으로 할당합니다.

작업선택 > IP관리 > MAC허용 기능을 이용하여 MAC허용 - 변경금지(모든 IP대역) 정책을 해제 할 수 있습니다.

1. MAC허용 - 변경금지(모든 IP대역) 선택

MAC허용 - 변경금지(모든 IP대역)을 적용할 노드를 선택 후, 작업선택 > IP관리 > MAC허용 - 변경금지(모든 IP대역) 을 클릭 합니다.



2. MAC허용 - 변경금지(모든 IP대역) 확인

MAC허용 - 변경금지(모든 IP대역) 설정 후, 관리 뷰에서 확인할 수 있습니다.



3. IP 변경

MAC허용 - 변경금지(모든 IP대역)은 매핑된 IP 외 다른 IP로 변경할 시 아래 그림과 같이 IP변경금지 위반 정책을 적용받습니다.



4. 다른 네트워크의 IP로 IP변경

MAC허용 - 변경금지(지정 IP대역) 기능과는 다르게 아래와 그림과 같이 다른 네트워크 IP로 IP변경 하여도 IP변경금지 위반 정책을 적용 받습니다.



MAC허용 - 변경금지(모든 IP대역) 수행 시, 반드시 시스템관리 > 센서설정 페이지의 설정항목 중 센서 운영모드가 Active여야 하고, 제어정책의 IP관리 차단 정책이 활성화 되어 있어야 정상적인 차단이 수행됩니다. IP변경하여 IP변경 위반 정책을 적용받은 후에도, 해당 노드의 네트워크가 제어가 되지 않는다면, 위 설정을 확인해 주시기 바랍니다.

센서설정은 [센서관리](#)를 참조해 주시기 바랍니다.

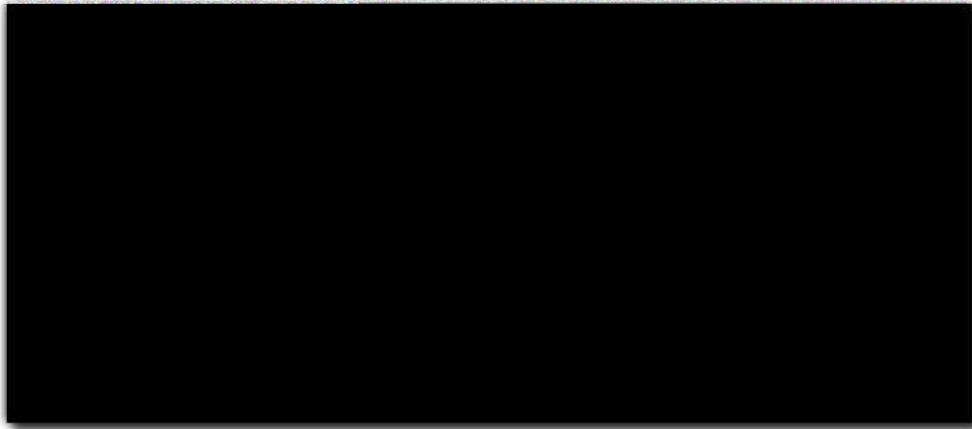
IP 및 MAC 차단

IP 및 MAC 차단

관리자는 원하는 노드의 IP와 MAC을 동시에 차단하여 단번에 네트워크를 차단할 수 있습니다.
네트워크 환경에 악영향을 끼치는 노드가 발생하거나, 위험 노드로 판단되는 노드를 별다른 정책이나 그룹을 만들지 않고 차단할 수 있습니다. 하지만, 해당 기능은 노드의 조건이나 상태를 검사하여 내려지는 차단이 아닙니다. 따라서, 차단해제 방법이 관리자의 IP 및 MAC 허용뿐이 없기 때문에 해당 명령은 신중을 기해야합니다.

1. IP 및 MAC 차단 선택

IP 및 MAC을 차단하고 싶은 노드를 선택 한 후, 작업선택 > IP관리 > IP 및 MAC 차단 을 선택합니다.



2. IP 및 MAC 차단 확인

관리 뷰에서 IP 와 MAC이 차단된 모습을 확인할 수 있습니다.



IP 및 MAC차단 수행 시, 반드시 시스템관리 > 센서설정 페이지의 설정항목 중 센서 운영모드가 Active여야 하고, 제어정책의 IP관리 차단 정책이 활성화 되어 있어야 정상적인 차단이 수행됩니다.
IP 및 MAC차단 수행 후에도, 해당 노드의 네트워크가 제어가 되지 않는다면, 위 설정을 확인해 주시기 바랍니다.
센서설정은 [센서관리](#)를 참조해 주시기 바랍니다.

IP 및 MAC 허용

IP 및 MAC 허용

관리자는 IP 혹은 MAC이 차단되어 네트워크 접속을 제어 받고 있는 노드를 IP 및 MAC 허용 기능을 통하여, 차단되어있는 IP 및 MAC을 차단 해제할 수 있습니다.

1. IP 및 MAC 허용 선택

IP 혹은 MAC이 차단되어있는 노드를 선택 후, 작업선택 > IP관리 > IP 및 MAC 허용 을 선택합니다.



2. IP 및 MAC 허용 확인

IP 및 MAC 허용 작업 진행 후, 관리 뷰에서 해당 노드의 IP 및 MAC 차단이 해제된 것을 볼 수 있습니다.



IP 충돌보호 및 변경금지 설정

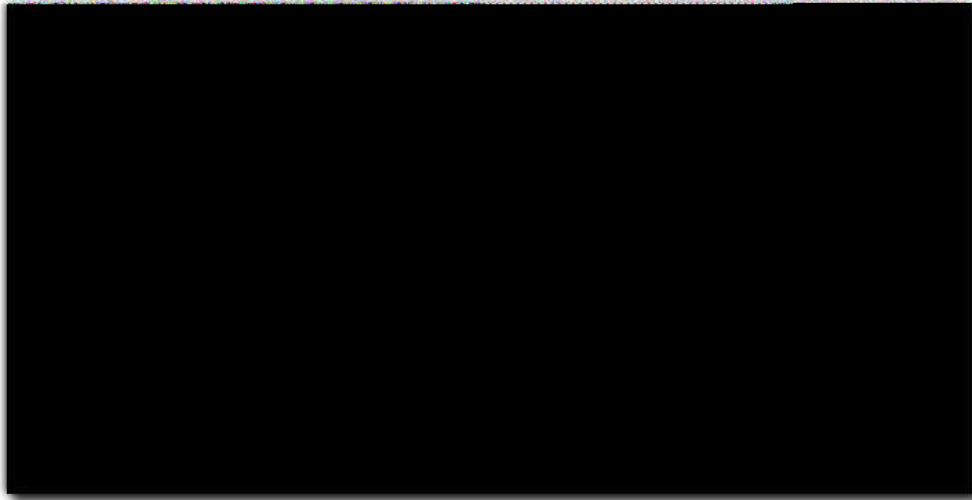
IP 충돌보호 및 변경금지 설정

해당 기능은 IP허용 - 충돌보호(지정MAC)와 MAC허용 - 변경금지(모든 IP대역)를 동시에 설정합니다.

충돌보호와 변경금지에 대한 자세한 내용은 [IP허용 - 충돌보호\(지정MAC\)](#)와 [MAC허용 - 변경금지\(모든 IP대역\)](#)를 참조해 주시기 바랍니다.

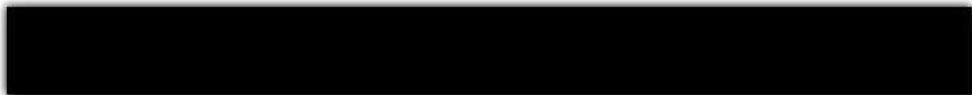
1. IP 충돌보호 및 변경금지

충돌보호와 변경금지를 설정하고 싶은 노드를 선택한 후, 작업선택 > IP관리 > IP 충돌보호 및 변경금지 설정 을 선택합니다.



2. IP 충돌보호 및 변경금지 설정 확인

IP 충돌보호 및 변경금지를 설정한 후, 관리 뷰의 노드상세정보 > IP관리 에서 이를 확인할 수 있습니다.



IP사용 신규노드정책 설정

IP사용 신규노드정책 설정

관리자는 미사용 IP에 IP사용 신규노드정책 설정하여 해당 IP를 사용하는 노드에게 신규노드정책을 적용합니다.
해당 노드가 사용중 IP인 경우, 설정된 IP사용 신규노드정책을 적용 받지 않습니다. (단, 사용중인 IP에 해당 하는 MAC이 변경 되면, 신규노드로 등록되어 그 정책을 적용 받습니다.)
미사용 IP에 IP사용 신규노드정책을 설정하고 싶은 경우 미사용 IP를 노드 관리 뷰에 등록하여야 합니다. 미사용 IP 등록방법은 시스템관리에서 미사용 IP 등록 부분을 참고 바랍니다.

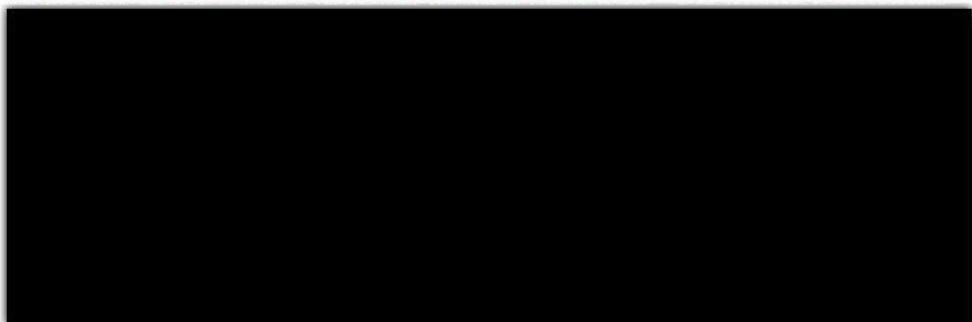
1. IP사용 신규노드정책 선택

작업선택 > iP관리 > IP사용 신규노드정책 을 클릭합니다.



2. IP사용 신규노드정책 설정

IP사용 신규노드정책 설정 팝업 창에서 MAC 허용, 총돌보호설정, 변경금지설정, 총돌보호/변경금지설정 중 한 가지를 선택하여 설정 버튼을 클릭합니다.



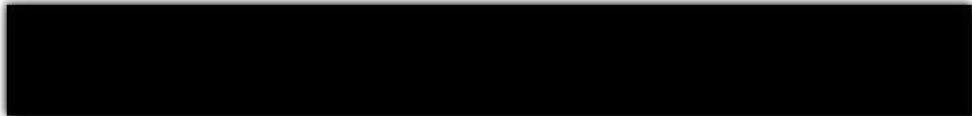
3. IP사용 신규노드정책 확인

관리 > 노드 > 노드상세정보 > IP관리에서 확인할 수 있습니다.



4. IP사용 신규노드정책 설정한 IP 사용

신규노드정책 설정한 IP 사용할 시 아래의 그림과 같이 신규노드정책을 적용받습니다.



IP사용 현재사용자인증제한 설정

IP사용 현재사용자인증제한 설정

현재사용자인증제한 기능은 현재 노드에 인증되어있는 인증 사용자 정보와 노드의 IP를 매핑 시켜 해당 노드에 다른 사용자의 ID로 인증을 할 수 없도록 하는 기능입니다.

1. IP사용 현재사용자인증제한 설정

IP사용 현재사용자인증제한을 설정하고 싶은 노드를 선택 후(현재 해당노드의 사용자인증 정책에 test1이라는 아이디로 설정되어 있는 상태), 작업관리 > IP관리 > IP사용 현재사용자인증제한 설정 을 선택합니다.



2. 사용자인증제한의 확인

관리뷰와 관리 > 노드 > 노드상세정보 > 정책 페이지에서 test1 계정으로 설정된 사용자 제한을 확인할 수 있습니다.



3. 다른 사용자의 접속 시도

test1계정으로 사용자인증제한이 설정되어 있는 노드에 other라는 계정으로 인증을 시도했을 시, 아래 그림과 같이 인증이 되지 않습니다.



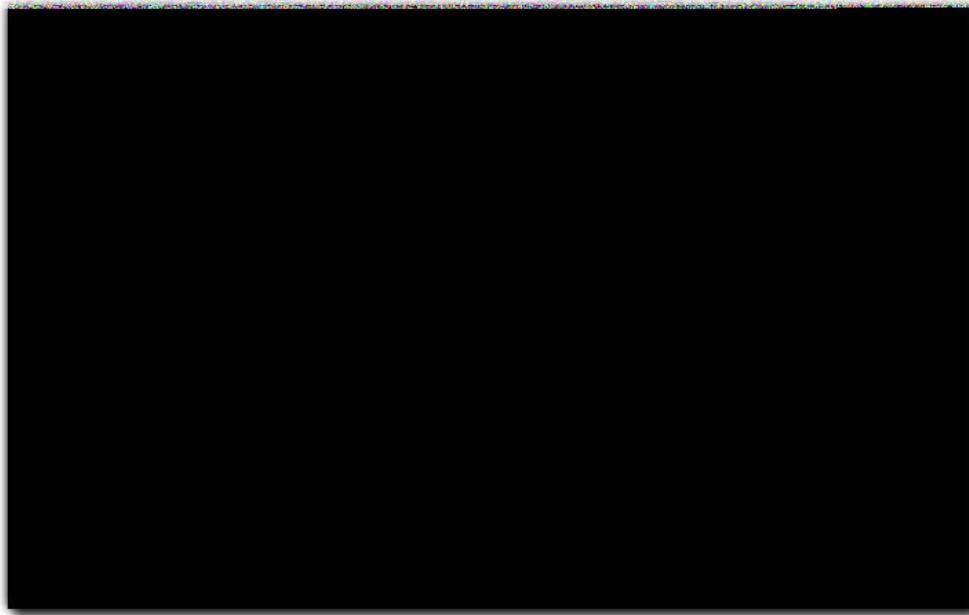
IP사용 현재사용자인증제한 해제

IP사용 현재사용자인증제한 해제

관리자는 IP사용 현재사용자인증제한을 해제할 수 있습니다.

1. IP사용 현재사용자인증제한 해제 선택

IP사용 현재사용자인증제한을 해제하고 싶은 노드를 선택 후, 작업관리 > IP관리 > IP사용 현재사용자인증제한 해제 를 선택합니다.



2. IP사용 현재사용자인증제한 해제 확인

노드상세정보 > 정책 페이지에서 test1 계정으로 걸린 사용자 제한이 해제되어있는 것을 확인할 수 있습니다.



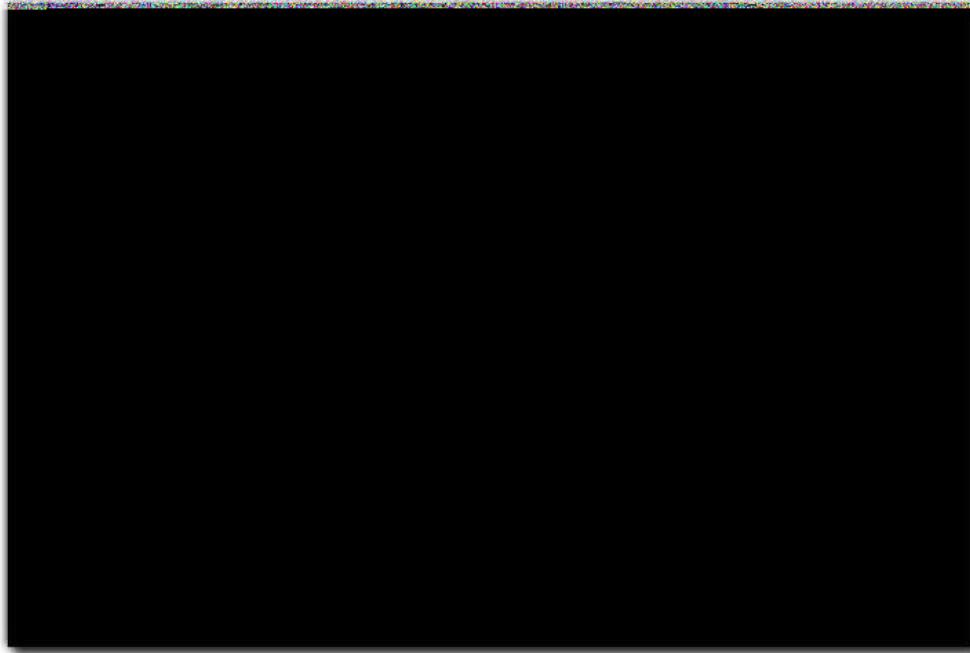
IP사용 호스트명제한 설정

IP사용 호스트명제한 설정

관리자는 IP사용 호스트명제한 설정 작업을 이용하여 많은 노드들의 호스트명을 일정하게 맞추어 관리할 수 있습니다. 또한 제어 정책에 따라 관리자가 설정한 호스트명이 아닐 시, 네트워크가 차단되도록 할 수 있습니다.

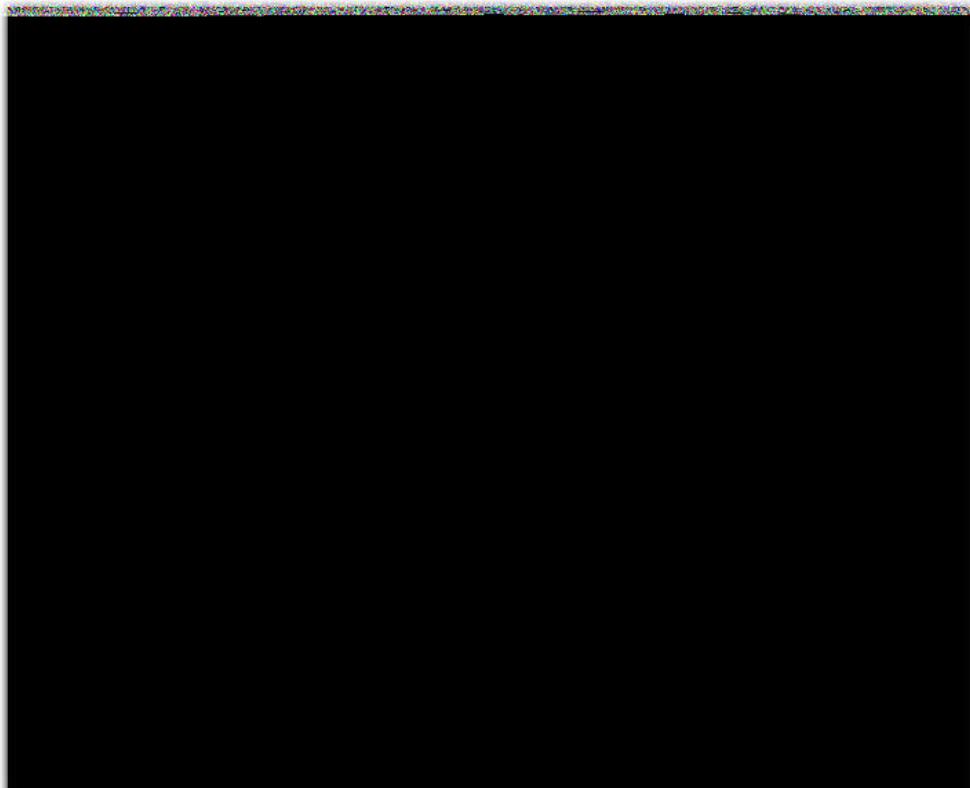
1. IP사용 호스트명제한 설정

IP사용 호스트명제한을 설정하고 싶은 노드를 선택 후, 작업선택 > IP관리 > IP사용 호스트명제한 설정 을 선택합니다.



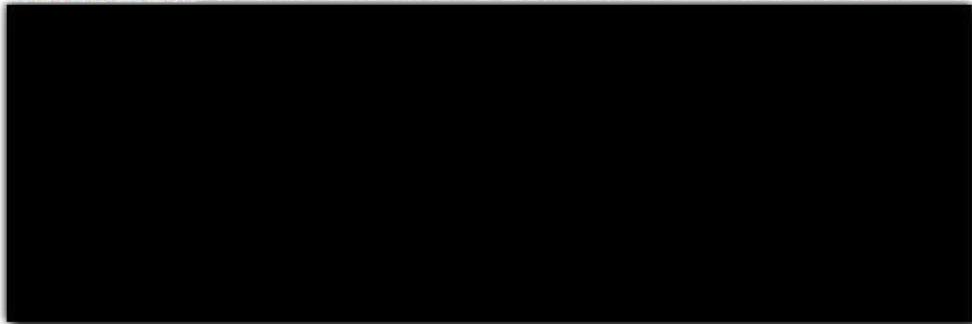
2. 호스트명 설정

관리자는 관리목적에 맞추어 호스트명을 설정합니다. 매크로를 클릭하여 원하는 목적에 맞는 호스트명을 설정할 수 있습니다.



3. 호스트명 제한 확인

노드상세정보 > 정책 페이지에서 아래 그림과 같이 김철수_100이라는 호스트명 제한이 설정되어 있는 것을 확인할 수 있습니다.
(호스트명 템플릿을 {AUTHNAME}_{IP3}으로 설정)

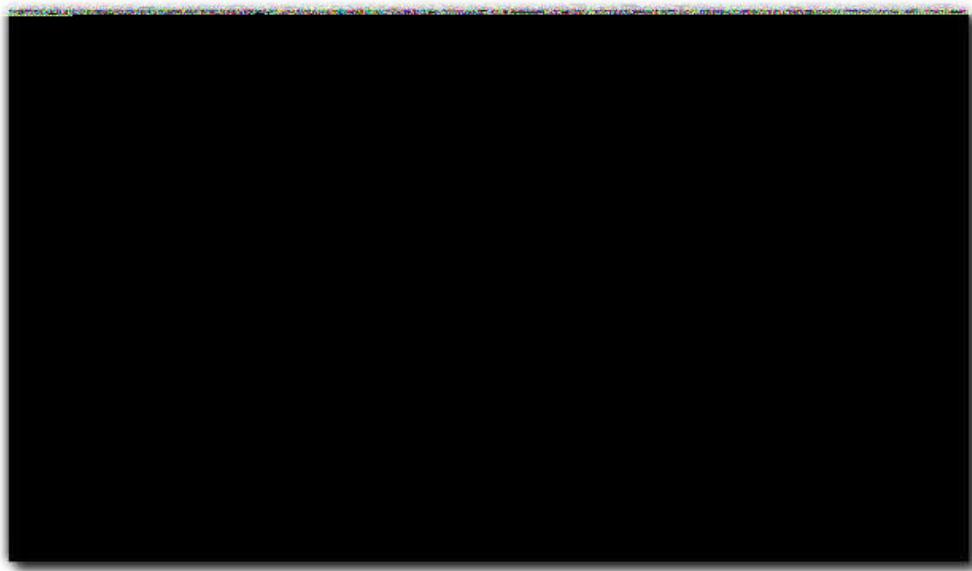


관리 뷰에서 호스트명을 위반한 노드는 정책컬럼에서 아이콘이 표시됩니다.



4. 호스트명 제한 제거

제어정책에서 호스트명 위반 노드 차단정책을 생성한 후(제어정책 생성법은 제어정책을 참조해주시기 바랍니다.)
호스트명을 위반한 노드로 네트워크 접속 시 아래 그림과 같이 CWP 페이지로 유도되며, CWP 페이지에서 컴퓨터 이름
변경아이콘을 이용하여 간편하게 호스트명을 변경할 수 있습니다.



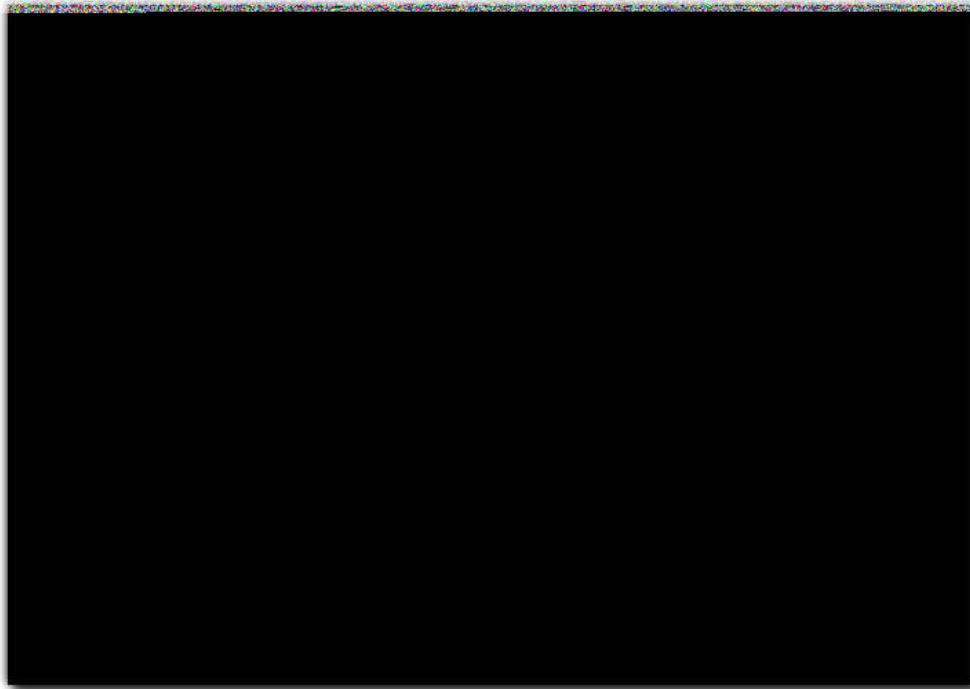
IP사용 호스트명제한 해제

IP사용 호스트명제한 해제

관리자는 호스트명 제한을 해제할 수 있습니다.

1. IP사용 호스트명제한 해제

IP사용 호스트명제한을 해제하고 싶은 노드를 선택 후, 작업관리 > IP관리 > IP사용 호스트명제한 해제 를 선택합니다.



2. IP사용 호스트명제한 해제

관리뷰와 노드상세정보 페이지에서 IP사용 호스트명제한이 해제된 것을 확인할 수 있습니다.



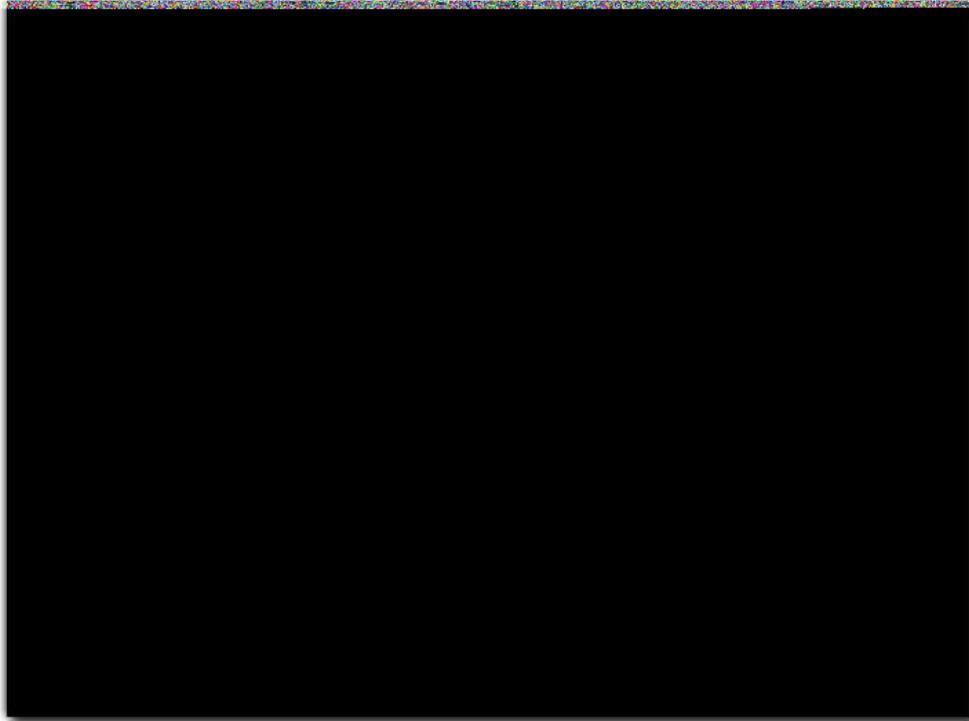
IP 사용시간 제한&해제 설정

IP 사용시간 제한/해제 설정

관리자는 IP 사용시간 설정을 통해 사용자에게 원하는 시간만큼만 IP를 할당해 줄 수 있습니다. 사용시간이 지나면 자동으로 IP가 차단됩니다.

1. IP 사용시간 제한/해제 설정

IP 사용시간을 제한/해제 하고싶은 노드를 선택 후, 작업선택 > IP관리 > IP 사용시간 제한/ 해제 를 선택합니다.



2. IP 사용시간 제한/해제 팝업

IP 사용시간 제한/ 해제를 선택하면 아래 그림과 같은 사용시간 설정 팝업이 생성되어, 시간을 설정할 수 있습니다.



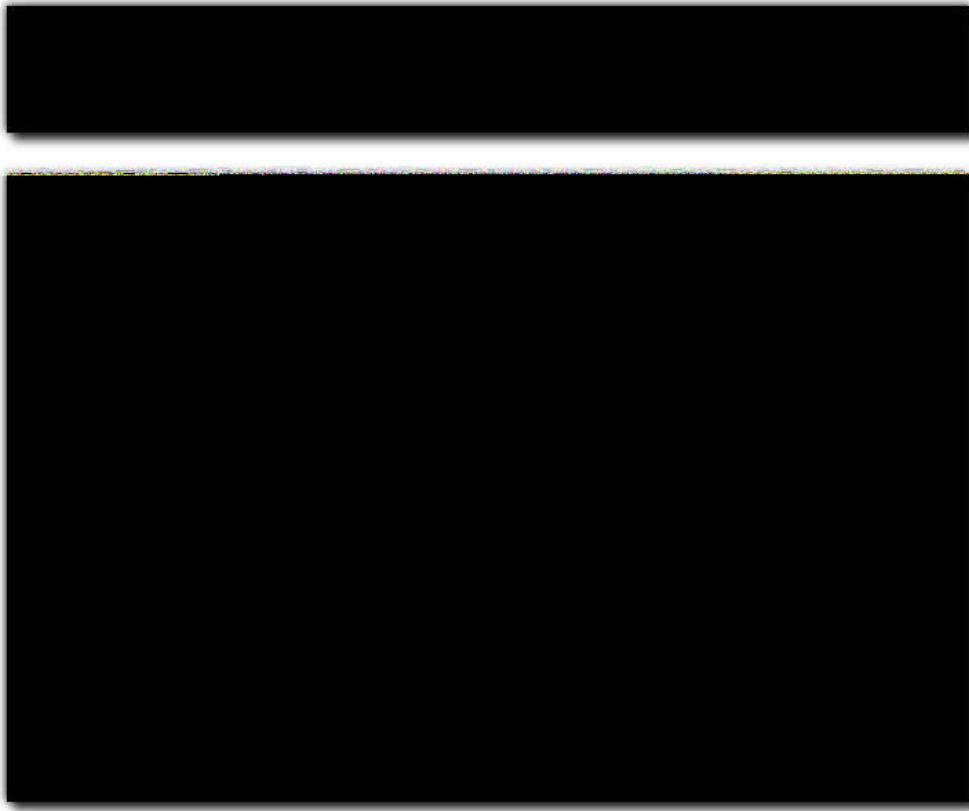
IP사용 시작/종료 항목에 있는 체크박스를 체크하여야만 IP사용 시작/종료를 설정할 수 있습니다.

IP사용 종료 항목만 설정하였을 경우 설정한 종료 시각 이전에는 IP를 사용할 수 있으며 설정한 종료 시각이 지났을 경우 IP가 차단됩니다.

IP/MAC 사용 시간을 만료한 노드의 처리 방법은 IP 관리에서 IP/MAC사용만료처리방법 항목을 참고하시기 바랍니다.

3. IP 사용시간 설정 확인

관리 뷰의 정책 컬럼의 아이콘과 노드상세정보 > IP관리 > IP정책 페이지에서 확인 가능합니다.



4. 시간 만료 시 IP 차단

ip 관리 페이지에서 IP/MAC사용만료처리방법 설정이 삭제안함 일 경우, 설정한 시간을 만료했을 시 IP가 자동 차단됩니다.



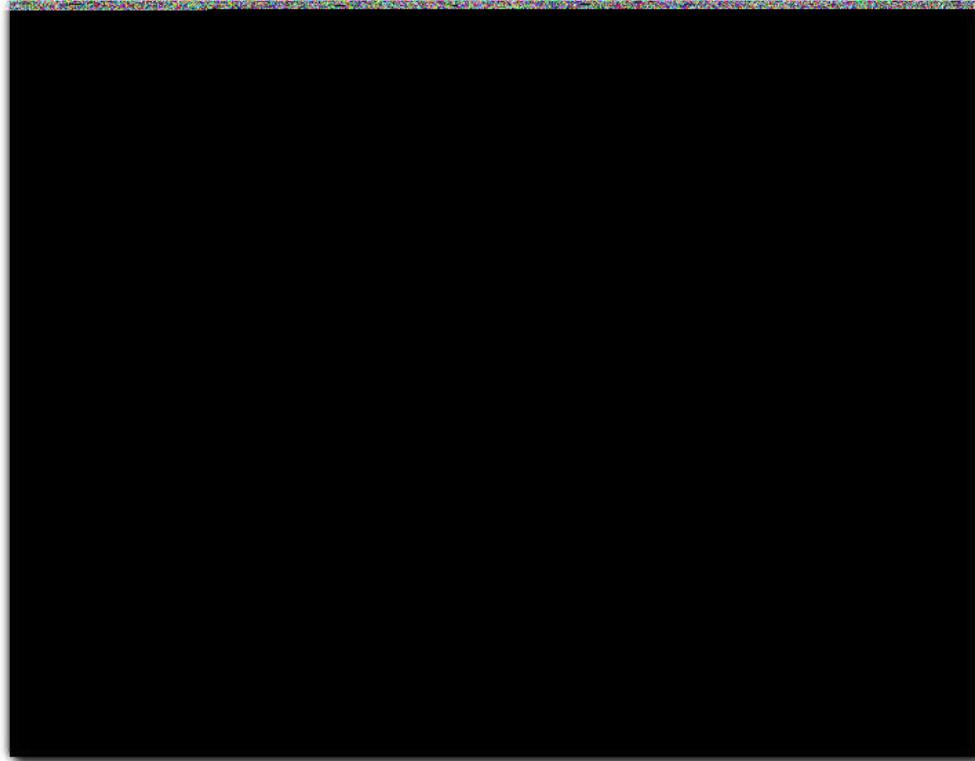
MAC 사용시간 제한&해제 설정

MAC 사용시간 제한/해제 설정

관리자는 MAC 사용시간 설정을 통해 사용자에게 원하는 시간만큼만 MAC을 할당해 줄 수 있습니다. 사용시간이 지나면 자동으로 MAC이 차단됩니다.

1. MAC 사용시간 제한/해제

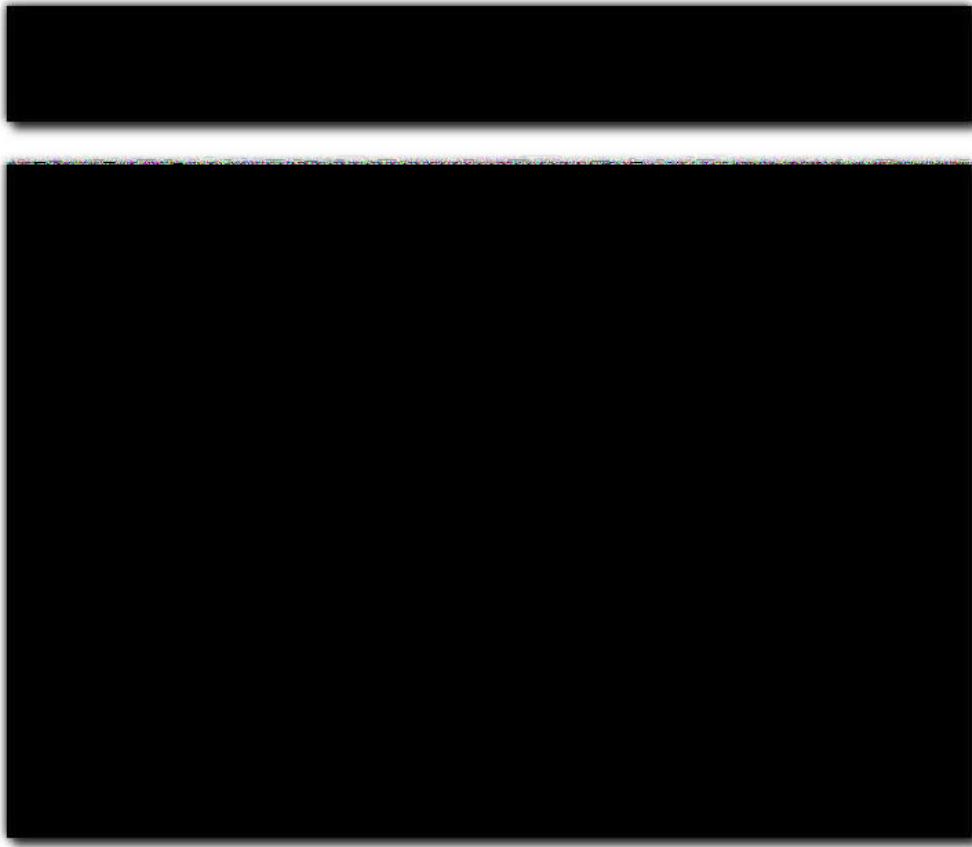
MAC 사용시간을 제한/해제 하고싶은 노드를 선택 후, 작업선택 > IP관리 > MAC 사용시간 제한/ 해제 를 선택합니다.



2. 상세 설정법은 [IP 사용시간 설정 페이지](#)의 IP 사용시간 제한/해제와 같습니다.

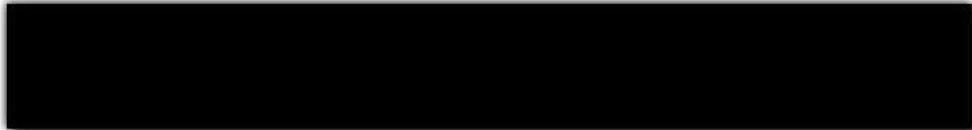
3. MAC 사용시간 설정 확인

관리 뷰의 정책 컬럼의 아이콘과 노드상세정보 > IP관리 > MAC정책에서 확인 가능합니다.



4. 시간 초과 시 MAC 차단

ip 관리 페이지에서 IP/MAC사용만료처리방법 설정이 삭제 안 함 일 경우, 설정한 시간을 초과했을 시, MAC이 자동 차단됩니다.



MAC 태그 설정

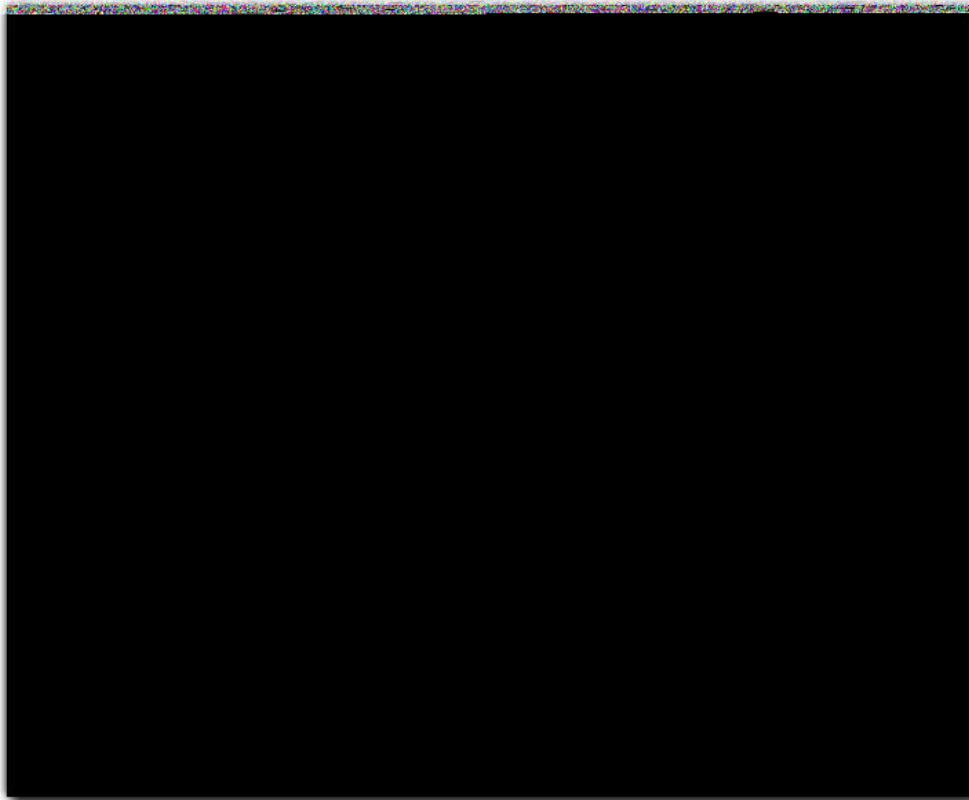
MAC 태그

MAC 태그는 MAC에 붙이는 일종의 꼬리표로, 관리자는 IP에 영향을 받지 않는 MAC에 태그를 설정합니다. 관리자는 MAC에 태그를 설정함으로써 장비의 IP가 변경되어도 해당 장비에 태그가 해제되지 않아 태그를 조건으로 설정한 정책은 계속적으로 정책을 내리고, 태그를 조건으로 노드그룹을 만들 수 있습니다.

태그를 설정하려면 먼저 태그가 생성돼 있어야 합니다. 태그 생성법은 [태그 관리를](#) 참조해 주시기 바랍니다.

1. MAC 태그 설정

MAC 태그를 설정하고 싶은 노드를 선택 후, 작업선택 > IP관리 > MAC 태그 설정 을 선택합니다.



2. 태그 설정 팝업

태그 설정을 선택하면 아래와 같은 태그설정 팝업생성되어 태그를 설정할 수 있습니다.

태그를 만드는 방법은 [태그 관리](#)를 참고하시기 바랍니다.

태그관리 페이지에서 만들어진 태그 목록들이 보이며, 태그유지기간을 설정할 수 있습니다.

기간 설정 시 해당 기간이 지나면 태그가 자동으로 회수됩니다.(아래 그림을 예로 보면, 방문자용 임시사용 태그는 12월 5일 오후 5시가 지나면 자동으로 회수됩니다.)



3. 태그확인

설정된 태그는 장비상세정보 > 기본정보 페이지와 장비상세정보 > IP관리 > MAC 정책 페이지에서 확인할 수 있습니다.

 마크 선택 시, 설정돼있던 태그가 해제됩니다.



IP 소유자&소유부서 설정

IP 소유자/소유부서 설정

관리자는 생성되어 있는 사용자/부서를 바탕으로 IP 소유자/소유부서 설정을 하여 IP에 소유자와 소유부서를 지정할 수 있습니다.
노드그룹을 생성 시, 소유자/소유부서를 조건으로 그룹을 생성할 수 있습니다.

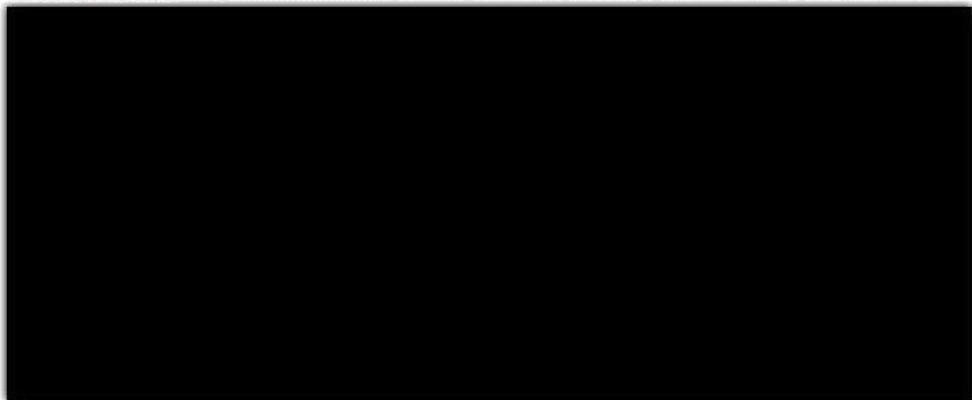
1. 소유자/소유부서 선택

작업선택 > IP관리 > IP 소유자/소유부서 설정 을 선택합니다.



2. 소유자/소유부서 설정

생성되는 팝업에서 소유자/소유부서를 설정할 수 있습니다.





3. 소유자/소유부서 설정 확인

노드상세정보 > IP관리 > IP정책에서 설정내용을 확인할 수 있습니다.



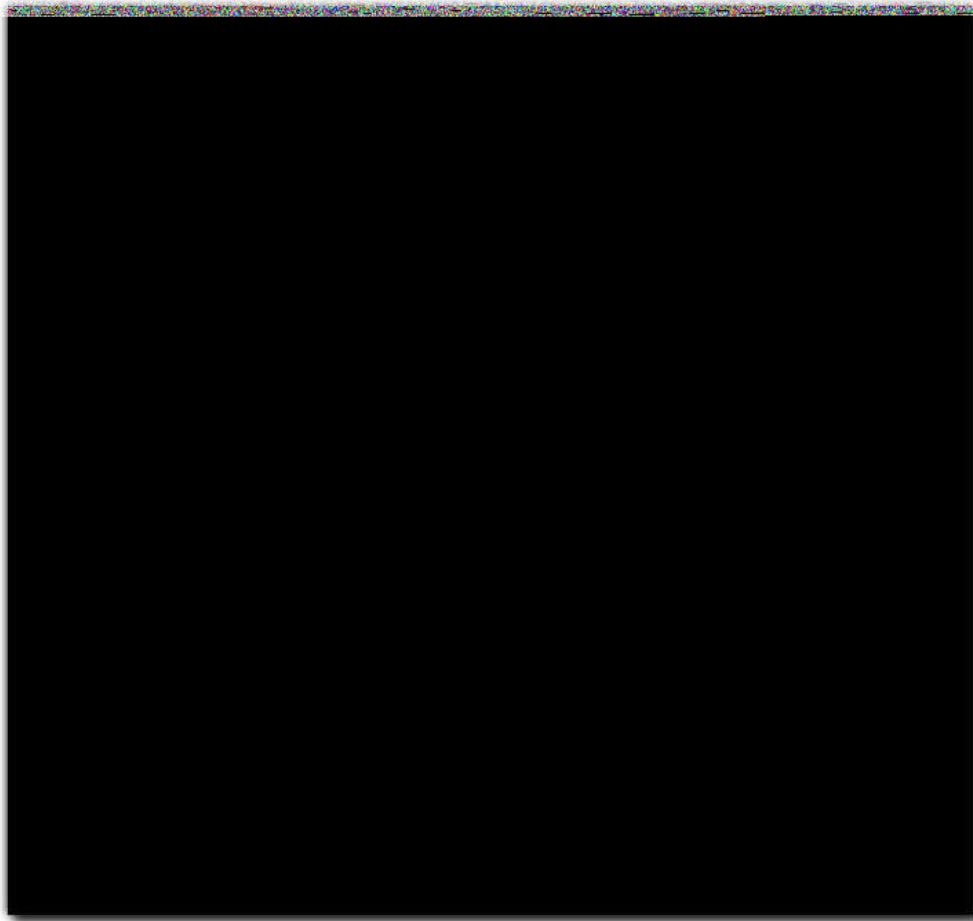
IP용도설정

IP용도설정

관리자는 선택한 노드 IP에 용도를 지정할 수 있습니다.
노드그룹 생성 시 용도를 조건으로 그룹을 생성할 수 있습니다.

1. IP용도설정 선택

작업선택 > IP관리 > IP용도설정 을 선택합니다.



2. 용도설정 팝업

용도설정을 선택하면 생성되는 팝업에서 IP용도를 선택할 수 있습니다.
IP용도에는 유동, 지정 IP 사용, 임시사용자 세 가지가 있습니다.



3. IP용도설정 확인

노드상세정보 > IP관리 > IP정책에서 설정된 용도를 확인할 수 있습니다.



노드 장비 관리

노드 장비 관리

관리자는 노드 > 노드장비관리 를 통하여, 노드를 직접 등록, 삭제하고 태그도 부여할 수 있습니다.

노드 관리의 항목은 다음과 같습니다.



- 노드등록
- 노드일괄등록
- 노드삭제
- 노드 태그 설정
- 사용자인증해제
- 사용자 재인증 설정&해제
- 노드위협해제
- 관리센서변경
- 노드속성 가져오기
- 장비속성 가져오기
- 장비 소유자설정
- 장비 소유부서설정

노드등록

노드등록

Genian NAC는 동작 중인 노드가 삭제되면 자동으로 재탐지하여 해당 노드를 노드 리스트에 다시 등록합니다. 하지만, 삭제된 직후 해당 노드의 통신이 끊겼거나, 삭제된 노드의 시스템이 종료된 경우 재탐지가 이루어지지 않습니다. 이때, 관리자는 노드 등록을 통하여 수동으로 노드를 등록할 수 있습니다.

1. 노드등록 선택

작업선택 > 노드관리 > 노드등록 을 선택합니다.



2. 노드등록 팝업

노드 등록을 선택하면 아래 그림과 같은 팝업이 생성되어, 노드를 등록할 수 있습니다.
IP와 MAC 주소를 기입하면 노드가 등록됩니다.

IP 주소 형태 : 예) 192.168.0.35
MAC 주소 형태 : 예) 40:61:86:EF:55:49



항목	설명
IP 주소	등록할 노드의 IP주소를 입력합니다.

미사용IP다중등록	다수의 노드를 등록할 경우 등록할 노드 수를 입력합니다, IP 뒷자리가 1씩 증가하며 생성됩니다.
IP정책설정	IP 충돌보호 설정된 상태로 노드가 생성됩니다.
IP사용 시작	IP 사용 시작 시각을 설정합니다.
IP사용 종료	IP 사용 종료 시각을 설정합니다, 설정한 시각이 지나면 IP가 차단됩니다.
IP사용 신규노드정책	IP신규노드정책이 설정된 상태로 노드가 생성되며, 이후 등록한 노드의 IP를 사용한 노드는 신규노드정책을 적용받습니다.
MAC 주소	등록할 노드의 MAC주소를 입력합니다.
MAC정책설정	MAC 변경금지 설정된 상태로 노드가 생성됩니다.
MAC사용 시작	MAC 사용 시작 시각을 설정합니다.
MAC사용 종료	MAC 사용 종료 시각을 설정합니다, 설정한 시각이 지나면 MAC이 차단됩니다.
관리센서	등록할 노드를 관리하는 센서를 설정합니다.
노드타입	등록할 노드의 노드타입을 설정합니다.
노드삭제 금지	노드삭제 금지 여부를 설정합니다.

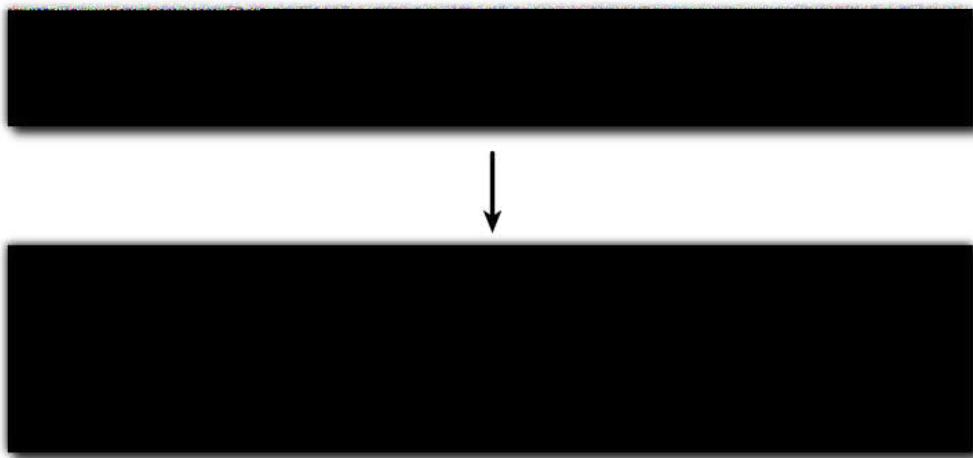
노드일괄등록

노드일괄등록

관리자는 CSV 파일을 이용하여 한번에 많은 양의 노드를 손쉽게 등록할 수 있습니다.
CSV 파일은 [노드속성 가져오기](#)를 참조해 주시기 바랍니다.

1. 노드일괄등록 csv 파일 생성

엑셀을 이용하여 노드 일괄 등록을 작성 합니다.
csv 파일에 작성한 설정값을 바탕으로 노드가 생성됩니다. 아래의 그림과 같이 csv 파일을 일괄 등록할 시
MAC DO:27:87:D2:98:0C, IP 172.29.56.5, IP사용 시작시간 2013년 7월 16일 10시 35분, iP사용 종료시간 2013년 7월 16일 10시
37분 으로 설정됩니다.
SENSORNID는 설정하지 않을 경우 업로드를 수행 시 선택한 센서의 NID가 적용됩니다.



더욱 다양한 설정을 하고 싶을 경우 아래의 표를 참고해 주시기 바랍니다.

항목	설명	입력
IP	IP	x.x.x.x 형식으로 입력
MAC	MAC	xx:xx:xx:xx:xx:xx 형식으로 16진수 입력
SENSORNID	센서 NID	유효한 센서의 노드ID
NAME	노드 이름	관리자 임의 입력
DESC	노드 설명	관리자 임의 입력
PERM	삭제 금지	삭제금지 on = 1 삭제금지 off = 0
GENIDEV	노드 태입	PC = 20 모바일 = 21 서버 = 40 네트워킹장비 = 60 무선접속장비 = 61 라우터 = 62 스위치 = 63 보안장비 = 64 프린터 = 80 VOIP = 90 기타 = 100
PLATFORM	플랫폼	관리자 임의 입력

IPBEGIN	IP사용시작	YYYY-MM-DD hh:mm:ss
IPEND	IP사용종료	YYYY-MM-DD hh:mm:ss
MACBEGIN	MAC 사용 사용시간 설정	YYYY-MM-DD hh:mm:ss
MACEND	MAC 사용 종료시간 설정	YYYY-MM-DD hh:mm:ss
IPALLOW	IP 허용 설정	IP 허용 on = 1
IPPROTECT	IP 충돌보호 설정	IP 충돌보호 on = 1
MACALLOW	MAC 허용	MAC 허용 on = 1
		IP 충돌보호 설정 off = 0
BLOCKIPCHANGE	IP 변경금지 설정	IP 변경금지 on = 1
		IP 변경금지 off = 0
ALLOWFIRSTMAC	신규노드정책 설정	신규노드정책 MAC 허용 on = 1
		신규노드정책 IP 충돌보호 on = 2
		신규노드정책 IP 변경금지 on = 3
		신규노드정책 IP 충돌보호 + IP 변경금지 on = 4
REASON	사유 입력	관리자 임의 입력
CUSTOM01~09	노드 사용자정의필드 1~9	관리자 임의 입력
DEVNAME	장비이름	관리자 임의 입력
DEVDESC	장비설명	관리자 임의 입력
DEVCUSTOM01~09	장비 사용자정의필드 1~9	관리자 임의 입력

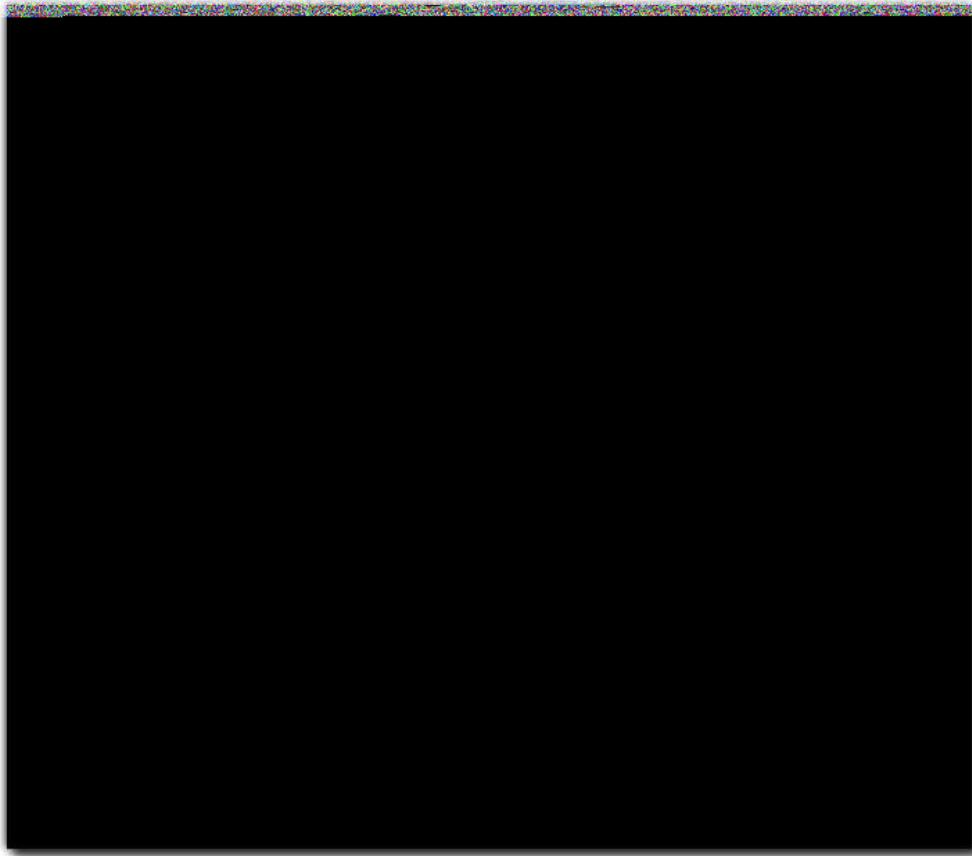
2. 노드일괄등록 선택

작업선택 > 노드관리 > 노드일괄등록 을 선택합니다.



3. 노드일괄등록 팝업

노드일괄등록을 선택 시 아래그림과 같은 팝업이 뜹니다.
CSV 파일을 업로드하고 관리센서를 선택합니다.



4. 노드일괄등록설정 확인

노드 관리 뷰와 노드 상세 정보 페이지에서 제대로 설정된 것을 확인할 수 있습니다.



노드삭제

노드삭제

관리자는 노드삭제를 이용하여 불필요한 노드를 삭제할 수 있습니다.
시스템과 통신이 제대로 동작하는 노드는 삭제를 하여도 재탐지를 통해 노드 리스트에 재등록됩니다.

1. 노드삭제 선택

삭제하고 싶은 노드를 선택 후, 작업선택 > 노드관리 > 노드삭제 를 선택합니다.



위 그림에서 삭제하려는 노드는 설치되어 있다가 현재는 장비를 다른곳으로 옮겨 노드 리스트에 필요가 없는 노드정보입니다.

2. 노드삭제 확인

노드삭제를 하고 난 후, 관리 뷰에서 노드가 정상적으로 삭제된 것을 볼 수 있습니다.



노드삭제 금지

노드삭제를 방지하는 노드삭제 금지 기능이 있습니다.

1. 노드 상세 정보

노드 상세 정보 페이지로 이동합니다.



2. 노드삭제 금지 설정

정책 > 노드관리설정 에 노드삭제 금지를 설정할 수 있는 항목이 존재합니다.
옵션을 On으로 선택하면 해당 노드는 삭제가 금지됩니다.



3. 노드삭제 금지 설정 확인과 삭제시도

노드삭제 금지가 설정 되어있는 모습을 아래 그림과 같이 확인할 수 있습니다.



노드삭제 금지가 설정되어 있는 노드를 삭제 시도 시, 아래와 같은 메시지를 띄우며 삭제가 되지 않습니다.



센터/센서의 삭제

1. 센터/센서 삭제 시도

일반 노드와 달리 센터/센서는 작업선택 > 노드관리 > 노드삭제에서 삭제 시도 시, 아래 그림과 같은 메시지를 출력하며 삭제되지 않습니다.



2. 센터/센서의 상세화면

센터/센서는 상세화면에서 삭제가 가능합니다.

센터/센서 삭제 시, 해당 장비가 가지고 있던 모든 정보도 함께 삭제되오니 주의해 주시기 바랍니다.



노드 태그 설정

노드 태그 설정

노드태그는 노드에 붙이는 일종의 꼬리표입니다. 관리자는 노드(IP+MAC)에 태그를 설정하여 해당 태그를 조건으로 그룹을 생성할 수 있습니다.

IP를 변경하여도 MAC이 변하지 않는 이상 태그 값이 계속 설정되어 있는 MAC태그와 달리, 노드태그는 노드(IP+MAC)에 설정되는 것이기 때문에, IP나 MAC변경 시에 태그가 해제됩니다.

태그를 설정할 당시의 IP와 MAC만이 해당 태그를 사용할 수 있습니다.

태그를 설정하려면 먼저 태그가 생성되어 있어야 합니다. 태그 생성 법은 [태그 관리](#)를 참조해 주시기 바랍니다.

1. 노드 태그 설정 선택

노드태그를 설정하고 싶은 노드를 선택 후, 작업선택 > 노드관리 > 노드 태그 설정 을 선택합니다.



2. 노드 태그 설정 팝업

노드 태그 설정을 선택하면 아래 그림과 같은 노드 태그 설정 팝업이 생성되어, 생성되어져 있는 태그를 선택할 수 있습니다.



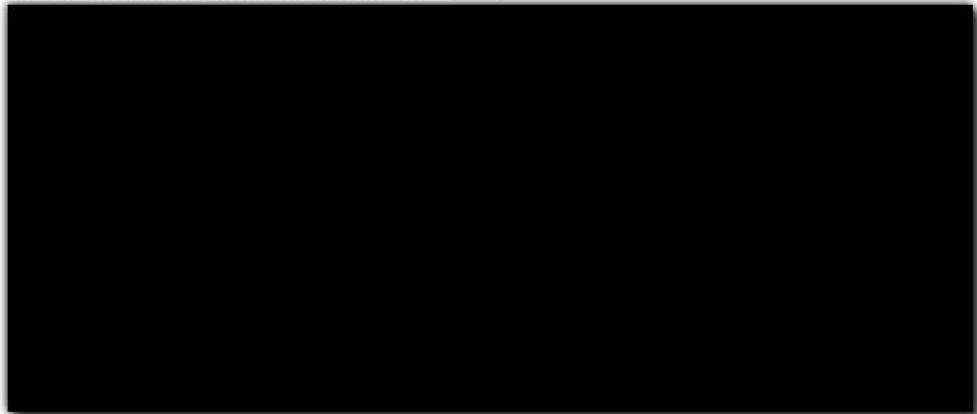
3. 노드 태그 설정 확인

같이 노드 상세 화면에서 설정한 태그를 확인할 수 있으며, 태그를 추가 및 삭제할 수 있습니다.



노드 태그 삭제

노드 태그의 설정내용을 삭제하는 법은 태그를 설정하는 절차와 같습니다. 단지, 삭제하고 싶은 태그를 설정하지 않고 설정을 버튼을 클릭합니다.



사용자인증해제

사용자인증해제

사용자인증해제 기능은 인증되어 있는 사용자의 인증 상태를 해제하는 기능입니다.
관리자가 인증되어있는 사용자의 인증을 해제하여 사용자의 재인증을 유도합니다.

1. 인증 내역 확인

노드 상세 정보 > 기본정보에서 인증 사용자 정보를 확인합니다.



2. 사용자인증해제 선택

노드 선택 후, 작업관리 > 노드관리 > 사용자인증해제 를 선택합니다.



3. 인증 내역 재확인

인증이 제대로 해제되었는지 노드 상태 정보 > 기본정보에서 인증 사용자 정보를 확인합니다.



사용자 재인증 설정&해제

사용자 재인증 설정/해제

사용자 재인증 설정/해제 이미 인증을 받은 사용자를 재인증 받도록 하고, 설정했던 재인증을 해제(설정취소)하는 기능입니다.

인증정보를 모두 삭제하여 인증을 해제하는 [사용자인증해제](#)와는 달리,

사용자 재인증은 사용자의 인증정보를 남겨두고 있기 때문에, 재인증 해제가 가능한 것입니다.(재인증 해제 시 남겨둔 인증정보를 다시 사용)

사용자 재인증 설정

관리자는 사용자 재인증이 필요한 노드에 대해, 사용자 재인증을 수행하게 할 수 있습니다.

1. 사용자 재인증 설정 선택

재인증을 할 노드를 선택 후, 작업선택 > 노드관리 > 사용자 재인증 설정 을 선택합니다.
재인증을 할 시 노드는 바로 미인증차단정책을 적용받아 네트워크가 차단됩니다.



2. 사용자 재인증 설정 확인

노드 상세 정보 > 기본정보에서 사용자 재인증 설정 후에도 인증정보가 남아있는 것을 확인할 수 있습니다.



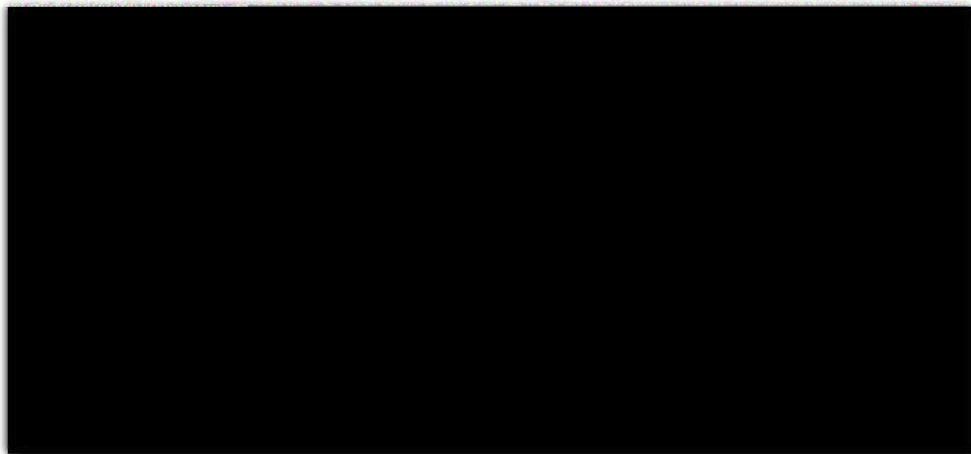
3. 사용자 재인증 CWP

사용자 인증정보가 남아있어도 인증 과정을 다시 거치지 않으면 네트워크가 차단되어 CWP 페이지로 이동하는 것을 확인할 수 있습니다.
인증을 다시 받으면 네트워크 차단이 풀리게 되고, 재인증 설정도 해제됩니다.



사용자 재인증 해제

관리자는 사용자 재인증이 설정되어있는 노드를 선택하여, 재인증 설정을 해제할 수 있습니다.
재인증이 설정되어 있던 노드에 재인증 해제 시, 재인증을 요구하지 않습니다.



노드위험해제

노드위험해제

위험감지는 정의되어있는 위험상황이 발생하였을 때, 위험을 발생시킨 노드가 어떤 노드인지 표시하여 주고, 제어정책을 통하여 해당 노드의 네트워크를 제어하는 역할을 합니다.

하지만 위험 조건에는 부합이나 악의적인 행동이 아닌 것을 관리자가 확인 후(예를들어, MAC 테이블을 채우기 위해 ARP Request Packet을 네트워크의 모든 노드에게 지속적으로 뿌리는 행위), 관리자는 노드에 걸려있는 위험상태를 해제할 수 있습니다.

위험은 정책 > 정책 > 노드정책 > 위험감지에서 정의할 수 있으며 자세한 내용은 위험감지를 참조해 주시기 바랍니다.

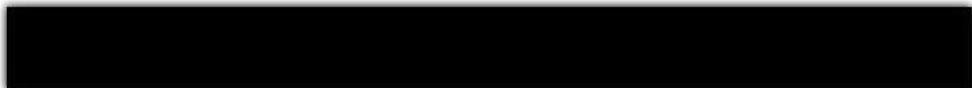
1. 노드위험해제 선택

위험 이벤트가 발생한 노드를 선택한 후, 노드위험해제를 선택합니다.



2. 노드위험해제 확인

관리 뷰에서 해당 노드의 위험상태가 해제된 것을 볼 수 있습니다.



관리센서변경

관리센서변경

관리자는 각 노드를 관리하는 관리센서를 원하는 센서로 변경할 수 있습니다.
관리센서변경 후, 해당노드는 변경 후 관리센서에 의해 관리받게 됩니다.

1. 관리센서변경 선택

관리센서를 변경할 노드를 선택 후, 작업선택 > 노드관리 > 관리센서변경 을 선택합니다.
노드 관리 뷰의 위치 컬럼에 해당 노드가 현재 어떤 관리센서에 속해있는지 확인할 수 있습니다.



2. 관리센서변경 팝업

관리센서변경을 선택하면 아래 그림과 같은 팝업이 생성되어 관리센서를 선택할 수 있습니다.



3. 관리센서변경 확인

S-172.29.56.87 의 관리를 받고있던 해당노드의 관리센서를 C-172.29.56.87로 바꾼 후, 관리센서가 제대로 변경된 것을 관리 뷰 및 노드 상세 페이지에서 확인할 수 있습니다.



노드속성 가져오기

노드속성가져오기

관리자는 노드속성가져오기 기능을 통하여, 많은 노드들의 속성을 한번에 설정할 수 있습니다.
CSV 파일을 이용하여, CSV 파일과 노드리스트의 IP를 비교하여 일치하는 노드에 해당 속성 값을 설정합니다.

1. 엑셀로 속성파일 작성

엑셀로 속성설정 파일을 작성 후, 다른 이름으로 저장을 이용하여 CSV파일을 생성합니다.

항목	설명	입력
IP	노드 속성을 변경할 IP를 입력합니다.	x.x.x.x
MAC	노드 속성을 변경할 MAC을 입력합니다.	aa:bb:cc:11:22:33
NAME	노드 이름을 입력합니다.	관리자 임의 입력
DESC	노드 설명을 입력합니다.	관리자 임의 입력
GENIDEV	노드 타입을 입력합니다.	PC = 20 모바일 = 21 서버 = 40 네트워킹장비 = 60 무선접속장비 = 61 라우터 = 62 스위치 = 63 보안장비 = 64 프린터 = 80 VOIP = 90 기타 = 100
PLATFORM	노드 플랫폼을 입력합니다.	관리자 임의 입력
IPBEGIN	IP 사용 시간을 입력합니다.	YYYY-MM-DD hh:mm
IPEND	IP 사용 종료 시간을 입력합니다.	YYYY-MM-DD hh:mm
NODETAG	생성되어 있는 태그 이름을 입력합니다. 태그는 설정 > 속성관리 > 태그관리에서 생성할 수 있습니다.	태그 이름
MACTAG	성되어 있는 태그의 이름을 입력합니다. 태그는 설정 > 속성관리 > 태그관리에서 생성할 수 있습니다.	태그이름
CUSTOM01~09	추가필드에 들어갈 내용을 입력합니다. 장비추가필드가 생성되어 있어야 합니다. 추가필드는 설정 > 추가필드관리 > 장비에서 생성할 수 있습니다.	관리자 임의 입력



CSV파일의 IP와 노드 리스트의 IP를 비교하여 IP가
일치하는 노드에 현재 속성 값으로 설정합니다.
현재 값으로 노드속성을 가져오면,
IP **100.100.100.40** 노드의 속성 값을
이름은 '개발pc'로 노드설명은 '개발용 pc입니다.'로 설정합니다.



다른이름으로 저장 선택 후,
파일형식을 CSV로 선택합니다.

2. 노드속성가져오기 선택

작업선택 > 노드관리 > 노드속성가져오기 를 선택합니다.



3. 노드속성가져오기 팝업

노드속성가져오기를 선택하면 팝업이 생성되어 위 과정에서 생성한 CSV 파일을 가져오기 할 수 있습니다.



4. 노드속성설정 확인

노드 상세 정보 페이지에서 노드속성이 제대로 설정된 것을 확인할 수 있습니다.



장비속성 가져오기

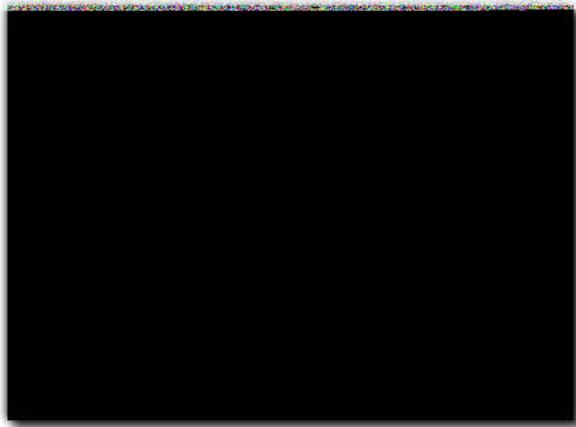
장비속성가져오기

관리자는 장비속성가져오기 기능을 통하여, 많은 장비들의 속성을 한 번에 설정할 수 있습니다.
CSV 파일을 이용하여, CSV 파일과 노드 리스트의 MAC을 비교하여 일치하는 노드에 해당 속성 값을 설정합니다.

1. 엑셀로 속성파일 작성

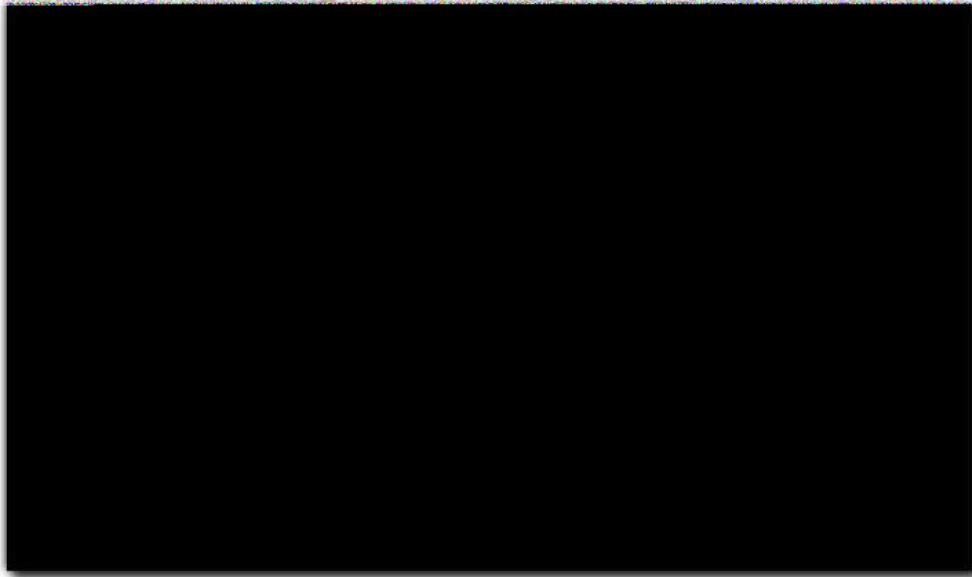
엑셀로 속성설정 파일을 작성 후, 다른이름으로 저장을 이용하여 CSV 파일을 생성합니다.

항목	설명	입력
MAC	장비 속성을 변경할 노드의 MAC을 입력합니다.	AA:BB:CC:11:22:33
DEVNAME	장비 이름을 입력합니다.	관리자 임의 입력
DEVDESC	장비 설명을 입력합니다.	관리자 임의 입력
MACBEGIN	MAC 사용 시간을 입력합니다.	YYYY-MM-DD hh:mm
MACEND	MAC 사용종료 시간을 입력합니다.	YYYY-MM-DD hh:mm
MACTAG	생성되어 있는 태그의 이름을 입력합니다. 태그는 설정 > 속성관리 > 태그관리에서 생성할 수 있습니다.	태그 이름
DEVCUSTOM01~09	추가필드에 들어갈 내용을 입력합니다. 장비추가필드가 생성되어 있어야 합니다. 추가필드는 설정 > 추가필드관리 > 장비에서 생성할 수 있습니다.	관리자 임의 입력



2. 장비속성 가져오기 선택

작업선택 > 노드관리 > 장비속성 가져오기 를 선택합니다.



3. 장비속성 가져오기 팝업

노드속성 가져오기를 선택하면 팝업이 생성되어 위 과정에서 생성한 CSV 파일을 가져오기 할 수 있습니다.



4. 노드속성 설정 확인

노드 상세 정보 페이지에서 노드속성이 제대로 설정된 것을 확인할 수 있습니다.



장비 소유자설정

장비 소유자설정

관리자는 장비에 대한 소유자를 설정할 수 있습니다.

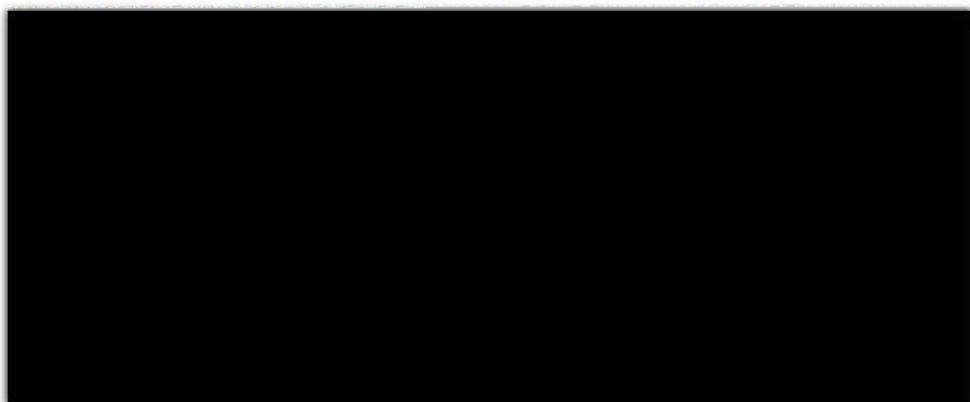
1. 장비소유자기능 선택

관리 > 노드 > 작업선택 > 장비 소유자 설정을 선택합니다.



2. 소유자의 ID 선택 팝업

사용자 ID를 입력하고 검색을 클릭하면 등록되어 있는 아이디가 검색 결과에 출력됩니다.



3. 장비소유자확인

관리 > 노드 > 노드 상세 정보(노드의 IP 클릭) > IP관리에서 소유자를 확인할 수 있습니다.



장비 소유부서설정

장비 소유부서설정

관리자는 장비에 대한 소유부서를 설정할 수 있습니다.

1. 부서생성

소유부서를 설정하기 위해서는 부서가 생성되어 있어야 합니다. 부서생성은 [사용자](#) 페이지에서 트리 뷰를 참고 바랍니다.

2. 장비 소유부서설정 선택

소유부서를 설정하고자 하는 장비를 선택하고 부서설정 기능을 선택합니다.



3. 장비 소유부서 선택팝업

장비 소유부서를 선택 후 설정 버튼을 클릭합니다.



4. 장비 소유부서 확인

관리 > 노드 > IP관리뷰에서 장비소유부서를 확인할 수 있습니다.



일괄작업

일괄작업

관리자는 노드 > 일괄작업 을 통하여 여러개의 노드를 한번에 설정, 제어할 수 있습니다.



- 노드그룹 지정&해제
- 노드속성변경
- 노드관리설정
- 노드대상 작업지시
- 에이전트액션 수행
- 인스턴트메시지 전송
- 이메일 전송
- 센서대상 작업지시
- 센서환경설정
- 무결성 검증

노드그룹 지정&해제

노드그룹 지정/해제

노드그룹 지정/해제를 통하여 많은 노드들을 한 번에 원하는 노드그룹으로 지정/해제할 수 있습니다.
노드그룹에 대한 설명은 [노드](#)를 참고 바랍니다.

노드그룹 지정

관리자는 여러 노드를 한 번에 원하는 OR 연산인 노드그룹에 포함시킬 수 있습니다.

1. 노드그룹 지정 선택

노드그룹을 지정할 노드를 선택 후(1개 혹은 그 이상), 작업선택 > 일괄작업 > 노드그룹지정/해제 를 선택합니다.



2. 노드그룹 지정 설정

원하는 노드그룹을 선택하고 실행 버튼을 클릭합니다.

OR 연산인 그룹만 선택 가능합니다, OR 연산은 [노드](#)의 기본정보설정을 참고하시기 바랍니다.
노드식별항목의 선택에 따라 해당 그룹에 해당노드의 IP/MAC 값이 선택된 노드그룹의 조건으로 입력됩니다.
입력된 조건에 의해 해당 노드는 선택된 노드그룹에 포함되게 됩니다.

아래 그림과 같이 노드식별을 MAC+IP 주소로 선택, 노드그룹을 TEST GROUP으로 선택합니다.



노드그룹 지정을 하기전에는 TEST GROUP 그룹에 172.29.56.15노드를 포함할 수 있는 조건이 없습니다.

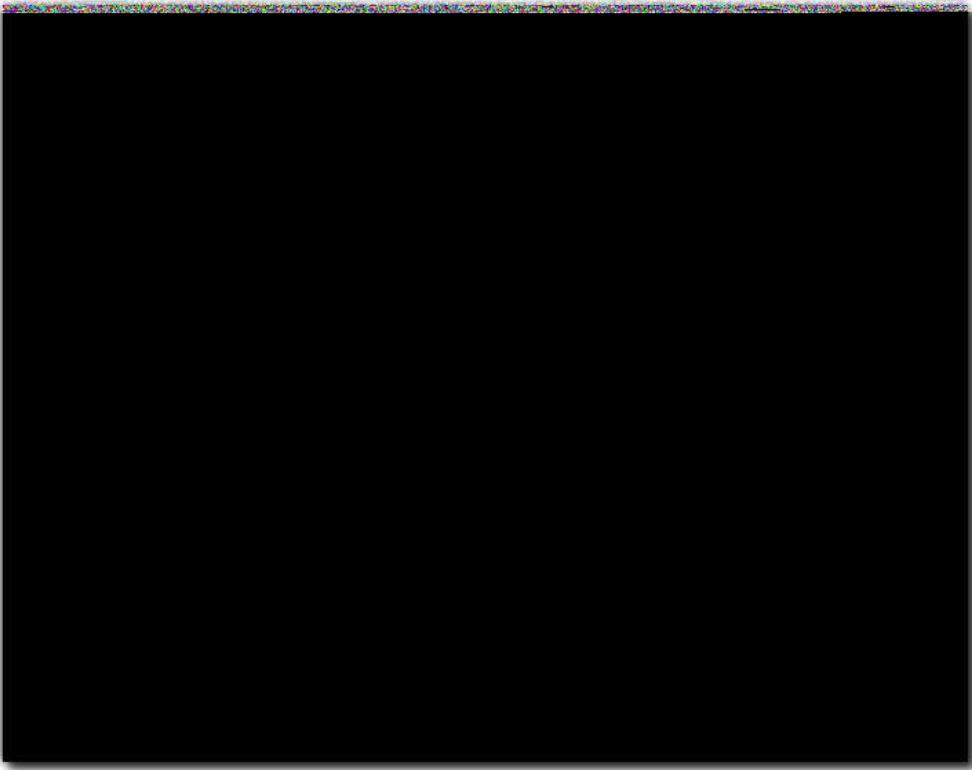


하지만 노드그룹을 지정하고 나서는 그룹조건에 해당 노드를 포함할 수 있도록 설정한 대로 해당 노드의 IP값이 조건으로 추가되어 있는 것을 확인할 수 있습니다.



3. 노드그룹 포함 확인

해당노드가 지정된 노드그룹으로 제대로 포함이 되었는지 노드 상세 페이지 > 정책현황 > 노드그룹 에서 확인할 수 있습니다.



노드그룹 해제

지정한 노드그룹을 해제할 수 있습니다.

1. 노드그룹 해제 설정

노드에 설정했던 노드그룹을 해제합니다.

동작선택을 노드그룹 해제로 선택합니다.



노드그룹을 해제할 때, 노드식별 값이 노드그룹을 지정할 때와 상이하다면 아래 그림과 같이 해제가 이루어지지 않습니다.
노드그룹을 지정할 때, 노드식별 값을 MAC+IP 주소로 설정했다면, 해제할 때도 노드식별 값을 MAC+IP 주소로 선택해야합니다.



노드속성변경

노드속성변경

관리자는 일괄작업항목의 노드속성변경 기능을 이용하여 여러 노드의 속성을 한번에 설정할 수 있습니다.

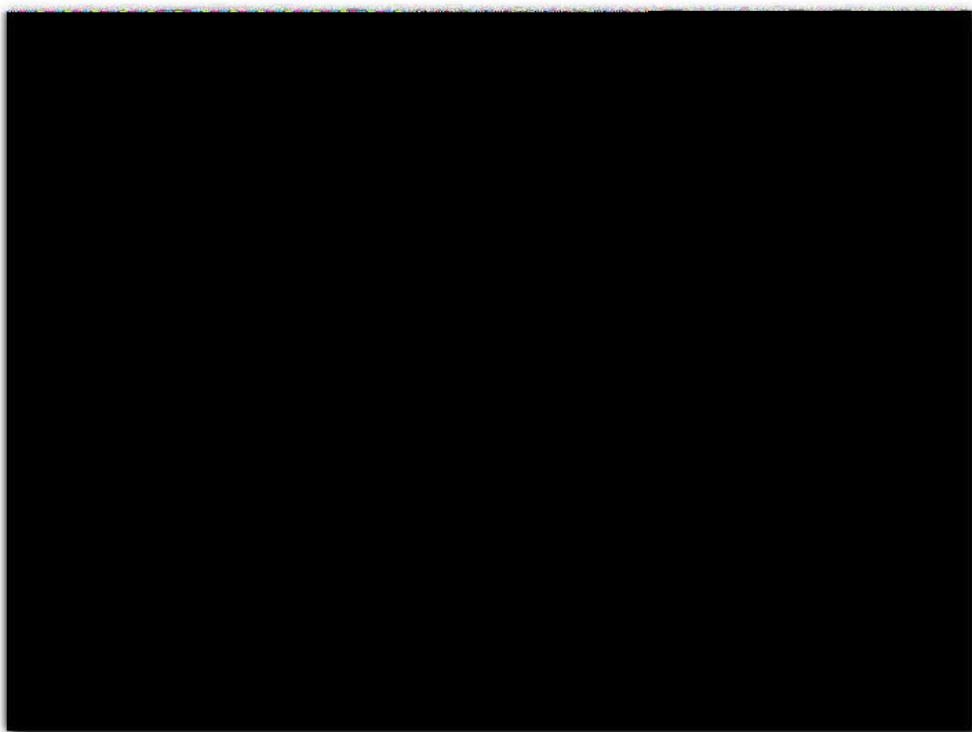
1. 노드속성변경 선택

노드속성을 변경 하고싶은 노드를 선택 후, 작업선택 > 일괄작업 > 노드속성변경 을 선택합니다.



2. 노드속성 설정

노드속성변경을 선택하면, 노드속성을 변경할 수 있는 페이지로 이동하게 됩니다.
변경하려는 속성의 체크박스에 체크를 할 시 해당 속성을 설정할 수 있습니다.



3. 노드속성변경 확인

노드속성변경이 잘 수행되었는지 노드 상세 페이지 > 기본정보에서 확인할 수 있습니다.



노드관리설정

노드관리설정

관리자는 노드관리설정 기능을 통해 노드의 제한감사기록 유무, 노드정보 스캐닝 유무, 노드삭제 금지 유무를 설정할 수 있습니다.

1. 노드관리설정 선택

관리자는 노드관리설정을 원하는 노드를 선택한 후, 작업선택 > 일괄작업 > 노드관리설정 을 선택합니다.



2. 노드관리설정

노드관리설정을 선택하면 설정할 수 있는 페이지로 이동하게 됩니다.
아래 그림과 같은 설정을 할 수 있습니다.



노드관리설정의 항목은 아래 표와 같습니다.

항목	설명
제한감사기록	센서에 의해 네트워크가 차단된 노드가 네트워크로 접근 시도 시, 접근기록을 로그로 남깁니다.
노드정보 스캐닝	노드의 운영체제와 열린포트정보를 스캐닝 할지의 여부를 선택합니다.
노드삭제 금지	노드를 삭제로부터 보호할지의 여부를 선택합니다.

노드대상 작업지시

노드대상 작업지시

관리자는 노드대상작업지시를 통하여 한 번에 많은 노드들에게 작업을 지시할 수 있습니다.

1. 노드대상 작업지시 선택

작업을 지시할 노드들을 선택한 후, 작업선택 > 일괄작업 > 노드대상작업지시 를 선택합니다.



2. 노드대상 작업지시 수행

노드대상작업지시를 선택하면, 수행시킬 작업을 선택할 수 있는 페이지로 이동합니다.



노드를 대상으로 내릴 수 있는 작업은 위 그림과 같이 9개의 작업을 수행할 수 있으며, 한 번에 하나의 작업만 수행할 수 있습니다. 각 작업의 설명은 아래 표와 같습니다.

작업 이름	설명
노드 상세정보 스캐닝 수행(센서)	Genian NAC Sensor가 해당 작업을 수행하며, 노드 OS, Open Port, NetBios 이름 검사 등 노드 정보 검사를 즉시 수행합니다.
에이전트액션 즉시수행(에이전트)	에이전트가 해당 작업을 수행하며, 선택한 노드가 받고 있는 정책 중, 해당 정책에 에이전트액션이 할당되어 있다면 액션을 즉시 수행합니다.
패치관리 즉시수행(에이전트)	에이전트가 작업을 수행하며, 노드와 Genian NAC에 설정되어있는 패치(Window, Office)를 확인하여, 패치가 필요한 항목을 즉시 패치합니다.
노드 자산정보 즉시전송(에이전트)	에이전트가 작업을 수행하며, 해당 노드의 하드웨어, 소프트웨어에 대한 정보를 수집하여 수집한 내용들을 센터에 전송합니다.
노드 정책 재적용(에이전트,센터)	선택한 노드에 대하여 정책을 적용시킵니다.(정책적용이 제대로 이루어지지 않았거나, 우선순위가 바뀐 정책에 대하여 정책적용을 다시 받을 때, 혹은, 변경정책적용 버튼을 누르지 않고 특정 노드의 정책만 재적용 할 때 사용합니다.)

에이전트 서비스 시작(에이전트)	Genian Agent가 설치된 노드의 Agent 서비스를 시작 상태로 변경합니다.
에이전트 서비스 중지(에이전트)	Genian Agent가 설치된 노드의 Agent 서비스를 중지 상태로 변경합니다.
에이전트 업데이트(에이전트)	에이전트의 버전이 업데이트 됐다면, 센터에 최신 에이전트를 업데이트 한 후, 해당 작업을 통하여 모든 노드에 에이전트를 업데이트할 수 있습니다.
센서 장애복구(에이전트)	해당 노드가 에이전트에 의해 받고 있는 ARP 포이즈닝을 해제하여 네트워크에 정상적으로 접근할 수 있도록 합니다.

에이전트액션 수행

에이전트액션 수행

관리자는 에이전트액션 수행 항목을 통하여, 선택한 노드들에게 액션을 즉시 수행하게 할 수 있습니다. 정책에 할당되어있지 않아도, 액션이 정의만 되어있다면 바로 적용이 가능합니다. 노드액션을 정의하는 방법은 [노드액션](#)을 참조해 주시기 바랍니다.

1. 에이전트액션 수행 선택

관리자는 원하는 노드를 선택하고, 작업선택 > 일괄작업 > 에이전트액션 수행 을 선택합니다.



2. 에이전트액션 수행 지시

에이전트액션 수행을 선택하면 미리 정의되어 수행 가능한 에이전트액션 목록 페이지로 이동합니다. 원하는 액션을 선택하여 실행합니다.
에이전트액션은 한 번에 하나씩만 선택 가능합니다.



인스턴트메시지 전송

인스턴트메시지 전송

관리자는 인스턴트메시지 기능을 통하여 노드들에게 메시지를 전송할 수 있습니다.
인스턴트메시지는 에이전트가 설치되고 동작 중인 노드만 받을 수 있습니다.

1. 인스턴트메시지 전송 선택

메시지를 보낼 노드를 선택한 뒤, 작업선택 > 일괄작업 > 인스턴트메시지 전송 을 선택합니다.



2. 인스턴트메시지 전송 팝업

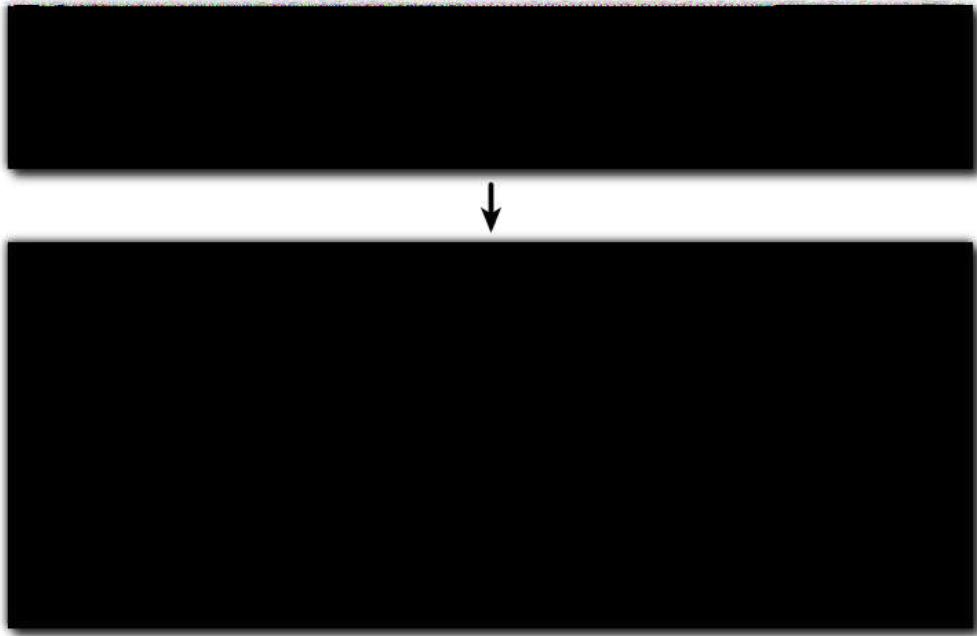
인스턴트메시지 전송을 선택하면 메시지 내용을 작성할 수 있는 팝업이 생성됩니다.
제목과 내용을 작성한 뒤, 전송 버튼을 누르면 해당 노드에게 메시지가 전송됩니다.



3. 인스턴트메시지 확인

인스턴트메시지를 받을 노드에서 인스턴트메시지가 정상적으로 수신된 것을 확인할 수 있습니다.

아래 그림과 같이 트레이 아이콘 쪽에 작은 팝업이 생성되고 해당 팝업을 누르면 인스턴트메시지를 확인할 수 있습니다.



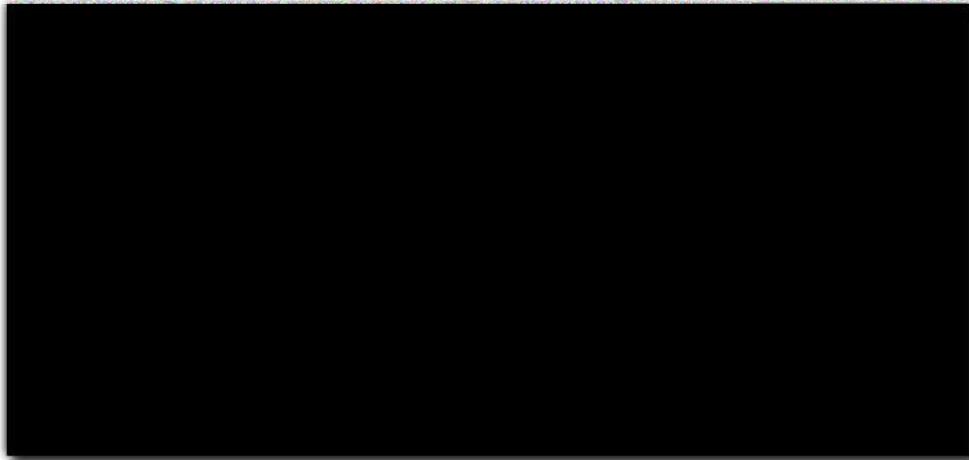
이메일 전송

이메일 전송

관리자는 인증을 받은 노드들에게 이메일 전송 기능을 이용하여 이메일을 보낼 수 있습니다.
인증을 받은 사용자 ID의 전자우편 항목을 참조하여 메일을 발송하며, 설정 > 환경설정 > 기타설정에서 메일서버 설정이 되어 있어야 이메일 전송 기능을 사용할 수 있습니다.
미인증 노드는 이메일을 전송 할 수 없습니다.

1. 이메일 전송 선택

이메일을 전송할 노드를 선택한 후 작업선택 > 일괄작업 > 이메일 전송 을 클릭합니다.



2. 이메일 전송

이메일 전송 팝업 창에 제목과 내용을 작성합니다.
내용을 HTML 형식으로 작성하였을 시 HTML을 선택하고, 일반적인 형식으로 작성하였을 시 TEXT를 선택합니다.
작성과 형식을 선택을 하였으면 전송 버튼을 클릭하여 이메일을 전송합니다.



센서대상 작업지시

센서대상 작업지시

관리자는 센서대상 작업지시 기능을 통하여 선택한 센서에 대한 작업을 지시할 수 있습니다.

1. 센서대상 작업지시 선택

작업을 지시할 센서를 선택 후, 작업선택 > 일괄작업 > 센서대상 작업지시 를 선택합니다.



2. 센서대상 작업지시 실행

센서대상 작업지시를 선택하면 작업을 선택하여 실행할 수 있는 페이지로 이동합니다.
지시를 내릴 작업을 선택 후 실행 버튼을 선택합니다. 한 번에 하나의 작업만 수행 가능합니다.



기능에는 서브넷 노드스캔과 배포 동기화가 있으며 해당 기능의 설명은 아래 표와 같습니다.

기능 이름	내용
서브넷 노드스캔 즉시수행	같은 서브넷상에 존재하는 노드를 즉시 스캔합니다.
배포 동기화 즉시수행	현재 센터가 배포하고 있는 파일을 해당 장비에도 동기화 하여 해당 장비에 속해 있는 노드들도 배포 파일을 다운 받을 수 있습니다.

센서환경설정

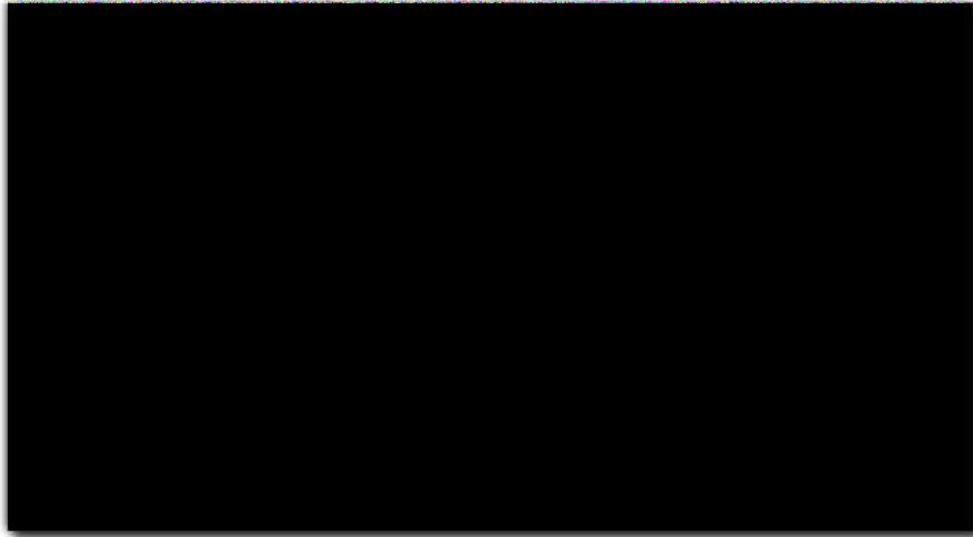
센서환경설정

관리자는 센서환경설정을 통하여 다수의 센서를 일괄적으로 설정할 수 있습니다.

각 센서의 환경설정은, 시스템 > 센서 IP 선택 > 센서설정 > 인터페이스 선택으로 센서설정 페이지로 이동하거나, 관리뷰 > 센서 IP 선택 > 설정 > 센서설정으로 센서설정 페이지로 이동하여 설정 가능합니다. 하지만, 센서의 수가 증가하게 되면 다수의 센서를 각 센서별로 설정하기에 많은 번거로움이 생깁니다. 따라서, 관리자는 작업선택 > 센서환경설정 이동하여 일괄적으로 센서를 설정할 수 있습니다.

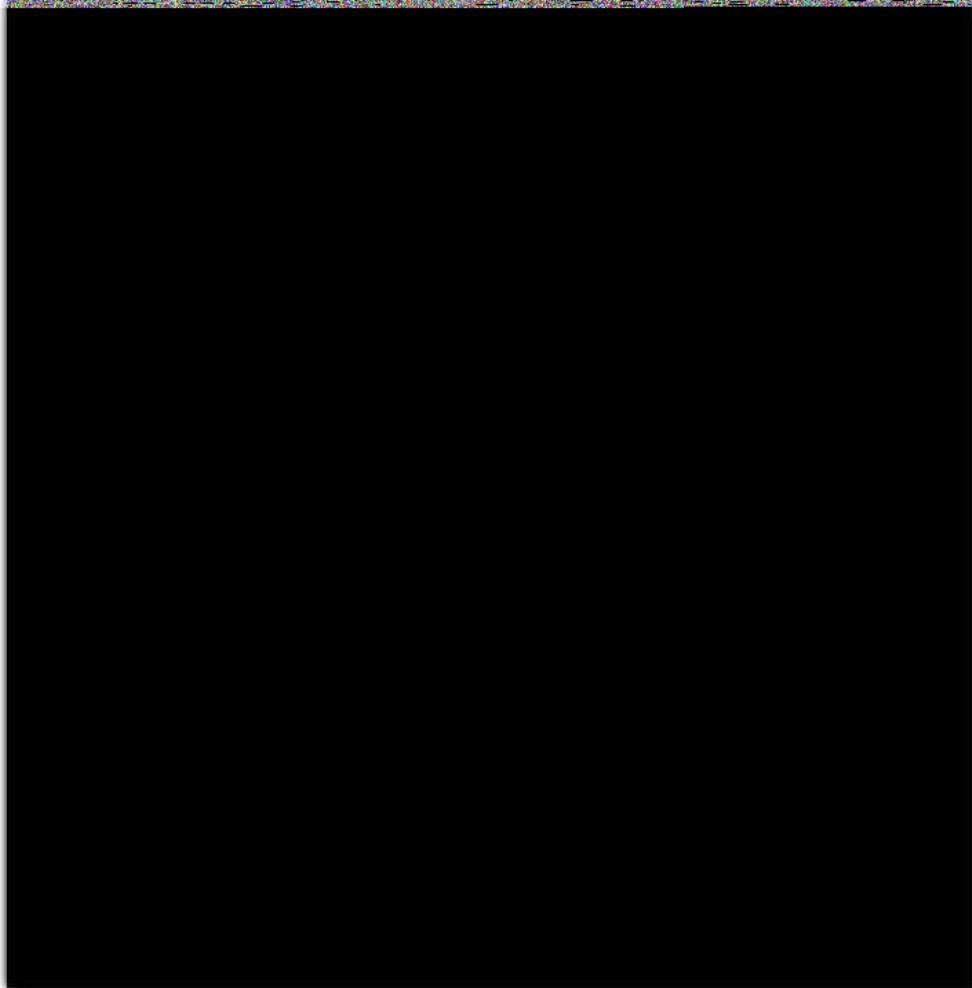
1. 센서환경설정 선택

환경설정을 원하는 다수의 센서를 선택한 뒤, 작업선택 > 센서환경설정 을 선택합니다.



2. 센서환경설정 실행

센서환경설정을 선택하면 환경설정을 할 수 있는 페이지로 이동합니다.
일반 센서환경설정과 다른 점은 설정 각 항목마다 체크를 하고 설정을 하여야 설정이 반영됩니다.



설정을 하고난 후, 실행버튼을 누르면 아래 메시지와 함께 설정이 변경됩니다.



무결성 검증

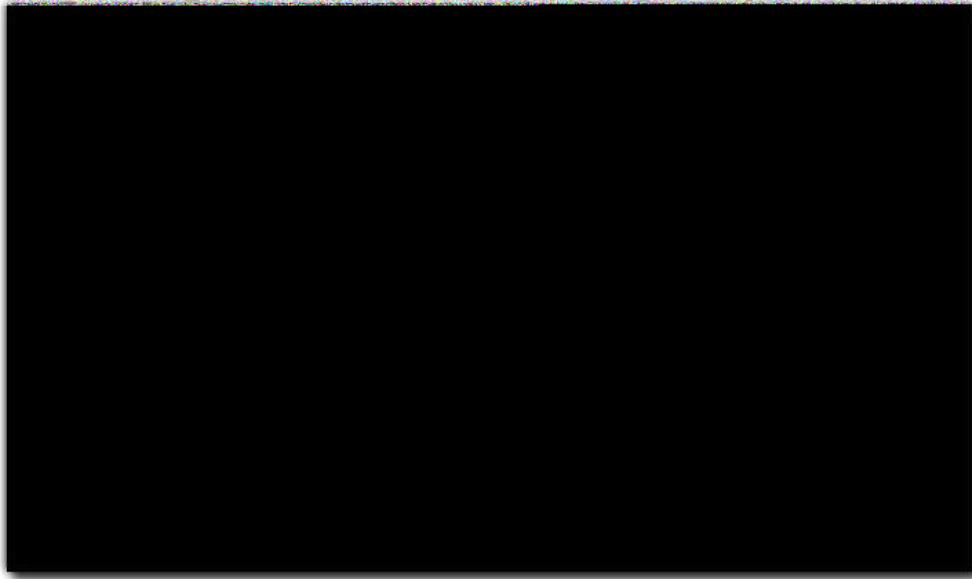
무결성 검증

센터, 센서, 노드에 설치된 에이전트가 타인 혹은 시스템에 의해 망설, 훼손, 손상, 변조되어 무결성이 지켜지지 않을 경우 NAC에 의한 정책 및 노드가 정상적으로 동작하지 않을 수 있습니다.

관리자는 노드에 설치된 에이전트의 무결성이 지켜지고 있는지 확인 할 수 있습니다.

1. 무결성 검증 선택

무결성 검사할 에이전트가 설치된 노드, 센서, 센터를 선택 후 관리 > 노드 > 작업선택 > 일괄작업 > 무결성 검증 을 클릭합니다.



2. 무결성 검사 수행

수행 시 다음과 같은 메시지가 출력됩니다.



3. 무결성 수행 결과

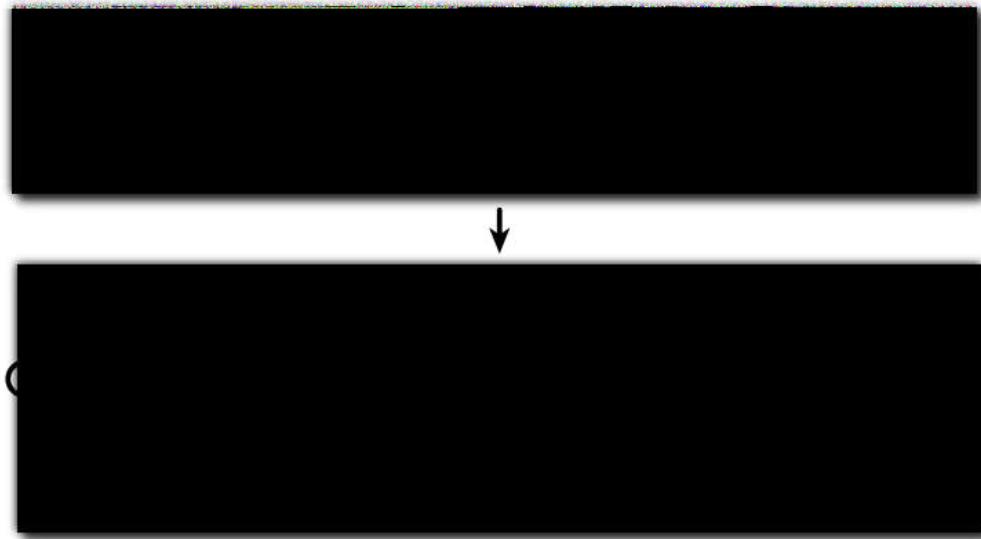
노드상세화면에서 무결성 결과를 확인할 수 있습니다.
에이전트 무결성 결과가 비정상일 경우 자동으로 에이전트 재설치를 수행합니다.



노드 - 노드 상세 정보

노드상세정보

관리자는 노드관리 페이지에서 각 노드의 IP를 선택하여 노드상세정보 확인, 작업지시, 설정 변경 등을 수행할 수 있습니다.



노드상세정보 페이지에서 수행할 수 있는 작업과 그 설명은 아래와 같습니다.

작업 이름	설명
① 노드목록	노드 상세 페이지로 이동하기 전의 관리 뷰로 이동하여 노드 목록을 불러옵니다.(뒤로가기 버튼과 비슷한 기능입니다.)
② 노드그룹 지정/해제	해당 노드를 특정 노드그룹의 조건에 부합하지 않더라도 원하는 노드그룹으로 지정/해제 할 수 있습니다. OR 연산으로 되어있는 그룹에만 지정/해제가 가능합니다. 설정법과 상세내용은 노드그룹 지정&해제 와 같습니다.
③ 인스턴트메시지 전송	관리자는 에이전트가 설치 및 동작하고 있는 해당 노드에게 1회성의 인스턴트메시지를 전송할 수 있습니다. 메시지 전송법과 상세내용은 인스턴트메시지 전송 을 참조해 주시기 바랍니다.
④ 접속인증페이지(CWP) 조회	선택한 노드가 정책 등에 의해 제어를 받았을 경우 정확한 상태를 알기 위해 사용되며, 접속인증페이지(CWP) 조회를 클릭할 시 해당 노드에서 직접 접속한것과 같은 CWP 페이지를 확인할 수 있습니다.
⑤ 노드대상 작업지시	해당노드에게 원하는 작업을 즉시 수행시킬 수 있습니다. 노드대상 작업지시의 항목과 세부내용은 노드대상 작업지시 를 참조해 주시기 바랍니다.
⑥ 정보&관리 탭	노드의 상세정보를 표시해주고, 노드설정을 할 수 있습니다. 각 탭의 내용은 해당페이지의 하위페이지에 기술되어 있습니다. [노드 상세 - 기본정보] [노드 상세 - 장비정보] [노드 상세 - 시스템정보] [노드 상세 - 네트워크정보] [노드 상세 - 소프트웨어정보] [노드 상세 - 패치정보] [노드 상세 - 이력관리] [노드 상세 - IP 관리] [노드 상세 - 정책] [노드 상세 - 정책현황]

노드 상세 - 기본정보

기본정보

노드상세 페이지의 기본정보 탭에는 해당 장비의 IP, MAC, 호스트명 등 노드의 기본적인 정보와 설명, 이름 등을 설정할 수 있습니다.



관리자가 설정할 수 있는 항목들을 빨간 테두리로 표시해 보았습니다.
각 항목의 설명은 아래 표와 같습니다.

항 목 이 름	설 명
IP 주소	노드의 IP 주소를 나타냅니다.
이름	관리자가 임의로 노드를 식별하는 이름을 설정할 수 있습니다.
도메인	노드의 도메인을 나타냅니다.
노드타입	관리자는 지정 기능을 이용하여 노드타입을 직접 지정할 수 있습니다. 타입에는 PC, 모바일, 서버, 네트워킹장비, 무선접속장비, 라우터, 스위치, 보안장비, 프린터, VOIP, 기타가 있습니다. 타입을 지정하지 않으면 Genian NAC가 수집한 정보를 기반으로 타입을 자동 설정합니다.
확인된 노드타입	관리자가 확인한 노드타입을 설정합니다. 설정한 타입은 Genian NAC에 의해 변경되지 않습니다.
플랫폼	관리자는 지정 기능을 이용하여 플랫폼을 직접 작성할 수 있습니다. 지정을 하지 않을 시에는 Genian NAC가 수집한 정보를 기반으로 플랫폼을 자동 설정합니다. 자동 설정된 플랫폼정보가 실제 플랫폼과 다를 시, 옆의 오탐보고 기능을 통하여 잘못된 플랫폼정보를 지니네트웍스에 보고합니다. 보고내용을 기반으로 플랫폼DB를 업데이트하여 플랫폼 오탐률을 줄입니다. 에이전트가 설치되어 있는 노드는 오탐보고를 하지 않습니다.
확인된 플랫폼	관리자가 확인한 플랫폼을 입력합니다. 입력한 플랫폼은 Genian NAC에 의해 변경되지 않습니다.
장비	MAC 주소가 같고 IP 주소는 다를 경우, 하나의 장비로 확인합니다. 하지만 하나의 장비가 각각 다른 IP와 MAC을 가지고 있을 경우 즉, 여러 인터페이스를 가진 장비일 경우 에이전트가 깔린 MAC과 IP를 기준으로 합쳐집니다. IP를 클릭 시 자세한 내용을 확인할 수 있습니다.
위치	노드를 탐지한 장비의 IP를 나타냅니다. IP 좌측에 문자는 S = SENSOR C = CENTER 입니다.
접속AP	노드가 이용하고 있는 AP의 SSID를 나타냅니다.
연결방식	노드의 네트워크 연결 방식을 나타냅니다. 네트워크정보 수집 플러그인을 적용 시 나타냅니다.

마지막 동작시각	마지막으로 동작한 시각을 나타냅니다, 노드의 동작상태가 DOWN 일 시 나타나는 정보입니다.
최초 등록	노드가 최초로 등록된 시각을 나타냅니다.
인증사용자	노드가 인증한 사용자를 나타냅니다.
현재 인증상태	노드의 현재 인증상태를 나타냅니다.
설명	노드에 대한 설명을 설정할 수 있습니다.
MAC 주소	노드의 MAC 주소를 나타냅니다.
호스트명	노드의 호스트명을 나타냅니다.
DNS 이름	노드의 DNS 이름을 나타냅니다.
NIC 벤더	노드의 NIC 벤더를 나타냅니다.
에이전트 버전	노드에 설치되어 있는 에이전트의 버전을 나타냅니다, 소프트웨어정보 수집 플러그인을 적용 시 나타냅니다.
노드 ID	NAC에서 부여한 노드의 고유ID를 나타냅니다.
센서 NID	노드를 관리 및 제어하는 센서의 노드 ID를 나타냅니다.
스위치,포트	노드와 연결된 스위치 이름 및 포트를 나타냅니다.
동작상태	노드의 동작상태를 나타냅니다, UP = 켜짐 DOWN = 꺼짐
최근 노드 검사	노드 상세정보를 스캐닝한 최근 시각을 나타냅니다.
가동률	노드 등록 후 현재시각 까지의 동작상태 UP 비율을 나타냅니다.
최근 사용자인증	사용자 인증한 최근 시각을 나타냅니다.
웹브라우저	노드의 User Agent 정보를 나타냅니다, CWP 페이지 접속 시 나타냅니다.
NAT IP	노드와 연결되어 있는 NAT 장비의 IP를 나타냅니다, Agent 설치 시 나타냅니다.
NAT Port	노드의 Source NAT Port를 나타냅니다.
NAT장비	노드가 NAT 장비일 시 체크됩니다, NAT 장비에 연결되어 있는 노드가 Agent를 설치 시 나타냅니다, NAT된 노드는 체크되지 않습니다.
무결성 검증	센서, 센터, 에이전트가 설치된 노드만 표시되며, 무결성 검사의 수행 결과를 나타냅니다.
태그	노드(IP+MAC)에 태그를 설정합니다. 노드태그에 관한 자세한 설명은 노드 태그 설정 을 참조해 주시기 바랍니다.

- **오탐지보고 팝업**

오탐지보고 버튼을 누르면 아래 그림과 같은 팝업이 생성됩니다. 해당 팝업을 통하여 당사에 오탐보고를 할 수 있습니다.



- **NAT 장비**

NAT 장비로 지정된 노드는 관리 뷰에서 NAT 아이콘과 NAT 장비라는 팝업이 아래 그림과 같이 표시됩니다.



노드 상세 - 장비정보

장비정보

장비정보 페이지를 통하여 장비의 이름과 설명을 설정할 수 있고, 장비의 ID와 장비내 노드를 확인할 수 있습니다.



관리자가 설정할 수 있는 항목들을 빨간 테두리로 표시했습니다.

각 항목의 설명은 아래 표와 같습니다.

항 목 이 름	설 명
장비명	장비에 이름을 설정할 수 있습니다.(IP를 변경하여도 변하지 않습니다.)
장비설명	장비에 설명을 설정할 수 있습니다.
제조일	장비의 제조일을 입력합니다.
구입처	장비의 구입처를 입력합니다.
내용연수 시작일	장비의 내용연수 시작일을 입력합니다.
내용연수 만료일	장비의 내용연수 만료일을 입력합니다.
일련번호	장비의 일련번호를 입력합니다.
구입가격	장비의 구입가격을 입력합니다.
책임자	장비의 책임자를 입력합니다.
책임부서	장비의 책임부서를 입력합니다.
메모	장비에 필요한 메모를 입력합니다.
장비삭제	장비를 노드리스트에서 삭제합니다. 장비 삭제 시 해당 장비가 가지고 있던 하위 장비의 정보들도 함께 삭제됩니다.

- 장비내 노드

Genian NAC는 여러가지 정보수집 방법을 통하여, 여러개의 MAC과 IP가 존재하는 하나의 장비를 탐지 가능합니다. 이렇게 하나의 장비라고 생각되는 노드들을 장비내 노드항목에 리스트 형식으로 나타냅니다.

노드 상세 - 시스템정보

시스템정보

에이전트가 플러그 인을 사용하여 노드의 시스템 내부 정보를 수집합니다.
따라서, 에이전트가 반드시 설치되어 있어야만 시스템 내부 정보 수집이 가능합니다.



위 그림은 시스템정보 페이지의 일부분이며, 항목과 그에 대한 내용은 아래 표와 같습니다.

항 목	내 용
마더보드정보	섀시 유형, 마더보드 제조사, CPU명, CPU 제조사, 리비전, 배터리, 온도
메모리 정보	메모리 전체크기, 사용중인 양(GB), 사용률(%)
저장장치 정보	장치명, 유형, 벤더명/모델명, 고유번호, 파일시스템, 총 용량, 사용된 용량(GB), 사용률(%)
운영체제 정보	운영체제명, 버전, 서비스팩, IE버전, 언어, 사용자, 조직, 컴퓨터명, 도메인, 제품 키, OS가 설치된시각, 방화벽 사용유무, 가동시간, 자동업데이트 시각, 예약작업 사용유무, 원격데스크탑 허용 유무
인터페이스 정보	연결방식, 이름, MAC, IP/NETMASK, 게이트웨이, 장치이름, 링크, 속도, 전송방식, 인터넷연결공유, Promiscuous, SSID
공유 정보	공유명, 타입, 권한, Everyone권한, 경로, 설명, 등록된 시각
사용자계정 정보	사용자명, 계정타입, 암호설정, 로그인 상태, 최근 비밀번호 변경
화면보호기 정보	사용여부, 비밀번호, 대기시간(분), 화면보호기 이름
GPI 검사결과	정책/항목이름, 결과, 검사시각
GPI 점수	규제정책이름, 점수, 검사시각
모니터 정보	모델명, 시리얼, 가로(mm), 세로(mm), 화면크기(inch), 입력타입
프린터 정보	프린터명, 장치명, 포트정보
계정비밀번호 검증 정보	사용자명, 검증결과, 검사시각
WMI 정보수집결과	클래스/속성명, 속성값

노드 상세 - 네트워크정보

네트워크정보

센서와 에이전트를 이용하여 네트워크 정보를 수집합니다.

- 트래픽 정보

Local Mirror 모드인 센서가 있어야 동작합니다.

Mirror 모드인 센서가 해당 노드에서 나가는 패킷을 모두 감지하여 그 정보를 통해 트래픽 정보로 표현합니다.

센서를 Local Mirror 모드로 생성하는 방법은 [시스템관리 페이지](#)의 센서설정 항목을 참조해 주시기 바랍니다.



- 탐지된 AP 목록

AP감지 플러그인을 사용하여 AP를 감지합니다.



- TCP 세션 정보

TCP 세션검사 플러그 인을 활용하여 TCP 세션정보를 감지합니다.



- 탐지된 서비스목록/열린포트 정보

에이전트 없이도 탐지 가능한 항목으로 Genian NAC 센서에 의해 감지되는 항목입니다.

현재 노드에서 동작 혹은 동작했었던 서비스를 감지하며, 열려있는 포트정보도 수집할 수 있습니다.



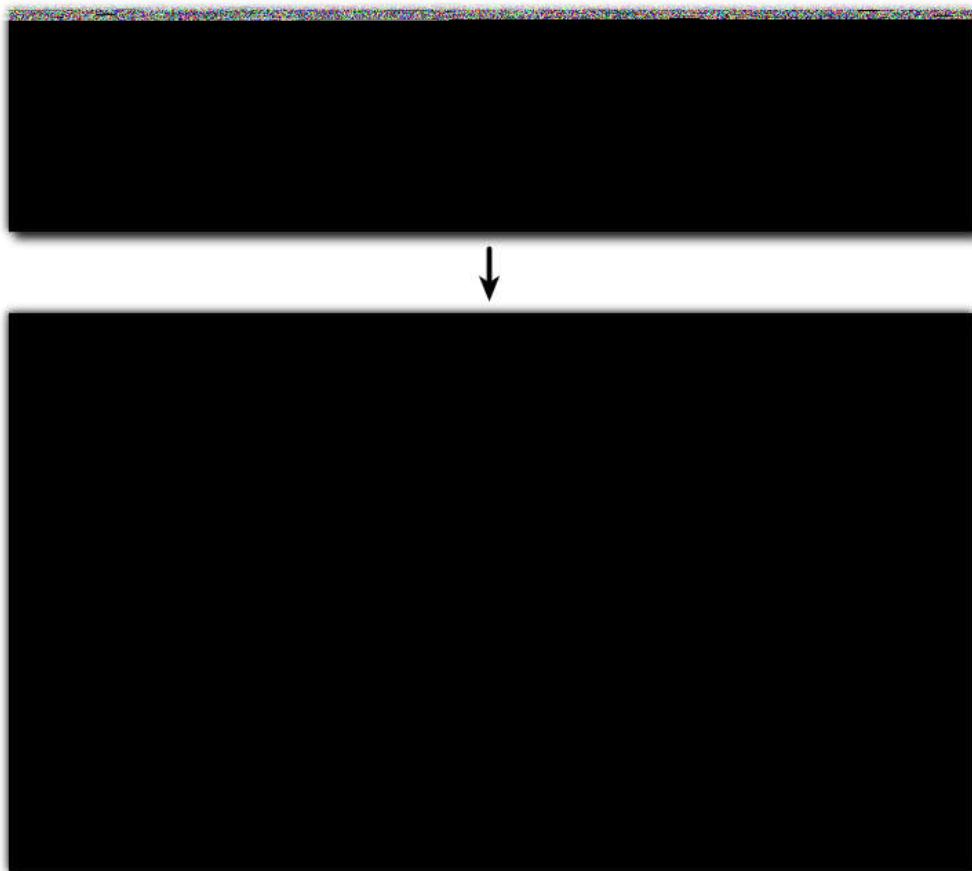
노드 상세 - 소프트웨어정보

소프트웨어정보

에이전트가 플러그 인을 사용하여 노드에 설치가 되어있는 소프트웨어 정보와 백신 정보를 수집하여, 해당 노드에 설치되어 있는 프로그램을 확인할 수 있습니다.
따라서, 해당 노드에 에이전트가 반드시 설치되어 있어야 하고, 노드 정책에서 소프트웨어정보 수집 노드액션이 설정되어 있어야 합니다.



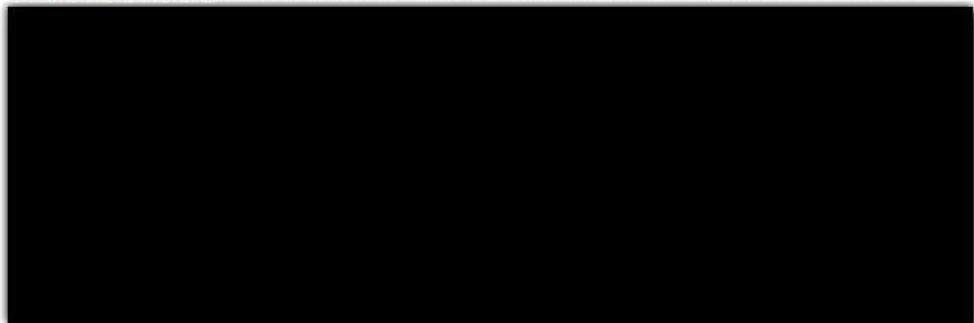
에이전트 정보 포함에 체크하면 Genian Agent 설치정보도 소프트웨어 정보에 포함됩니다.



노드 상세 - 패치정보

패치정보

패치정보 페이지에서 해당노드가 적용받고있는 패치모음과, 최근 수행결과를 확인할 수 있습니다.



- 패치정보

패치의 제목을 선택하면 해당 패치의 상세 정보가 팝업형태로 표시됩니다.



노드 상세 - 이력관리

이력관리

이력관리를 통해 해당 노드의 이력(로그를 통하여)을 조회할 수 있습니다.



아래 그림은 로그 종류를 노드관리로 변경한 모습입니다.



노드 상세 - IP 관리

IP 관리

관리 뷰의 작업선택 > IP 관리에서 하는 작업들을 노드 상세 페이지 > IP 관리에서도 할 수 있습니다.

- IP 정책

IP 차단, IP 충돌보호 설정/해제, IP 사용시간 제한/해제를 수행할 수 있습니다.



각 항목과 설명은 아래 표와 같습니다.

항 목	설 명
IP 차단	해당 노드의 IP를 차단하여 해당 노드의 네트워크를 차단합니다.(위 그림에선 100.100.100.15) 해당 기능의 상세설명은 IP차단 을 참조해 주시기 바랍니다.
IP허용 - 충돌보호 설정/해제	충돌보호설정을 선택하고 MAC 추가 버튼과 삭제 버튼을 통해 MAC을 지정합니다. 충돌보호해제를 선택 시, 설정되어있던 MAC 값들이 모두 삭제됩니다. 다른 사용자가 사용자와 같은 IP를 사용할 경우에 IP 충돌보호가 설정되어 있으면 다른 사용자의 IP가 차단 됩니다. 해당 기능의 상세설명은 IP허용 - 충돌보호(지정MAC) 를 참조해 주시기 바랍니다.
IP 사용시간 시작/종료	IP의 사용시간을 제한/해제하는 기능으로, IP 사용 시작 및 종료에 체크를 하고 사용자가 원하는 날짜와 시간을 선택하여 설정합니다. 해당기능의 상세설명은 IP 사용시간 설정 페이지 를 참조해 주시기 바랍니다.
IP 신규노드정책	미사용 IP에 정책을 할당하는 기능으로, IP 신규노드정책이 설정되어 있는 미사용 IP를 사용하는 사용자는 설정된 IP 신규노드정책을 적용받습니다. 해당 기능의 상세설명은 IP사용 신규노드정책 설정 을 참조해 주시기 바랍니다.

- MAC 정책

MAC 차단, MAC 변경금지 설정/해제, MAC 태그관리, MAC 사용시간 제한/해제를 수행할 수 있습니다.



각 항목과 설명은 아래 표와 같습니다.

항 목	설 명
MAC 차단	해당 노드의 MAC을 차단하여, 해당 노드의 네트워크를 차단 합니다.(위 그림에선 00:1D:92:0F:79:39) 해당 기능의 상세설명은 MAC차단 을 참조해 주시기 바랍니다.
MAC허용 - 변경금지 설정/해제	MAC허용 - 변경금지(지정 IP대역), MAC허용 - 변경금지(모든 IP대역) 중 하나를 선택하고 IP 추가 버튼과 삭제 버튼을 통해 IP를 지정합니다. 변경금지해제를 선택 시, 설정되어있던 IP 값들이 모두 삭제됩니다. 해당기능의 상세설명은 MAC허용 - 변경금지(모든 IP대역) , MAC허용 - 변경금지(지정 IP대역) 를 참조해 주시기 바랍니다.
태그	MAC에 태그를 설정하여, 쉽게 식별할 수 있게 합니다. 해당기능의 상세설명은 MAC 태그 설정 을 참조해 주시기 바랍니다.
MAC 사용시간 시작/종료	MAC의 사용시간을 제한/해제하는 기능으로, MAC 사용 및 종료에 체크하고 사용자가 원하는 날짜와 시간을 선택하여 설정합니다. 해당기능의 상세 설명은 MAC 사용시간 설정 페이지 를 참조해 주시기 바랍니다.

노드 상세 - 정책

정책

노드 상세 페이지 > 정책에서 사용자인증, 호스트명 제한, 노드 관리 설정을 할 수 있습니다.

- 사용자인증 정책

사용자인증에 대한 설정을 할 수 있습니다.



항목에 대한 설명은 아래 표와 같습니다.

항 목 이 름	설 명
사용자인증 노드정책준수	이 항목에 체크를 하게되면 해당노드는 노드정책에서 정의한 사용자인증 정책을 따르게됩니다.
사용자인증 적용 - 모든 사용자	해당 노드에 어떤 사용자든 인증만 거치면 네트워크를 사용할 수 있습니다.
사용자인증 적용 - 사용자제한	해당 항목에 할당되어있는 사용자와 사용자그룹만이 현재 노드에서 인증을 받을 수 있습니다.

- 호스트명 제한 정책

현재 노드를 사용하는 노드에 호스트명 제한을 설정하여 지정한 호스트명이 아닐시에는 호스트명 위반상태로 상태가 변경됩니다. 해당 항목의 자세한 상세 내용은 [IP 사용 호스트명제한 페이지](#)를 참조해 주시기 바랍니다.



- 노드 관리 설정

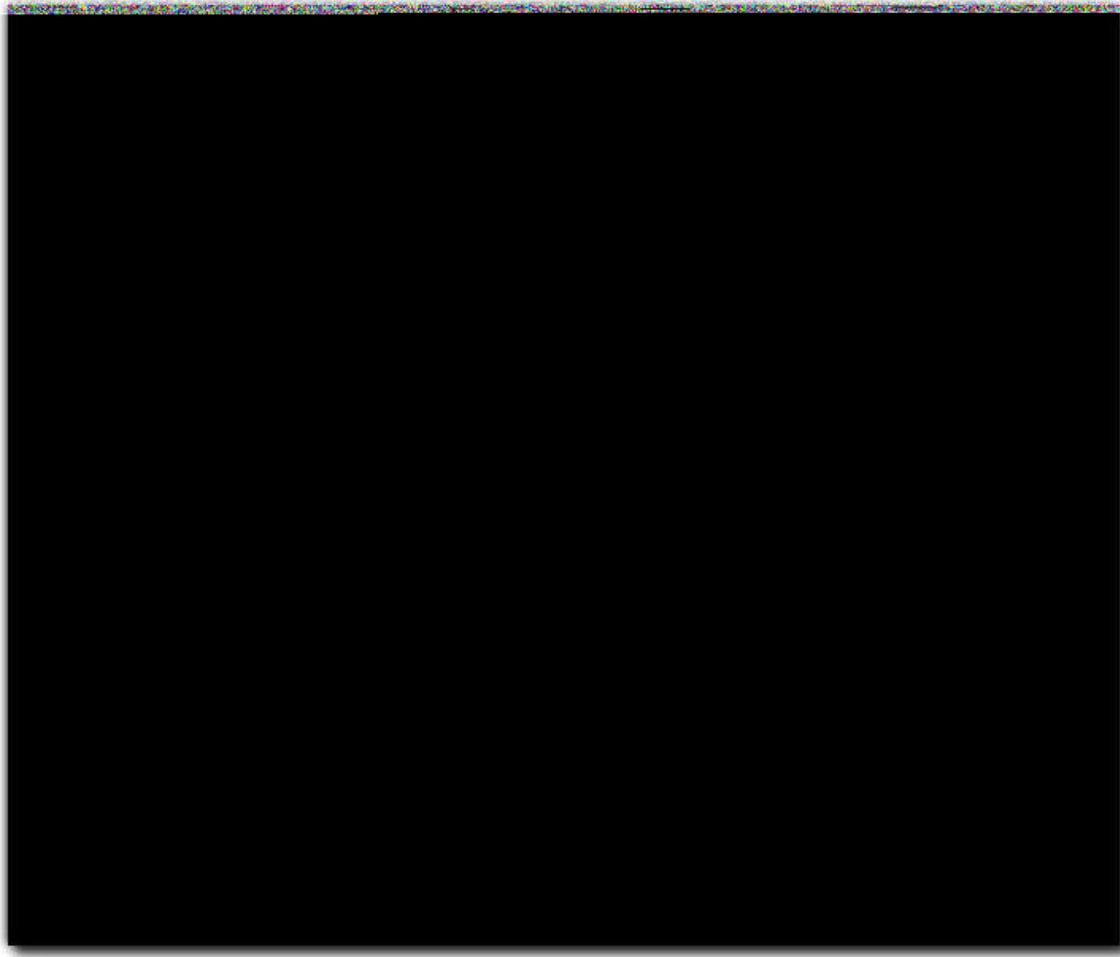
제한감사기록, 노드정보 스캐닝, 노드삭제 금지 유무를 설정합니다.
해당 설정의 상세설명은 [노드정책설정 페이지](#)를 참조해 주시기 바랍니다.



노드 상세 - 정책현황

정책현황

정책현황 페이지를 통하여 관리자는 해당 노드가 받고 있는 정책, 속해있는 노드그룹, 장치제어정책, 발생시킨 위험, 에이전트액션 수행결과를 볼 수 있습니다.



각 항목의 설명은 아래와 같습니다.

항목	설명
노드&제어 정책	해당 노드가 받고 있는 제어정책, 노드정책을 나타냅니다.
사용자동의	해당 노드가 보안서약 및 사용자정보를 동의한 시각을 나타냅니다.
노드 그룹	해당 노드가 속해 있는 노드그룹을 나타냅니다.
장치제어정책	해당 노드가 받고 있는 장치제어 정책을 나타냅니다. 장치제어 정책을 적용받지 않을 시 출력되지 않습니다.
위험감지	해당 노드에 발생한 위험감지를 나타냅니다.
에이전트액션 수행결과	해당 노드가 받고 있는 에이전트 액션의 수행결과를 나타냅니다.

IP주소

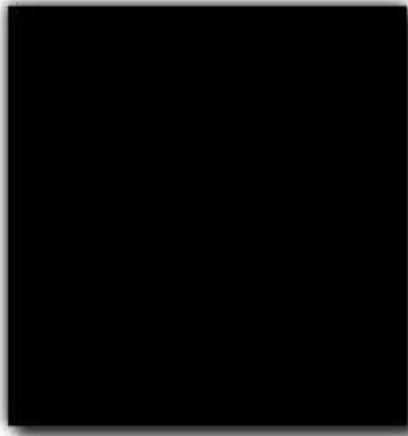
IP주소

관리자는 관리 > IP주소 를 이용하여 센서가 관리하는 IP대역을 대상으로 에이전트 사용 및 설치, 노드 UP DOWN, IP사용 현황 등을 확인할 수 있으며, IP Matrix view를 통하여 센서가 관리하는 IP대역의 IP를 관리 할 수 있습니다.

IP주소의 뷰 구성은 트리뷰와 관리뷰로 구성되었습니다.

- **트리 뷰**

상위트리에 센터가 있으며, 하위트리에서 센터와 연결되어 있는 센서를 확인할 수 있습니다.
센서를 클릭할 시 클릭한 센서가 관리하는 IP대역의 IP Matrix View를 확인할 수 있습니다.
IP주소의 트리 뷰는 관리 > 노드 의 트리 뷰와 연동되어 있습니다.



- **관리 뷰**

센서의 정보와 노드, 에이전트, IP에 대한 정보를 테이블 형식으로 확인할 수 있습니다.
내보내기 기능이 있으며, 센서 이름 항목에 있는 센서 IP를 클릭할 시 클릭한 센서가 관리하는 IP대역의 IP Matrix View를 확인할 수 있습니다.



트리 뷰

관리자는 트리 뷰에서 IP의 현재 상태를 확인하고 싶은 센서의 IP를 클릭하여 클릭한 센서가 관리하는 IP대역의 IP Matrix View를 확인할 수 있습니다.

- **트리 뷰**

센서의 IP를 클릭하여 클릭한 센서가 관리하는 IP대역의 IP Matrix View를 확인할 수 있습니다.



관리 뷰

센서의 정보와 노드, 에이전트, IP에 대한 정보를 테이블 형식으로 확인할 수 있습니다.

- 항목

IP 주소 관리 뷰에 다양한 항목이 있으며 항목을 보고 해당 센서가 관리하는 IP대역의 에이전트, 노트, IP사용 현황을 알 수 있습니다.

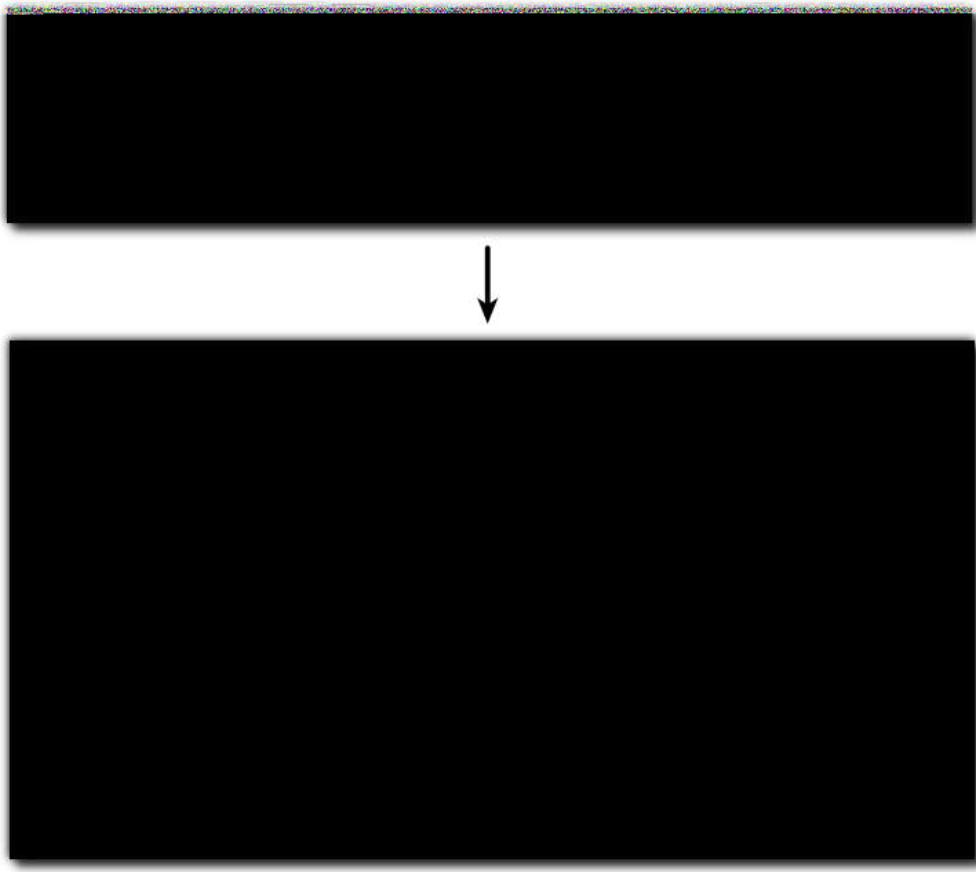


항목에 대한 내용은 아래의 표와 같습니다.

항목	내용
장비명	센서의 호스트명을 확인할 수 있습니다.
센서명	NAC에서 설정한 센서의 이름을 확인할 수 있으며, 센서 이름을 클릭하여 해당 센서가 관리하는 IP Matrix View를 확인 할 수 있습니다.
인터페이스명	인터페이스 이름을 확인할 수 있습니다.
IP	센서의 IP 및 서브넷을 확인할 수 있습니다.
노드개수	센서에 포함되어 있는 노드 수를 확인할 수 있습니다.
UP노드 비율	노드개수/UP노드를 백분율로 나타냅니다.
IP사용개수	센서가 관리하는 IP대역 중 사용되고 있는 IP 개수를 확인할 수 있습니다.
IP사용현황	센서가 관리하는 IP대역 중 사용되고 있는 IP 백분율을 나타냅니다.
DHCP Pool	센서가 관리하는 DHCP 대역을 나타냅니다.

- 센서 IP Matrix View

센서이름을 선택하여 해당 센서가 관리하는 IP대역의 IP Matrix View를 확인하여 IP 현황을 알 수 있습니다.

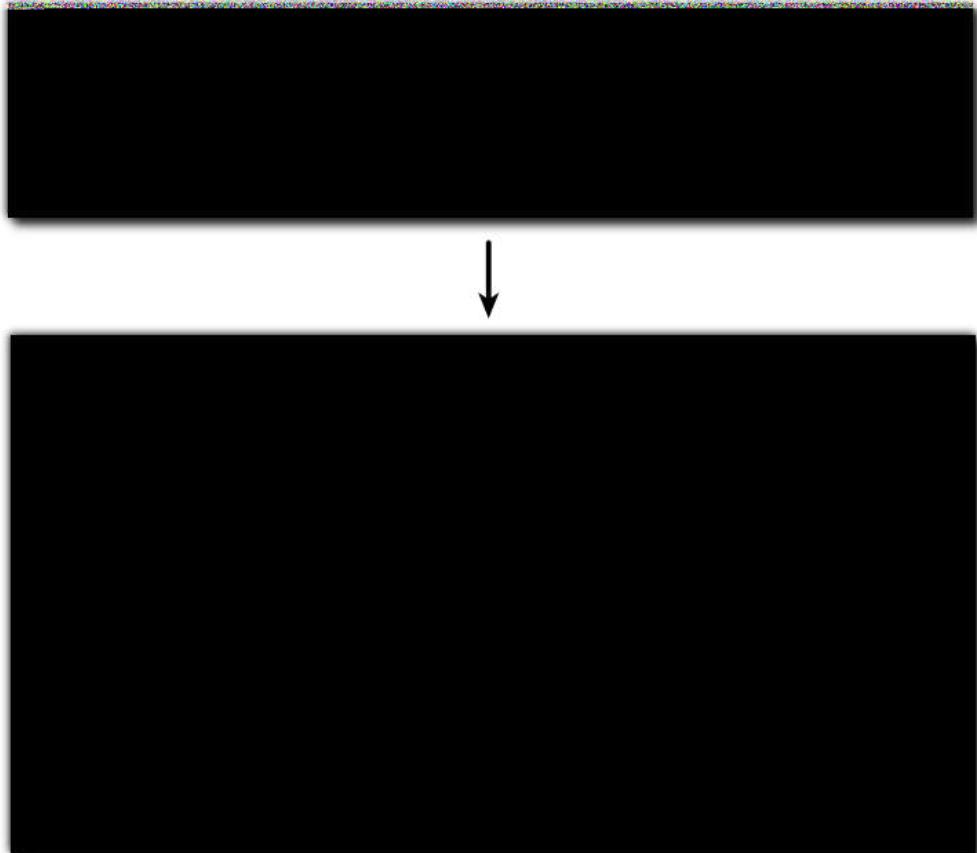


IP주소 - IP Matrix View

IP Matrix View란?

IP주소 - IP Matrix View는 센서가 관리하는 IP 대역의 현황 쉽게 파악할 수 있으며, IP를 선택하여 IP차단, 총돌보호 등의 설정을 할 수 있습니다.

IP의 상태별로 기호가 바뀌며, 관리자는 기호를 확인하여 IP 상태를 확인할 수 있습니다. 관리자는 기호의 색상을 변경할 수 있습니다. IP Matrix View는 센서 이름을 클릭하여 접속할 수 있습니다.



IP Matrix View

- IP Matrix View

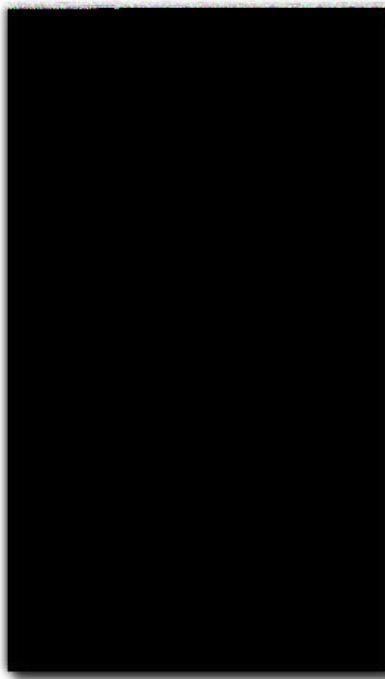
IP Matrix View 페이지의 기능은 아래와 같습니다.



작업 이름	설명
① 작업선택	IP를 선택한 후 작업선택 기능을 이용하여 다양한 설정을 할 수 있습니다. 현재 사용중이지 않은 IP에 설정을 할 경우 노드가 설정된 IP를 사용하게 되면 노드에게 설정값이 적용됩니다. 자세한 사항은 IP Matrix View - 작업선택 을 참고 바랍니다.
② 선택취소	여러 IP를 선택한 경우, 선택취소 버튼을 클릭하여 모든 IP 선택을 취소합니다.
③ 노드관리	관리 > 노드 의 관리 뷰와 같이 노드를 테이블 형식으로 보여주는 페이지로 이동합니다.

- Legend

상태에 따른 IP를 표현할 기호가 담긴 뷰입니다. 기호의 그림을 클릭할 시 IP Matrix View에 해당 기호는 제외시키고 볼 수 있으며, 해당 센서의 Netmask, gateway를 확인할 수 있습니다.
관리자는 기호의 색상과 속성을 변경할 수 있습니다.



상태	설명
사용중 IP	현재 노드 관리 뷰에 등록되어 있는 IP를 나타냅니다.
미사용 IP	현재 사용중이지 않는 IP를 나타냅니다.
Net/Broad IP	네트워크 주소와 브로드캐스트 주소를 나타냅니다.
DHCP Pool	DHCP로 사용할 IP 대역을 나타냅니다.
IP차단	IP가 차단된 상태의 IP를 나타냅니다.

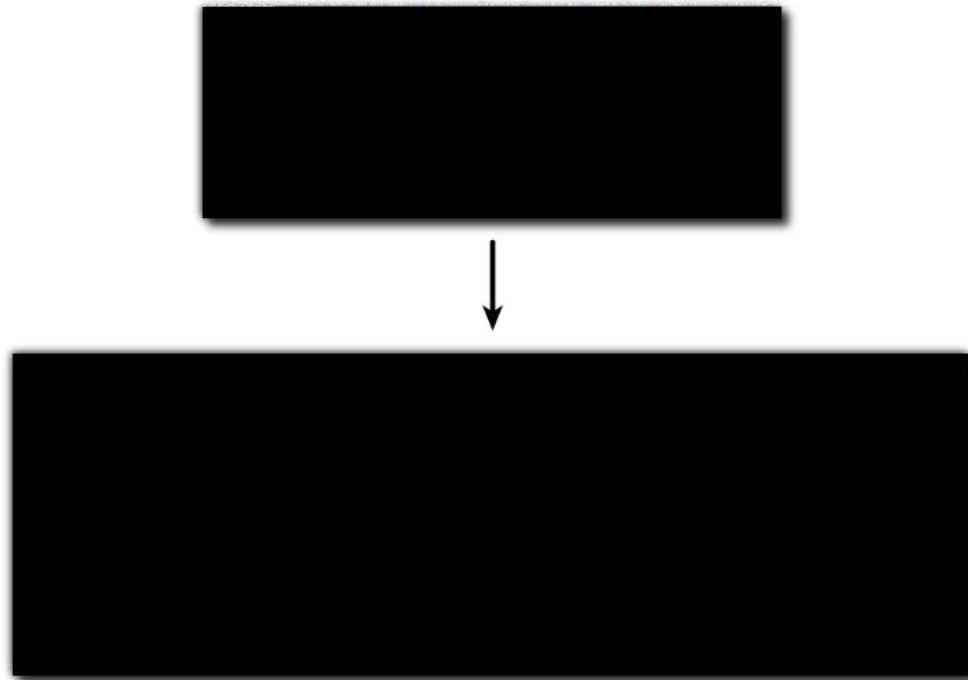
Node Up	동작상태가 UP인 IP를 나타냅니다.
DHCP	DHCP로 할당받은 IP를 나타냅니다.
iP Reserved	예약된 IP를 나타냅니다.

- Legend 속성 설정

- Legend 기호 우측에 있는 수레바퀴 모양의 아이콘을 클릭합니다.



- 속성 설정 팝업창에서 속성과 속성색상을 선택 후 저장버튼을 클릭합니다. 총돌보호를 적용 중인 IP는 아래 그림과 같이 표시됩니다.



- IP 상세보기

IP Matrix View에서 마우스 커서를 IP에 가져다 놓을 시 해당 IP의 노드타입, IP, MAC, 인증정보, 부서, 호스트, 플랫폼, 동작상태, 정책현황 등을 알 수 있고, 표시되는 IP를 클릭할 시 해당 IP의 상세정보 페이지로 이동됩니다.



IP Matrix View - 작업선택

IP Matrix View - 작업선택

관리자는 관리 > IP주소 > IP Matrix View > 작업선택에서 IP관련 작업을 할 수 있습니다.
IP Matrix View의 작업선택 기능은 관리 > 노드 의 작업항목과 같습니다.



작업항목	내용
노드등록	관리자가 수동으로 노드를 등록합니다, 노드등록 을 참고바랍니다, IP 다중 선택 후 노드등록 시 MAC 없이 선택한 IP로 노드가 등록됩니다.
노드삭제	사용하지 않는 IP를 반납하여 해당 IP를 다른 사용자가 사용할 수 있도록 합니다, 자세한 내용은 노드삭제 을 참고바랍니다.
IP차단	IP를 차단 하여 네트워크를 사용하지 못하게 합니다, 자세한 내용은 IP차단 을 참고바랍니다.
IP(모든MAC)허용 - 총돌보호해제	총돌보호 설정을 해제 합니다, 자세한 내용은 IP허용 - 총돌보호해제 을 참고바랍니다.
IP(지정MAC)허용 - 총돌보호설정	해당 IP를 현재 사용자 외 다른 사용가 사용하지 못하도록 합니다, 자세한 내용은 MAC허용 - 변경금지(지정 IP대역) 를 참고바랍니다.
IP 총돌보호 및 변경금지 설정	해당 IP를 현재 사용자 외 다른 사용자가 사용하지 못하도록 하고, 현재 사용자는 IP를 변경할 수 없도록 합니다, 자세한 내용은 IP 총돌보호 및 변경금지 설정 을 참고바랍니다.
IP사용 신규노드정책 설정	미사용 IP에 IP사용 신규노드정책 설정하여 해당 IP를 사용하는 노드에게 신규노드정책을 적용합니다, 자세한 내용은 IP사용 신규노드정책 설정 을 참고바랍니다.
IP 사용시간 제한/해제 설정	IP를 사용할 수 있는 사용시간을 설정하고, 설정된 사용시간 해제할 수 있습니다, 자세한 내용은 IP 사용시간 제한&해제 설정 을 참고바랍니다.
IP 소유자 설정	IP에 소유자를 설정한 IP를 사용할 시 해당 노드는 설정한 소유자로 설정됩니다, 자세한 내용은 IP 소유자&소유부서 설정 을 참고바랍니다.
IP 소유부서 설정	IP소유부서를 설정한 IP를 사용할 시 해당 노드는 설정한 소유부서에 속하게 됩니다, 자세한 내용은 IP 소유자&소유부서 설정 을 참고바랍니다.
IP 용도 설정	IP용도를 설정한 IP를 사용할 시 해당 노드는 설정한 용도를 적용받습니다, 자세한 내용은 IP용도설정 을 참고바랍니다.

스위치

스위치

센서와 연결된 스위치를 확인 할 수 있으며, 스위치 포트의 트래픽이나 연결상태, 접속정보, 속도 등의 정보를 확인 할 수 있습니다. 스위치의 뷰 구성은 트리 뷰, 관리 뷰, 현황&필터 뷰로 구성되어 있습니다.

- 트리 뷰

센서와 연결된 스위치를 확인 할 수 있습니다.
해당 스위치를 클릭할 시 관리 뷰를 통하여 스위치 정보를 확인 할 수 있습니다.



- 현황&필터 뷰

모든 스위치의 연결상태, 보안상태, Duplex, 802.1x 등의 현황을 그래프로 확인 할 수 있습니다.



- 관리 뷰

스위치 포트의 접속 정보, 연결상태, Duplex, 속도, 트래픽, 포트보안, 802.1x 등의 정보를 확인 할 수 있으며, 작업선택을 클릭하여 관리 뷰를 편집 할 수 있습니다.



트리 뷰

관리자는 트리 뷰를 통하여 센서와 연결된 스위치를 확인 할 수 있습니다.

- 전체 스위치포트

관리자는 전체스위치포트를 클릭하여 모든 스위치의 포트에 대한 정보를 관리 뷰를 통하여 확인 할 수 있으며, 확인하고 싶은 스위치의 이름을 클릭하여 해당 스위치의 포트의 정보만 관리 뷰를 통하여 확인 할 수 있습니다.



- 스위치관리

관리자는 스위치관리를 클릭하여 해당 센서와 연결된 스위치를 확인 할 수 있으며, 스위치의 동작시간, 시리얼넘버, 모델명 등의 스위치 정보를 테이블 형식으로 확인 할 수 있습니다. 작업선택 > 삭제 버튼으로 스위츠를 삭제할 수 있습니다.



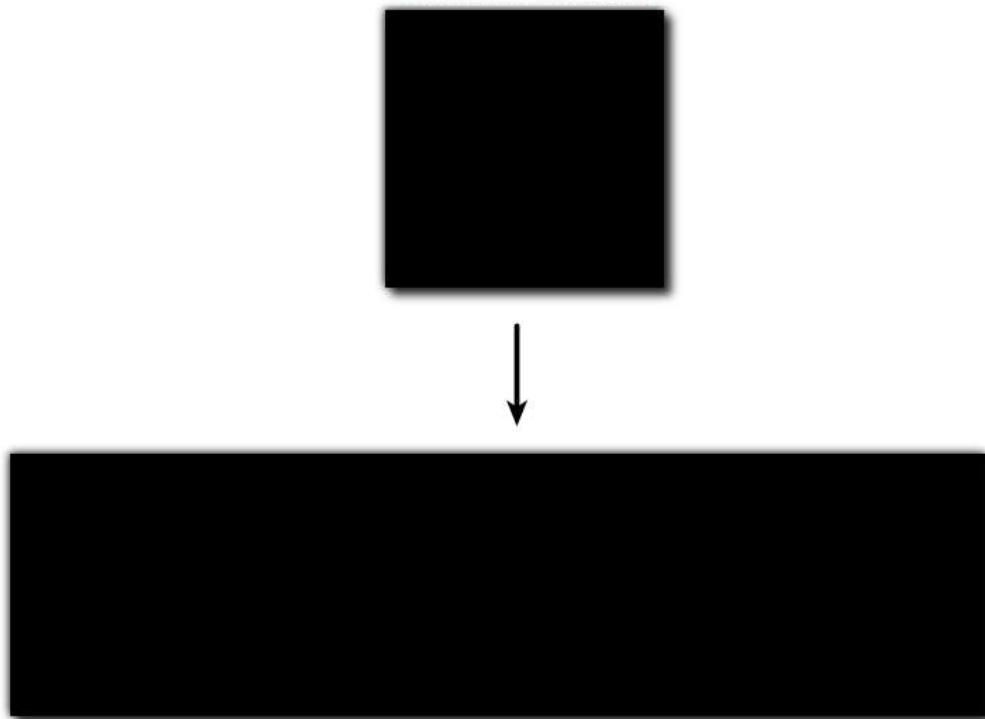
현황&필터 뷰

트리 뷰에서 선택한 스위치의 연결상태, 포트보안, Duplex, 802.1x 등의 현황을 테이블 형식으로 확인 할 수 있습니다.

- 현황&필터

관리자는 트리 뷰에서 스위치를 선택한 후 현황&필터에서 확인하고 싶은 정보를 클릭할 시 아래의 그림과 같이 그래프로 정보를 확인할 수 있습니다.

그래프에서 나타내는 숫자를 클릭할 시 해당 스위치 포트들을 관리 뷰를 통하여 확인 할 수 있습니다.



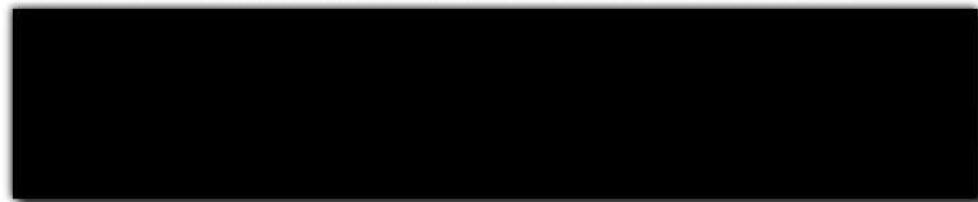
관리 뷰

관리자는 관리 뷰를 통하여 스위치 포트의 트래픽, 접속 정보, Utilization, VLAN ID, 포트보안, 802.1x, 속도에 대한 정보를 테이블 형식으로 확인할 수 있습니다.

디스크 모양을 클릭하여 스위치 포트 정보를 엑셀파일로 내보내기 할 수 있습니다.

- 항목

스위치 관리 뷰에 다양한 항목이 있으며, 항목을 보고 스위치에 대한 정보를 확인할 수 있습니다.
항목은 작업선택 > 관리뷰 편집 으로 편집 할 수 있습니다.



항목에 대한 내용은 아래의 표와 같습니다.

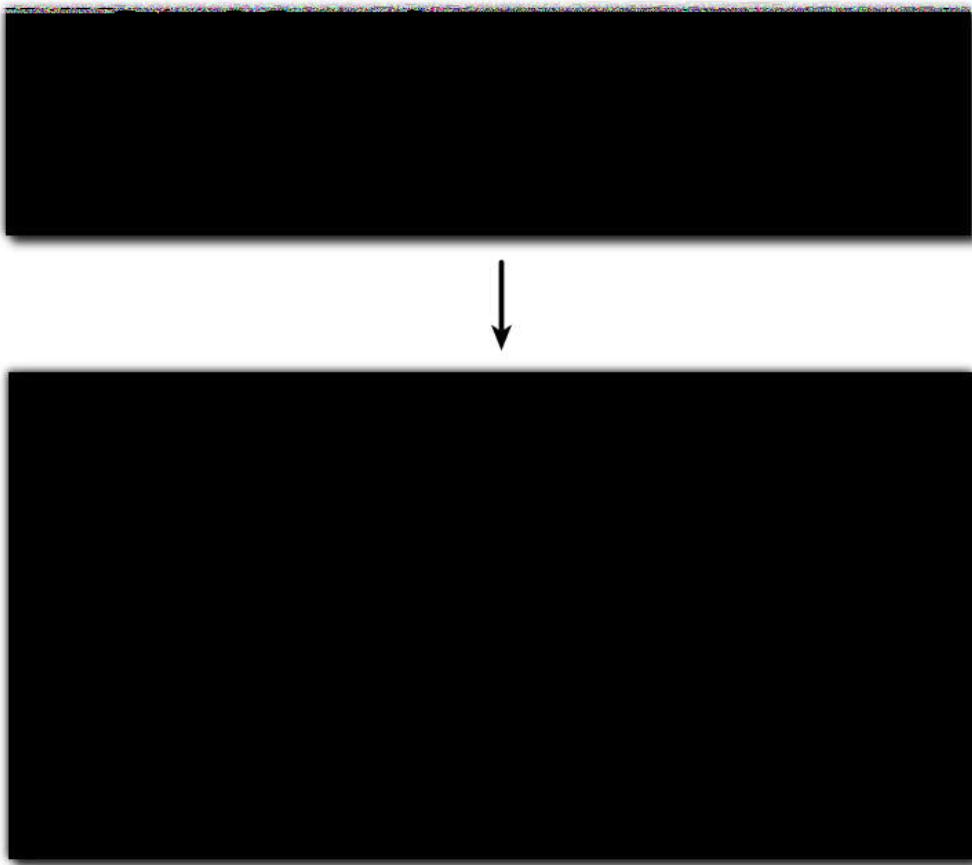
항목	내용
스위치/포트#	스위치의 이름과 스위치 포트 번호를 나타냅니다.
이름	스위치 포트의 이름을 나타냅니다.
설명	스위치 포트의 설명을 나타냅니다.
접속사용자	해당 포트를 사용 중인 사용자 중 사용자 인증을 받은 사용자의 이름을 나타냅니다.

접속호스트	해당 포트를 사용 중인 사용자의 호스트명을 나타냅니다.
접속 IP/MAC	해당 포트를 사용 중인 IP/MAC을 나타냅니다. 마우스 오버 시 상세히 볼 수 있습니다.
노드	해당 포트를 사용 중인 사용자 중 NAC에 노드로 등록되어 있는 노드를 나타냅니다.
MACs	해당 포트를 사용 중인 모든 MAC를 나타냅니다. Trunk Port일 경우 표시되지 않습니다.
타입	해당 스위치 포트의 타입(전화라인, 파워라인 등등)을 나타냅니다.
연결	해당 스위치 포트의 사용 여부를 나타냅니다.
관리자Down	해당 스위치 포트를 관리자가 "shutdown" 하였을 경우 표시됩니다.
Duplex	해당 스위치 포트의 Duplex 모드를 나타냅니다.
속도	해당 스위치 포트의 인터넷 속도를 나타냅니다.
트래픽	SNMP 검색주기 동안의 트래픽량을 1초당 트래픽량(bps)으로 나누어 표시합니다. SNMP 검색주기는 노드관리 에서 노드 위치검색의 검색주기를 참고바랍니다.
Utilization	트래픽 사용률을 나타내며, 사용률이 높을 경우 과부화가 일어날 수 있습니다.
VLAN ID	VLAN ID를 나타냅니다.
Trunk Port	해당 스위치 포트가 Trunk Port 일 경우 Trunk 라고 출력됩니다.
포트보안	해당 스위치 포트의 포트보안 설정 유무를 나타냅니다.
802.1x설정	해당 스위치 포트에 802.1x 설정 유무를 나타냅니다.
허용MAC개수	해당 포트에 연결 할 수 있는 MAC의 개수를 나타냅니다.
스위치	스위치 이름을 나타냅니다.
포트#	포트 번호를 나타냅니다.
수신	수신 누적 트래픽량을 나타냅니다.
송신	송신 누적 트래픽량을 나타냅니다.
포트보안상태	포트보안이 설정되었을 때 포트보안의 상태를 표시합니다. 예 : 허용 MAC 개수를 초과할 경우 포트보안을 위반하였기 때문에 포트보안상태 항목에 차단으로 표시됩니다.
802.1x상태	802.1x가 설정되었을 때 802.1x의 상태를 표시합니다.
갱신시각	스위치 정보를 갱신한 시각을 나타냅니다.
스위치	스위치의 이름을 나타냅니다.

네트워크 - 스위치 상세 정보

스위치 상세 정보

관리자는 네트워크 페이지에서 스위치의 이름을 선택하여 스위치 상세 정보를 확인 할 수 있습니다.



스위치 상세 정보 페이지의 내용은 아래와 같습니다.

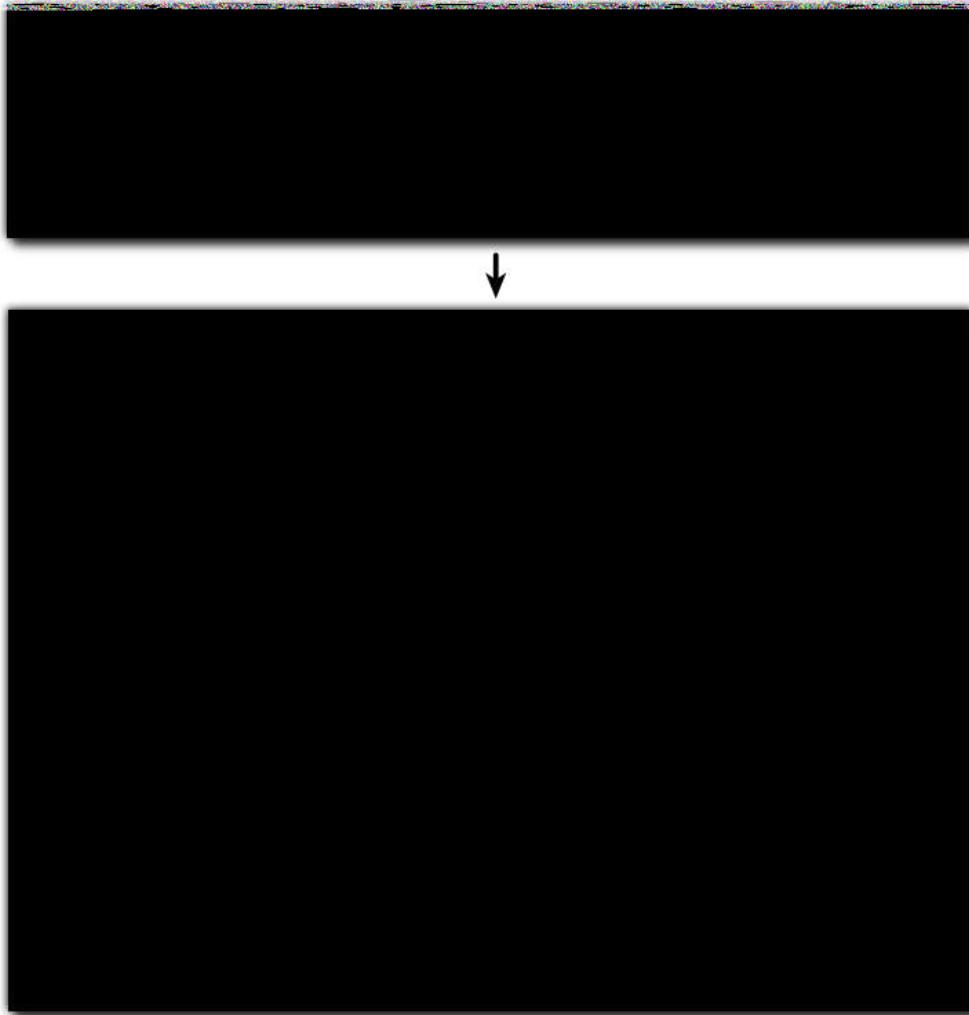
항목	내용
스위치ID	스위치의 MAC을 나타냅니다.
스위치명	스위치의 이름을 나타냅니다.
IP주소	스위치 IP
가용/전체 포트	스위치 포트 중 사용하는 포트의 개수와 전체 포트의 개수
포트보안	포트보안 지원 여부를 나타냅니다.
802.1x	802.1x 지원 여부와 현재 사용 여부를 나타냅니다.
갱신시각	스위치 정보를 갱신한 시각을 나타냅니다.
동작시간	스위치의 동작 시간을 나타냅니다.
シリ얼넘버	스위치의シリ얼넘버
모델명	스위치의 모델명
설명	스위치에 대한 설명
SNMP 버전	SNMP 통신을 위해 SNMP 버전을 선택 할 수 있습니다.
SNMP 정보수집	스위치 정보수집을 비활성화 할 수 있습니다.
Read Community	SNMP의 RO 권한의 Community를 설정 할 수 있습니다.
Write Community	SNMP의 RW 권한의 Community를 설정 할 수 있습니다.

네트워크 - 포트 상세 정보

포트 상세 정보

관리자는 네트워크 페이지에서 포트 이름을 클릭하여 포트 상세 정보를 확인 할 수 있습니다.

- 기본정보



포트 상세 정보의 기본정보 내용은 아래와 같습니다.

항목	내용
이름	포트의 이름
설명	포트 설명, 관리 > 스위치 > 스위치관리 > 스위치상세정보에 Write Community가 설정되었을 경우 설명을 수정할 수 있습니다.
연결상태	현재 포트 사용 여부
Duplex	Duplex 모드를 나타냅니다.
트래픽	SNMP 검색주기 동안의 트래픽량을 1초당 트래픽량(bps)으로 나누어 표시합니다. SNMP 검색주기는 노드관리에서 노드 위치검색의 검색주기를 참고바랍니다.
수신	수신 누적 트래픽량을 나타냅니다.
VLAN ID	VLAN ID를 나타냅니다.
포트보안	포트보안 설정 유무를 나타냅니다.
802.1x설정	802.1x의 설정 유무를 나타냅니다.
허용MAC개수	해당 포트에 연결 할 수 있는 MAC의 개수를 나타냅니다.

포트#	포트 번호를 나타냅니다.
타입	포트의 타입(전화라인, 파워라인 등등)을 나타냅니다.
관리자Down	관리자가 포트를 "shut down" 하였을 경우 표시됩니다. 관리 > 스위치 > 스위치관리 > 스위치상세정보 에 Write Community가 설정되었을 경우 NAC에서 포트를 shut down 할 수 있습니다.
속도	인터넷 속도를 나타냅니다.
Utilization	트래픽 사용률을 나타내며, 사용률이 높을 경우 과부화가 일어날 수 있습니다.
송신	송신 누적 트래픽량을 나타냅니다.
Trunk Port	해당 스위치 포트가 Trunk Port 일 경우 Trunk 라고 출력됩니다.
포트보안상태	포트보안이 설정되었을 때 포트보안의 상태를 표시합니다. 예 : 허용 MAC 개수를 초과할 경우 포트보안을 위반하였기 때문에 포트보안상태 항목에 차단으로 표시됩니다.
802.1x상태	802.1x가 설정되었을 때 802.1x의 상태를 표시합니다.
노드	포트에 연결된 노드 수를 표시합니다.
MACs	포트에 연결된 MAC 수를 표시합니다.
갱신시각	스위치 정보를 갱신한 시각을 나타냅니다.

- 접속정보

관리자는 접속정보에서 해당 포트에 접속한 사용자를 확인 할 수 있으며, 접속한 사용자의 MAC, NIC벤더, IP, 호스트명, 인증사용자, 부서명, 위치, 최근접속일자를 확인 할 수 있습니다.

관리 버튼을 클릭 할 시 해당 포트에 접속한 사용자 중 노드 관리 뷰에 등록되어 있는 사용자를 확인 할 수 있습니다.



무선랜

무선랜

최근의 무선환경, BYOD 환경은 연결성, 이동성이 뛰어나고 업무활용도가 높아 업무적인 생산성에 많은 도움이 되지만 보안관리 측면에서는 취약점이 많습니다.

무선환경을 관리하기 위해선 정확한 WAP 감지가 관건입니다. Genian WNAC는 전용 전용무선센서인 Air-Sentry 와 단말에 설치된 Agent를 기반으로 하여 무선 AP를 감지합니다.

Genian WNAC는 기존 NAC가 담당하던 유선에 국한된 환경에 무선 센서를 통합하여 적은 센서로도 최고의 시너지효과를 납니다.

Agent WiFi Plugin은 단말에 설치되는 Agent 내의 무선 plugin으로, Agent가 설치 된 단말이 하나의 센서 역할을 하며, 단말 기반의 WAP 정보 수집을 하여, Air-Sentry WiFi Sensor의 보조 역할을 수행합니다.

Genian WNAC은 이러한 이중 수집구조로 더욱 넓은 범위, 고정 위치(Air-Sentry), 사용자 기반 위치(Agent WiFi plugin)의 AP정보를 수집할 수 있습니다.

무선랜의 뷰 구성

무선랜 관리 페이지 구성은 아래와 같이 트리 뷰, 필터 뷰, 관리 뷰로 나누어져 있습니다.

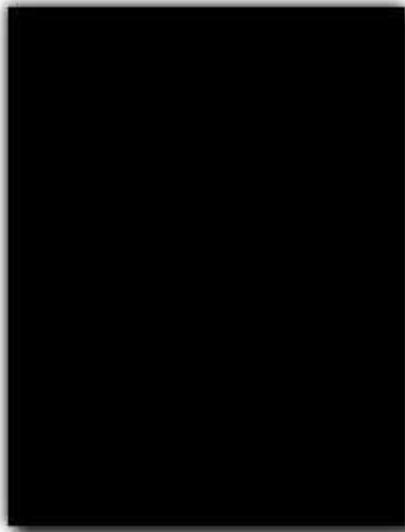
- 트리 뷰

각 무선센서가 수집한 AP를 볼 수 있습니다.



- 필터 뷰

트리 뷰에서 필터링 된 AP들을 바탕으로, 필터 뷰에서는 원하는 조건에 대한 AP만 출력합니다.
조건에는 상태별, 채널별, 신호강도별 등이 있습니다.



- 관리 뷰

트리 뷰와 필터 뷰에서 선택된 조건에 의해 걸러진 노드들이 테이블 형식으로 표시되는 뷰입니다.
작업선택 버튼을 이용하여 무선랜 삭제, 태그할당, 그룹지정/해제 등의 작업을 수행할 수 있습니다.



트리 뷰

트리 뷰에 전체 무선랜 AP, 전체 무선랜 Client를 선택하여 관리 뷰를 통해 무선센서가 탐지한 AP 및 Client를 확인할 수 있습니다. 또한, 특정 무선센서를 선택하여 해당 무선센서가 수집한 AP만을 관리 뷰에서 확인할 수 있습니다.

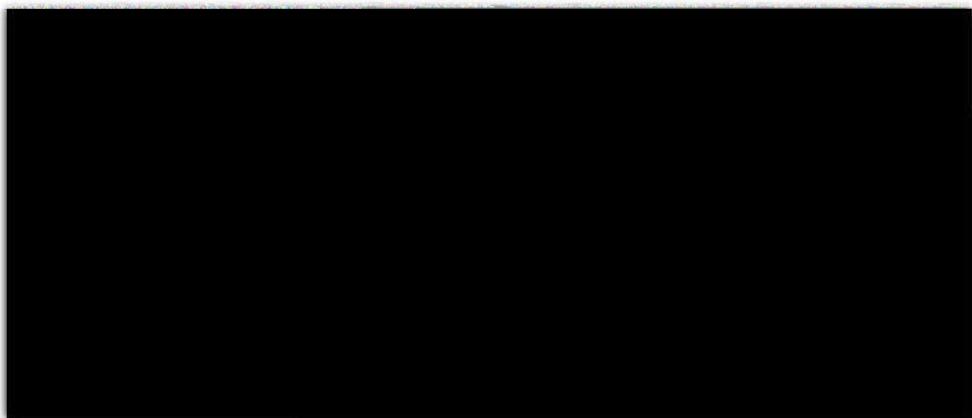
- 무선랜 AP

각 무선센서를 선택하여 선택한 무선센서가 탐지한 AP를 확인할 수 있습니다.



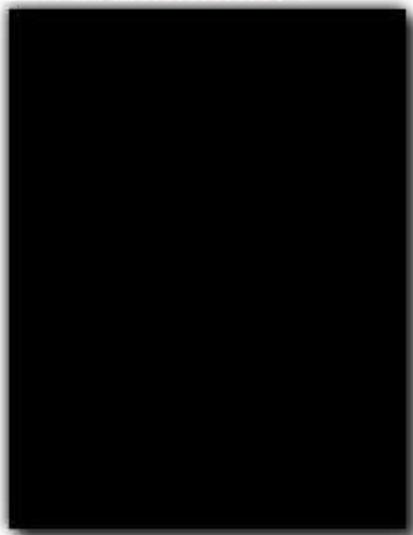
- 무선랜 Client

무선센서가 탐지한 AP에 접근한 Client를 관리 뷰에서 확인할 수 있습니다.



필터 뷰

필터뷰를 통해 관심항목만 선택하여 볼 수 있습니다.



필터 항목은 아래 표와 같습니다.

항 목	세 부 항 목
무선랜그룹	관리자가 만든 그룹
무선랜상태	동작중, 내부, SoftAP, AdHoc, 접속기록, 내부자접속, Hidden
보안설정	프로토콜(OPEN, WEP, WPA, WPA2, WPA or WPA2) 인증방식(PSK, 802.1X)
채널	2.4G 5G
프로토콜	B, G, B/G, B/G/N, A, A/N, AC, AC/N
신호강도	아주높음, 높음, 보통, 낮음, 아주낮음
등록일자	오늘, 1일 이상, 7일 이상, 30일 이상
태그	관리자가 생성해놓은 태그
접속AP	AP별 접속단말 현황을 원 그래프 형식으로 나타냅니다.
중복감지무선랜	두 가지 이상의 위치를 가지고 있는 무선랜을 나타냅니다.

관리 뷰

- 항목

무선랜 관리 뷰에 다양한 항목이 있으며, 항목을 보고 무선랜에 대한 정보를 확인할 수 있습니다.
항목은 작업선택 > 관리뷰 편집 으로 편집할 수 있습니다.



항목	내용
내부	AP가 센서와 같은 네트워크에 속하면 내부에 체크가 됩니다. 탐지에 의해 자동으로 체크가 됩니다.
접속(내부)	AP에 접속한 단말 중 NAC에 등록된 노드의 수를 나타냅니다.
접속(전체)	AP에 접속한 단말의 수를 나타냅니다.
동작	AP의 동작상태를 나타냅니다.
SSID	AP의 고유 식별자를 나타냅니다.
MAC	AP의 MAC을 나타냅니다.
제조업체	AP의 제조업체를 나타냅니다.
암호화방식	AP가 사용중인 암호화 방식을 나타냅니다.
규약	AP가 지원하는 규약을 나타냅니다.
채널	AP의 채널을 나타냅니다.
신호강도(dBm)	AP의 신호강도를 나타냅니다.
위치	AP를 탐지한 무선센서를 나타내며, 신호가 강한 순으로 정렬됩니다.
등록시각	NAC에 해당 AP가 등록된 시각을 나타냅니다.
이름	AP에 설정한 이름을 나타냅니다.
마지막 동작시각	AP의 동작상태가 DOWN 일 경우에 나타나며, UP에서 DOWN으로 변경된 시각을 나타냅니다.
SoftAP	AP가 SoftAp 일 경우 체크로 표시됩니다.
AdHoc	AdHoc 모드를 사용중일 경우 표시됩니다.
Hidden	Hidden 설정이 적용된 AP일 경우 체크로 표시됩니다.
태그	AP에 설정한 태그를 나타냅니다.

- 무선랜 Client 항목

무선랜 관리 뷰에 다양한 항목이 있으며, 항목을 보고 무선랜에 대한 정보를 확인할 수 있습니다. 항목은 작업선택 > 관리뷰 편집으로 편집할 수 있습니다.



항목	내용
MAC	Client의 MAC을 나타냅니다.
NIC벤더	Client의 NIC벤더를 나타냅니다.
접속 AP	Client가 접속한 AP의 SSID를 나타냅니다.
IP	NAC 노드로 등록된 Client의 경우 Client의 IP를 나타냅니다.
상태	NAC 노드로 등록된 Client의 경우 Client의 상태를 나타냅니다.
호스트명	NAC 노드로 등록된 Client의 경우 Client의 호스트명을 나타냅니다.
인증사용자	NAC 노드로 등록된 Client의 경우 인증사용자의 이름을 나타냅니다.
위치	NAC 노드로 등록된 Client의 경우 Client를 노드로 등록한 장비를 나타냅니다.
최근접속일자	Client가 AP에 최근에 접속한 일자를 나타냅니다.
등록시각	Client가 최초로 AP에 접속한 시각을 나타냅니다.
부서명	NAC 노드로 등록된 Client의 경우 인증사용자의 부서명을 나타냅니다.

- 작업선택

관리 뷰는 센서별, 필터로 걸러진 무선랜 목록을 나타내어 주고 작업선택버튼을 통하여 여러가지 작업을 지원합니다.



- 무선랜 등록

관리자는 SSID가 수집되지 않는 AP에 접속이 필요한 경우 수동으로 무선랜을 등록하여 AP에 접근할 수 있습니다. 무선랜 등록 방법은 [노드등록 페이지](#)를 참고해 주시기 바랍니다.

- 무선랜 삭제

관리자는 관리 범위에서 벗어난, 관리할 필요가 없는 무선랜을 삭제할 수 있습니다. 삭제 방법은 [항목 삭제](#)를 참고해 주시기 바랍니다.

- 무선랜 태그설정

관리자는 무선랜에 미리 만들어진 태그를 할당하여 관리할 수 있습니다. 태그할당 과정은 [노드태그](#)를 할당하는 것과 같습니다. 상세내용은 [노드 태그 설정](#)을 참조해 주시기 바랍니다.

- 무선랜 그룹지정/해제

원하는 원하는 만큼의 무선랜을 선택하여 원하는 무선랜 그룹속에 포함/해제할 수 있습니다. 단, 무선랜그룹의 조건연산이 OR인 그룹만 포함/해제가 가능합니다.
그룹지정/해제 과정은 노드그룹 지정/해제와 같습니다. 상세내용은 [노드그룹 지정&해제](#)를 참조해 주시기 바랍니다.

- 무선랜 속성변경

관리자는 무선랜의 이름, 설명, 삭제금지를 변경할 수 있습니다.
변경방법은 원하는 항목을 체크하면 해당 항목에 대한 설정을 변경할 수 있습니다.
변경내용을 확인하는 방법은 [무선랜 상세 - 기본정보](#)에서 확인할 수 있습니다.



무선랜 - 무선랜 상세 정보

무선랜 상세 정보

무선랜 상세 정보 페이지를 통하여 해당 AP의 기본정보, 위치정보, 접속정보, 이력관리를 확인할 수 있습니다.

상세 정보를 확인하고 싶은 AP의 MAC을 아래와 같이 선택하면 상세 정보 페이지로 이동합니다.



무선랜 상세 - 기본정보

기본정보

기본정보 페이지에서는 해당 AP의 MAC 암호화 방식, SSID 등을 확인할 수 있고, 삭제금지, 내부AP 설정, 이름등을 설정할 수 있습니다.



각 항목에 대한 설명은 아래 표와 같습니다.

항 목 이 름	설 명
DeviceID	Genian NAC가 AP를 관리하기 위하여 붙인 ID
SSID	AP의 고유 식별자
MAC	해당 AP의 MAC
제조업체	해당 AP 제조업체
암호화방식	해당 AP가 사용중인 암호화 방식
등록시각	NAC에 해당 AP가 등록된 시각
동작상태	해당 AP의 동작상태를 나타냅니다.
마지막 동작시각	AP의 동작상태가 DOWN 일 경우에 나타나며, UP에서 DOWN으로 변경된 시각을 나타냅니다.
채널	AP의 채널을 나타냅니다.
규약	해당 AP가 지원하는 규약을 나타냅니다.
내부	해당 AP가 센서와 같은 네트워크에 속하면 내부에 체크가 됩니다. 탐지에 의해 자동으로 체크가 됩니다.
삭제금지	항목에 체크하게 되면 해당 AP는 삭제로부터 보호됩니다.
SoftAp	AP가 SoftAp 일 경우 체크로 표시됩니다.
이름	해당 AP를 쉽게 식별할 수 있는 이름을 설정할 수 있습니다.
Hidden	Hidden 설정이 적용된 AP일 경우 체크로 표시됩니다.
Adhoc	AdHoc 모드를 사용중일 경우 AdHoc 항목에 체크 표시로 표시됩니다.
설명	AP에 대한 설명을 설정할 수 있습니다.
장비내 노드	해당 AP에 접속되어 있는 노드들의 목록을 나타냅니다.
장비내 무선랜	하나의 장비에 여러개의 MAC과 여러 SSID를 가지고 있어도, Genian NAC은 하나의 장비라는 유추가 어느정도 가능합니다. 유추해낸 결과 값은 해당 항목에 표시합니다.
태그	AP에 꼬리표와 같은 태그를 설정하여 편리하게 관리할 수 있습니다 . 태그는 미리 생성되어 있어야 하며, SSID나 MAC 변경 시 태그는 해제됩니다.

무선랜 상세 - 위치정보

위치정보

선택한 AP를 탐지해낸 센서와 탐지해낸 센서의 신호강도를 표시합니다. 센서의 MAC 선택 시, 노드관리 페이지에서 선택한 MAC이 자동 검색됩니다.



위 그림을 보면 센서외에 에이전트도 표시된 것을 볼 수 있습니다.
Genian WNAC는 무선센서 뿐만아니라, 에이전트도 탐지하기 때문에 해당 페이지에 표시됩니다.
호스트명, 인증사용자, 부서명 컬럼은 에이전트만 가질 수 있는 값들이기에 에이전트만 해당됩니다.

무선랜 상세 - 접속정보

접속정보

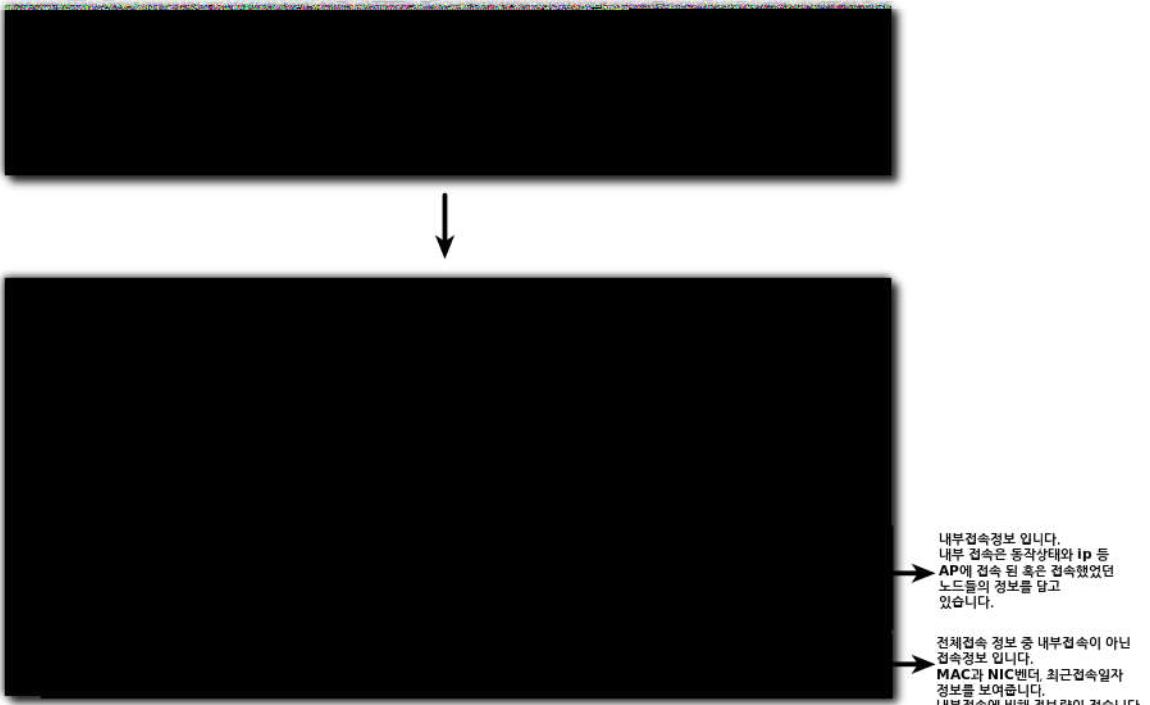
접속정보 페이지를 통하여 해당 AP에 접속했던 노드들의 기록과 현재 사용중인 사용자를 확인할 수 있습니다. 접속정보를 보는 방법에는 무선랜 상세 페이지 > 접속정보 으로 보는방법과, 관리 > 무선랜 > 접속정보 컬럼의 링크를 선택하여 볼 수 있습니다.

아래 그림은 관리 뷰에서 접속컬럼의 링크를 선택하여 접속정보 페이지로 이동하는 모습입니다.



여기서 내부접속이란, Genian NAC의 노드리스트에 노드기록이 존재하는 노드가 해당 AP에 접속하였을때를 말하는 것입니다. 즉, 내부접속이란 DB에 노드정보가 저장되어있는 노드가 AP에 접속 하는것을 말합니다.

아래는 무선랜 목록에서 AP의 MAC을 선택하여 상세 페이지로 이동 한 후, 접속정보를 보는 과정입니다.



무선랜 상세 - 이력관리

이력관리

해당 AP에 관련된 이력을 볼 수 있습니다.
MAC, SSID, 관리노드 중 하나를 선택하여 검색이 가능하며,
전체로그, 노드관리, 노드정보 등 로그의 종류를 선택하여 검색이 가능합니다.



사용자

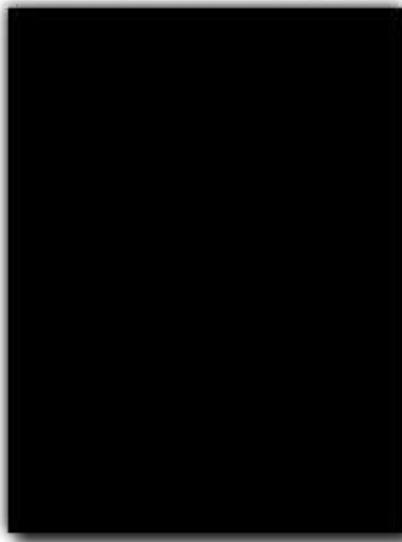
사용자 관리

관리자는 사용자관리 페이지를 통하여 일반사용자, 여러 권한을 가진 관리자들을 통합하여 관리할 수 있습니다.

사용자 뷰는 아래와 같이 세개의 뷰로 이루어져 있습니다.

- 트리 뷰

사용자를 전체사용자, 전체관리자, 부서관리, 직급관리로 나누어 출력합니다.
또한, 부서, 직급별을 선택하면 관리 뷰에서 부서/직급의 관리가 가능해집니다.



- 필터 뷰

사용자의 직급, 연동구분, 관리역할, 용도, 상태, 사용자그룹, 태그 등의 현황을 간략하게
조회하여 더욱 쉽게 사용자를 관리할 수 있습니다.



- 관리 뷰

트리 뷰와 필터 뷰를 거쳐 걸러진 사용자들의 정보를 테이블형식으로 출력합니다.
내보내기 기능과 작업선택버튼을 통한 사용자 관리 기능과 빠른검색기능이 있습니다.
또한, 트리 뷰에서 부서별, 직급별이 선택 되었다면, 부서/직급 뷰가 선택 가능해 지고 부서/직급을 관리할 수 있습니다.



관리 뷰

- 항목

사용자 관리 뷰에 다양한 항목이 있으며, 항목을 보고 사용자에 대한 정보를 확인 할 수 있습니다.
항목은 작업선택 > 관리뷰 편집 으로 편집 할 수 있습니다.

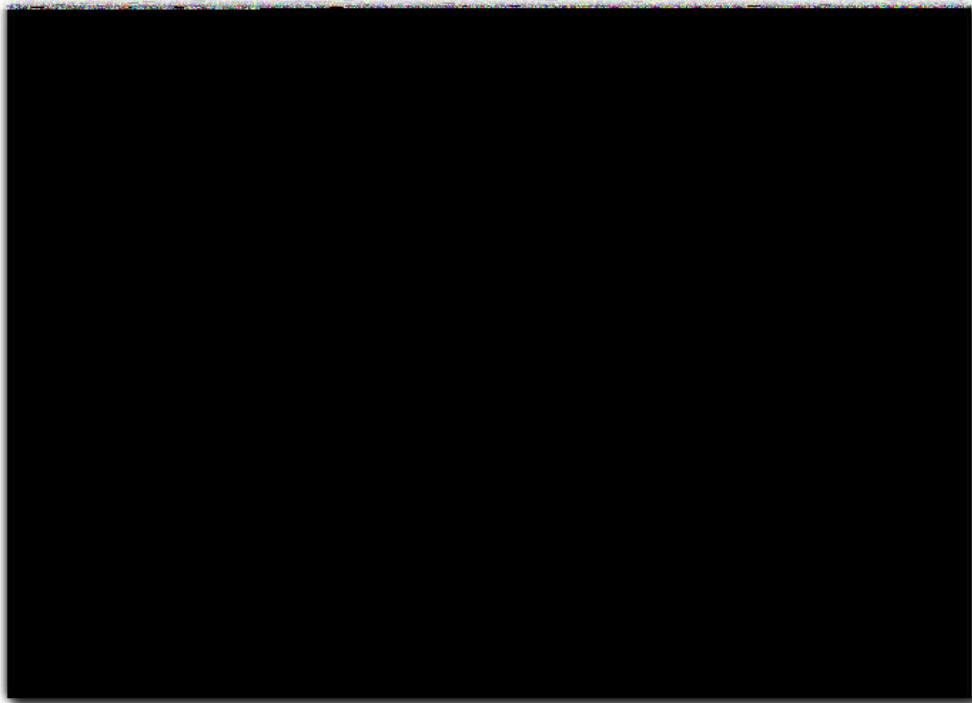


항목에 대한 내용은 아래의 표와 같습니다.

항목	내용
사용자ID	ID를 나타냅니다.
이름	사용자의 이름을 나타냅니다.
용도	ID의 용도를 나타냅니다.
상태	정상과 사용중지가 있으며, 사용중지 상태일 경우 해당 ID로 접속을 할 수 없습니다.
관리역할	권한을 나타냅니다.
부서명	사용자가 속해 있는 부서를 나타냅니다.
직급	사용자의 직급을 나타냅니다.
설명	사용자의 설명을 나타냅니다.
인증노드 수	사용자의 ID로 인증을 받은 노드의 수를 나타냅니다, 클릭 할 시 인증 받은 노드를 확인 할 수 있습니다.
최근인증경과	최근에 인증 받은 시각에서 얼마의 시간이 경과했는지 나타냅니다.
최근인증	최근에 인증 받은 날짜와 시간을 나타냅니다.
IP제한	사용자 ID로 인증을 허용할 IP 개수를 나타냅니다, 아무것도 나타나지 않을 시 허용할 IP 개수를 제한하지 않습니다.
MAC제한	사용자 ID로 인증을 허용할 MAC 개수를 나타냅니다, 아무것도 나타나지 않을 시 MAC 개수를 제한하지 않습니다.
인증허용IP	인증을 허용할 IP를 나타내며 그 외의 IP는 해당 ID로 인증 할 수 없습니다.
인증허용MAC	인증을 허용할 MAC을 나타내며 그 외의 MAC은 해당 ID로 인증 할 수 없습니다.
계정사용만료	ID의 계정만료가 며칠인가를 나타내며, 사용자 ID를 클릭 할 시 더욱 상세한 만료 날짜와 시간을 확인 할 수 있습니다.
PW변경강제	작업선택 > 비밀번호변경 강제화 설정 작업이 수행될 시 표시되며, 다음 로그인 할 때 비밀번호를 무조건 변경하여야 합니다.
태그	사용자 ID에 설정되어 있는 태그를 나타냅니다.
중지사유	계정 상태가 중지일 경우 중지된 사유를 나타냅니다.

- **작업선택**

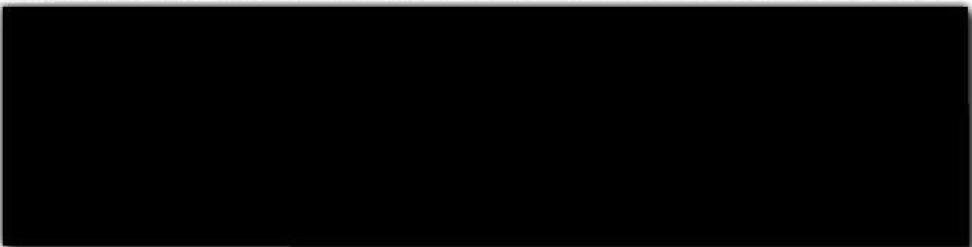
관리자는 작업선택 메뉴를 통하여 사용자 ID를 관리 할 수 있습니다.
자세한 내용은 [사용자 - 작업선택](#)을 참고 바랍니다.



트리 뷰

- 전체사용자

모든 사용자(관리자 포함)를 보여주고 사용자 ID를 클릭하여 사용자 정보를 확인할 수 있습니다.



- 전체관리자

노드 > 사용자 > 트리뷰에서 전체관리자를 선택하여 전체관리자 페이지에 접속할 수 있습니다.
전체관리자 페이지는 권한을 가진 사용자들 즉 관리자들만 모아 놓고, 관리제한 설정을 한눈에 확인할 수 있어 관리자들을 쉽게 관리할 수 있습니다.



노드제한, 사용자제한, 로그제한, 내보내기제한에 대한 내용은 아래의 표와 같습니다.

항목	내용
노드제한	관리제한 설정에서 노드 관리범위 제한이 설정되어 있을 시 표시됩니다. 관리제한 설정에 대한 설명은 사용자 등록&삭제 에서 관리자 설정을 참고 바랍니다.
사용자제한	관리제한 설정에서 사용자 관리범위 제한이 설정되어 있을 시 표시됩니다.
로그제한	관리제한 설정에서 감사로그 검색범위 제한이 설정되어 있을 시 표시됩니다.
내보내기제한	관리제한 설정에서 파일 내보내기 제한이 설정되어 있을 시 표시됩니다.

- 부서/직급 관리

노드 > 사용자 > 트리뷰에서 부서관리/직급관리를 선택하면 관리 뷰에서 부서/직급 관리 뷰 페이지에 접속할 수 있습니다.
부서/직급 관리 뷰에서 작업선택을 통한 부서/직급의 추가, 삭제 등의 관리가 가능합니다.

- 부서 추가

- 작업선택 > 추가를 선택하면 부서를 추가할 수 있는 페이지로 이동하게 됩니다.

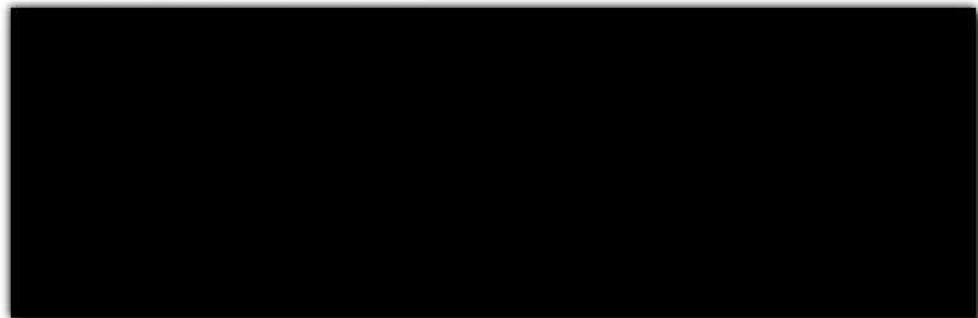


- 부서코드와 부서명을 입력 합니다



- 상위부서를 설정하기 위해 assign을 클릭 합니다.

상위부서가 필요 하지 않을 경우는 어떠한 설정도 하지 않고 넘겨주시면 됩니다.



-
4. 관리자가 원하는 상위부서를 선택 합니다.

상위부서를 설정할 경우 해당 부서는 설정한 상위부서의 하위부서로 생성 됩니다.



5. 노드그룹을 설정하기 위해 할당 버튼을 클릭 하거나 노드그룹 ID를 타이핑합니다.



6. 관리자가 원하는 노드그룹을 클릭 합니다

노드그룹을 설정할 경우 IP신청서 신청 시 설정한 노드그룹에 포함되어 있는 IP를 할당 받게 됩니다.



-
7. 작성이 완료되었으면 아래의 생성버튼을 클릭 합니다.

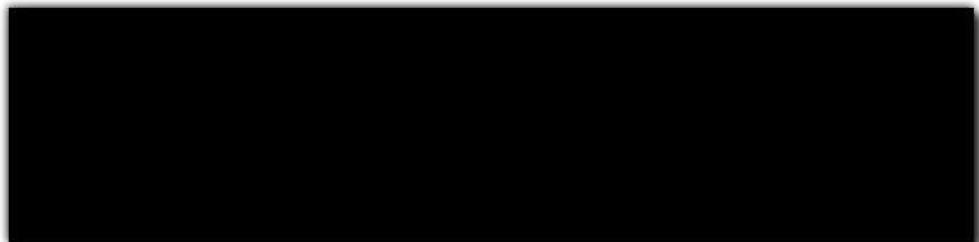


- 직급 추가

1. 작업선택 > 추가 를 선택하면 직급을 추가할 수 있는 페이지로 이동하게 됩니다.



2. 직급코드와 사용하고 싶은 직급명을 입력 후 추가 버튼을 클릭 합니다.



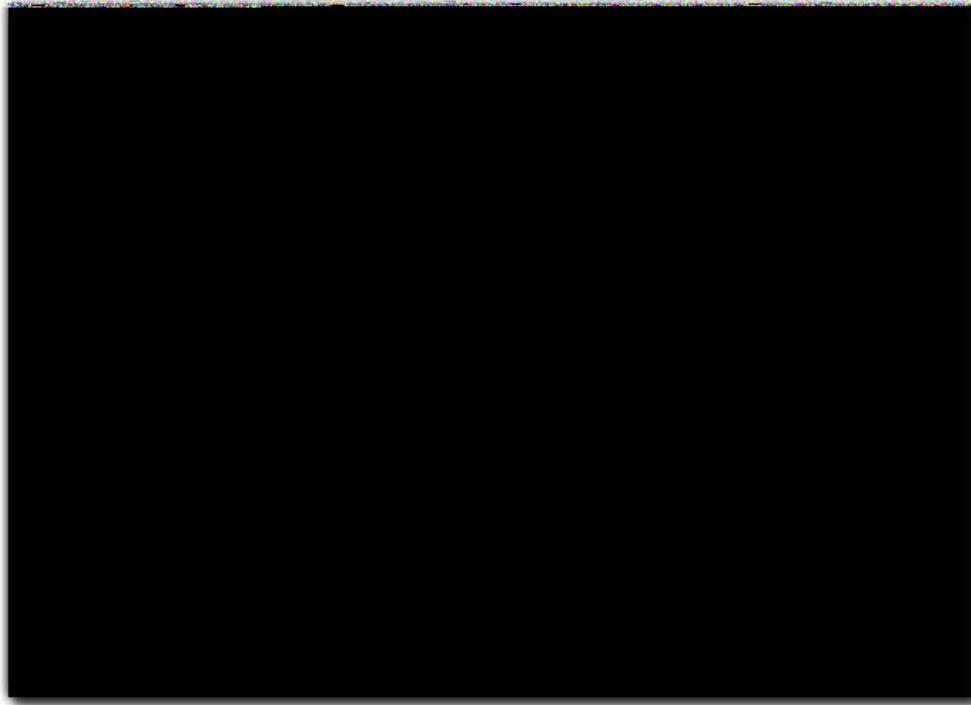
- 부서&직급 삭제

관리자는 필요없는 부서, 직급을 삭제할 수 있습니다.
삭제 절차는 항목 [삭제](#)를 참조해 주시기 바랍니다.

사용자 - 작업선택

사용자 작업선택

관리자는 관리 > 사용자 > 작업선택에서 관리자 등록, 태그 설정, 비밀번호 강제화 등의 작업을 수행하여 사용자의 ID를 관리 할 수 있습니다.
IP관리의 세부 항목은 다음과 같습니다.



- 사용자 등록&삭제
- 사용자 태그 설정
- 사용자그룹 지정&해제
- 사용자용도 설정
- 인증제한 설정
- 정상 상태로 변경
- 사용중지 상태로 변경
- 비밀번호변경 강제화 설정
- 비밀번호변경 강제화 설정(임시비밀번호 발급)
- 사용자만료시각 변경

사용자 등록&삭제

사용자등록

관리자는 사용자등록을 통하여 일반사용자를 등록할 수 있고, 목적에 따른 권한을 부여한 관리자를 등록할 수 있습니다.

- 기본 사용자 등록

1. 기본설정

사용자의 ID와 이름, 용도 등을 설정합니다.



기본설정의 항목과 그에대한 설명은 아래와 같습니다.

항 목 이 름	설 명
사용자 ID	사용자가 사용할 ID를 입력합니다.
이름	사용자의 이름을 입력합니다. 아이디를 분실하여 아이디를 찾기를 이용할 때 필요한 정보입니다.
관리역할	관리자 권한을 부여하기 위해 설정합니다. 일반사용자는 <선택안함>을 선택합니다. 권한의 종류에는 관리역할 을 참조하시기 바랍니다. 권한을 할당할 때 필요한 역할에 맞는 권한을 할당하고, 필요한 역할 이외 다른 기능을 사용할 수 있는 권한은 할당하지 않도록합니다.
설명	부가 설명을 입력합니다.
용도	설정안함, 임시계정, 일반계정 중 선택합니다.
상태	정상과 사용중지 중 선택합니다.
계정사용 만료	계정사용 만료일을 지정합니다. 지정일을 넘으면 해당 ID는 사용이 불가합니다.
태그	사용자에 대해 꼬리표와 같은 태그를 부여합니다. 태그를 조건으로 그룹을 만들 수 있습니다.

2. 비밀번호 설정

비밀번호를 설정합니다. 비밀번호변경 강제를 선택 시, 사용자 혹은 관리자가 해당 ID로 로그인 하였을때, 비밀번호를 반드시 변경해야합니다.



항목	설명
비밀번호	사용할 비밀번호를 입력합니다. 보안을 위해 비밀번호는 대문자/소문자/숫자/특수문자 중 3가지 규칙 조합 및 9자리 이상의 비밀번호를 입력합니다.
비밀번호 확인	비밀번호 확인을 위해 사용할 비밀번호 항목에서 입력했던 비밀번호를 입력합니다.
비밀번호변경 강제	최초 로그인 시 비밀번호를 한번 변경하여야 합니다.

3. 인증제한 설정

해당 사용자가 인증가능한 IP 와 MAC 의 개수를 설정하고, 인증가능한 IP와 MAC의 범위를 제한 합니다.



항목	설명
IP 인증제한	중복 인증을 허용할 IP의 개수를 설정합니다. 0으로 입력 시 중복 인증을 제한 하지 않습니다. 기본 값은 0이며 256개 까지 설정할 수 있습니다.
MAC 인증제한	중복 인증을 허용할 MAC의 개수를 설정합니다. 0으로 입력 시 중복 인증을 제한 하지 않습니다. 기본 값은 0이며 256개 까지 설정할 수 있습니다.
장비 인증제한	중복 인증을 허용할 디바이스의 개수를 설정합니다. 0으로 입력 시 중복 인증을 제한 하지 않습니다. 기본 값은 0이며 256개 까지 설정할 수 있습니다.
인증허용 IP	인증을 허용할 IP를 입력합니다. 입력한 IP 외에는 인증을 할 수 없습니다. 입력하지 않을 시 어떠한 IP도 인증 가능합니다. 최대 20개까지 설정할 수 있습니다.
인증허용 MAC	인증을 허용할 MAC를 입력합니다. 입력한 MAC 외에는 인증을 할 수 없습니다. 입력하지 않을 시 어떠한 MAC도 인증 가능합니다. 최대 14개까지 설정할 수 있습니다.
인증제한 예외노드그룹	인증 제한을 예외시킬 노드그룹을 할당합니다. 할당한 노드그룹에 포함되는 노드는 IP/MAC/장비 인증제한, 인증허용 IP/MAC 옵션에 제한받지 않습니다.

4. 추가정보 설정

사용자에대한 조직명, 직급 등 추가정보를 설정합니다.



항목	설명
조직명	소속된 조직(회사, 학교 등)명 입력합니다.
부서명	소속된 부서명을 설정합니다. 부서 생성방법은 사용자페이지 를 참고하시기 바랍니다.
직급	직급을 설정합니다. 직급 생성 방법은 사용자페이지 를 참고하시기 바랍니다.
전화번호	사무실 전화번호를 입력합니다.
휴대폰	휴대폰 번호를 입력합니다. 아이디/비밀번호를 분실하여 아이디/비밀번호 찾기를 이용할 때 필요한 정보입니다.
전자우편	E-mail 주소를 설정합니다. 아이디/비밀번호를 분실하여 아이디/비밀번호 찾기를 이용할 때 필요한 정보입니다.
사용자그룹	사용자가 속해져 있는 사용자 그룹을 나타냅니다. 사용자 그룹에 대한 내용은 사용자 를 참고 바랍니다.

- 관리자 설정

위 과정에서 관리역할 항목에서 관리자 권한을 부여하고 모든 설정 후, 생성을 하였다면 관리자계정이 생성되었을 것입니다. 일반계정과는 달리 관리자를 생성 후에는 관리자설정이라는 탭이 생성되며 로그인, 알람정보, 관리제한을 설정할 수 있습니다.

- 로그인 설정

관리자 계정으로 로그인할 수 있는 IP를 조회할 수 있습니다 또한, 로그인 시 SMS, OTP를 인증을 받도록 하는 2단계 보안 인증을 설정할 수 있습니다.



항목	옵션	설명
관리WEBUI 접속 IP1		해당 관리자 계정을 이용하여 WEBUI에 접속할 수 있는 IP를 조회할 수 있습니다. 해당 항목에 없는 IP는 해당 관리자 계정으로 WEBUI에 접속할 수 없으며, 해당 항목에 IP는 시스템 > 센터 IP 클릭 > 환경설정에서 CLI 콘솔 접속 IP에 설정한 값이 해당 항목에 그대로 입력됩니다. 센터의 CLI 콘솔 접속 IP를 입력하여야 적용됩니다. 아무것도 입력되어 있지 않을 시 최초 로그인한 IP가 입력 됩니다
관리WEBUI 접속 IP2		해당 관리자 계정을 이용하여 관리 WEBUI에 접속할 수 있는 IP를 조회할 수 있습니다. 해당 항목에 없는 IP는 해당 관리자 계정으로 WEBUI에 접속할 수 없으며, 해당 항목에 IP는 시스템 > 센터 IP 클릭 > 환경설정에서 CLI 콘솔 접속 IP에 설정한 값이 해당 항목에 그대로 입력됩니다. 센터의 CLI 콘솔 접속 IP를 입력할 시 적용되지 않으며 센터의 CLI 콘솔 접속 IP를 입력하여야 적용됩니다.
2단계 인증	사용안함	2단계 인증을 사용하지 않습니다.
	SMS	관리WEBUI에 접속 할 시 SMS 수신번호 항목에 입력되어 있는 수신번호로 인증번호가 전송됩니다. 전송된 인증번호를 입력하여 관리WEBUI에 접속 할 수 있습니다. 해당 옵션을 사용하기 위해서는 설정 > 환경설정 > 관리콘솔설정에 접속하여 2단계 인증 사용여부를 설정해주어야 합니다.
	OTP	관리WEBUI에 접속 할 시 Google OTP를 이용하여 인증번호를 발급받고 해당 인증번호를 입력하여야 관리WEBUI에 접속 할 수 있습니다. 해당 옵션을 사용하기 위해서는 설정 > 환경설정 > 관리콘솔설정에 접속하여 2단계 인증 사용여부를 설정해주어야 합니다.
언어	한국어	해당 관리자 ID로 웹 접속할 시 웹에 보여지는 문자들이 한국어로 나타납니다.
	English	해당 관리자 ID로 웹 접속 할 시 웹에 보여지는 문자들이 영어로 나타납니다.
타임존	국가	해외에서 NAC를 관리 할 때 사용하는 옵션이며, 해당 관리자 ID로 웹 접속 할 시 웹에서 보여지는 시간들을 설정한 국가의 시간으로 보여지게 됩니다.
API 키		신규 키 생성을 클릭 시 API 키가 생성되며 해당 키를 이용하여 특정 NAC관리콘솔 화면을 호출할 수 있습니다. 호출URL형식 https://(CENTERIP)/mc2/faces/frontpage.xhtml?apiKey=(APIKEY)folder=(호출페이지폴더명)&selectedPage=(호출페이지xhtml)

2. 알람정보 설정

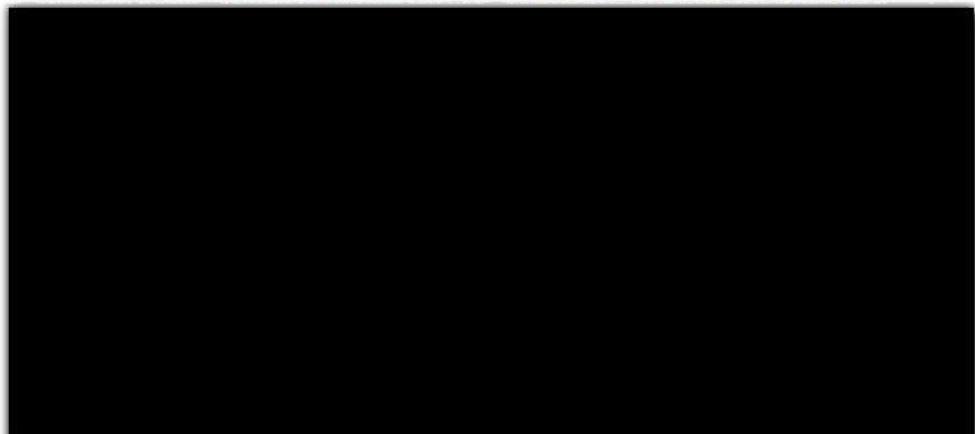
사용자가 사용자 등록과 IP 신청을 할 경우 아래항목의 SMS수신번호와 이메일에 적힌곳으로 알람이 송신됩니다.
이메일의 경우 설정 > 환경설정 > 기타설정에서 메일서버설정이 필요합니다.



항목	옵션	설명
알람수신설정	사용자등록	사용자가 사용자 등록 신청을 할 시 관리자에게 아래의 SMS수신번호, 이메일 설정을 바탕으로 알람수신(문자, 이메일)을 받을 수 있습니다.
	IP신청	사용자가 IP 신청을 할 시 관리자에게 아래의 SMS수신번호, 이메일 설정을 바탕으로 알람수신(문자, 이메일)을 받을 수 있습니다.
	장치신청	사용자가 장치신청을 할 시 관리자에게 아래의 SMS수신번호, 이메일 설정을 바탕으로 알람수신(문자, 이메일)을 받을 수 있습니다.
SMS수신번호		알람수신(문자)을 받을 SMS수신 가능한 휴대폰 번호를 입력합니다. ',' 이용하여 여러개의 휴대폰 번호를 설정할 수 있습니다. (예 : 010-1234-5678,01012357890)
발신번호		SMS에 표시할 발신번호를 입력합니다.
이메일		알람수신(이메일)을 받을 이메일 주소를 입력합니다. ',' 이용하여 여러개의 이메일을 설정할 수 있습니다. (예 : asd123@naver.com,geniNAC@gennetworks.com) 이메일 항목은 필수로 입력해야 하는 정보입니다.
관리자 푸시 토큰		

3. 관리제한 설정

최고관리자는 일반관리자들의 역할에 따라 관리 권한에 제한을 할 수 있습니다.
제한할 항목을 선택하여 해당 항목의 사용할 기능을 선택합니다.



제한 항목과 그에대한 설명은 아래 표와 같습니다.

항 목 이 름	설 명

노드 관리 범위 제한	정책그룹/관리센서(정책그룹과 관리센서는 둘 중 하나만 선택가능) or 노드타입 지정을 통하여 노드의 관리 범위를 제한합니다.
노드 관리 명령 제한	작업선택(IP관리, 노드관리, 일괄작업) 명령을 할당하여 관리명령을 제한합니다.
노드 관리 뷰 제한	관리 뷰(요약뷰, 노드뷰, ip관리뷰, 위험뷰, 패치관리뷰 등등)를 할당하여 관리 뷰 사용권한을 제한합니다.
노드 상세보기 제한	노드 상세 페이지(기본정보, 장비정보, 시스템정보, 네트워크정보 등등)의 접근권한을 제한합니다.
사용자 관리 범위 제한	부서를 할당하여 할당해준 부서만 관리할 수 있도록 제한합니다.
사용자 관리 명령 제한	사용자 작업선택 명령을 할당하여 관리명령을 제한합니다.
감사로그 검색 범위 제한	선택한 검색필터만 이용할 수 있도록 하여 감사로그의 검색범위를 제한합니다.
파일 내보내기 제한	파일 내보내기 기능을 제한합니다.
대시보드 위젯 제한	선택한 위젯만 추가할 수 있도록 하여 대시보드에서 추가할 수 있는 위젯을 제한합니다.

4. 선택한 관리자로 전환

해당 기능은 관리자들의 권한을 확인하기 위해 사용됩니다.

관리역 할이 Superadmin으로 설정된 계정만 사용 가능한 기능이며, 다른 관리자 계정의 관리자 설정에 접속하여 "선택한 관리자로 전환" 클릭 할 시 선택한 관리자로 자동 로그인 하여 해당 관리자가 어느 정도 까지의 권한을 가졌는지 직접 UI를 통하여 확인할 수 있습니다. 현재 접속 중인 관리자에게 해당 기능을 사용할 시 접속 중인 관리자는 로그아웃 됩니다.

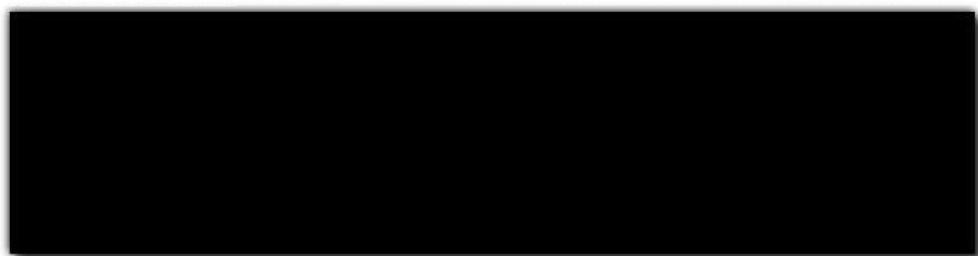


5. 알람테스트

이메일을 입력 후 수정버튼을 클릭할 시 알람테스트 버튼이 활성화됩니다.

알람테스트를 하기 위해서는 메일서버를 설정하여야 하며, 메일서버 설정방법은 [기타설정](#)을 참고바랍니다.

알람서버를 설정하였으면 알람테스트 버튼을 클릭하여 입력한 이메일로 메일이 정상적으로 오는지 확인할 수 있습니다.



사용자 삭제

관리자는 필요없는 사용자를 삭제할 수 있습니다.

사용자 삭제 진행과정은 [항목 삭제](#)를 참조 바랍니다.



관리자가 사용자를 삭제했을 경우 삭제한 사용자에 대해서 더 이상 인증을 할 수 없으므로 주의하시기 바랍니다.

사용자 태그 설정

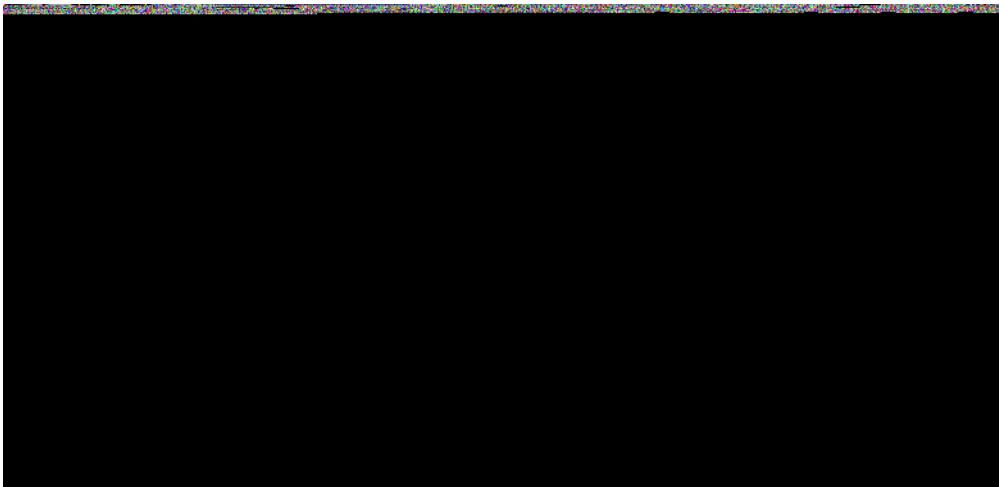
사용자 태그 설정

Genian NAC는 사용자에게 꼬리표와 같은 태그를 설정하여 관리상의 편의를 제공합니다.
해당 태그를 조건으로한 그룹을 생성할 수 있습니다.

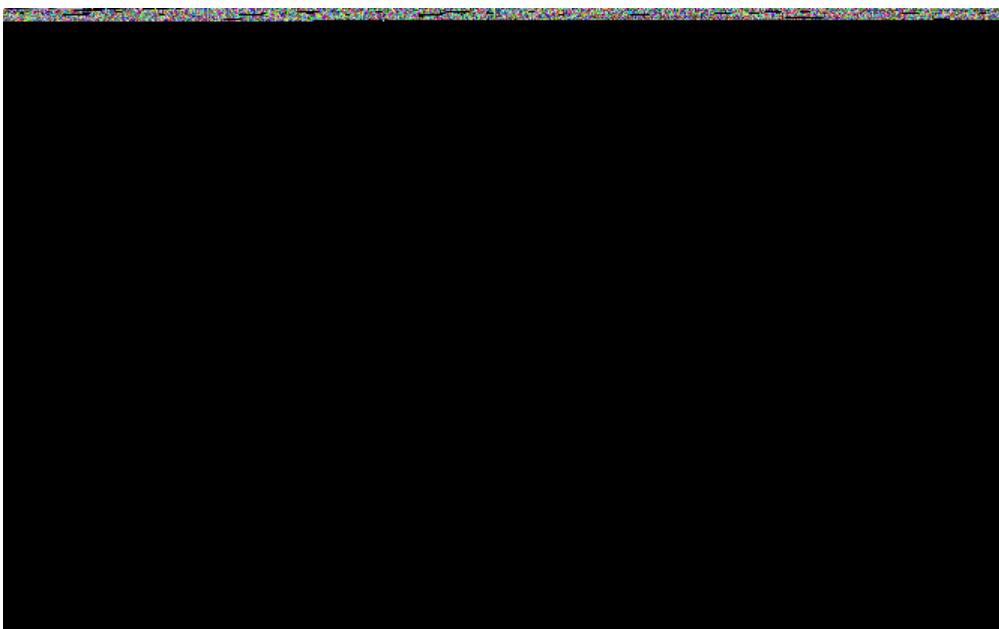
태그는 미리 생성되어 있어야 할당이 가능 합니다.

태그의 생성법은 [태그 관리](#)를 참조해 주시기 바랍니다.

아래 그림과 같이 태그를 할당하고 싶은 사용자를 ①번과 같이 선택 후, 작업선택 > 사용자 태그 설정 을 선택합니다.
사용자 태그 설정 팝업이 생성되면 미리 생성되어져 있는 ②번과 같이 태그를 선택 하고 태그에 대한 설명이 필요할 경우 태그 설명에 작성합니다. ③설정을 눌러 태그설정을 완료합니다.



사용자 상세 페이지에서 태그가 제대로 할당된 것을 확인할 수 있습니다.
해당 페이지에서도 태그 할당과 해제가 가능합니다.



사용자 태그 해제

해제하는 방법은 설정하는 절차에서 입력한 항목을 삭제하거나 해제한 후에 설정버튼을 클릭하시면 설정이 해제되는 것을 확인할 수 있습니다.

사용자그룹 지정&해제

사용자그룹 지정/해제

관리자는 사용자그룹 지정 기능을 이용하여 사용자의 상태나 조건에 관계 없이, 사용자를 원하는 그룹에 포함시킬 수 있습니다.

아래 그림은 기술연구소에 속해있는 사용자들을 사업부 그룹에 할당하는 과정입니다.

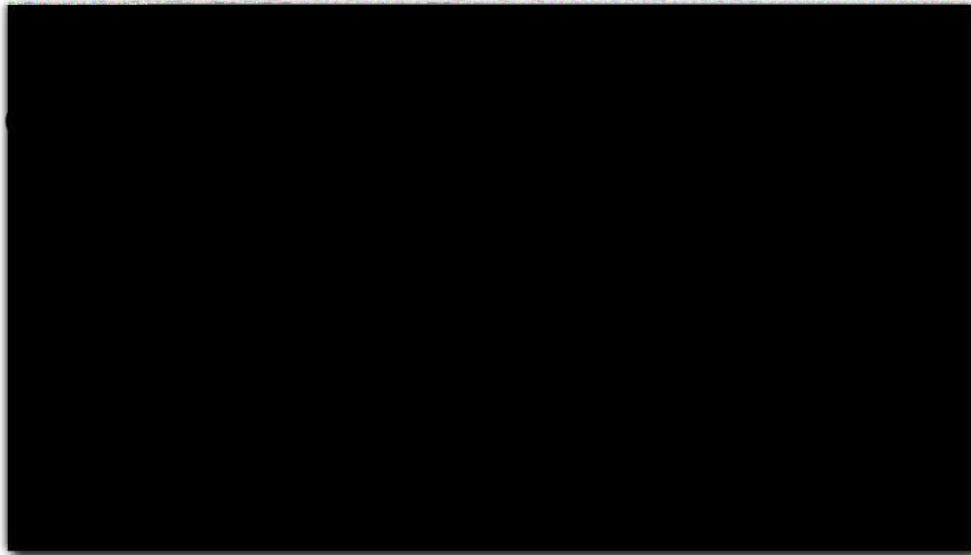
아래 그림의 ①번과 같이 어떠한 그룹에 포함시킬 사용자를 선택한 후, 작업선택 > 사용자그룹 지정 을 선택합니다.

사용자그룹 지정을 선택하면 그룹을 지정할 수있는 팝업이 아래 그림과 같이 생성됩니다.

②와 같이 사용자그룹 지정을 할려면 조건연산이 OR인 사용자 그룹이 생성되어 있어야 합니다. 사용자 그룹 생성 방법은 [사용자](#)을 참고바랍니다.

조건연산 OR인 사용자 그룹을 생성하였으면, 원하는 사용자그룹을 선택합니다.

③과 같이 포함시킬 사용자 그룹을 선택 후, 설정 버튼을 누릅니다.



사용자용도 설정

사용자용도 설정

관리자는 사용자용도 설정을 통하여 사용자의 용도를 변경할 수 있습니다.

1. 사용자용도 설정 선택

사용자용도를 변경하고 싶은 사용자를 선택 후 작업선택 > 사용자용도 설정 을 선택합니다.



2. 사용자용도 설정

변경 하고 싶은 사용자용도를 선택 후 설정 버튼을 클릭합니다.
사용자용도를 생성하고 싶은 경우 [사용자용도를 참고바랍니다.](#)



3. 사용자용도 설정 완료

아래의 그림과 같이 일반계정이었던 계정이 임시계정으로 변경되었습니다.



인증제한 설정

인증제한 설정

인증제한을 이용하여 하나의 계정이 인증을 받을 수 있는 최대 IP, MAC, 장비(IP+MAC)의 개수를 설정할 수 있습니다.

1. 인증제한 설정 선택

인증제한을 설정하고 싶은 사용자를 선택한 후, 작업선택 > 인증제한 설정 을 선택합니다.



2. 인증제한 설정

인증허용할 IP, MAC, 장비의 개수를 입력합니다. 하나의 계정을 입력한 IP, MAC, 장비 개수만큼 인증 할 수 있으며, 0을 입력 시 IP, MAC, 장비 개수 제한없이 인증할 수 있습니다.
1개의 IP만 인증을 할 수 있도록 제한하고 싶은 경우 아래의 그림과 같이 설정합니다.



3. IP/MAC 인증제한 설정이 된 사용자가 다른 노드에 인증 시도 시

IP 인증제한이 1로 설정된 사용자가 하나의 노드에서 인증과정을 수행하고, 다른 노드에 다시 로그인을 시도하면 아래 그림과 같이 인증이 되지 않습니다.

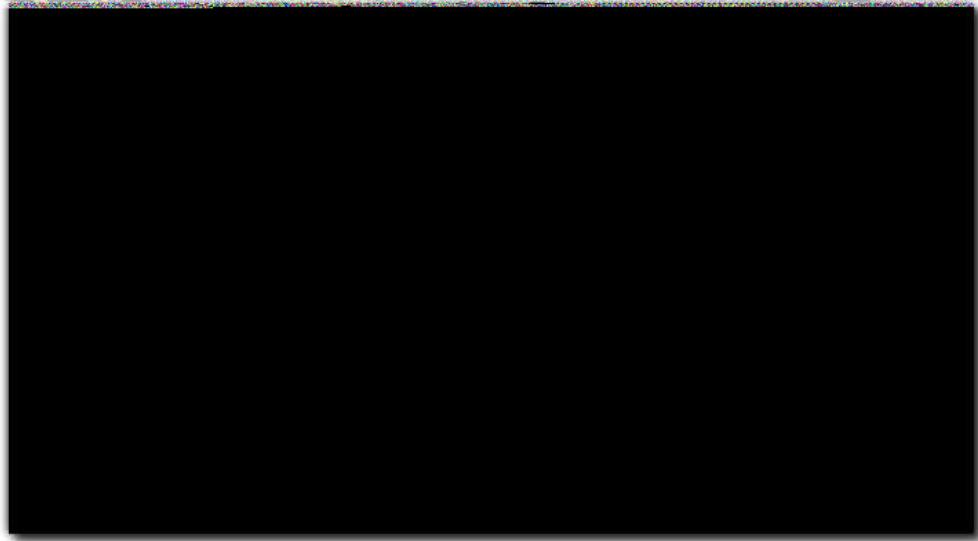


정상 상태로 변경

정상 상태로 변경

사용중지 상태로 되어있는 사용자 계정의 상태를 정상상태로 변경하여 계정을 다시 사용할 수 있게 합니다.

아래 그림과 같이 사용중지 상태의 사용자를 선택하고 작업선택 > 정상상태 변경 을 선택하면 사용중지 상태의 상태가 정상으로 변경되며, 계정을 사용할 수 있게됩니다.



아래 그림은 사용중지 상태의 사용자가 정상상태로 변경 된 후, 정상적으로 로그인이 된 모습입니다.



사용중지 상태로 변경

사용중지 상태로 변경

계정상태를 사용중지로 바꾸어 해당 계정을 더이상 사용할 수 없도록 합니다.

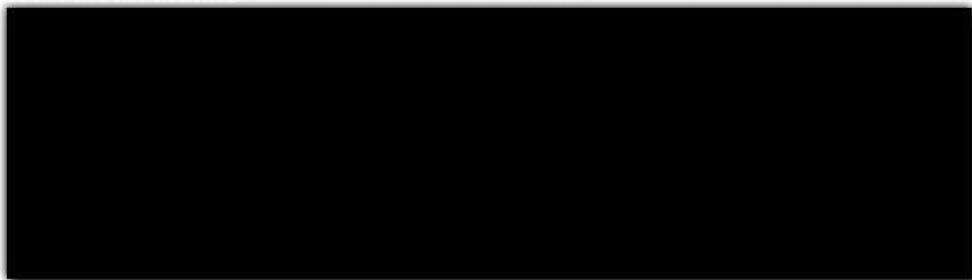
1. 사용중지 상태로 변경 선택

사용중지를 시킬 사용자를 선택 후, 작업선택 > 사용중지상태로 변경 을 선택합니다.



2. 상태 확인

관리 뷰의 상태컬럼이 사용중지로 변경된 것을 확인할 수 있습니다.



3. 사용중지 상태 사용자의 로그인 시도

아래 그림과 같이 사용중지 상태의 사용자는 로그인을 할 수 없습니다.



비밀번호변경 강제화 설정

비밀번호변경 강제화 설정

비밀번호변경을 강제화 하는 설정을 하여 사용자가 로그인을 할 때, 비밀번호를 변경하지 않으면 로그인이 되지 않도록 합니다.

1. 비밀번호변경 강제화 설정 선택

비밀번호변경 강제화를 설정하고 싶은 사용자를 선택 후, 작업선택 > 비밀번호변경 강제화 설정 을 선택합니다.



2. 변경강제 확인

비밀번호변경 강제화를 설정유무는 노드 관리 뷰에서 확인할 수 있습니다.



3. 변경강제가 설정된 사용자의 로그인 시도

아래 그림은 비밀번호변경 강제화가 설정된 사용자가 로그인을 하였을 때 나타나는 화면입니다.



비밀번호변경 강제화 설정(임시비밀번호 발급)

비밀번호변경 강제화 설정(임시비밀번호 발급)

임시비밀번호를 발급하고 비밀번호변경을 강제화 합니다.
사용자가 비밀번호를 잊어버렸을 시 사용하는 기능입니다.
발급받은 임시비밀번호로 로그인하면 비밀번호를 변경하는 페이지로 이동됩니다.

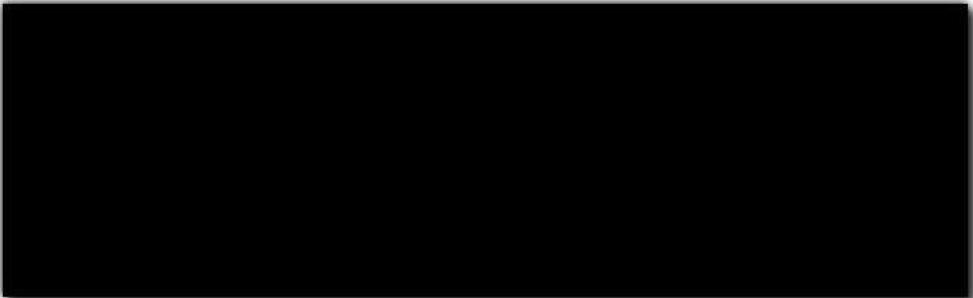
1. 비밀번호변경 강제화 설정(임시비밀번호 발급) 선택

비밀번호변경 강제화 설정(임시비밀번호 발급)을 원하는 사용자를 선택한 후, 작업선택 > 비밀번호변경 강제화 설정(임시비밀번호 발급) 을 선택합니다.



2. 비밀번호변경 강제화 설정(임시비밀번호 발급) 관리 뷰 확인

비밀번호변경 강제화 설정(임시비밀번호 발급)가 설정된 모습을 관리 뷰에서 확인 가능합니다. 임시비밀번호를 지정하고 싶을 경우 설정 > 환경설정 > 사용자관리 에서 임시비밀번호를 매크로를 이용하여 지정할 수 있습니다.



3. 비밀번호변경 강제화 설정(임시비밀번호 발급) 설정 사용자가 로그인 시도

비밀번호변경 강제화 설정(임시비밀번호 발급)된 사용자가 발급된 임시 비밀번호로 로그인을 하면 비밀번호 변경 페이지로 이동합니다.
관리자가 사용자에게 임시 비밀번호를 인스턴트 메시지 등의 방법으로 알려주어야 합니다.



사용만료시각 변경

사용만료시각 변경

사용자의 계정사용만료 시각을 일괄적으로 설정할 수 있는 기능입니다.

1. 사용만료시각 선택

계정사용만료 시각 설정이 필요한 사용자를 선택한 후, 작업선택 > 사용만료시각 을 선택합니다.



2. 사용만료시각 설정

계정사용만료 항목 클릭 시 출력되는 달력에서 계정사용만료 시각을 설정합니다.



3. 사용만료시각 변경 확인

사용만료시각 변경 설정 시 관리 뷰에서 설정 유무를 확인할 수 있습니다.



신청

신청서 관리

신청서의 종류에는 사용자의 신규계정 신청을 관리하는 사용자 신청서, 신규 IP 신청과 반납, 장비변경 신청 등을 관리하는 IP 사용 신청서, 제한된 장비를 신청하는 장치사용신청서가 있습니다.

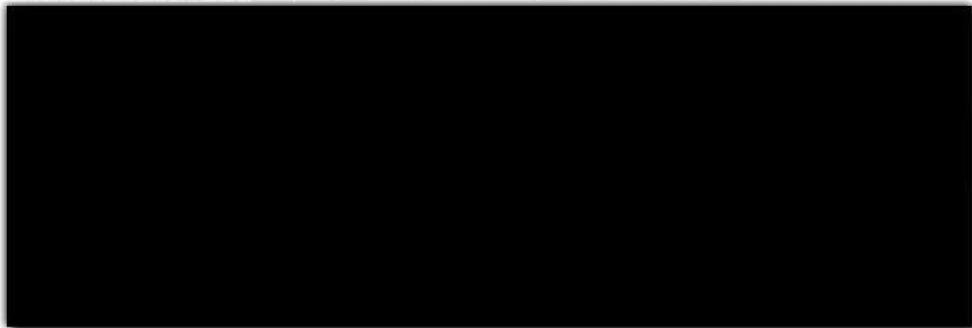
- 사용자신청서

사용자가 사용자 등록을 CWP 페이지에서 신청할 시 해당 페이지에서 사용자 등록 신청서를 확인하여 처리할 수 있습니다.



- IP사용신청서

사용자가 IP 사용신청을 CWP 페이지에서 신청할 시 해당 페이지에서 IP 사용신청서를 확인하여 처리할 수 있습니다.



- 장치사용신청서

사용자가 제한된 장비를 사용하기 위해 장치사용자신청을 에이전트에서 할 시 해당 페이지에서 장치사용자신청서를 확인하여 처리할 수 있습니다.



- 에이전트 인증코드

사용자가 에이전트를 삭제하기 위해 원격 에이전트 삭제기능을 이용하여 코드를 관리자에게 보내주면 관리자는 해당 페이지에서 코드를 이용하여 인증 코드를 확인할 수 있습니다.



사용자신청서

사용자 신청서 관리

계정이 없는 일반 사용자가 CWP(접속인증) 페이지에서 사용자 등록 신청을 하면 관리자가 해당 사용자에게 계정을 할당 할 수 있습니다. CWP페이지에 대해서는 [접속인증페이지\(CWP\)](#)를 참고바랍니다.

사용자 등록 신청 on/off

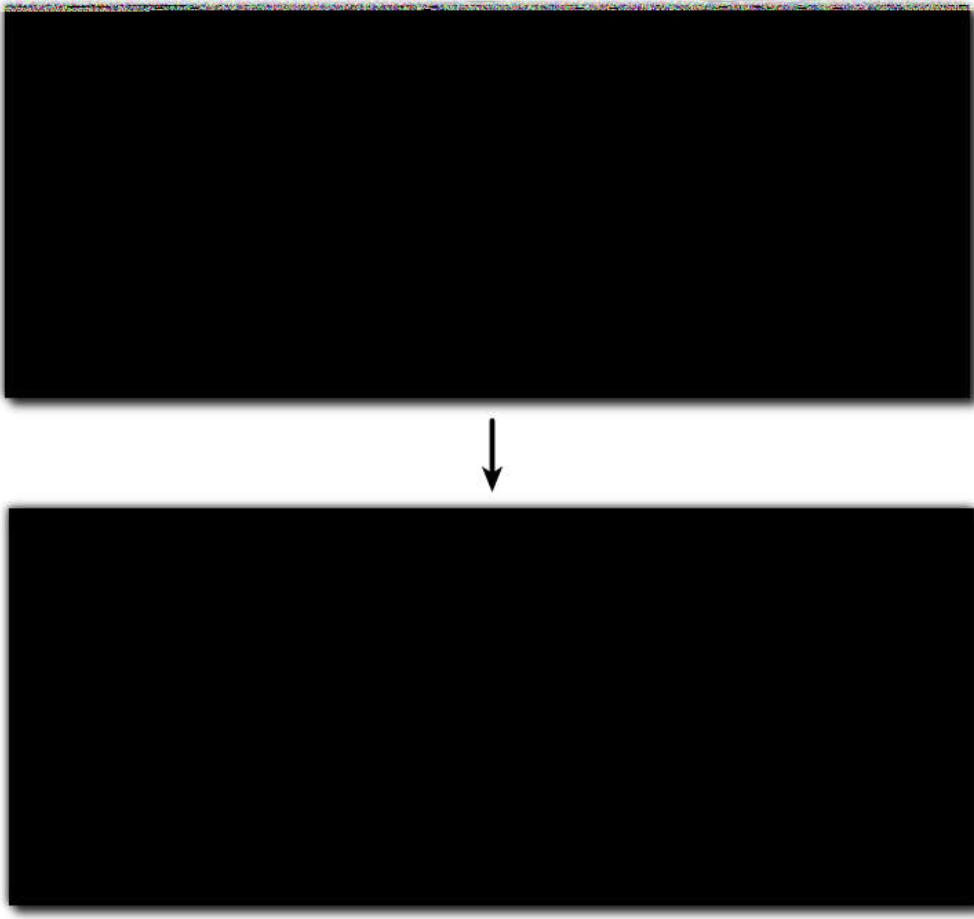
관리자는 사용자 등록 신청의 사용 유무를 설정하여 사용자가 신규 사용자 등록을 할 수 있도록 합니다.

- 정책 > 노드 정책에서 사용자가 적용받고 있는 노드 정책에 접속하여 사용자가 사용자 등록을 할 수 있도록 설정합니다.



사용자 등록 페이지	on을 선택할 시 CWP페이지에 사용자 등록 아이콘을 표시합니다, off를 선택할 시 표시하지 않습니다.
외부 등록 페이지	<p>외부 사용자 등록 페이지를 사용할 경우 해당 페이지의 URL을 입력하면 입력한 URL에 접속이 됩니다. 예: http://www.naver.com</p> <p>으로 설정할 경우 CWP페이지에서 사용자 등록을 클릭하면 http://www.naver.com</p> <p>으로 접속됩니다, http://을 입력은 필수사항입니다.</p>
사용자 동의 페이지	on을 선택할 시 사용자 등록을 할 경우 사용자 동의 페이지를 나타나고, off를 선택할 시 나타나지 않습니다.. 사용자 동의 페이지는 동의페이지 를 참조 바랍니다.

-
2. 사용자 등록 페이지에서 on을 선택할 경우 아래와 같은 아이콘이 CWP페이지에 표시됩니다.



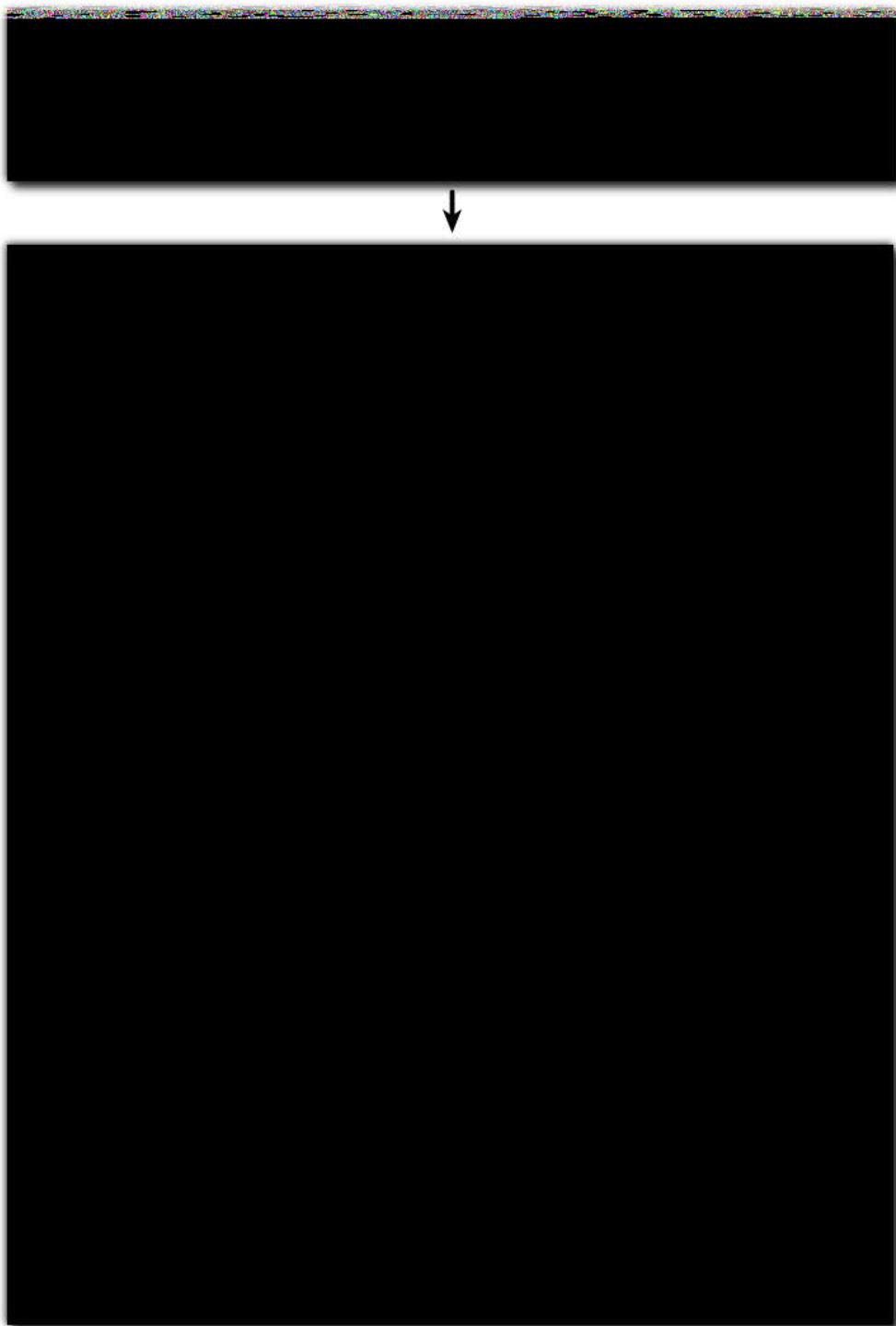
신규 등록

- 관리 > 신청 > 사용자신청서 > 신규등록 페이지에서 사용자가 등록한 신청서를 처리할 수 있습니다.

신청서 처리란에 승인, 버튼이 존재하여 관리자는 손쉽게 신청서를 관리할 수 있습니다.
또한 작업선택버튼을 통해 여러개의 신청서를 한번에 일괄 승인/거부 할 수 있습니다.



- 신청서 번호를 클릭 시 신청서 내용을 수정하여 승인/거부 할 수 있습니다.

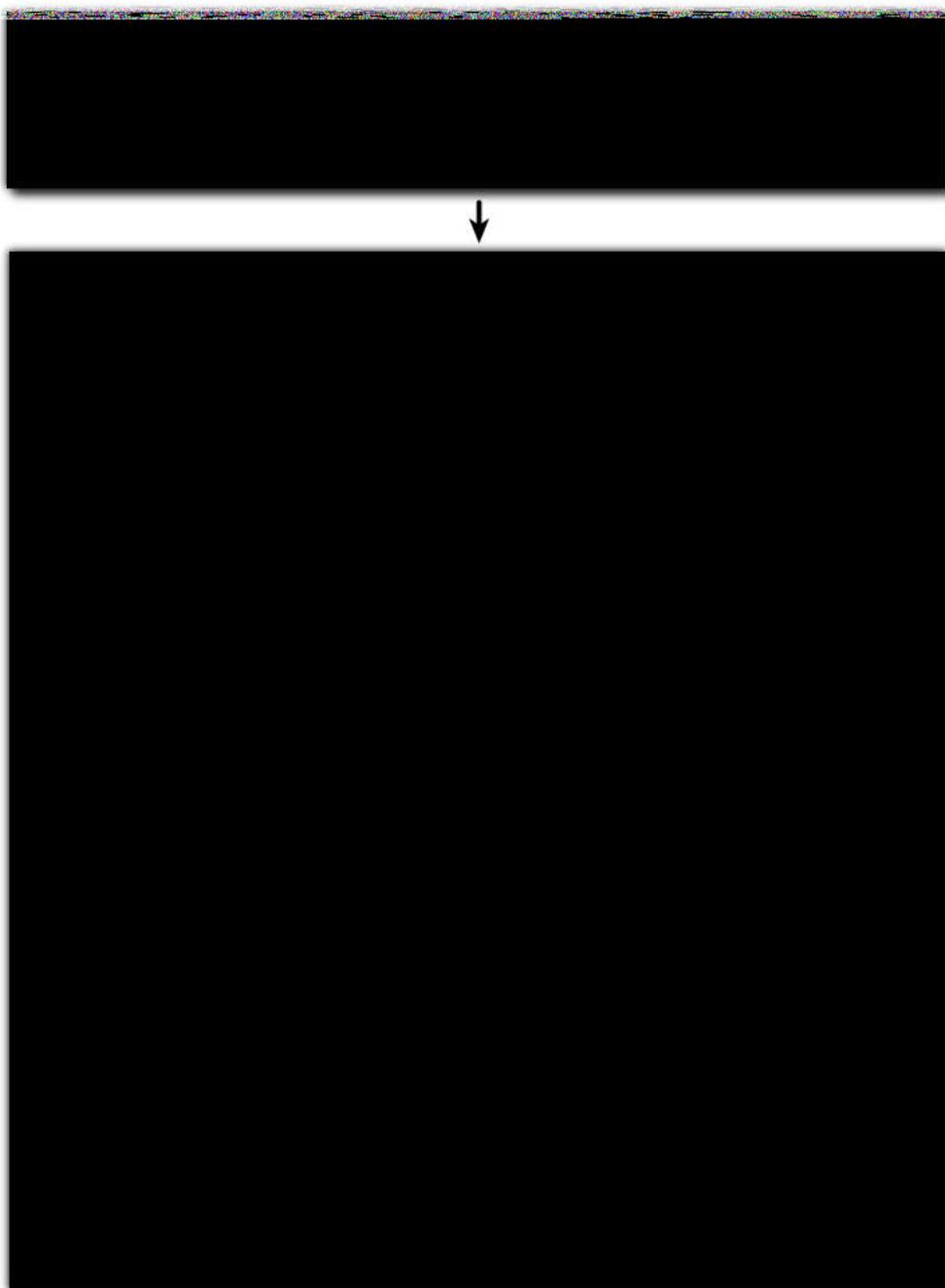


결과 조회

- 관리 > 신청 > 사용자신청서 > 결과조회 페이지에서 승인/거부한 신청서 내역을 확인할 수 있습니다.



- 결과 조회에서 신청서 번호를 클릭 시 신청서의 상세정보를 확인할 수 있습니다.



IP 사용신청서

IP 사용 신청서 관리

IP에 문제가 생길 경우 새로 IP를 할당 받아야 하는 일반 사용자가 CWP 페이지에서 IP 사용 신청을 하여 관리자가 해당 사용자에게 IP를 할당하고, 사용자가 필요없게 된 IP는 IP를 반납 신청을 하여 관리자가 해당 사용자의 IP를 반납 처리를 하여 IP를 회수할 수 있습니다.

IP 사용 신청 on/off

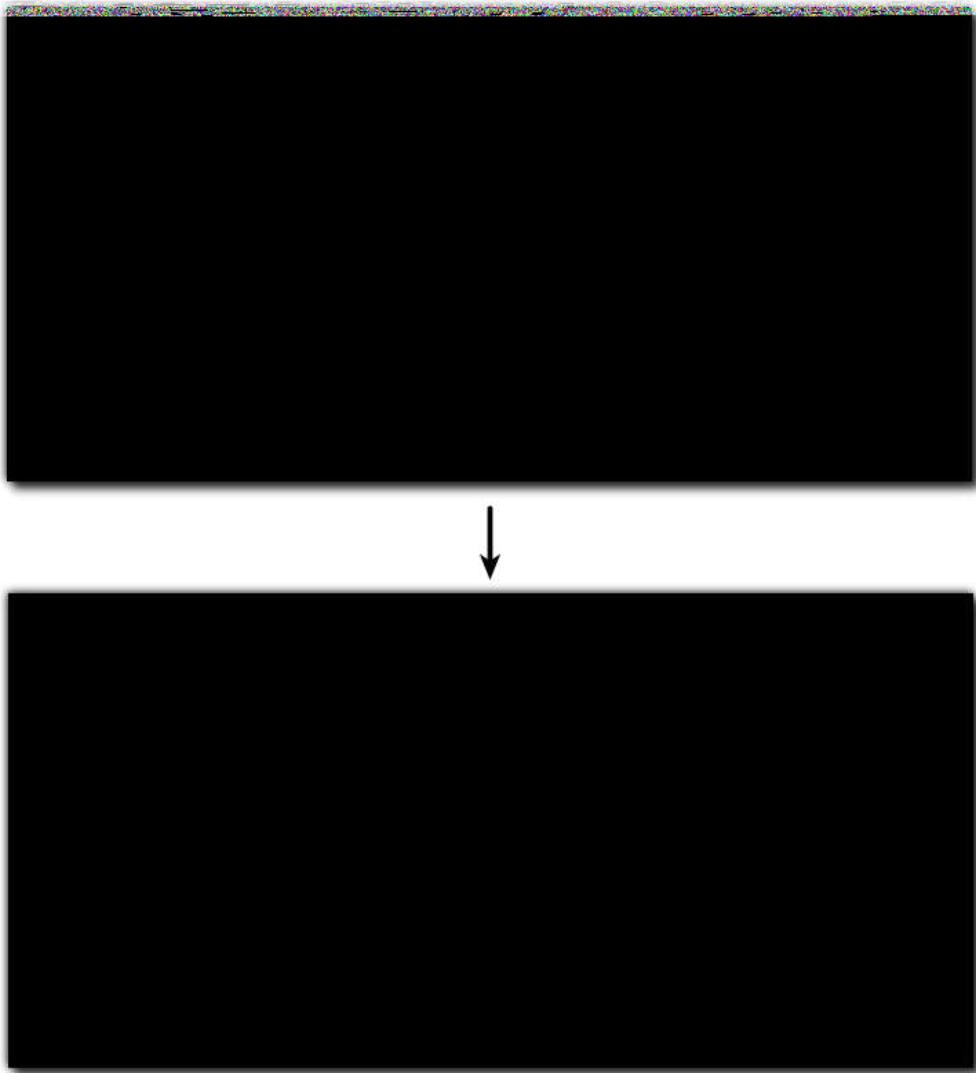
IP 관련 차단이나 IP를 할당받지 못한 사용자는 CWP 페이지에서 IP 사용 신청을 해야 합니다.
관리자는 IP 사용 신청의 사용 유무를 설정하여 사용자가 IP 신청 할 수 있도록 하고, GUESST 자동 로그인의 사용여부를 선택 합니다.

- 설정 > 환경설정 > IP 관리 에 접속하여 IP 사용 신청의 사용 유무를 설정합니다.



IP 사용 신청	on으로 선택할 시 IP에 문제가 생길 경우, cwp 페이지에 IP 신청 등록 아이콘을 표시하고, off를 선택할 시 표시를 하지 않습니다.
자동 로그인	on으로 선택할 시 계정이 없는 사용자일 경우에도 임시 계정으로 신청이 가능하고, off를 선택할 시 임시 계정이 아닌 일반 계정만으로만 신청이 가능합니다.

-
2. IP 사용 신청을 on으로 선택할 경우 아래와 같은 아이콘이 cwp 페이지에 표시됩니다.



IP 신규 신청서 처리

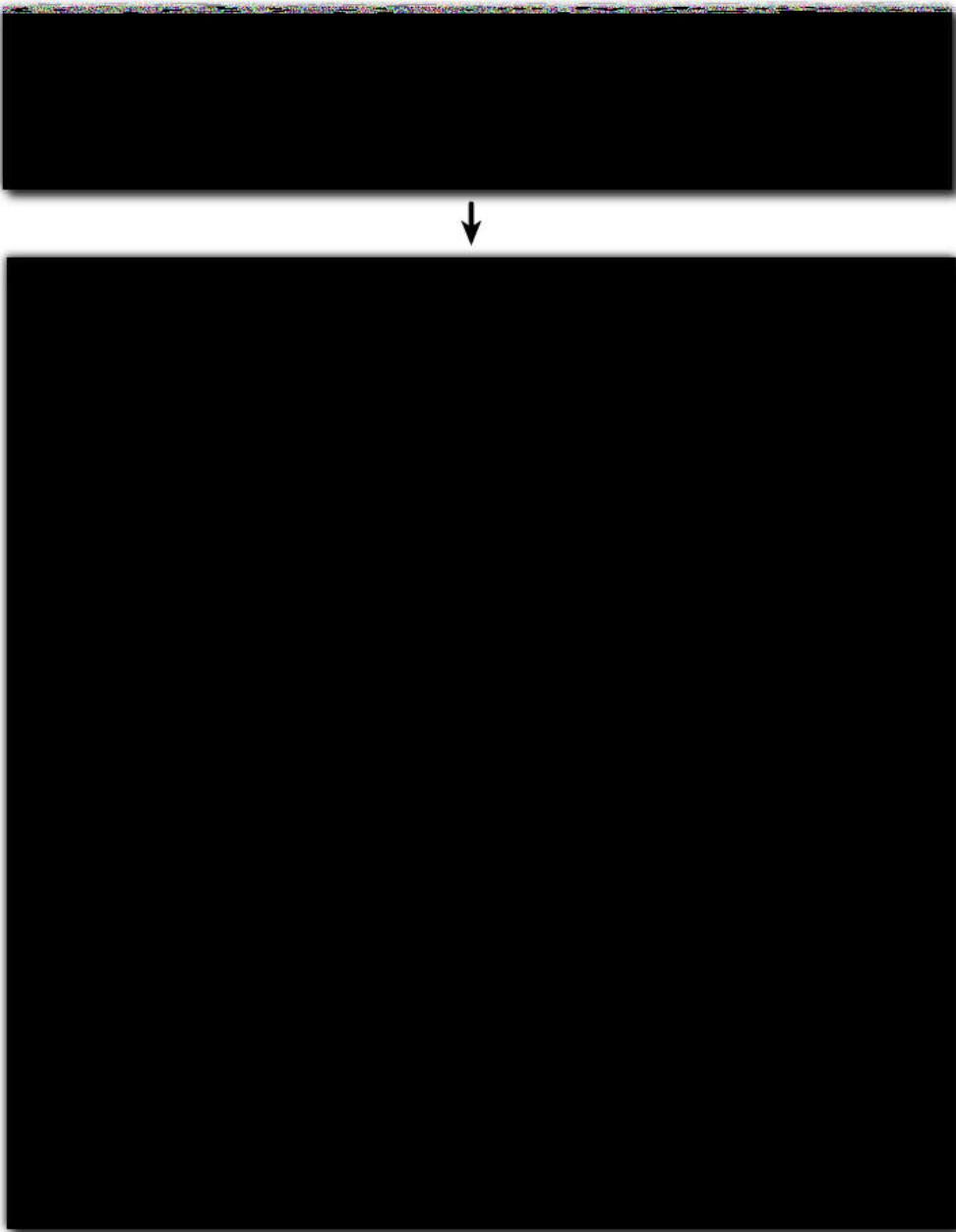
- 관리 > 신청 > IP신규/반납 을 클릭하여, IP 신청서에 신청서 처리 부분에서 선택을 클릭하여 사용자에게 IP를 할당하고, 거부를 클릭하여 IP를 할당하지 않습니다.



- IP할당 시, 경고 표시가 뜬다면 IP 신규할당 및 IP 반납에 문제가 발생할 수 있습니다.



3. 신청서 번호를 클릭 시 신청서 내용을 수정하여 승인/거부 할 수 있습니다.
아래 그림과 같이 용도와 IP할당 방식에 대하여 선택할 수 있으며, 추가필드 내용을 수정할 수 있습니다.
할당 버튼을 선택하여 자동으로 IP를 할당할 수 있고, 직접 버튼을 선택하여 원하는 IP를 선택하여 할당할 수 있습니다.
수정 가능한 추가필드 입력타입은 문자열, 문자열제한, 문자열 패턴, 멀티라인, 사용자설정목록(체크박스제외),
시스템설정목록(다중선택, 체크박스제외), 부서선택기 입니다.



IP 반납 신청서 처리

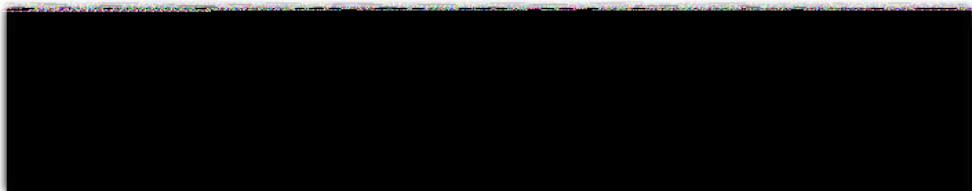
- 관리 > 신청 > IP 신규/반납 을 클릭하여, IP 신청서에 반납을 클릭하여 IP를 회수할 수 있고, 거부를 클릭하여 회수를 거부할 수 있습니다. 선택 버튼을 클릭 시 추가필드 내용을 수정할 수 있습니다.



- IP 할당 시, 경고 표시가 나타날 경우 IP 신규 할당 및 IP 반납에 문제가 발생할 수 있습니다.



- 신청서 번호를 클릭 시 신청서 내용을 수정하여 반납/거부 할 수 있습니다.



장비변경

- 관리 > 신청 > IP 사용신청서 > 장비변경 을 클릭 합니다.

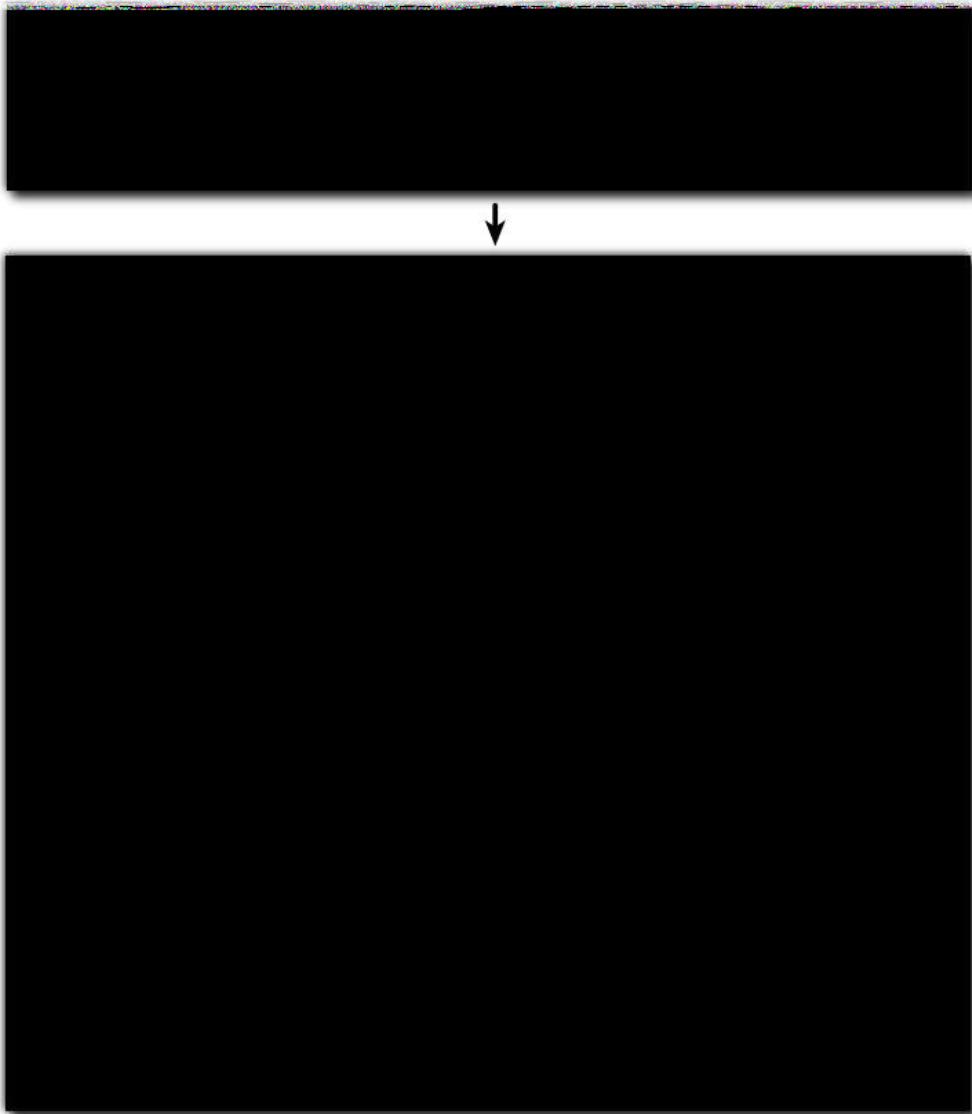
사용자의 LAN카드나 PC교체시에 사용되는 신청서입니다.

할당된 IP는 MAC과 연결지어 등록시키기 때문에, 장비의 변동사항이 발생하면 할당된 IP 이더라도 MAC주소가 달라지면 사용할 수 없습니다.

변경할 PC에 IP를 할당하기 전에 장비변경 신청을 합니다. 관리자는 장비변경 신청서를 확인 후 확인 버튼을 클릭하여 신청서를 수락하면 변경된 MAC으로 할당된 IP가 다시 매칭하게 됩니다.



- 신청서 번호를 클릭 시 신청서 내용을 수정하여 승인/거부 할 수 있습니다.

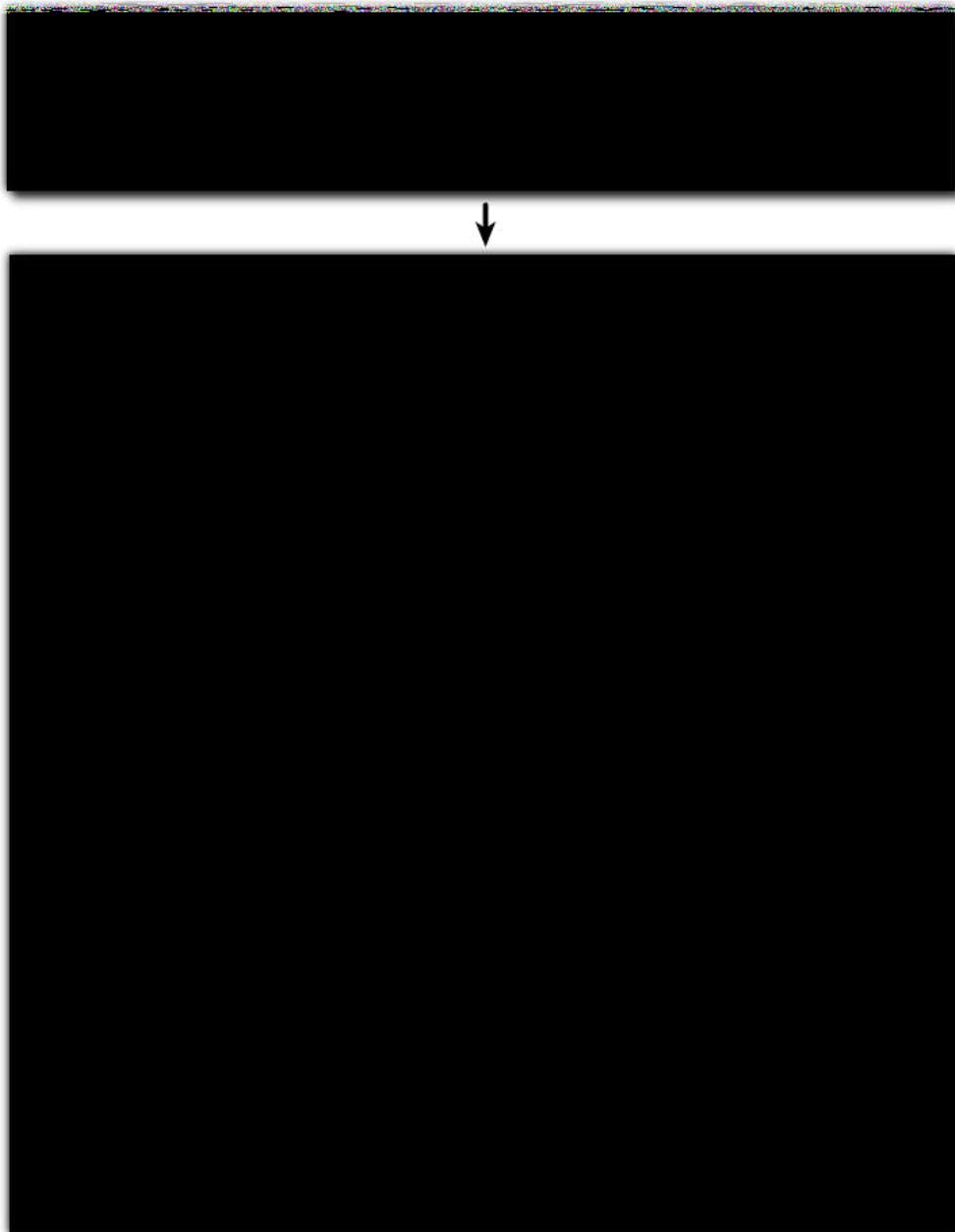


사용자변경

1. 관리 > 신청 > iP 사용신청서 > 사용자변경 을 클릭 합니다.
사용자변경 신청서는 관리자만 신청할 수 있으며, 현재 사용중인 IP의 소유자를 변경 시에 사용되는 신청서입니다.



2. 신청서 번호를 클릭 시 신청서 내용을 수정하여 승인/거부 할 수 있습니다.



메일승인대기

- 관리 > 신청 > IP 사용신청서 > 메일승인대기 를 클릭 합니다.
설정 > 속성관리 > 용도관리 > IP용도 에서 승인자 이메일 승인 기능 사용 시에 메일 승인 및 거부 처리가 되지 않는 대기 상태인 신청서를 확인할 수 있습니다.
작업선택 > 승인메일 재전송 으로 재전송할 수 있습니다.



결과조회

- 관리 > 신청 > 결과조회 를 클릭하여 IP 신규/반납/변경에 대한 신청서 처리 결과를 확인할 수 있습니다.
신청서 번호를 클릭 시 상세정보를 확인할 수 있습니다.



단계별승인

- 관리 > 신청 > IP 사용신청서 > 단계별승인 을 클릭 합니다.
설정 > 속성관리 > 용도관리 > IP용도 에서 단계별 승인 기능 사용 시에 단계별신청서를 승인 및 거부할 수 있습니다.
승인 시 다음 단계로 넘어가며 거부 시 해당 단계에서 신청서가 거부 처리됩니다.
해당 단계에 승인 및 거부를 할 수 있는 관리자가 없다면 자동승인되어 다음 단계로 넘어가게 됩니다. 우선사용승인 시 즉시 IP가 할당되며 신청서는 다음단계로 넘어갑니다. 다음 단계에서 거부 시 할당된 IP는 차단됩니다.



장치사용신청서

장치사용신청서 관리

차단된 장치(USB, 외장하드, USB 무선 랜카드 등이 장치제어 플러그인을 통해 차단되어 있는 상태의 장치)는 장치 사용신청서를 통하여 사용신청을 하고, 관리자의 승인을 거쳐 사용할 수 있습니다.
관리자는 해당 신청서를 확인하고 장치 사용을 승인/거부 할 수 있습니다.

장치사용신청서 on/off

장치 제어를 받고 있는 장치를 사용할려면 장치 사용 신청서를 신청 해야 합니다.
관리자는 노드정책에서 장치제어 노드액션을 할당하여 장치 사용 신청서의 사용 유무를 설정할 수 있습니다.

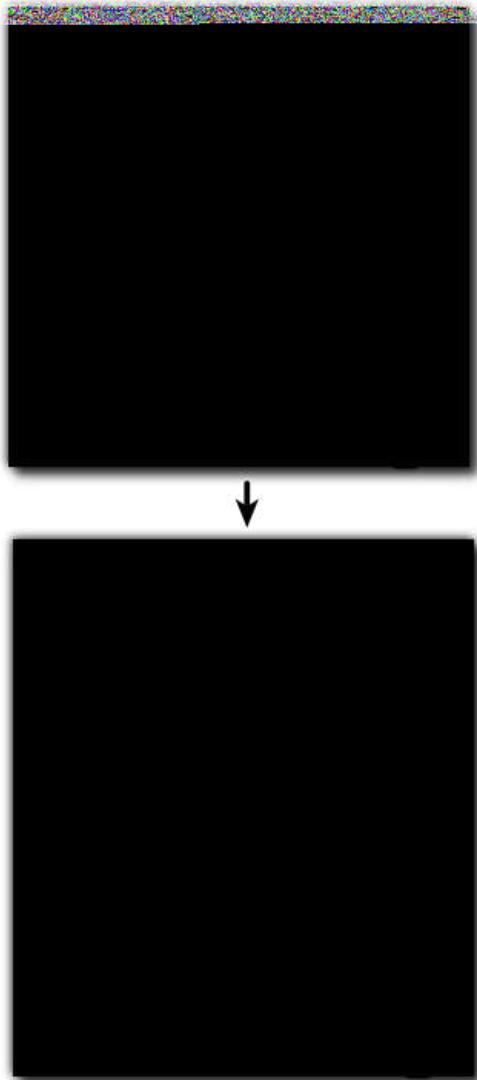
- 정책 > 노드정책 > 노드 액션 > 장치 제어 을 클릭합니다. 노드 액션에 장치 제어가 없다면 노드정책을 참고하여 장치 제어 액션을 추가 합니다.



- 장치사용신청서의 유무와 자동 승인 등의 설정을 할 수 있습니다. 자세한 사항은 [플러그인](#)을 참고바랍니다.

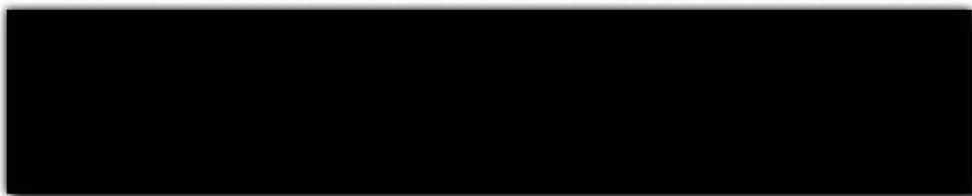


3. 장치사용신청서 on으로 설정할 시 다음과 같이 트레이 아이콘 우클릭 시 장치사용신청서가 표시됩니다.



장치사용신청서 처리

- 관리 > 신청 > 장치사용신청서 > 신규등록 페이지에서 사용자가 신청한 장치사용신청서를 처리할 수 있습니다.
신청서처리 항목에 있는 승인, 거부 버튼을 클릭하여 장치사용신청서를 거부할지 승인할지를 선택할 수 있습니다.
신청서 번호 항목의 번호를 클릭하여 장치사용 신청서를 더욱 상세히 확인하고 신청서를 승인할 수 있습니다.



결과조회

- 관리 > 신청 > 장치사용신청서 > 결과조회 페이지에서 승인, 거부한 신청을 확인할 수 있습니다

승인한 신청서에 대해서는 사용종료 버튼을 이용해서 다시 장치 제어를 적용시킬 수 있습니다.



에이전트 인증코드

에이전트 인증코드

사용자가 에이전트를 삭제하기 위해 에이전트의 원격 에이전트 삭제를 이용할 때 필요한 인증코드를 발급 받기 위하여 에이전트 코드를 관리자에게 알려주고, 관리자는 에이전트 인증코드 발급 페이지에서 에이전트 코드를 입력하여 원격 에이전트 삭제 기능에 필요한 인증코드를 발급 받을 수 있습니다.

발급 받은 인증코드를 사용자에게 알려주면 사용자는 원격 에이전트 삭제 기능을 사용하여 에이전트를 삭제할 수 있습니다.

에이전트 인증코드 발급

- 에이전트 트레이 아이콘을 우클릭하여 원격 에이전트 삭제 버튼을 클릭합니다.



- 에이전트 코드를 확인하고 관리자에게 코드를 알려줍니다.
이때 창을 닫거나 생성버튼을 눌러 에이전트 코드가 달라질 경우 관리자에게 알려준 에이전트 코드로 발급받은 인증 코드는 사용할 수 없으니 주의하시기 바랍니다.



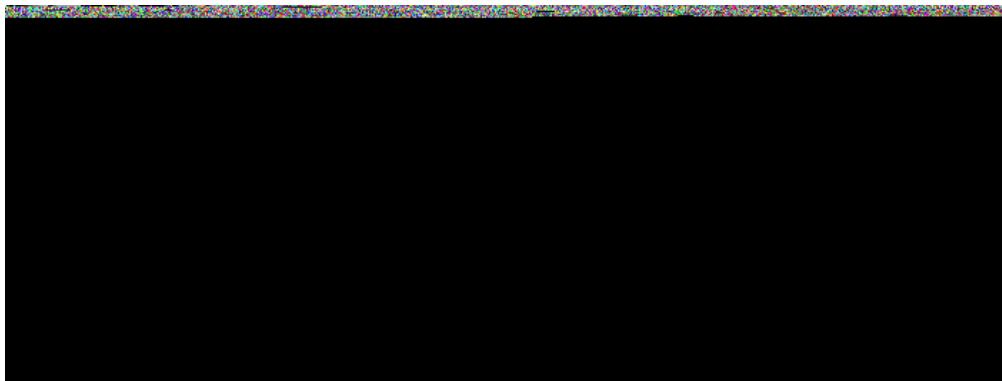
- 에이전트 코드에 사용자에게 받은 에이전트 코드와 발급사유를 입력합니다.



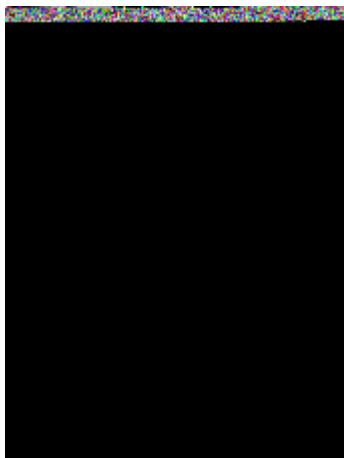
-
4. 인증코드 발급 버튼을 클릭하여 인증코드를 발급받습니다. 발급받은 인증코드를 사용자에게 알려줍니다.



5. 인증코드란에 관리자에게 받은 인증코드를 입력하고 삭제 버튼을 클릭합니다.



6. 에이전트가 사라졌는지 아래의 그림과 같이 확인 합니다.



정 책

정책

정책탭에서는 사용자 그룹을 만들고, 정책을 수립하며, 권한과 조건에 이용되는 객체를 생성할 수 있습니다.

- 정책 : 무선랜 정책을 이용하여 Air-Sentry의 AP 기능 수행할 수 있도록 하고 노드정책, 제어정책을 이용하여 노드를 제어할 방책을 마련하는 탭입니다.
 - 그룹 : 다양한 조건들을 통하여 그룹을 생성하고 장치그룹을 이용하여 장치를 제어할 기기를 설정할 수 있는 탭입니다.
 - 객체 : 네트워크, 서비스, 시간을 설정하고 세 가지의 설정으로 하나의 권한을 생성할 수 있는 탭입니다.
-
- 정책
 - 그룹
 - 객체

정책

정책

정책은 만들어진 그룹에 만족해야할 조건이나 권한을 할당하는 것으로, 노드정책과 제어정책이 있습니다.
노드정책은 노드 내부 시스템의 설정을 변경하고 제어하며, 제어정책은 네트워크의 제어를 담당합니다.

- 노드정책

에이전트와 인증관련 정책을 수립하고, 노드액션을 이용하여 내부를 제어하고, 위험감지를 통해 노드의 위험을 재빨리 발견할 수 있습니다.



- 제어정책

CWP 옵션과 스위치포트차단 설정을 하고, 그룹 및 제어액션을 설정하여 제어 받을 노드를 선택하고 권한을 생성하고 할당하여 네트워크 제어를 할 수 있습니다.



- 무선랜정책

AP, Client 프로파일을 이용하여 Air-sentry를 AP로 설정할 수 있습니다.



- 컴플라이언스정책

다수의 노드그룹을 설정하여 설정한 노드그룹에 노드 포함되었는지 O, X로 확인할 수 있습니다.



노드정책

노드정책이란?

노드정책은 사용자들의 노드들을 제어하고 관리하는데 있어 필요한 내부 시스템의 정보들을 수집하고 무엇을 제어할 것인지에 대해 정하는 것을 말합니다.

- 노드정책에는 사용자인증 정책, 에이전트 정책, 관리 정책, 노드액션, 위험감지의 항목들이 있습니다.

위 항목들의 간단한 설명은 아래 표와 같습니다.

항 목	설 명
인증 정책	사용자인증 방법과 재인증 방법 등 인증관련 각종 설정을 할 수 있습니다.
에이전트 정책	에이전트 사용 여부와 트레이 아이콘 표시 여부 등 에이전트에 관련된 설정을 할 수 있습니다.
관리 정책	신규노드 호스트명제한 및 비활성노드삭제 등 노드 관리에 필요한 설정을 할 수 있습니다.
노드액션	각종 플러그인으로 사용자 시스템의 설정 값을 설정하고 제어할 수 있습니다.
위험감지	위험 상황이 발생하였을 때, 원인제공자를 찾고 로그를 남겨 상황을 기록합니다.

관리자는 정책그룹을 만들고 하나 혹은 여러 개의 정책그룹을 노드정책에 할당 한 후, 위 네 가지의 항목들을 정의하면 그것이 하나의 노드정책이 되는 것입니다.

이때, 하나의 노드가 두 개 이상의 그룹에 속하여 여러 정책을 동시에 받는 상황이 올 수 있습니다.

동시에 여러 정책을 받는 노드는 관리자가 설정한 순서를 통하여 우선순위가 제일 높은 순서의 정책 한 가지만 받게 됩니다.

노드정책에는 default로 기본정책이 생성되어 있으며 해당 정책은 삭제가 불가능하며, 다음과 같은 노드액션과 위험감지가 할당되어 있습니다.

노드액션	모니터정보 수집, 프린터정보 수집, 모양 및 개인설정, 네트워크 공유풀더, 소프트웨어정보 수집, 네트워크정보 수집, 운영체제정보 수집, 윈도우 업데이트, 하드웨어정보 수집, 백신정보 수집
위험감지	Ad Hoc 네트워크 연결, ARP Bomb, ARP Spoofing, MAC/IP Clone, Multihomed, Port Scan, 알수없는 서비스 요청, 잘못된 게이트웨이 사용



제품 초기설치 시 기본정책이라는 것이 존재합니다. 삭제와 그룹할당이 불가능한 이 정책은 관리자가 설정한 정책 중 아무정책에도 포함되지 않은 노드들을 위하여 존재하는 정책입니다. 센서가 수집한 노드목록에 포함되어있는 노드들은 어떠한 그룹에 속하지 않더라도 제어를 위해 하나도 빠짐없이 정책을 받아야 하기 때문입니다.

노드정책 생성

1. 노드정책 마법사

정책 > 정책 > 노드 정책 > 작업선택 > 생성 을 선택하여 노드정책 마법사를 띠웁니다.



2. 정책 선택

정책을 생성하기 위해 신규 생성, 기존 정책 기반으로 생성 두 가지 생성 방법 중 한 가지를 선택하여 다음 버튼을 누릅니다.



이름	설명
신규 생성	정책을 새롭게 생성합니다.
기존 정책 기반으로 생성	기존에 생성되어 있는 정책 중 하나를 선택하여 선택한 정책의 기본 설정 값을 제외한 모든 설정 값을 똑같이 가져옵니다.

3. 정책 기본설정

정책기본설정의 간단한 항목 설명은 아래 그림과 표와 같습니다.
ID, 설명, 우선순위, 적용모드를 설정하고 다음 버튼을 누릅니다.



이 름	설 명
ID	정책을 식별 할 이름을 입력합니다. 해당란은 반드시 채워야 다음단계로 진행할 수 있습니다
설명	해당 정책에 대한 설명을 기입하는 곳입니다.
순서	정수로 기입하며, 낮은 숫자일수록 우선순위가 높습니다. 자세한 내용은 정책의 순서 변경을 참고해 주십시오.

적용모드	사용함/사용안함 옵션이 있고, 사용함 옵션 선택 시 정책을 생성하면서 사용항목의 체크 박스에 체크가 되어 생성됩니다. 적용은 되지 않으며 적용하려면 반드시 변경정책적용 아이콘을 눌러주어야 합니다.
------	--

4. 노드그룹설정

정책을 할당하기 위해서는 정책을 받을 그룹이 먼저 생성되어져 있어야 합니다.
그룹은 특정한 조건을 만족한 노드의 모임입니다. 노드 정책에 그룹을 할당할 시 그룹에 포함되어 있는 노드들은 관리자가 설정한 노드 정책을 적용 받게 합니다.
그룹의 특정조건은 IP대역, 운영체제별 그룹 등 수많은 조건들로 그룹을 생성할 수 있으며 자세한 내용은, [노드](#)를 참고 바랍니다.
노드그룹에는 정책그룹과 상태그룹이 있는데, 노드정책은 정책그룹만을 사용합니다.

정책이 적용될 대상인 노드그룹을 더블클릭, 혹은 드래그로 할당하고 다음 버튼을 누릅니다.



5. 정책세부 설정

세부내용으로 인증정책과 에이전트정책으로 구분되어 있는 사항에 해당하는 기능을 활성화하거나 항목에 적합한 설정값을 입력하고 다음 버튼을 누릅니다.



각종 항목과 설정값의 의미는 아래와 같습니다.

정 책	항 목	세 부 옵 션	설 명
인증정책	인증방법	호스트인증	노드의 MAC과 IP를 가지고 인증하는 방식, 식별되지 않는 사용자가 발생할 수 있습니다.
		비밀번호인증	사용자가 등록한 ID와 PASSWORD로 인증하는 방식, 전화기, TV, 프린트 등의 사용자 인증을 할 수 없는 장비들의 경우 문제가 발생할 수 있습니다.
		인증방식	CWP 페이지에서 인증 시 인증시도할 인증서버 및 우선순위를 설정할 수 있습니다. 상단에 있는 인증서버부터 인증시도하고 인증 실패 시 다음 하단에 있는 인증서버로 인증시도합니다.
		2단계 인증	사용안함일 경우 2단계 인증을 사용하지 않으며, SMS일 경우 사용자 인증 시 사용자 정보 중 휴대폰 항목에 입력된 휴대폰 번호로 발송된 인증번호를 입력하여야만 사용자 인증 할 수 있습니다.
인증대체정보	사용안함		인증대체정보 옵션을 사용하지 않습니다.
		Active Directory	ActiveDirectory에서 인증된 사용자 값을 가져와서 인증된 사용자로 인식되도록 하는 방식, AD서버가 구축되어 있어야 사용할 수 있습니다.
		연동API	외부 프로그램에서 제공된 DLL을 이용하여 에이전트에 인증대체 정보를 얻어와서 인증된 사용자로 인식되도록 하는 방식, 연계된 서버에서 문제가 발생할 경우 API 인증에 문제가 발생할 수 있습니다.
		GenianAPI	GENIAN API를 이용하여 인증된 노드ID를 얻는 방식, 연계된 서버에서 문제가 발생할 경우 API 인증에 문제가 발생할 수 있습니다.
AD 허용 도메인명			인증대체정보의 Active Directory를 설정하면 활성화되며, AD 대체인증이 허용 가능한 도메인명을 설정합니다. 여러 개일 경우 콤마(,)로 구분합니다. (예 : 'www.testdomain.com' 일 경우 'testdomain'만 입력), 빈 칸일 경우 도메인을 검사하지 않습니다.
2단계 인증	사용안함		사용자 인증 시 2단계 인증을 사용하지 않습니다.
		SMS	사용자 인증 시 사용자 정보 중 휴대폰 항목에 입력된 휴대폰 번호로 발송된 인증번호를 입력하여야만 사용자 인증 할 수 있습니다.
	인증 사용자그룹	그룹선택	사용자그룹을 설정하면 설정된 사용자 그룹에 포함된 사용자만 사용자 인증을 할 수 있습니다.(포함되어 있지 않은 노드들은 인증과정을 거치지 못함)
인증만료 자동로그아웃	on, off		최초 인증시각으로 부터 지정 시간후에 자동으로 인증상태가 해제됩니다.

	인증유효시간		자동로그인 설정이 on일 경우 활성화되며, 인증할 시 설정한 시간만큼 인증이 유효하고 설정한 시간이 지나면 인증이 해제됩니다. default : 24시간 최소값 : 1시간 최대값 : 1년
	미사용노드 자동로그아웃	on, off	노드 상태가 DOWN일 시 지정 시간후 자동으로 인증상태가 해제됩니다.
	미사용노드 인증유효시간		미사용노드 자동로그아웃 설정이 On일 경우 활성화되며, 지정한 시간동안 노드가 DOWN 상태일 시 인증이 해제 됩니다.
	주기적 재인증	사용안함, 매달, 매주, 매일	지정된 주기마다 인증상태가 해제되어 사용자가 재인증을 받도록 하기위한 방법을 선택.
	요일	월, 화, 수, 목, 금, 토, 일	주기적 재인증 설정이 매주일 경우 활성화되며, 매주 어떤 요일에 재인증을 수행할 것인지 선택합니다.
	날짜		주기적 재인증 설정이 매달일 경우 활성화되며, 매달 며칠날 재인증을 수행할 것인지 입력합니다.
	시각		주기적 재인증 설정이 매주, 매달, 매월일 경우 활성화되며, 재인증을 수행할 시각을 설정합니다.
	인증만료전알림	분, 시간, 일, 주, 개월	주기적 재인증에 의해 인증이 만료되기 설정한 시각 전에 에이전트 알람이 팝업됩니다. 에이전트가 설치되어 있어야합니다.
	사용자인증페이지	URL	별도의 사용자인증 페이지를 사용할 때 해당 URL을 입력합니다. 입력할 시 CWP 페이지에 인증 아이콘을 클릭 시 설정한 URL로 접속됩니다.
	윈도우 시작시 재인증	on, off	시스템 부팅 시 인증상태가 해제되어 사용자가 다시 인증을 받도록 하기위한 여부 선택.
	사용자명 출력이름		ID 입력 텍스트 박스에 붙여줄 이름을 입력합니다. 다국어 설정을 할 시 "공용어"/{default}{ko}"한국어"/{ko}{en}"영어"/{en} 형식으로 입력합니다. {/default} 앞에 작성된 문장은 사용자의 os언어가 한국어 및 영어가 아닐 경우 보여집니다. {ko} {/ko} 중간에 있는 문장은 사용자 os언어가 한국어일 경우 보여지고 {en} {/en} 중간에 있는 문장은 사용자 os언어가 영어일 경우 보여집니다.
	비밀번호 출력이름		PASSWORD 입력 텍스트 박스에 붙여줄 이름을 입력합니다. 다국어 설정을 할 시 "공용어"/{default}{ko}"한국어"/{ko}{en}"영어"/{en} 형식으로 입력합니다. {/default} 앞에 작성된 문장은 사용자의 os언어가 한국어 및 영어가 아닐 경우 보여집니다. {ko} {/ko} 중간에 있는 문장은 사용자 os언어가 한국어일 경우 보여지고 {en} {/en} 중간에 있는 문장은 사용자 os언어가 영어일 경우 보여집니다.
	사용자 등록 페이지	on, off	CWP 페이지에 사용자등록을 할 수 있는 사용자 등록 아이콘을 사용자들에게 보여줄지의 여부를 선택합니다.
	외부등록페이지		사용자 등록에 사용될 WEBPAGE의 URL을 설정합니다. 설정하지 않을 경우 Genian NAC에서 제공하는 사용자등록페이지가 사용됩니다.
	사용자동의 페이지	on, off	사용자 등록을 할 때 필요한 약관을 확인하고 동의할 수 있는 페이지를 사용자들에게 보여줄지의 여부를 선택합니다. 사용자정보 동의페이지만 출력됩니다.
에이전트 정책	사용여부	on, off, delete	on = 사용, off = 사용안함, delete = 에이전트 삭제 off, delete으로 설정할 경우 에이전트에 대한 제어정책에 의하여 노드들이 차단될 수 있습니다.
	CWP 자동설치	on, off	CWP 페이지에 접속할 시 자동으로 에이전트를 설치합니다.
	에이전트삭제시간	시간, 일 주, 개월	에이전트가 센터로 접속이 되지 않는 시간이 설정한 시간 이상이 되면 에이전트를 삭제합니다. 0으로 입력할 시 해당 기능을 사용하지 않습니다. default : 30일 최소값 : 0 최대값 : 1년
	Dissolvable Agent	on, off	PC 구동 시 에이전트가 정보수집 플러그인을 수행하고 정보수집이 완료되면 에이전트를 종료합니다. 플러그인의 제어기능은 동작하지 않으며 수행불가 플러그인은 노드액션 설정에서 플러그인 명에 취소선이 출력됩니다.
	Agent FailSafe 사용	on, off	에이전트가 센터와 통신이 되지 않을 경우, 에이전트 동작을 중지할지의 여부를 선택합니다.
	AFS 대기시간	정수로 기입, 단위로는 분, 시간, 일, 주 ,개월	Agent FailSafe Mode 모드로 들어가기전 대기시간을 설정합니다. default : 1시간 최소값 : 0 최대값 : 1년

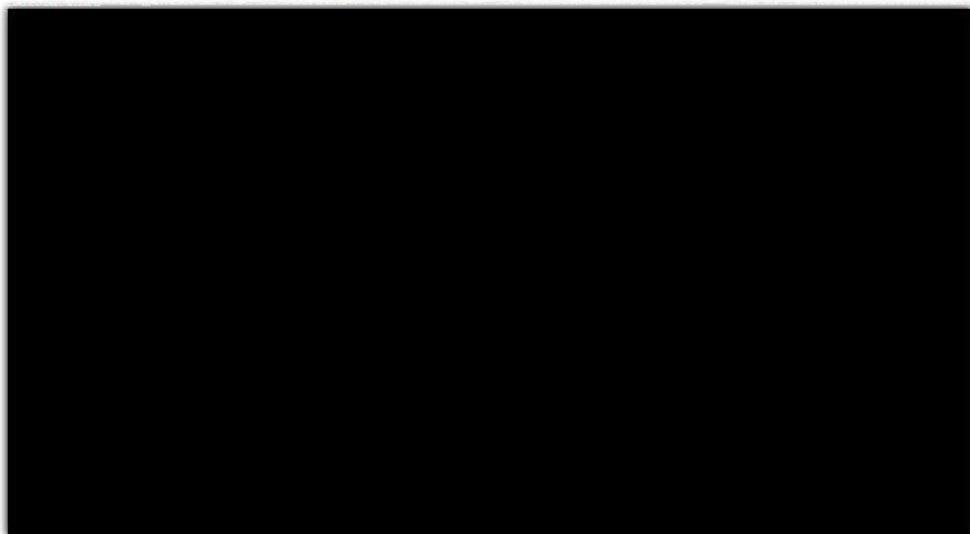
	트레이 아이콘 표시	on, off	트레이 창에 Agent 아이콘을 표시해 줄지 여부선택.
	수행 계정	PC에 로그인된 계정	PC에 로그인된 계정으로 에이전트가 실행됩니다.
	별도의 수행계정 설정		아이디와 비밀번호를 설정하고 동일한 아이디와 비밀번호가 계정으로 있을 경우 에이전트가 실행됩니다. 설정한 아이디와 비밀번호와 맞지 않는 계정일 경우 에이전트는 실행되지 않습니다.
	로컬 시스템 계정		시스템 계정으로 에이전트가 실행됩니다.
	아이디		수행계정 설정이 별도의 수행계정 설정일 경우에 활성화 되며, 에이전트를 수행할 계정의 아이디를 입력합니다.
	비밀번호		수행계정 설정이 별도의 수행계정 설정일 경우에 활성화 되며, 에이전트를 수행할 계정의 비밀번호를 입력합니다.
	정책변경검사주기	시간, 일, 주, 개월	에이전트 변경에 대한 정보를 설정한 시간을 주기로 하여 센터에서 확인 합니다. default : 4시간 최소값 : 1시간 최대값 : 4시간
	에이전트정보삭제	정수로 기입. 단위로는 시간, 일, 주, 개월	설정된 기간이상 업데이트 되지 않는 에이전트정보를 삭제 합니다. default : 30일 최소값 : 0 최대값 : 1년
관리정책	신규노드 호스트명 제한	on, off	신규로 등록되는 노드들에 대해 호스트명을 제한할지 선택합니다.
	호스트명템플릿		신규 호스트명제한 설정이 on일 경우 활성화되며, 호스트명을 입력합니다. 신규노드는 호스트 템플릿에 설정한 호스트명 외에 다른 호스트명을 사용할 시 호스트명제한 위반하게 됩니다. 기존 노드는 영향을 받지 않습니다.
	비활성노드삭제	정수로 기입, 단위로는 시간, 일, 주, 개월	설정된 기간이상 다운 상태를 유지하는 노드를 삭제 합니다. default : 30일 최소값 : 0 최대값 : 1년
	Design Template		CWP2 페이지 디자인 템플릿을 설정합니다. 디자인 템플릿은 설정 > 접속인증페이지(CWP) > 디자인 템플릿에서 생성 할 수 있습니다.

6. 노드액션 설정

노드액션은 PC전원제어, IE보안옵션제어 등 플러그인을 활용하여 사용자의 시스템의 설정 값을 바꾸고, 제어를 수행 합니다.

관리자는 노드정책에 액션을 할당함으로써 그룹에 알맞는 액션을 수행하게끔 하여 손쉽게 사용자 시스템의 정보를 수집, 제어할 수 있습니다.

해당 노드정책에 적용할 노드액션을 더블클릭 혹은 드래그로 할당하고 다음 버튼을 누릅니다.



7. 위험감지 설정

위험감지 기능은 관리자가 정의한 위험상황이 발생하였을 때, 해당 위험의 원인제공자를 찾아내고 로그를 통하여 상황을 기록합니다.

관리자는 노드정책에 위험을 할당함으로써 원하는 그룹에 대해서만 위험에 대한 감지기능을 켤 수 있습니다.

해당 노드정책에 적용할 위험을 더블클릭 혹은 드래그로 할당하고 확인 버튼을 누릅니다.



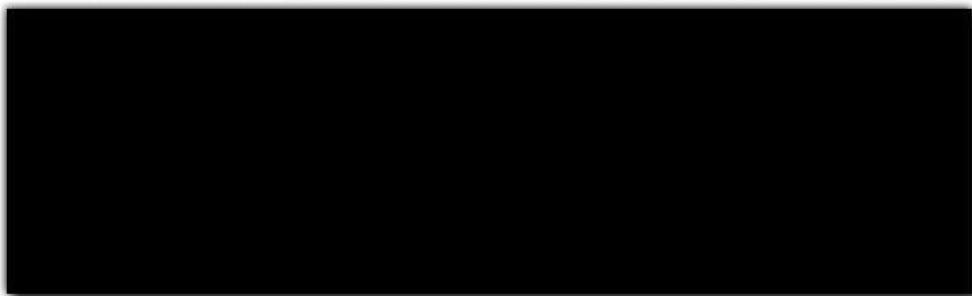
노드정책 즉시적용

정책의 설정값 중 대기시간을 갖는 설정값이 있더라도, 즉시적용을 이용하면 대기시간 없이 즉시 정책을 수행할 수 있습니다.

- 정책 > 정책 > 노드정책에서 즉시적용을 수행하고 싶은 정책의 ID의 맨 앞에 체크박스를 클릭하여 체크표시를 합니다.



- 작업선택 > 즉시적용를 클릭합니다.



- 원하는 작업에 대하여 체크박스에 체크를 하여주시고 즉시적용 버튼을 누릅니다.



노드정책 삭제

관리자는 필요없는 노드정책을 삭제할 수 있습니다.

노드정책 삭제 진행과정은 항목 [삭제](#)를 참조 바랍니다.

노드액션

노드액션이란?

노드액션이란 Agent와 Plug-in을 이용하여, 사용자의 시스템을 제어하거나 시스템의 설정값을 변경하는 것을 말합니다.
노드 액션은 노드정책에서 노드 액션을 설정해주어야 사용할 수 있으며, 해당 노드 정책을 받고 있는 노드들은 해당 노드 정책에 설정 되어 있는 노드 액션을 적용 받습니다.

노드액션 생성

1. 노드액션 추가

정책 > 정책 > 노드정책 > 노드액션 > 작업선택 > 추가 를 선택합니다.



2. 기본설정

액션의 이름, 설명, CWP 메시지를 설정합니다.



항목	설명
라벨	임의의 라벨명을 입력합니다. 라벨은 정책에서 액션과 같이 할당할 수 있으며 동일한 라벨명을 가진 액션들이 할당됩니다.

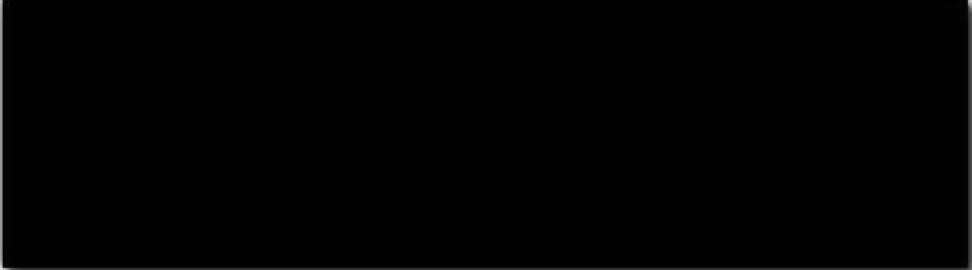
3. 액션 수행조건 설정

액션이 수행될 액션 검사조건을 설정합니다.

액션 검사조건이란 아이템과 조건으로 이루어져있으며, 설정해놓은 검사조건과 사용자 노드의 상태가 일치할 때 액션 수행설정의 플러그인이 동작됩니다.

예를들어, 액션 검사조건의 아이템 : 파일 , 조건 : 존재하면, 설정 : %ProgramFiles%\\NATEON\\BIN\\NateOnMain.exe(네이트온 메신저)로 설정하고

액션 수행설정의 플러그인 선택을 인터페이스 제어로 했을 경우, 네이트온 메신저 파일이 존재하면 인터페이스 제어를 수행합니다.



액션 검사조건의 아이템과 조건, 설정값은 아래 표와 같습니다.

조건연산	조건설정		
	아이템	조건	설정
AND, OR	프로세스	동작하면, 동작하지 않으면	프로세스이름
		해쉬값이 같으면, 다르면	해쉬경로, 해쉬값
AND, OR	파일	존재하면, 존재하지않으면	파일경로, 버전
		버전이 같으면, 버전이 다르면	파일경로, 버전
		보다낮은 버전이면, 보다높은 버전이면	파일경로, 버전
		해쉬값이 같으면, 해쉬값이 다르면	해쉬경로, 해쉬값
		날짜가 특정기간 이내이면, 날짜가 특정기간 이외이면	기간, 일
AND, OR	레지스트리	존재하면,존재하지않으면	Key, Name, Value
		같으면, 다르면	Key, Name, Value
		보다낮은 버전이면, 보다높은 버전이면	Key, Name, Value
AND, OR	서비스팩버전	같으면, 다르면	설정값
		보다낮은 버전이면, 보다높은 버전이면	설정값
AND, OR	서비스	존재하면, 존재하지않으면	설정값
		동작하면, 동작하지 않으면	설정값
	시스템	센터시각과 차이가 보다 크면, 센터시각과 차이가 보다 작으면	분, 시간, 일, 주, 개월
AND, OR	인증사용자	인증사용안함	
		인증됨	
		인증되지 않음	

4. 액션 수행설정

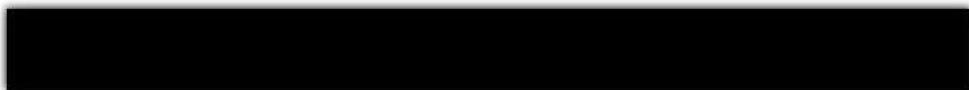
플러그인의 종류를 선택하고 플러그인의 세부 설정을 합니다.

플러그인은 앞으로 더욱더 많은 플러그인이 추가될 예정입니다.
플러그인의 종류와 자세한 내용은 [플러그인](#)을 참고해 주십시오.



5. 적용언어 설정

노드액션이 수행될 적용언어(OS 언어)를 선택합니다.
체크가 되어있는 OS언어를 사용하고 있는 노드만 노드액션을 수행합니다.



6. 적용OS 설정

노드액션이 수행될 OS를 선택합니다.
체크가 되어있는 OS를 사용하고 있는 노드만 노드액션을 수행합니다.



7. 할당

노드액션을 추가 후에는 노드정책을 생성하고 반드시 정책에 할당하여야 만든 노드액션을 사용할 수 있습니다.
노드정책에서의 노드액션 할당법은 [노드정책](#) - 노드정책 생성 - 6번 항목을 참고해 주시기 바랍니다.

8. 노드액션 할당 확인

노드액션이 노드정책에 잘 할당되었다면, 노드액션 페이지의 i 표시 아이콘에 마우스를 올리면 어떤 정책에 할당되었는지 확인할 수 있습니다.



노드액션의 삭제

관리자는 필요하지 않은 노드액션을 삭제할 수 있습니다.

노드액션의 삭제 방법은 [항목 삭제](#)를 참조해 주십시오.

위험감지

위험감지란?

위험감지란 관리자가 정의한 위험상황이 발생하였을 때, 해당 위험의 원인제공자를 찾아내고 로그를 통하여 상황을 기록하는 것을 말합니다.

위험감지는 네트워크상의 커다란 위협을 가할 수 있는 여러 가지 상황들을 감지하여 관리자에게 문자, 메일 등 알람 서비스를 통하여 보다 신속하고 효과적으로 위험 상황에 대하여 대응할 수 있도록 합니다.

위험감지 생성과 할당

관리자는 Genian NAC에 미리 정의되어 있는 여러 가지 위험 이벤트를 이용하여, 혹시모를 위험상황에 대비할 수 있습니다.

1. 위험감지 생성

정책 > 정책 > 노드정책 > 위험감지 > 작업선택 > 생성 을 선택합니다.



2. 기본정보, 중요도, 적용모드 입력

위험감지를 식별할 수 있는 ID와 설명, 중요도와 적용모드를 설정합니다. 해당 위험이 감지된 노드가 CWP 페이지에 접속하였을 시 보여줄 CWP메시지를 설정합니다.



중요도와 적용모드의 내용은 아래와 같습니다.

옵션	설명
중요도	미설정, 낮음, 중간, 높음
적용모드	사용함, 사용안함
예외 노드그룹	예외 노드그룹에 포함된 노드는 위험이 감지되어도 예외처리 합니다.

3. 위험 이벤트 선택

감지를 원하는 위험을 선택하고 신규위험감지를 생성합니다.
현재 Genian NAC에 정의되어 있는 위험은 총 17개이며, 추후에 더 추가될 수 있습니다.



위험 이벤트에 관한 상세설명은 아래 표와 같습니다.

위험 이벤트 이름	옵션	옵션 설명
노드가 지정된 그룹에 포함됨	노드그룹 지정	위험 이벤트를 발생시킬 노드그룹 선택
다수의 IP를 소유한 시스템이 발견됨	동시보유IP수 지정	노드가 동시에 보유한 IP가 설정된 수 이상이면 감지
알 수 없는 노드 발견	없음	어느 그룹에도 속하지 않는 노드가 발견됨
포트스캔 감지됨	감지기간(초)	이벤트 감지를 위한 정보 축적시간
	접근포트수	감지기간 동안 지정된 포트 수 이상의 접근시 위험으로 탐지
	공격자 검색방법(MAC+IP, IP)	위험 탐지시 공격자 노드를 검색할 방법 선택
제공하지 않는 서비스 요청 감지됨	감지기간(초)	이벤트 감지를 위한 정보축적시간
	접근포트수	감지기간 동안 지정된 포트 수 이상의 접근시 위험으로 탐지
	공격자 검색방법(MAC+IP, IP)	위험탐지시 공격자 노드를 검색할 방법 선택
여러 네트워크(센서)에 속한 노드 발견	없음	하나의 시스템이 동시에 둘 이상의 네트워크(센서에) 포함 됨
클라이언트에게 허용되지 않은 IP를 가진 인터페이스가 존재함	인가된 인터페이스 IP 그룹	인터페이스의 IP주소가 지정된 그룹에 포함되는지 여부검사
	알려진 네트워크 자동포함	Genian에서 알려진 네트워크를 인가된 인터페이스 IP그룹에 자동포함 (예 : 센서의 네트워크)
	에이전트 인터페이스 차단	위험으로 감지된 인터페이스를 에이전트가 사용금지 시키도록 할지 여부선택
클라이언트에게 허용되지 않은 IP를 가진 게이트웨이가 존재함	인가된 게이트웨이 IP 그룹	시스템에 설정된 게이트웨이 주소가 인가된 IP영역인지 확인
	알려진 게이트웨이 자동포함	Genian에서 알려진 게이트웨이를 인가된 게이트웨이 주소에 포함 (예 : 센서의 게이트웨이)
	에이전트 인터페이스 차단	위험으로 감지된 인터페이스를 에이전트가 사용금지 시키도록 할지 여부선택
ARP Bomb	감지기간(초)	이벤트 감지를 위한 정보축적시간 (3~30초)

	요청횟수	감지기간 동안 지정된 횟수이상 ARP Request시 위험으로 탐지
	공격자 검색방법(MAC+IP, IP)	위험탐지시 공격자 노드를 검색할 방법 선택
DNS Record 질의	제외시킬 네트워크 그룹	탐지에서 제외시킬 네트워크 그룹 선택
	요청횟수	감지기간 동안 지정된 횟수 이상 Query시 위험으로 탐지
	감지기간(초)	위험감지를 위한 정보축적시간 (5~30초)
바이러스 감염 노드 발견	없음	백신 프로그램에 의해서 치료불가능한 바이러스에 감염된 노드가 발견됨
ARP 변조공격(spoofing)	감지기간(초)	위험감지를 위한 정보축적시간(3~600초)
	공격횟수	감지기간 동안 지정된 횟수 이상의 ARP 변조패킷을 보낼경우 위험으로 탐지
SNMP 차단요청	SNMP Trap OID	SNMP Trap 식별을 위한 OID
	차단대상 IP OID	차단대상 노드의 IP 정보를 가진 OID
	차단대상 MAC OID	차단대상 노드의 MAC 정보를 가진 OID
	차단사유 OID	차단사유 정보를 가진 OID
	해제대상 IP OID	해제대상 노드의 IP 정보를 가진 OID
	해제대상 MAC OID	해제대상 노드의 MAC 정보를 가진 OID
	해제사유 OID	해제사유 정보를 가진 OID
	필터링 대상 OID	수신된 SNMP Trap에 대한 필터링을 수행할 대상 OID
	필터링 정규식	필터링을 위한 정규식 입력
MAC + IP 클론 감지	MAC Spoofing 감지(on,off)	MAC Spoofing (사용자가 인터페이스 MAC을 임의의 값으로 변경하는 행위) 노드를 Clone 노드로 감지여부

4. 위험의 할당

위험감지 기능은 반드시 노드정책에 할당하고, 사용 항목이 활성화 되어 있어야 합니다.

할당하는 방법은 [노드정책](#)의 노드정책생성 - 7번 항목을 참조해 주십시오.

위험감지를 정책에 할당해놓고, 사용하고 싶지 않을 때는 정책에서 할당한 위험을 삭제하지 않아도 단순히 사용항목의 체크 박스만 해제해도 사용이 중지됩니다.

위험감지 삭제

관리자는 필요없는 위험감지를 삭제할 수 있습니다.

위험감지 삭제 진행과정은 [항목 삭제](#)를 참조 바랍니다.

제어정책

제어정책이란?

제어정책이란 노드정책이 정의한 방법을 토대로 얻은 내부시스템의 정보들을 이용하여 각 그룹별로 네트워크 접근권한을 부여하는 것을 말합니다.

Genian NAC가 네트워크를 제어하는 간단한 절차는 아래와 같습니다.

1. 관리자가 분류 가능한 조건을 가지고 정책상태그룹을 만들고 그 그룹에게 권한을 부여합니다.
2. 센터는 센서가 수집한 노드 정보를 가지고 각 노드를 위 관리자가 만든 그룹 속에 포함시킵니다.
3. 노드가 어떠한 그룹 속에 포함되면 그 그룹은 이미 권한이 정의되어 있기 때문에 권한 이상의 행동을 할 수 없습니다.
4. 만약 노드가 정의된 권한 이상의 네트워크 접근을 시도 할 때는 Genian NAC가 관리자가 설정한 CWP 페이지로 사용자를 유도합니다.
관리자는 CWP 페이지를 설정하여 사용자로 하여금 추가조건(사용자 인증, 에이전트 설치 등)을 만족하게 하거나, 인터페이스 제어를 통하여 권한 이상의 네트워크 접근 시도를 원천봉쇄합니다.
5. 제어정책에는 아래의 그림과 같이 총 8개의 기본적으로 생성되어 있는 정책이 있습니다.



제어정책 역시 노드정책과 마찬가지로 여러개의 그룹에 동시에 속한 노드가여러개의 정책을 한번에 받을경우, 순위를 통하여 우선순위가 제일 높은 정책 한 가지만 받게됩니다.

- CWP 페이지로 리다이렉션 하여 조건만족 유도시키기 위해 최소 DNS 권한이 있어야 CWP 페이지에 접속할 수 있습니다.
- 제품 초기설치 시 기본정책이라는 것이 존재합니다. 삭제와 그룹할당이 불가능한 이 정책은 관리자가 설정한 정책 중 아무정책에도 포함되지 않은 노드들을 위하여 존재하는 정책입니다.
센서가 수집한 노드목록에 포함되어있는 노드들은 어떠한 그룹에 속하지 않는 노드가 있더라도 제어를 위해 하나도 빠짐없이 정책을 받아야 하기 때문입니다.
- 제어정책에는 네트워킹 장비들을 그룹으로 만들고, 예외정책을 생성하여 모든 정책으로부터 제외시켜 행여나 네트워킹 장비가 차단되는 일이 없도록 해야합니다.

제어정책 생성

제어정책을 생성할 수 있습니다.

1. 제어정책 생성

정책 > 정책 > 제어정책 > 작업선택 > 생성 버튼을 클릭하여 제어정책 마법사 창을 띠웁니다.



2. 정책 선택

정책을 생성하기 위해 신규 생성, 기존 정책 기반으로 생성 두 가지 생성 방법 중 한 가지를 선택하여 다음 버튼을 누릅니다.



이름	설명
신규 생성	정책을 새롭게 생성합니다.
기존 정책 기반으로 생성	기존에 생성되어 있는 정책 중 하나를 선택하여 선택한 정책의 기본 설정 값을 제외한 모든 설정 값을 똑같이 가져옵니다.

3. 정책기본설정

생성할 제어정책의 이름과 설명, 적용순위인 순서와 적용모드를 설정하고 다음 버튼을 누릅니다.



이 름	설 명
ID	정책을 식별할 정책의 이름을 말합니다. 해당란은 반드시 채워야 다음단계로 진행할 수 있습니다
설명	해당 정책에 대한 설명을 기입하는 곳입니다.
순서	정수로 기입하며, 낮은 숫자일수록 우선순위가 높습니다. 더욱 자세한 내용은 정책의 순서 변경을 참고해 주십시오.

적용모드	사용함/사용안함 옵션이 있고, 사용함 옵션 선택 시 정책을 생성하면서 사용항목의 체크 박스에 체크가 되어 생성됩니다. 적용은 되지 않으며 적용하려면 반드시 변경정책적용 아이콘을 눌러주어야 합니다.
------	--

4. 노드그룹 할당

정책을 할당하기 위해서는 정책을 받을 그룹이 먼저 생성되어져 있어야 합니다.
그룹은 같은 정책을 적용받을 노드의 모임입니다. 언제든 변할 수 있는 노드의 상태를 감지하여 네트워크를 제어하는 제어정책은 정책그룹과 상태그룹 모두 다 이용합니다.

해당 제어정책의 제어를 받을 노드그룹을 할당하고 다음 버튼을 누릅니다.



5. 권한 할당

권한은 네트워크, 서비스, 시간 객체로 이루어져 있으며, 사용자들의 네트워크를 제한합니다.
해당 제어정책에 맞는 권한을 할당하고 다음 버튼을 누릅니다.



차단된 사용자가 CWP 페이지에 접속하게 할려면 DNS권한을 할당해주어야합니다. DNS권한 조차 없을 경우 CWP페이지에 접속을 하지 못하여 차단을 해제할 수 있는 방법을 사용자에게 제시해 줄수 없습니다.

6. 제어옵션 설정

제어옵션에는 크게 CWP옵션과, 스위치 포트 차단 옵션이 있습니다.
CWP옵션은 CWP 페이지에 관련된 설정을 할 수 있고, 스위치 포트 차단 옵션에서는 SNMP를 이용한 인터페이스 차단에 관한 설정을 할 수 있습니다.



세부항목에 대한 간단한 설명은 아래와 같습니다.

제어옵션	세부옵션	내용
CWP 페이지	CWP 사용안함	제어정책에 의해 차단 시 CWP 페이지로 리다이렉션 하지 않습니다.
	표준 CWP 페이지	제어정책에 의해 차단 시 CWP 페이지로 리다이렉션합니다.
	보안서약 페이지	제어정책에 의해 차단 시 보안서약 페이지로 리다이렉션합니다. 보안서약 페이지는 설정 > 접속인증페이지(CWP) > 동의페이지에서 설정할 수 있습니다.
	사용자정의 페이지	제어정책에 의해 차단 시 사용자가 정의한 페이지로 리다이렉션합니다. 보안서약 페이지 사용 시 보안서약 동의 후 리다이렉션됩니다.
URL		리다이렉션 시킬 주소를 입력합니다. 미 입력 시 기본 CWP를 사용합니다.
보안서약 완료 메시지		보안서약 동의 후 출력할 메시지를 입력합니다.
사용자 메시지		CWP 페이지에서 해당 제어정책을 적용받고 있는 사용자에게 표시할 메시지를 입력합니다.
스위치 포트 차단	포트 차단 수행(on,off)	노드가 연결된 스위치 포트를 SNMP를 통하여 차단을 수행할지 여부를 선택합니다. 스위치에 SNMP 관련 설정이 적용되어 있어야합니다.
SNMP Version	Version 2c, Version 3	스위치와 통신할 SNMP Version을 설정합니다.
SNMP Community		쓰기권한을 가진 SNMP Community를 입력합니다.
Community		SNMP Version0 Version 2c일 경우 활성화되며, SNMP의 Community를 입력합니다.
Security Name		SNMP Version1 Version 3일 경우 활성화되며, SNMP의 Security Name을 입력합니다.
Security Level		SNMP Version1 Version 3일 경우 활성화되며, SNMP의 Security Level을 설정합니다.
Port Description		스위치 포트 차단 수행 이후에 해당 포트의 Description을 설정 내용으로 업데이트합니다.

차단 방지 문자열		스위치에서 포트의 Description을 설정했을 경우 스위치 포트 차단 시 Description과 차단 방지 문자열을 비교하여 Description에 차단 방지 문자열이 존재할 경우 스위치 포트 차단을 수행하지 않습니다.
차단포트 MAC 개수		차단을 수행할 스위치 포트에 등록된 MAC이 설정된 개수 이하일때만 포트 차단을 수행합니다.
RADIUS CoA	On, Off	RADIUS CoA를 통한 스위치 제어를 수행할지 여부를 선택합니다. 스위치에 RADIUS CoA 관련 설정이 적용되어 있어야합니다.
CoA Command		스위치에 제어할 방식을 설정합니다.
Generic-CoA Attributes		CoA Command 설정이 Generic-CoA일 경우 입력한 설정이 스위치에 전송됩니다.

7. 제어액션 할당

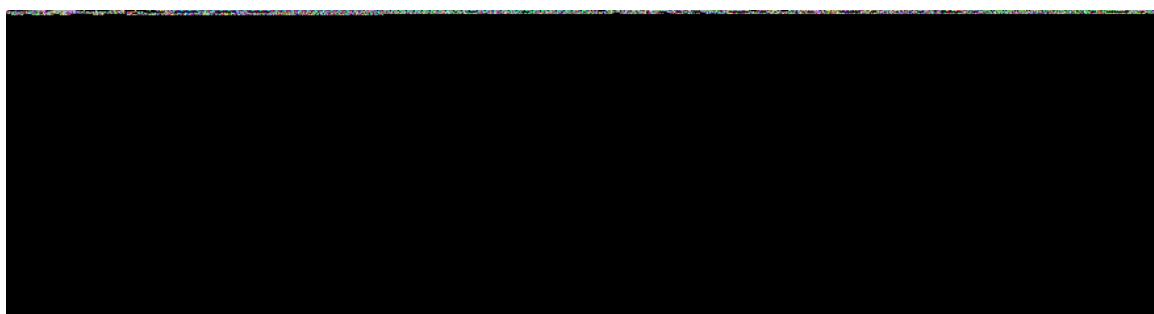
제어액션을 이용하여 사용자에게 네트워크 차단뿐만 아니라 닫기를 할 수 없는 메시지를 사용자 PC에 띄고, 사용자 PC를 재부팅 등의 제어를 할 수 있습니다.
제어액션을 생성하는 방법은 [제어액션](#)을 참고 바랍니다.

해당 제어정책에 적용할 대상 제어액션을 할당하고 확인 버튼을 누릅니다.



제어정책 차트

실시간으로 Active 모드 센서와 Passive 모드 센서 및 제어정책 의해 차단된 노드의 비율을 차트로 확인할 수 있습니다.



제어정책 삭제

관리자는 필요없는 제어정책을 삭제할 수 있습니다.

제어정책 삭제 진행과정은 [항목 삭제](#)를 참조 바랍니다.

제어액션

제어액션이란?

노드들이 제어정책에 위배되는 행동을 하여 제어정책에 의한 제어를 받을 때 제어와 함께 수행되는 액션입니다. 제어액션에는 PC 전원제어, 사용자 메시지, 인터페이스 제어가 존재합니다.

제어액션 추가와 할당

관리자는 플러그인을 통하여 제어액션을 추가/할당 하여 제어액션을 사용할 수 있습니다.

1. 제어액션 추가

정책 > 정책 > 제어정책 > 제어액션 > 작업선택 > 추가 를 선택합니다.



2. 기본설정

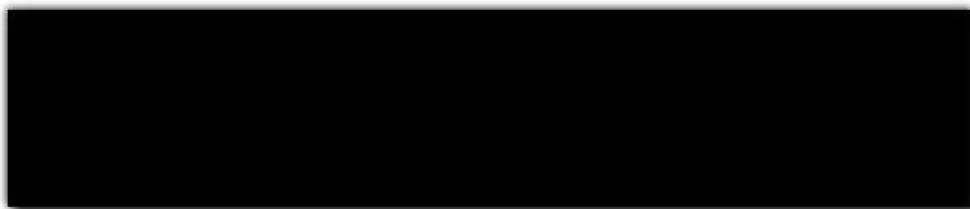
이름과 설명, CWP 메시지를 입력합니다.



3. 액션 검사조건

액션이 수행될 액션 검사조건을 설정합니다.

액션 검사조건이란 아이템과 조건으로 이루어져있으며, 설정해놓은 검사조건과 사용자 노드의 상태가 일치 할 때 액션 수행설정의 플러그인이 동작됩니다.



조건연산	조건설정		
아이템	조건	설정	
AND, OR	프로세스	동작하면, 동작하지 않으면	프로세스 이름
		해쉬값이 같으면, 다르면	해쉬경로, 해쉬값
AND, OR	파일	존재하면, 존재하지않으면	파일경로, 버전
		버전이 같으면, 버전이 다르면	파일경로, 버전
		보다낮은 버전이면, 보다높은 버전이면	파일경로, 버전

		해쉬값이 같으면, 해쉬값이 다르면	해쉬경로, 해쉬값
		날짜가 특정기간 이내이면, 날짜가 특정기간 이외이면	기간, 일
AND, OR	레지스트리	존재하면,존재하지않으면	Key, Name, Value
		같으면, 다르면	Key, Name, Value
		보다낮은 버전이면, 보다높은 버전이면	Key, Name, Value
AND, OR	서비스팩버전	같으면, 다르면	설정값
		보다낮은 버전이면, 보다높은 버전이면	설정값
AND, OR	서비스	존재하면, 존재하지않으면	설정값
		동작하면, 동작하지 않으면	설정값
	시스템 정보	센터시각과 차이가 보다 크면, 센터시각과 차이가 보다 작으면	분, 시간, 일, 주, 개월

4. 액션 수행설정

플러그인을 선택하고 플러그인의 세부 설정을 합니다.

플러그인 개수는 약 3가지이며, 앞으로 더욱더 많은 플러그인이 추가될 예정입니다.
플러그인의 종류와 자세한 내용은 [플러그인](#)을 참고 바랍니다.



5. 적용언어 설정

제어 액션이 수행될 적용 언어(OS 언어)를 선택합니다.
체크가 되어있는 OS 언어를 사용하고 있는 노드만 제어 액션을 수행합니다.



6. 적용OS 설정

제어 액션이 수행될 OS를 선택합니다.
체크가 되어있는 OS를 사용하고 있는 노드만 제어 액션을 수행합니다.



7. 할당

제어 액션을 생성한 후 제어 정책을 생성할 때 생성한 제어 액션을 사용할 수 있습니다.
제어 정책에서 제어 액션 할당 방법은 제어정책에서 7번 항목을 참고 바랍니다.

8. 제어액션 할당 확인

제어액션이 어느 정책에 할당되었는지 i 표시의 아이콘에 마우스를 올리면 어느 정책에서 제어액션을 사용하고 있는지 확인할 수 있습니다.



제어액션의 삭제

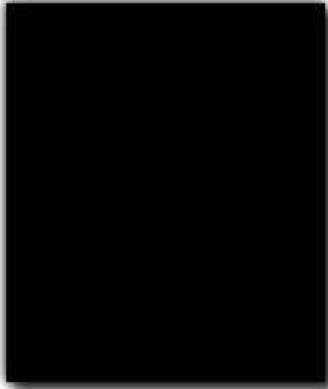
관리자는 필요하지 않은 제어 액션을 삭제할 수 있습니다.

제어 액션 삭제 방법은 [항목 삭제](#)를 참조 바랍니다.

무선랜정책

무선랜정책이란?

무선랜정책이란 AP 프로파일, Client 프로파일을 할당하여 Air-sentry의 AP기능을 사용하는 정책입니다.



- 무선랜정책을 생성하기 위해서는 다음 2가지 항목이 필요합니다.
 - [AP프로파일](#) : Air Sentry AP설정을 위한 프로파일 설정
 - [Client 프로파일](#) : 무선연결관리자(WCM)에서 사용할 AP 접속용 프로파일 설정

무선랜정책 생성

1. 무선랜정책 생성

정책>정책>무선랜정책>작업선택>생성 버튼 클릭하여 무선랜정책 생성 창에 접속 합니다.



2. 기본정보 설정

SSID, 태입, 설명, 적용모드를 설정합니다.



이름	옵션	내용
SSID		무선랜정책을 식별할 이름을 설정합니다.
태입	단독	AP 프로파일, Client 프로파일을 설정할 수 있으며, 설정한 AP 프로파일에 사용되는 Client 프로파일을 설정할 수 있습니다.
	패턴	Client 프로파일만 설정 가능하며 정규식을 이용하여 정규식에 맞는 무선네트워크가 있을 경우에 사용되는 Client 프로파일을 설정 할 수 있습니다.
설명		해당 SSID 추가적인 설명이 필요할 경우 입력 합니다.
적용모드	사용함	해당 무선랜정책을 사용합니다.
	사용안함	해당 무선랜정책을 사용 하지 않습니다.

3. RADIUS 인증허용 사용자 그룹

인증을 허용할 사용자 그룹을 설정합니다.



이름	내용
인증허용 사용자 그룹	암호방식이 WPA,WPA2-Enterprise일 경우 사용되며, 사용자 그룹을 지정하여 해당 사용자 그룹에 포함되어 있는 사용자만 인증을 허용하여 AP를 사용할 수 있지만, 포함되어 있지 않는 사용자는 인증을 할 수 없어 AP를 사용할 수 없습니다.

4. AP 프로파일 설정

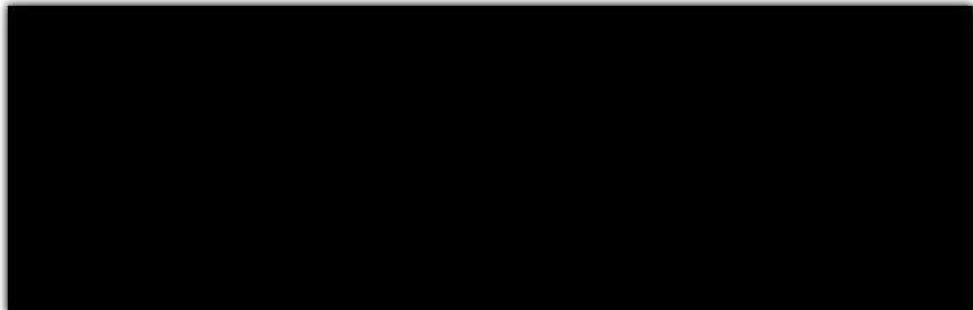
설정할 AP 프로파일, 적용대상을 선택합니다.



이름	옵션	내용
AP 프로파일		생성한 AP 프로파일을 설정 합니다.
적용대상	모든 Air-Sentry	모든 Air-Sentry 선택됩니다.
	태깅된 Air-Sentry	Air-Sentry에 설정되어 있는 태그를 검색하여 해당 태그가 설정되어 있는 Air-Sentry 모두가 선택됩니다.
동작시간		시간 객체를 할당하여 AP의 동작시간을 설정합니다. 설정한 시간 객체 외의 시간 또는 선택안함으로 설정되어 있을 시 AP는 동작하지 않습니다. 시간객체에 대한 내용은 시간 을 참고바랍니다.
접근제어		AP를 사용하는 사용자에게 할당할 권한을 설정합니다. 권한에 대한 내용은 권한 을 참고바랍니다.

5. Client 프로파일 설정

설정할 Client 프로파일, 허용 MAC 목록을 설정합니다.



AP프로파일

AP프로파일이란?

Air-sentry 제품에 AP(무선 네트워크)기능을 추가 할 때 사용되는 프로파일입니다.

AP프로파일 생성

1. 기본설정 입력

ID, 설명, Hidden AP을 설정합니다.



이름	옵션	내용
ID		AP 프로파일의 식별할 수 있는 이름을 입력합니다.
설명		추가적으로 필요한 설명을 입력합니다.
Hidden AP	on	Air-sentry AP의 SSID를 브로드 캐스트 하지 않습니다. 즉, 다른 노드가 무선랜 탐지할 때 해당 AP를 탐지하지 못합니다.
	off	Air-sentry AP의 SSID를 브로드 캐스트 합니다.

2. 보안설정

AP 보안을 위해 보안방식을 선택 후 보안 방식에 맞게 보안설정을 입력합니다.



이름	옵션	내용
보안방식	Open	AP에 보안을 설정하지 않습니다.
	WEP	AP에 패스워드 형식으로 보안 설정합니다.
	WPA,WPA2-Personal	AES, TKIP 방식으로 보다 높은 보안으로 패스워드를 설정합니다.
	WPA,WPA2-Enterprise	RADIUS 서버를 이용한 보안 방식으로 RADIUS 서버를 설정하여 RADIUS 서버에 저장되어 있는 ID, Password를 입력해야 AP를 사용할 수 있습니다.
보안 설정	Open	별도의 설정이 필요 없는 항목입니다.
	WEP	WEP 키 길이 : 64 bit 5자리 패스워드, 128 bit 13자리 패스워드 보안 키 (ASCII 5자리) : WEP 키 길이 설정이 64 bit 일 경우에 활성화 되며, 5자리 패스워드를 입력합니다. 보안 키 (ASCII 13자리) : WEP 키 길이 설정이 128 bit 일 경우에 활성화 되며, 13자리 패스워드를 입력합니다.
	WPA,WPA2-Personal	보안모드 : Auto(WPA ro WPA2), WPA Only, WPA2 Only 중 한가지를 선택합니다. 암호화 유형 : Auto, AES, TKIP 중 한가지를 사용 할 수 있습니다. Auto는 AES, TKIP 중 한가지를 자동으로 사용 합니다. 보안 키 : 관리자가 설정하고 싶은 패스워드를 영문 관계없이 8자리~63자리를 입력합니다.
	WPA,WPA2-Enterprise	보안 모드 : Auto(WPA ro WPA2), WPA Only, WPA2 Only 중 한가지를 선택합니다. 암호화 유형 : Auto, AES, TKIP 중 한가지를 사용 할 수 있습니다. Auto는 AES, TKIP 중 한가지를 자동으로 사용 합니다. Primary RADIUS 서버IP : 인증에 사용할 RADIUS 서버의 IP를 입력합니다. 포트번호 : RADIUS 서버의 포트를 입력합니다. 보안 키 : RADIUS 인증을 위한 보안 키를 입력 합니다. Secondary RADIUS = Primary RADIUS server이 동작하지 않을 시 Secondary RADIUS server을 사용합니다. 단 RADIUS 설정 및 바라보는 DB는 서로 같아야합니다. 서버IP : 인증에 사용할 RADIUS 서버의 IP를 입력합니다. 포트번호 : RADIUS 서버의 포트를 입력합니다. 보안 키 : RADIUS 인증을 위한 보안 키를 입력 합니다.

Client 프로파일

Client프로파일이란?

무선연결관리자(WCM)에서 사용할 AP 접속용 프로파일 설정입니다.
Client 프로파일은 사용자가 무선 네트워크를 사용할 때 필요한 설정 및 암호를 자동으로 설정합니다.

Client프로파일 생성

1. 기본설정

설명, Hidden AP 연결, 자동연결을 설정합니다.



이름	옵션	내용
ID		Client 프로파일을 식별할 수 있는 이름 입력합니다.
설명		추가적으로 필요한 설명을 입력합니다.
Hidden AP 연결	on	Hidden AP를 자동으로 연결 합니다.
	off	Hidden AP를 연결 하지 않습니다.
자동연결	on	무선 네트워크가 범위 내에 있을 때 자동으로 연결합니다.
자동연결	off	무선 네트워크가 범위내에 있어도 연결하지 않습니다.

2. 보안설정

사용할 AP 프로파일과 동일하게 보안방식을 설정하고 보안방식에 맞게 보안설정을 합니다.



이름	옵션	내용
보안방식	Open	별도의 설정이 필요없는 항목입니다.
	WEP	보안방식이 WEP으로 설정되어 있는 AP에 접속할 때 선택합니다.
	WPA,WPA2-Personal	보안방식이 WPA,WPA2-Personal으로 설정되어 있는 AP에 접속할 때 선택합니다.
	WPA,WPA2-Enterprise	보안방식이 WPA,WPA2-Enterprise으로 설정되어 있는 AP에 접속할 때 선택합니다.
	802.1X	보안방식이 802.1X으로 설정되어 있는 AP에 접속할 때 선택합니다.
보안설정	Open	별도의 설정이 필요없는 항목입니다.
	WEP	보안 키 : AP 프로파일에 설정한 WEP의 보안 키를 입력합니다.
	WPA,WPA2-Personal	보안모드 : AP 프로파일에 설정한 보안모드랑 동일하게 설정합니다. 암호화 유형 : AP 프로파일에 설정한 암호화 유형과 동일하게 설정 합니다. 보안 키 : AP 프로파일에 설정한 보안 키를 입력합니다.
	WPA,WPA2-Enterprise	보안 모드 : AP 프로파일에 설정한 보안모드랑 동일하게 설정합니다. 암호화 유형 : AP 프로파일에 설정한 암호화 유형과 동일하게 설정합니다. 자격 증명 기억 : 자격 증명을 했을 시 다음에 접속할 때 자격 증명을 수행하지 않습니다. 네트워크 인증방법 : 네트워크 인증방법을 선택합니다. 서버 인증서 유효성 확인 : 서버 인증서 유효성 확인을 할지 안할지 설정합니다. 빠른 다시 연결 사용 : 연결이 실패 했을 경우, 빠르게 다시 연결 합니다. 인증모드 : 인증모드 지정안함, 사용자 또는 컴퓨터 인증, 컴퓨터 인증, 사용자 인증, 게스트 인증 중 한가지를 선택합니다. Windows로그인 정보 사용 : RADIUS서버가 active directory와 인증 연동 되어 있을 시 active directory를 이용하여 인증할 수 있습니다. SSO 사용 : SSO를 사용합니다. 로그인 직전 수행 : 원도우 로그인을 하기 전에 무선랜인증을 하여 네트워크를 연결할 수 있도록 합니다. 최대 지연 : 최대 지연시간을 설정합니다. 추가 대화 상자 표시 : SSO를 진행하는 동안 추가 대화 상자 표시를 허용합니다. 가상 LAN 사용 : 컴퓨터 및 사용자 인증에 별도의 가상 LAN을 사용합니다.
	802.1X	자격 증명 기억 : 자격 증명을 했을 시 다음에 접속할 때 자격 증명을 수행하지 않습니다. 네트워크 인증방법 : 네트워크 인증방법을 선택합니다. 서버 인증서 유효성 확인 : 서버 인증서 유효성 확인을 할지 안할지 설정합니다. 빠른 다시 연결 사용 : 연결이 실패 했을 경우, 빠르게 다시 연결 합니다. 인증모드 : 인증모드 지정안함, 사용자 또는 컴퓨터 인증, 컴퓨터 인증, 사용자 인증, 게스트 인증 중 한가지를 선택합니다. Windows로그인 정보 사용 : RADIUS서버가 active directory와 인증 연동 되어 있을 시 active directory를 이용하여 인증할 수 있습니다. SSO 사용 : SSO를 사용합니다. 로그인 직전 수행 : 원도우 로그인을 하기 전에 무선랜인증을 하여 네트워크를 연결할 수 있도록 합니다. 최대 지연 : 최대 지연시간을 설정합니다. 추가 대화 상자 표시 : SSO를 진행하는 동안 추가 대화 상자 표시를 허용합니다. 가상 LAN 사용 : 컴퓨터 및 사용자 인증에 별도의 가상 LAN을 사용합니다.

Windows 업데이트 정책

Windows 업데이트 정책이란?

Genian NAC는 Windows OS 와 Office 제품군에 대한 패치조사 및 미 패치 시스템에 대한 패치수행 기능을 제공합니다. 패치관리를 통하여 프로그램상의 각종 버그와 취약점을 신속하게 패치할 수 있습니다.

Windows 업데이트 정책 생성

1. Windows 업데이트 정책 생성

정책 > 정책 > Windows 업데이트 정책 > 작업선택 > 생성 을 선택합니다.



2. 기본정보 입력

정책을 식별할 ID와 설명을 기입합니다.



3. 자동승인 설정

- 제품

패치를 자동 승인할 windows, office를 선택합니다.



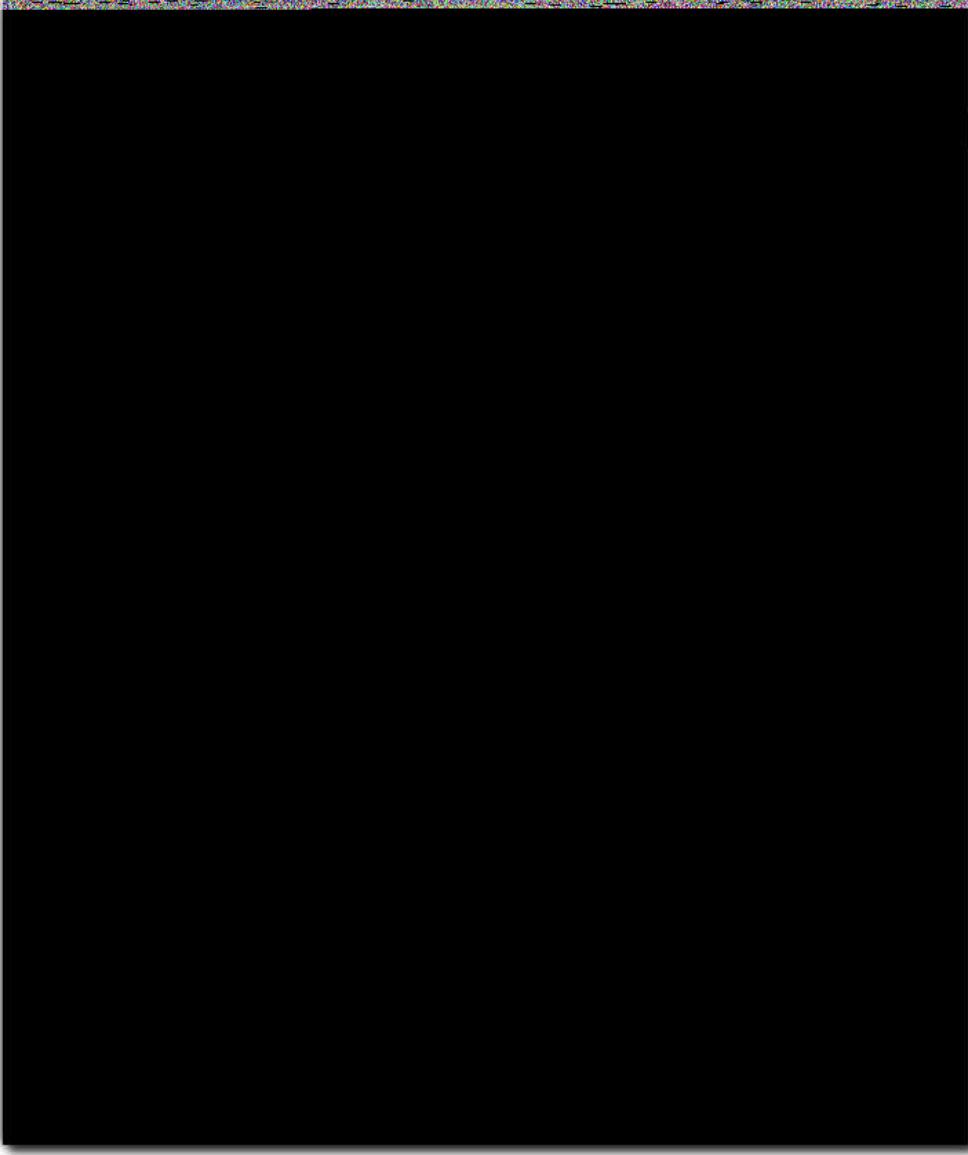
- **분류**

자동 승인할 패치 종류를 선택합니다. 예로 기능 팩을 선택할 시 제품에서 선택한 windows, office의 기능 팩 관련된 패치들이 모두 설치 승인 됩니다.
해당 패치 모음을 적용받는 노드들은 설치 승인된 패치들을 모두 받게 됩니다.



4. Windows 업데이트 정책 수정

Windows 업데이트 정책 수정페이지에서 자동승인 제품군과 패치의 종류를 수정할 수 있으며, 관리자 승인 초기화 작업을 진행할 수 있습니다.
관리자 승인 초기화 버튼은 패치항목별 설정에서 관리자가 따로 승인/미승인 처리한 패치를 Default상태로 변경합니다.



패치항목별 설정

기본정보 탭 옆의 패치항목별 설정 탭에서는 패치명, 릴리즈 날짜로 패치를 검색할 수 있습니다. 또한, 패치 개별로 설치 승인/미승인 상태를 변경하고, 승인 초기화 작업을 진행할 수 있습니다.



Windows 업데이트 정책 삭제

관리자는 필요없는 Windows 업데이트 정책을 삭제할 수 있습니다.

패치삭제 진행과정은 [항목 삭제](#)를 참조해 주십시오.



Windows 업데이트 정책을 삭제할 시 해당 Windows 업데이트 정책을 복구할 수 없습니다.

패치항목 일괄설정

관리자는 여러개의 Windows 업데이트 정책에 원하는 개별 패치에 대하여 설치를 승인/미승인하거나 초기화할 수 있습니다.

1. 일괄설정

원하는 Windows 업데이트 정책 항목의 체크박스에 체크하고,
정책 > 정책 > Windows 업데이트 정책 > 작업선택 > 패치항목 일괄설정 을 선택합니다.



2. 설치/설치안함/초기화

원하는 패치를 선택한 후, 설치/설치안함/초기화 중 원하는 설치 모드를 선택하고 실행버튼을 누릅니다.
설치 모드를 선택 시 선택한 패치는 설치승인으로 설정되며, 설치안함 모드를 선택 시 선택한 패치는 설치미승인으로 설정됩니다.
초기화 모드는 선택한 패치의 설치승인상태를 Default 상태로 초기화합니다.



장치제어 정책

장치제어 정책이란?

장치제어 정책은 복제가 쉬운 디지털 정보의 특성을 악용하여 개인이 가지고 다니는 장치(CD, USB 등)를 통하여 발생할 수 있는 기밀정보의 유출 또한, 네트워크가 연결된 곳이라면 순식간에 퍼지는 악성코드와 바이러스에 감염된 장치를 무분별하게 사용하는 사용자의 장치를 제어하여 장치로 인해 일어날 수 있는 보안 위협 상황들을 미연에 방지할 수 있습니다.

장치제어 정책 추가

관리자는 미리 생성되어진 장치그룹을 이용하여 장치를 허용 또는 제어할 수 있습니다.

1. 장치제어 정책 추가

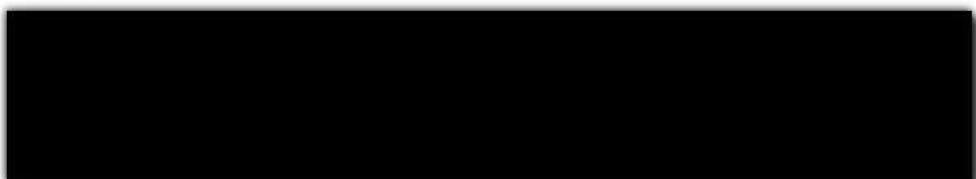
정책 > 정책 > 장치제어 정책 > 작업선택 > 추가 를 선택합니다.



2. 기본정보 입력

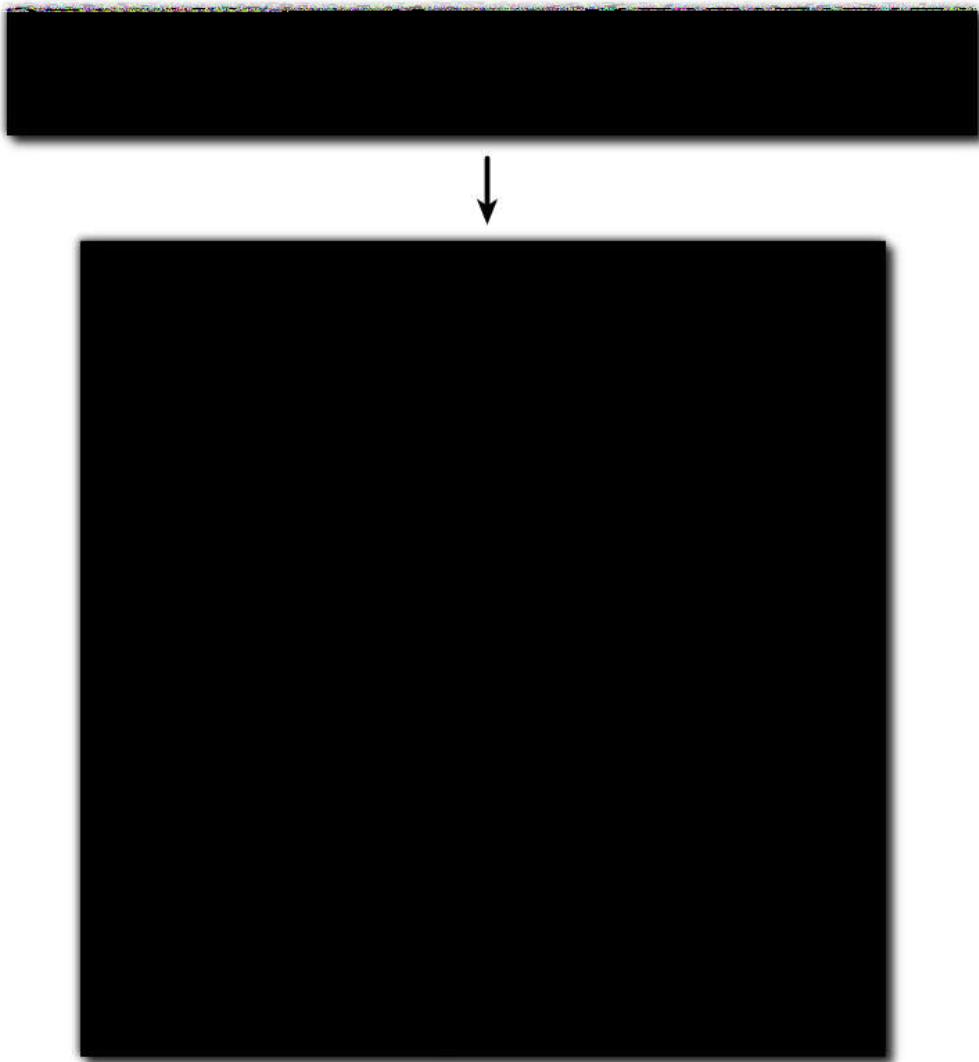
장치제어 정책을 식별할 ID와 설명, 사용유무를 선택합니다.

사용유무의 사용할 옵션 선택 시 정책을 생성하면서 사용항목의 체크 박스에 체크가 되어 생성됩니다.
적용은되지 않으며 적용하려면 반드시 변경정책적용 아이콘을 눌러주어야 합니다.



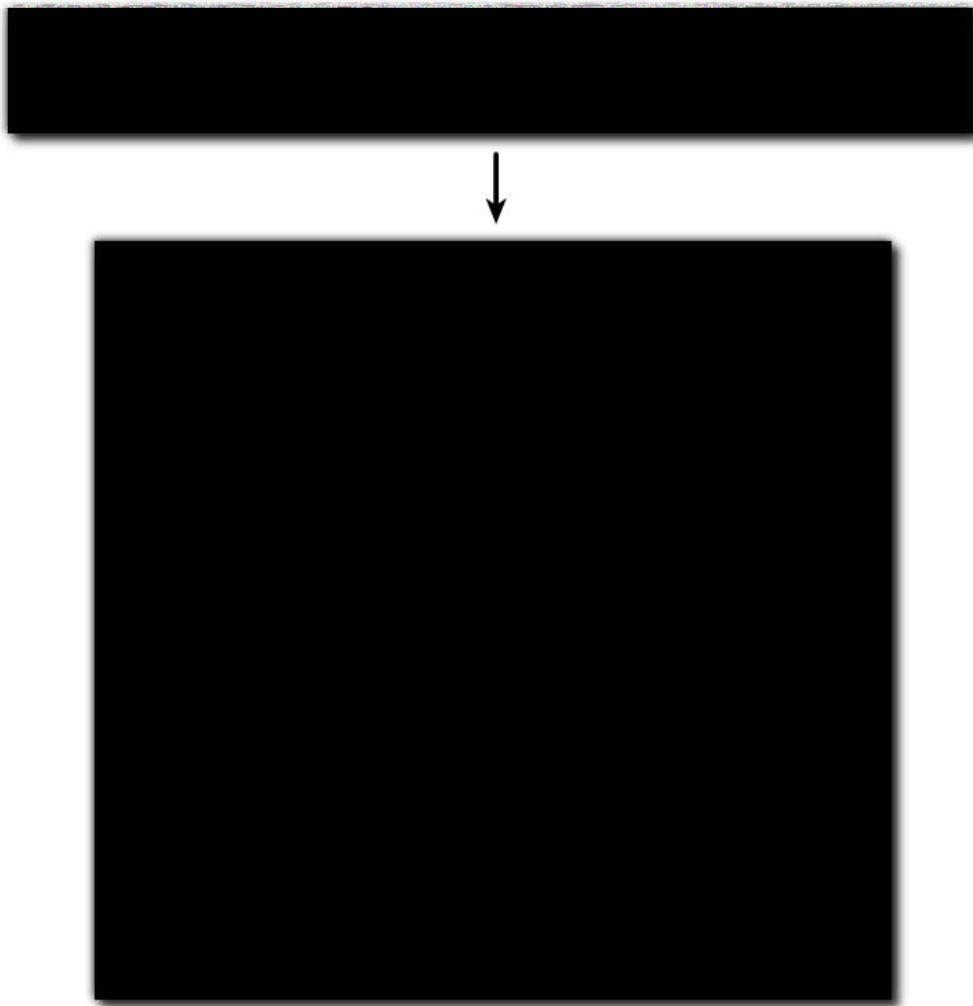
3. 노드그룹 선택

해당 장치제어 정책을 적용할 노드그룹을 할당합니다. 정책그룹과 상태그룹 둘 다 할당 가능합니다.



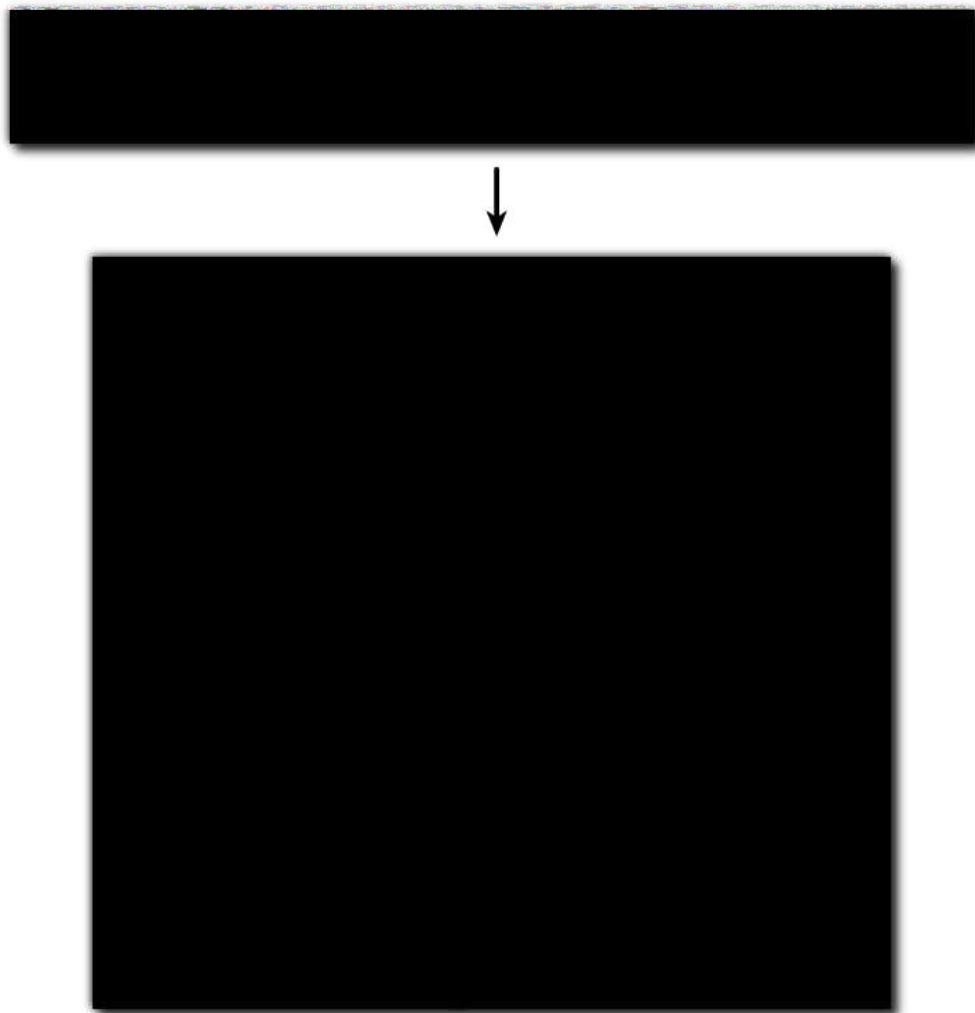
4. 차단장치 선택

차단할 장치 그룹을 선택 합니다. 장치 그룹 생성은 [장치그룹](#)을 참조하기 바랍니다.



5. 차단예외장치 선택

허용할 장치그룹을 할당 후 하단의 추가 버튼을 클릭합니다.



장치제어 정책 삭제

관리자는 필요없는 장치제어 정책을 삭제할 수 있습니다.

장치제어 정책 삭제 진행과정은 [항목 삭제](#)를 참조해 주십시오.

장치그룹

장치그룹이란?

장치그룹은 USB 등의 사용자 장치들을 Genian NAC에서 관리할 수 있도록 장치의 정보들을 미리 정의해 놓은 그룹입니다.

장치그룹 생성과 할당

관리자는 장치관리자에서 얻은 정보들을 바탕으로 장치그룹을 정의할 수 있습니다.

1. 장치그룹 생성

정책 > 정책 > 장치제어 정책 > 장치그룹 > 작업선택 > 생성 을 선택합니다.



2. 기본정보 입력

장치그룹을 식별할 ID와 설명을 입력합니다.



3. 조건설정

장치를 그룹에 포함시키기 위해 장치를 식별할 수 있는 정보들을 입력합니다.



위 그림에서 기입 내용에 대한 설명은 아래 표와 같습니다.

항 목	설 명
클래스명	장치관리자에서 확인할 수 있으며, 해당 장치가 어떤 클래스에 속하는지를 나타냅니다.(필수기입항목)
장치명	해당 장치의 정확한 이름을 장치관리자에서 확인하여 기입해야 합니다.(필수기입항목)
장치설명	해당 장치에 대한 설명을 기입합니다.
이동장치 속성	설정안함, 예, 아니오 중 선택할 수 있습니다.
USB제조사	USB의 제조사를 기입합니다.
USB모델	USB의 모델명을 기입합니다.
USB시리얼	USB의 시리얼을 기입합니다.

4. 장치명 확인

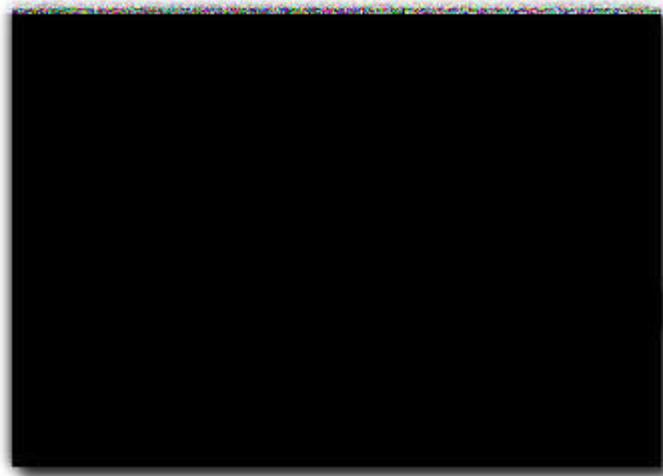
- 장치를 식별할 때 쓰이는 클래스명, 장치명은 장치관리자에서 확인할 수 있습니다.
 - 클래스명, 장치명



- USB 제조사, USB 모델, USB 시리얼은 USB Device Tree Viewer.exe 프로그램에서 확인할 수 있습니다.
 USB Device Tree Viewer 다운로드 URL : <http://www.uwe-sieber.de/usbtreeview>
 - USB 제조사, USB 모델, USB 시리얼



장치제어는 장치관리자에서 사용이나, 사용안함을 설정할 수 있는 장치만 제어가 가능합니다.



장치 그룹 삭제

관리자는 필요없는 장치 그룹을 삭제할 수 있습니다.

장치 그룹 삭제 진행과정은 [항목 삭제 페이지](#)를 참조 바랍니다.

컴플라이언스정책

컴플라이언스정책이란?

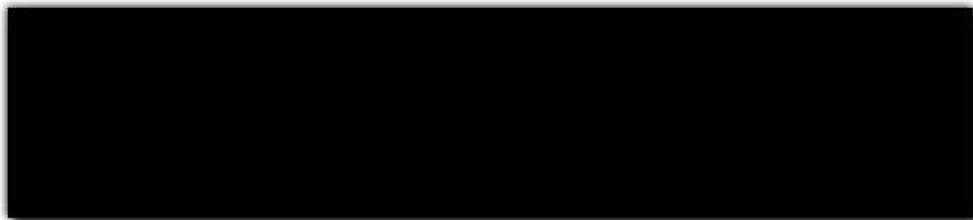
컴플라이언스정책이란 다수의 노드그룹을 설정하여 노드가 설정한 노드그룹에 포함되었는지 O, X로 식별할 수 있는 정책입니다.
아래 그림은 컴플라이언스정책 생성 후 관리 > 노드 > 현황 & 필터 > 컴플라이언스정책에서 확인할 수 있습니다.



컴플라이언스정책 생성

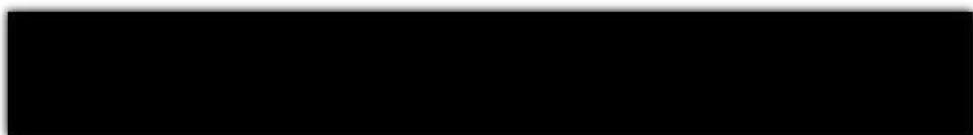
1. 컴플라이언스정책 생성

정책>정책>컴플라이언스정책>작업선택>생성 버튼 클릭하여 컴플라이언스정책 생성 페이지로 접속합니다.



2. 기본정보 설정

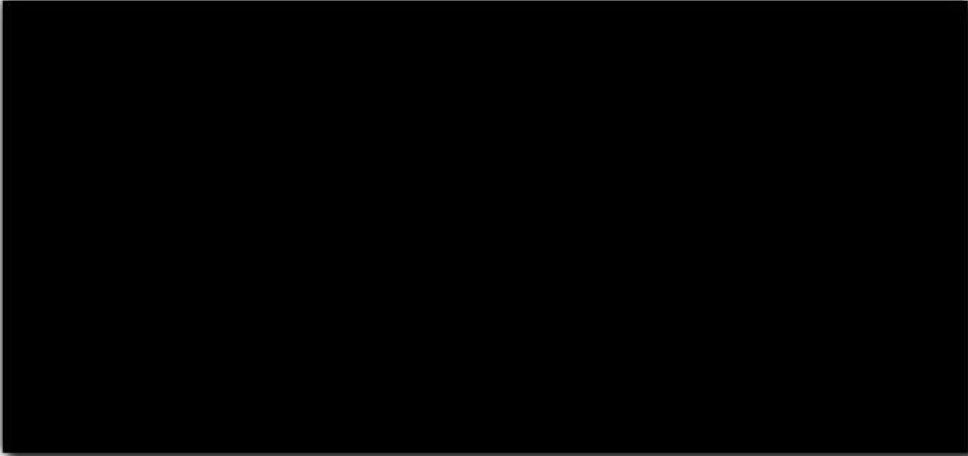
ID, 설명을 입력합니다.



이름	내용
ID	컴플라이언스정책을 식별할 이름을 입력합니다.
설명	해당 정책에 대한 설명을 입력합니다.

3. 조건설정

조건 설정 후 추가 버튼을 클릭하고, 생성 버튼을 클릭하여 컴플라이언스 정책 생성을 완료합니다.



항목	옵션	내용
항목	노드그룹	설정할 그룹을 설정합니다.
조건	속하면	설정 항목에서 설정한 그룹에 속하면 만족으로 표시합니다.
	속하지 않으면	설정 항목에 설정한 그룹에 속하지 않으면 만족으로 표시합니다.
설정	노드그룹	생성되어 있는 정책그룹, 노드그룹을 선택합니다.
설정설명		해당 설정에 대한 설명을 입력합니다.
약어		설정한 노드그룹을 식별할 약어를 입력합니다. 설정 시 노드그룹의 이름이 약어로 출력됩니다.

4. 확인

관리 > 노드 > 필터 뷰 > 컴플라이언스 정책에서 생성된 컴플라이언스 정책명을 클릭하여 내용을 확인할 수 있습니다.



항목	설명
IP	등록된 모든 노드의 IP를 나타냅니다.
MAC	등록된 모든 노드의 MAC을 나타냅니다.
사용자	사용자 인증을 받았을 시 인증된 사용자 ID를 나타냅니다.
만족현황	만족한 조건 수와 최대 조건 수를 나타냅니다.
조건	설정한 조건명이 출력되며, 설정한 조건을 만족하였을 경우 "O" 만족하지 않았을 경우 "X" 가 출력됩니다.

그룹

그룹

관리자는 그룹 기능을 통해서 단말의 장치별, 사용자의 상태별, 노드의 특정한 상태별로 그룹을 생성 할 수 있습니다. 정책 생성시, 정책을 적용받을 그룹을 설정하여 해당 그룹만 정책을 적용할 수 있도록 합니다. 기본적으로 그룹은 노드그룹, 무선랜그룹, 사용자그룹, 장치그룹이 있습니다.

- 노드

노드 그룹은 상태그룹과 정책 그룹이 있으며 정책 받을 대상을 생성 되어 있는 노드 그룹에서 할당하여 노드 그룹에 포함된 노드들에게 정책을 적용할 수 있습니다.



- 무선랜

무선랜 그룹을 이용하여 해당 그룹에 속한 무선랜에 대해 정책을 적용할 수 있습니다.



- 사용자

사용자 그룹을 이용하여 사용자 그룹에 속한 사용자에 대해 정책을 적용할 수 있습니다.



- 장치

장치 그룹을 이용하여 장치 그룹에 속한 장치에 대하여 장치 제어를 할 수 있습니다.



노드

노드그룹이란

노드그룹이란 항목, 조건, 설정값으로 이루어진 조건과 연산을 통해 설정된 노드의 그룹입니다.
관리자에 의해 생성된 그룹은 정책을 받는 주체이며, 정책에 있어서 가장 중요한 요소입니다.
따라서, 관리자는 정책 수립시 제일 먼저 생각해야 할 부분이며, 명확한 조건과 계획을 세워 그룹을 나누어야 합니다.
정책에 할당된 노드그룹은 다른 정책에 할당할 수 없습니다.

정책그룹

정책그룹은 유동성이 적은 조건들로 이루어져있는 그룹입니다.

정책그룹으로 생성 및 설정할 수 있는 항목은 다음과 같습니다.

항 목
IPv6 주소
IP 주소
MAC 주소
MAC+IP 주소
시간
노드타입
센서
등록일자
IP 관리
에이전트
인증 사용자
태그
정책그룹
장비 소유자

상태그룹

상태그룹은 동적인 조건들을 많이 포함하는 다양한 조건들로 구성되어 있습니다.

상태그룹으로 생성 및 설정할 수 있는 항목은 다음과 같습니다.

기본 항목	정책 항목	센서정보 항목	에이전트 정보 항목	장비정보	추가설정 정보 항목
IP 주소	노드정책	센서	에이전트 상태	장비명	GPI 점수
MAC 주소	노드그룹	플랫폼	시스템	장비설명	GPI 검사결과
MAC+IP 주소	제어 정책	노드타입	운영체제 업데이트	제조일	
시간	인증 사용자	열린포트	에이전트 액션	구입처	
등록일자	태그	서비스	소프트웨어	내용연수 시작일	
NAT	IP 관리	업 / 다운상태	가동시간	내용연수 만료일	
연결포트	호스트명 제한	호스트 / 도메인 명	백신정보	일련번호	
이름 / 설명		트래픽	네트워크	구입가격	
접속AP		운영체제유형	계정 비밀번호 검증	책임자	
장비 내 무선랜			WMI 정보 수집	책임부서	
위험감지			USB 장치 정보	메모	
장비 소유자			시스템사용자계정		

서약동의					
IPv6 주소					

정책 / 상태그룹의 생성

여러가지 조건으로 정책 / 상태그룹을 생성 할 수 있습니다.

- 노드그룹 트리 뷰에서 새로운 정책/ 상태그룹을 생성하기 위해 그룹 생성을 선택합니다.



- 노드 그룹 기본 설정

ID, 설명, CWP메시지, 적용모드, 노드관리 기본뷰등을 기본정보에 설정 합니다.



항목	내용
카테고리	카테고리를 선택합니다. 카테고리는 관리 > 노드의 트리뷰와 현황&필터뷰에서 확인할 수 있습니다.
ID	그룹을 식별할 수 있는 ID를 입력 합니다.
설명	그룹이 어떤 기능을 하는 지에 대한 설명을 입력 합니다.
CWP메시지	해당 그룹에 포함되어 있는 노드는 CWP 페이지에 접속할 시 입력한 문구가 나타납니다.
적용 모드	사용함, 사용 안함 중 사용함을 선택하여 생성 후 바로 사용할 수 있고, 사용 안함을 선택하여 생성하여도 그룹을 사용하지 않을 수 있습니다.
감사로그	on off가 있으며 on일 경우 해당 노드 그룹의 변경사항들에 대해 로그를 기록하고 off일 경우 해당 노드그룹의 변경사항들에 대해 로그를 기록하지 않습니다.
노드관리 기본뷰	관리 > 노드 > 현황&필터 > 노드그룹 에 그룹 선택 시 그룹에 설정된 노드관리 뷰로 보여집니다. 노드관리 뷰는 노드에서 관리 뷰를 참고바랍니다.
해제유보	상태그룹에만 있는 옵션이며, 노드그룹에 포함되어 있던 노드가 상태변경에 따라 노드그룹에서 해제될 경우 설정한 기간동안 해제되는것을 보류합니다.

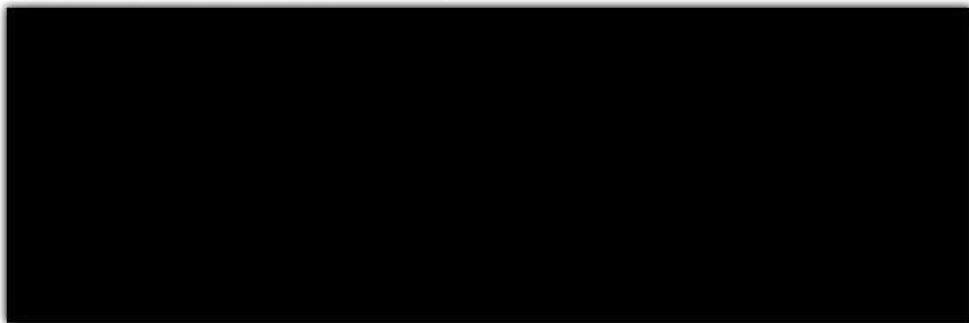
카테고리 생성

노드그룹 생성 시 카테고리를 지정할 수 있으며 다양한 노드그룹을 카테고리로 분류하여 관리할 수 있습니다.

- 정책 > 그룹 > 노드 > 작업선택에서 카테고리 생성을 클릭합니다.



- 상위 카테고리, 이름을 설정 후 생성 버튼을 클릭합니다. 상위 카테고리 선택 시 하위 카테고리로 생성됩니다.



- 관리 > 노드 > 트리뷰 > 그룹에서 생성된 카테고리를 확인할 수 있습니다. 할당된 노드그룹이 없는 카테고리는 트리뷰 옵션인 트리편집이 ON되어야 확인할 수 있습니다.



대상노드리스트 확인

해당 그룹에 속해있는 노드들을 확인 할 수 있습니다.

- 만들어진 그룹ID를 선택 후, 대상 노드 리스트를 선택하면 해당 그룹에 속해있는 노드들의 목록이 보입니다.



노드 그룹 삭제

관리자는 필요없는 노드 그룹을 삭제할 수 있습니다.

노드 그룹 삭제 진행과정은 [항목 삭제](#)를 참조 바랍니다.

카테고리 삭제

관리자는 필요없는 카테고리를 삭제할 수 있습니다.

- 관리 > 노드 > 트리뷰 > 그룹에서 트리편집 아이콘을 클릭합니다.



- 삭제할 카테고리에 우클릭 후 삭제 버튼을 클릭합니다.



무선랜

무선랜그룹이란?

Genian NAC는 에이전트와 무선센서를 통하여 무선랜정보를 수집합니다.
관리자는 다양한 아이템과 조건을 통하여 무선랜 그룹을 만들고, 아이템과 조건들을 바탕으로 수집한 무선랜정보를 비교하여 무선랜들을 그룹속에 포함 시킵니다.

무선랜그룹 생성

관리자는 많은 아이템, 조건들을 통해 무선랜그룹을 생성할 수 있습니다.

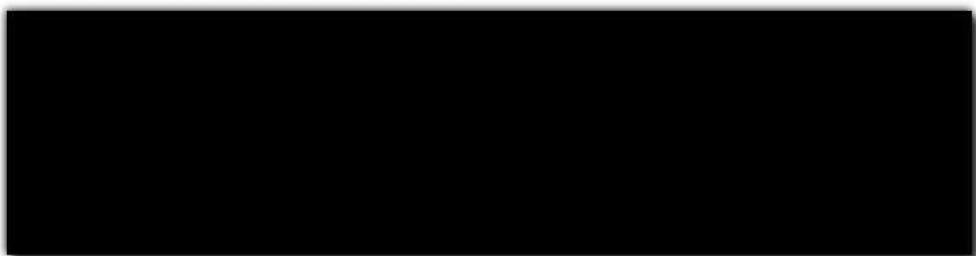
1. 무선랜 등록

정책 > 정책 > 그룹 > 무선랜 > 작업선택 > 생성 을 선택합니다.



2. 기본정보입력

무선랜그룹을 식별할 ID와 설명, 적용모드, 조건연산을 입력합니다.



항목	내용
ID	그룹을 식별할 수 있는 ID를 입력 합니다.
설명	그룹이 어떤 기능을 하는 지에 대한 설명을 입력 합니다.
적용 모드	사용함, 사용 안함 중 사용함을 선택하여 생성 후 바로 사용할 수 있고, 사용 안함을 선택하여 생성하여도 그룹을 사용하지 않을 수 있습니다.
감사로그	on off가 있으며 on일 경우 해당 노드 그룹의 변경사항들에 대해 로그를 기록하고 off일 경우 해당 노드그룹의 변경사항들에 대해 로그를 기록하지 않습니다.
조건 연산	AND와 OR이 있으며 AND일 경우 모든 조건에 충족해야 그룹에 속하고 OR일 경우 여러 조건 중 한 가지만 충족하여도 그룹에 속합니다.

3. 조건설정

그룹을 나눌 기준이되는 아이템과 조건을 설정하고 등록버튼을 눌러 신규 무선랜을 등록합니다.



아이템과 조건의 상세내용은 아래표와 같습니다.

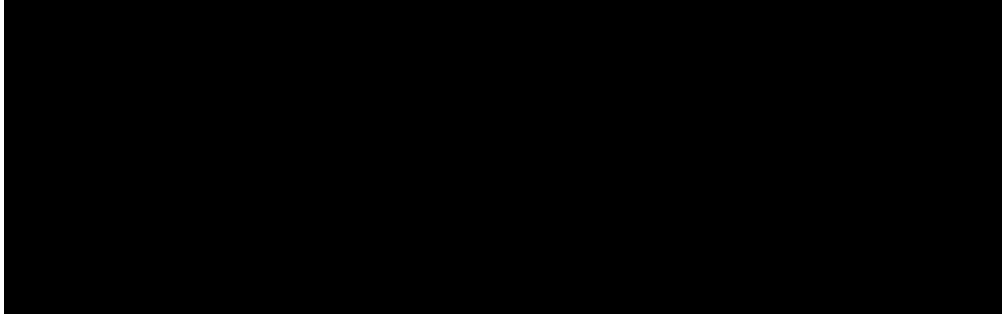
아 이 템	조 건
SSID	같으면, 다르면 문자열 포함하면, 포함하지 않으면 정규식 매칭
MAC 주소	MAC이 같으면, 다르면 알려진 MAC OUI 가 같으면, 다르면 Vendor 명이 해당 문자열 포함하면 MAC주소 정규식매칭
MAC+SSID	와 같으면
상태 및 속성	내부망 Soft AP Ad hoc
보안설정	프로토콜이 같으면, 다르면 인증방법이 같으면, 다르면
802.11 프로토콜	802.11 프로토 콜이 같으면, 다르면
인가상태	동일장비에 차단된 노드가 존재하면, 존재하지 않으면
태그	태그가 존재하면, 존재하지 않으면
무선랜 그룹	무선랜 그룹에 속하면, 속하지 않으면

무선랜 그룹의 할당

- 만들어진 무선랜 그룹을 대상으로 정책을 내리고 싶다면, 무선랜 그룹을 제어정책에 포함시켜야 합니다. 하지만 제어정책에서 사용할 수 있는 그룹은 정책그룹과 상태그룹 두 그룹뿐입니다.

따라서, 만들어진 무선랜그룹을 상태그룹에 포함시켜야 합니다.

무선랜그룹을 대상으로한 정책세우는 순서는 아래 그림과 같습니다.



- 위 그림을 보면 예시 정책을 하나 세워 보겠습니다.

정책의 내용은 'SSID가 geninetworks 인 무선랜 그룹에게 DNS권한만 준다.' 입니다.

1. 무선랜 그룹 생성

아이템 = SSID, 조건 = 같으면, 설정 = geninetworks 로 조건을 설정하여 무선랜그룹을 만듭니다.



위 그림 사용항목에 체크가 되어 있어야만 뒤 과정에서 무선랜 그룹을 포함시킬 수 있습니다.
체크가 되어있지 않다면 상태그룹을 만들때 무선랜그룹을 할당할 수 없습니다.

2. 무선랜그룹을 포함한 상태그룹 생성

상태그룹에 무선랜그룹을 포함시키는 과정입니다.



3. 할당과 권한부여

무선랜그룹 할당과 권한을 부여하는 과정은 제어정책을 참조해 주십시오.

무선랜 그룹 삭제

관리자는 필요없는 무선랜 그룹을 삭제할 수 있습니다.

무선랜 그룹 삭제 진행과정은 [항목 삭제](#)를 참조 바랍니다.

사용자

사용자 그룹이란?

사용자들을 구분하는 조건들을 이용하여, 그룹을 생성하기 위한 기준을 세우는 것입니다.
사용자들은 부서명, 직급, 회사명 등이 있습니다.

사용자그룹 생성

관리자는 조건을 이용하여 사용자그룹을 생성할 수 있습니다.

1. 사용자그룹 생성

정책 > 그룹 > 사용자 > 작업선택 > 생성 을 선택합니다.



2. 기본정보 입력

그룹을 식별할 ID와 설명, 적용모드와 조건연산을 설정합니다.



3. 조건설정

사용자들을 구분할 조건을 선택하고 등록 버튼을 누릅니다.



그룹을 나눌 아이템과 조건의 상세내용은 아래 표와 같습니다.

아이템	조건	아이템	조건
사용자 ID	같으면, 다르면	비밀번호	설정유무(사용자의 비밀번호가 설정되었는지의 여부)
	문자열 포함하면, 포함하지 않으면		비밀번호 변경 강제(비밀번호 강제가 설정되었는지의 여부)
	문자열로 시작하면, 시작하지 않으면	관리자권한	같으면, 다르면
	정규식 매칭		설정유무
부서	같으면, 다르면	전화번호	설정유무
	속하면	휴대전화 번호	설정유무
	문자열 같으면, 다르면	이메일 주소	설정유무

	설정유무(부서명이 설정되었는지의 여부)	인증상태	같으면(인증됨, 인증되지않음)
	정규식 매칭	마지막 인증시각	특정일자 이전, 이후에 인증된
직급	같으면, 다르면		특정시간 이내, 이후에 인증된
	문자열 같으면, 다르면	동기화 여부	같으면, 다르면(로컬생성, 동기화사용자)
	설정유무(직급이 설정되었는지의 여부)	태그	존재하면, 존재하지 않으면
	정규식 매칭	장비인증제한	설정유무
회사명	같으면, 다르면	계정중지사유	같으면, 다르면
	문자열 포함하면, 포함하지 않으면		
	정규식 매칭		
	설정유무(회사명이 설정되었는지의 여부)		
계정용도	같으면, 다르면(임시계정, 일반계정)		
계정상태	같으면, 다르면(정상, 사용중지)		
사용자 그룹	속하면, 속하지 않으면		
설명	같으면, 다르면		
	문자열 포함하면, 포함하지 않으면		
	설정유무(설명이 설정되었는지의 여부)		
	정규식매칭		
IP 인증제한	설정유무(IP인증이 설정되었는지의 여부)		
MAC 인증제한	설정유무(MAC인증이 설정되었는지의 여부)		
만료시각	설정유무(사용자의 만료시각이 설정되었는지의 여부)		

사용자 그룹의 할당

사용자 그룹은 노드그룹의 노드그룹에 포함시켜 사용하여야 합니다.
정책그룹에 사용자 그룹을 포함시켜 정책을 수립하여 사용자 그룹에 포함된 사용자들을 제어할 수 있습니다.
사용자 그룹 할당 방법은 무선랜 그룹 할당과 유사하므로 [무선랜](#)을 참고하시면 더욱 쉽게 할 수 있습니다.

- 사용자 그룹을 포함한 정책그룹 생성

노드그룹에 생성되어 있는 사용자그룹을 포함시킬 수 있습니다. 사용자 그룹에 속해 있는 사용자ID로 인증한 노드는 해당 그룹에 포함 됩니다.



사용자그룹 삭제

관리자는 사용하지 않는 사용자그룹을 삭제할 수 있습니다.

삭제 방법은 [항목 삭제](#)를 참조하시기 바랍니다.

객체

객체

네트워크, 서비스, 시간 객체를 관리자가 설정하여 설정한 객체를 이용하여 다양한 권한을 생성할 수 있습니다. 차후, 제어 정책에 권한을 할당하여 노드들을 효율적으로 제어 할 수 있습니다.

- 권한

네트워크, 서비스, 시간 세 가지의 객체를 이용하여 권한을 설정합니다.



- 네트워크

네트워크 객체를 이용하여 네트워크 범위를 설정합니다.



- 서비스

서비스 객체를 이용하여 다양한 네트워크 차단을 설정합니다.



- 시간

시간 객체를 이용하여 시간에 대한 범위를 설정합니다.



권한

권한이란?

권한이란 제어정책에서 정책적용 대상이 되는 노드그룹과 함께 반드시 필요한 부분으로, 노드그룹이 정책을 받을 대상을 정의한 것이라면, 권한은 그룹들이 가질 네트워크의 사용 가능한 범위를 객체를 이용하여 정의한 것입니다.

권한의 생성과 할당

관리자는 네트워크, 서비스, 시간객체를 이용하여 권한을 생성할 수 있습니다.

1. 권한의 생성

정책 > 정책 > 제어정책 > 권한 > 작업선택 > 생성버튼을 클릭합니다.



2. 권한 설정

권한을 식별할 ID와 권한에 대한 설명을 입력하고, 미리 생성되어있는 객체를 선택합니다.

속하지 않는 옵션에 체크하게되면 해당 객체를 제외한 나머지를 가르키게 됩니다.

예를들어, 서비스 객체를 PERM-DNS로 선택 후, 속하지 않는 체크 박스를 체크하게되면 PERM-DNS 서비스를 제외한 나머지 서비스 권한이 할당됩니다.

각 객체에 있는 +버튼을 이용하면 해당 객체를 생성할 수 있으며, +버튼 우측에 있는 펜모양 버튼을 클릭 시 선택된 객체의 상세화면을 확인할 수 있습니다.

아래의 그림에 설정되어 있는 권한은 모든 IP대역(네트워크 객체)에게 언제든지(시간 객체) 네트워크(서비스 객체)를 사용할 수 있게 한다는 권한을 뜻합니다.
설정값을 모두 입력한 후 생성버튼을 누릅니다.



3. 권한의 할당

만들어진 권한은 제어정책에 할당하여 사용하여야 합니다.

할당방법은 제어정책의 제어정책생성 - 5번 항목을 참조해 주십시오.

권한의 삭제

관리자는 더 이상 필요가 없는 권한을 삭제할 수 있습니다.

권한의 삭제 방법은 [항목 삭제](#)를 참조하여 주십시오.

네트워크

네트워크 객체란?

다른정책에 의해 사용되어질 네트워크 범위를 정의하며 노드그룹, 권한 등에서 사용됩니다.
네트워크의 범위는 IP를 사용하여 정의하며, 방식에는 Netmask를 이용하는 방식과 Range를 이용하는 방식이 있습니다.

네트워크 객체의 생성

- 네트워크 객체 생성
정책 > 정책 > 객체 > 네트워크 > 작업선택 > 생성 을 선택합니다.



2. 기본설정

그룹ID, 설명을 기입합니다.



이름	내용
ID	객체를 식별할 ID를 입력합니다.
설명	해당 그룹에 추가적인 설명이 필요할 경우 입력합니다.

3. 포함그룹

네트워크 객체는 이미 만들어진 네트워크 객체를 포함할 수 있습니다.
단, @NET-ALL은 포함할 수 없습니다.



4. 네트워크 IP

IP를 이용하여 네트워크 범위를 나눕니다. 범위를 나누는 방식에는 Netmask를 이용하는 방식과 Range를 이용하는 방식이 있습니다.

- IP/Netmask 방식

IP를 입력 후 키보드의 Tab키를 입력할 시 해당 IP에 맞는 Netmask가 자동으로 설정 됩니다.
설정한 IP를 사용하고 있는 노드는 객체에 포함 됩니다.



- Range 방식

IP의 범위를 입력할 시 해당 IP 범위에 있는 IP를 사용하는 노드들이 객체에 포함 됩니다.



- FQDN 방식

동적으로 변경되는 IP 정보를 확인하기 위해 도메인 정보를 입력하여 해당 도메인의 IP정보를 네트워크 객체로 활용 합니다.
주로 유동적인 목적지 주소에 대한 권한을 설정하기 위해 사용 됩니다.



네트워크 객체 삭제

관리자는 필요없는 네트워크 객체를 삭제할 수 있습니다.

네트워크 개체 삭제 진행과정은 [항목 삭제](#)를 참조 바랍니다.

서비스

서비스객체란?

서비스객체는 노드들에 권한 할당시 허가 또는 금지할 서비스(TCP, DNS 등의 네트워크 서비스)를 정의하기 위해 생성하는 객체입니다.

서비스그룹 생성

관리자는 권한을 생성하는데 필요한 서비스그룹을 생성할 수 있습니다.

1. 서비스그룹 생성

정책 > 객체 > 서비스 > 작업선택 > 생성 을 선택합니다.



2. 기본설정

서비스객체를 식별할 ID와 설명을 입력합니다.



이름	내용
ID	객체를 식별할 ID를 입력합니다.
설명	해당 그룹에 추가적인 설명이 필요할 경우 입력합니다.

3. 포함그룹

서비스객체는 미리 정의되어있는 다른 서비스객체를 포함할 수 있습니다.



4. 서비스 포트

서비스를 구분지어주는 포트번호를 입력합니다.

FTP 서비스를 객체로 등록하고 싶은경우,
프로토콜에는 TCP, 연산자는 ==, 포트는 20, 21번을 추가해주고 생성을 누릅니다.



서비스 객체 삭제

관리자는 필요없는 서비스 객체를 삭제할 수 있습니다.

서비스 객체 삭제 진행과정은 항목 [삭제](#)를 참조 바랍니다.

시간

시간객체란?

날짜, 시간대, 요일 등의 시간범위를 정의하며, 정책이나 그룹, 권한에서 사용됩니다.

시간객체의 생성

관리자는 원하는 범위의 날짜, 시간, 요일을 선택하여 시간객체를 생성할 수 있습니다.

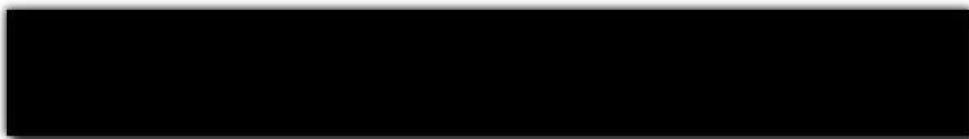
1. 시간객체 생성

정책 > 객체 > 시간 > 작업선택 > 생성 을 선택합니다.



2. 기본설정

시간객체를 식별할 ID와 설명을 입력합니다.



이름	내용
ID	객체를 식별할 ID를 입력합니다.
설명	해당 그룹에 추가적인 설명이 필요할 경우 입력합니다.

3. 포함그룹

시간객체는 미리 정의되어있는 다른 시간객체를 포함할 수 있습니다.



4. 시간 객체

범위로 지정하고 싶은 날짜와 시간대, 요일을 선택합니다.



시간 객체 삭제

관리자는 필요없는 시간 객체를 삭제할 수 있습니다.

시간 객체 삭제 진행과정은 [항목 삭제](#)를 참조 바랍니다.

설정

설정

관리자는 설정탭을 통하여 속성, CWP 페이지, 환경설정을 할 수 있습니다.

- 속성관리 : 용도관리를 이용하여 IP신청서, 사용자신청서를 관리하고 태그 및 노드타입을 추가할 수 있는 탭입니다.
 - 접속인증페이지(CWP) : CWP를 관리할 수 있고 사용자에게 보여줄 메시지를 관리 할 수 있는 탭입니다.
 - 서비스 : NAC에서 제공하는 별도의 서비스 RADIUS 관련 설정할 수 있는 탭입니다.
 - 사용자인증 : 사용자 계정 및 동기화 관련된 설정을 할 수 있는 탭입니다.
 - 환경설정 : 노드관리, IP관리, 무선랜관리 등의 환경설정을 할 수 있는 탭입니다.
-
- 속성관리
 - 접속인증페이지(CWP)
 - 서비스
 - 사용자인증
 - 환경 설정

속성관리

속성관리

속성관리는 노드타입 관리, 태그 관리, 노드 사용자정의 필드, 장비 사용자정의 필드, 사용자 사용자정의 필드로 구성되어 있습니다.

- 노드타입 관리

관리자는 노드 타입 관리를 이용하여 노드를 식별할 수 있는 아이콘을 생성할 수 있습니다.



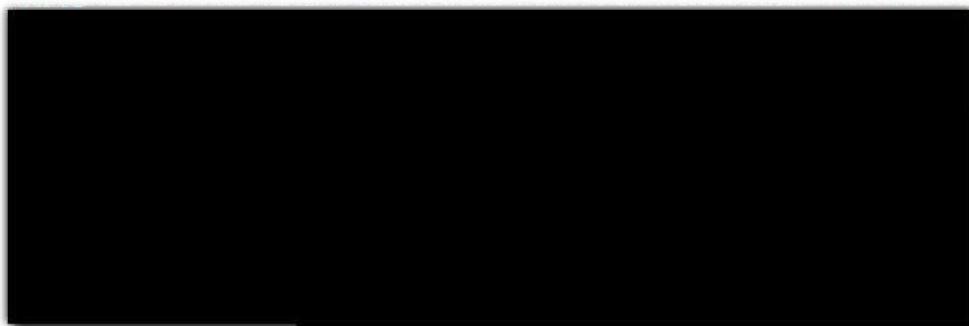
- 태그 관리

태그 관리 기능을 이용하여 관리자가 원하는 태그를 생성하여 사용할 수 있습니다.



- 추가필드관리

추가필드관리를 이용하여 추가으로 필드가 필요할 경우 필드를 생성하여 사용할 수 있습니다.



- 용도관리

사용자, IP 신청할 때 설정하는 용도에 대한 설정을 할 수 있습니다.



노드타입 관리

노드타입 관리란?

노드타입이란 센터, 센서, PC, 네트워킹 장비 등 노드의 종류를 말하며, 각 타입에 따라 구분이 쉽도록 각기 다른 아이콘을 제공합니다. 관리자는 Genian NAC가 제공하는 기본적인 아이콘과 타입에서 추가로 필요한 아이콘과 타입을 새로이 추가할 수 있습니다.

신규 노드타입 등록/삭제

- 신규 노드타입 등록

설정 > 속성관리 > 노드타입 관리 > 작업선택 > 추가 버튼을 선택합니다.



아이콘 등록/관리 버튼을 선택하여 아이콘을 업로드할 수 있습니다.

- 파일선택 버튼을 선택하여 업로드할 아이콘 파일(JPG/GIF)을 선택합니다.
- 업로드 버튼을 선택하여 아이콘 이미지를 업로드한 후 닫기 버튼을 선택합니다.



업로드 시킨 이미지를 선택한 후, 노드타입명을 기입하고 추가버튼을 선택합니다.



- 신규 노드타입 삭제

신규로 추가한 노드타입을 선택한 후 작업선택의 삭제를 이용하여 추가한 노드타입을 삭제합니다.



- 신규 추가한 아이콘 삭제

신규 노드타입을 등록할때 추가하였던 신규 아이콘은 노드타입을 삭제하여도 삭제되지 않습니다.
추가 아이콘을 삭제하려면 설정 > 속성관리 > 노드타입 관리 > 작업선택 > 추가 버튼을 선택하고,
아이콘 등록/관리에서 지우고 싶은 신규 추가 아이콘을 선택한 후, 아이콘 삭제버튼을 선택해 주시기 바랍니다.



태그 관리

태그란?

태그는 관리자가 IP, MAC, 사용자 등에게 붙이는 일종의 꼬리표로써, 태그를 이용하여 더 쉽게 사용자 및 노드를 관리할 수 있습니다. 태그를 이용하여 그룹을 생성하거나, 복잡한 IP, MAC과 같은 식별자 대신, 태그를 이용하여 노드를 식별할 수 있습니다.

태그의 추가

1. 태그추가

설정 > 속성관리 > 태그관리 > 작업선택 > 생성 을 선택합니다.



2. 태그 정보입력

태그의 이름과 설명 기간을 설정하고 추가버튼을 누릅니다.



태그에는 기간을 설정할 수 있습니다. 태그에 기간을 설정하게 되면 설정기간 후에는 자동으로 태그가 해제됩니다. 기간설정의 종류에는 무제한, 기간, 기간+해제시간이 있습니다. 설명은 아래 표와 같습니다.

항목	옵션	내용
이름		태그명을 입력합니다.
설명		태그에 대한 설명을 입력합니다.
색상설정	색상	색상을 선택합니다.
기간설정	무제한	태그가 해제되지 않습니다.
	기간	단위로는 시간과 일이 있으며, 태그가 부여된 시점에서 부터 설정된 시간 경과후 태그가 자동해제 됩니다. (태그 부여시간 12시이고 기간을 5시간으로 설정했을 때, 오후 5시에 태그 자동해제)
	기간+해제시각	일을 설정하고 해제시각을 설정합니다. 태그가 부여된 시점에서 부터 설정된 일만큼 경과후 해제시각에 자동해제됩니다. (1일 15시로 설정하였을 경우, 내일 15시에 태그 자동해제)

관리역할 제한	관리 역할을 지정하여 지정된 관리 역할을 가지고 있는 관리자만 태그를 할당 및 삭제할 수 있고, 지정된 관리 역할 외 다른 관리역할을 가진 관리자는 태그를 할당 및 삭제할 수 없습니다.
------------	---

태그삭제

관리자는 사용하지 않는 태그들을 삭제할 수 있습니다.

태그 삭제방법은 [항목 삭제](#)를 참고하시기 바랍니다.

추가필드관리

노드/장비/사용자/IP신청서 추가필드관리란?

사용자 정의 필드는 기본으로 제공되는 노드/장비/사용자/IP신청서 정보에 관리자가 정의한 필드를 생성하여 기본정보 이외의 정보를 추가로 입력받아 저장할 수 있습니다.

필드는 9개까지 사용할수 있으며, 입력타입에는 텍스트박스, 체크박스, 드롭다운 메뉴, 리스트 박스 외 다양한 타입이 있습니다.

추가필드 생성

관리자가 필요한 노드 사용자정의 필드를 생성할 수 있습니다.

1. 사용자 정의필드 추가

설정 > 속성관리 > 추가필드관리 > 노드, 장비, 사용자, IP신청서 > 작업선택 > 추가 를 선택합니다.



2. 필드 설정

관리자는 사용필드, 필드명, 필드설명, 입력타입 및 입력 타입에 대한 상세기능을 작성 및 선택합니다.



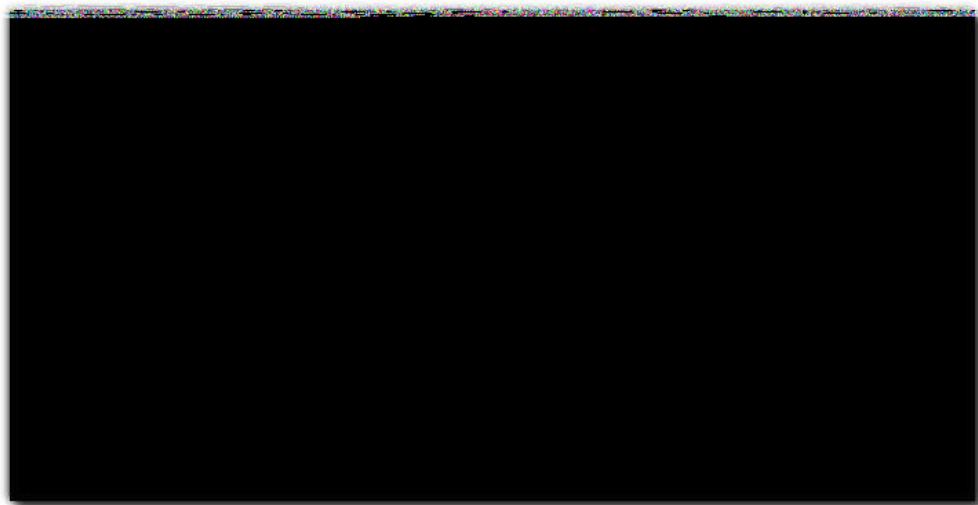
입력타입의 상세설명은 아래 표와 같습니다.

항목	설명(포함된 기능)
문자열입력	사용자가 직접 텍스트 형식으로 입력할 수 있는 텍스트 박스형식으로 필드를 생성합니다.(입력필드 넓이를 설정할 수 있습니다.)
문자열입력(입력길이제한)	사용자가 직접 텍스트 형식으로 입력할 수 있는 텍스트 박스형식으로 필드를 생성합니다, 입력길이제한을 설정 시 해당 필드는 필수로 입력하여야 합니다, 입력하지 않을 시 필드가 추가된 페이지에 있는 설정들을 수정이 할 수 없습니다.(입력필드 넓이, 입력길이제한을 설정할 수 있습니다.)
멀티라인 문자열입력	문자열입력보다 보다 넓은 텍스트 박스형식으로 필드를 생성합니다.(입력필드넓이, 입력필드라인수, 입력길이제한을 설정할 수 있습니다.)

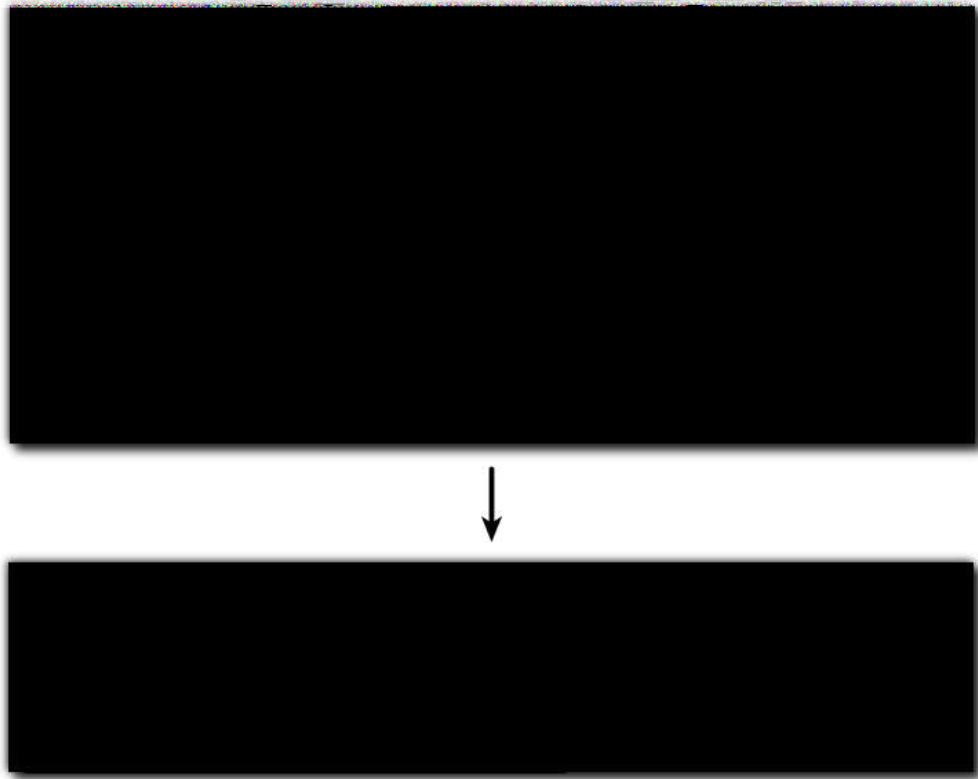
문자열패턴 입력	관리자가 설정한 정규식패턴에 맞게 입력하였는지 체크하는 텍스트 박스형식의 필드를 생성합니다.(입력필드넓이, 패턴, 입력길이제한을 설정할 수 있습니다.)
날짜입력	사용자가 날짜를 입력할 수 있도록 달력 형식으로 필드를 생성합니다.(입력날짜제한, 범위를 설정할 수 있습니다.)
날짜시각입력	사용자가 체크박스에 체크 후 날짜, 시간을 입력할 수 있도록 필드를 생성합니다. (입력날짜제한, 범위를 설정할 수 있습니다.)
IP 입력	사용자가 IP를 입력하였는지 체크하는 텍스트 박스형식의 필드를 생성합니다.(입력필드넓이를 설정할 수 있습니다.)
MAC 입력	사용자가 MAC을 입력하였는지 체크하는 텍스트 박스형식의 필드를 생성합니다.(입력필드넓이를 설정할 수 있습니다.)
읽기 전용	사용자가 입력은 할 수 없고 읽기만 할 수 있는 텍스트 박스형식의 필드를 생성합니다.(입력필드넓이를 설정할 수 있습니다.)
사용자설정목록	관리자가 직접 추가하는 항목과 값을 드롭다운메뉴 형식으로 만들어 필드를 생성합니다.(필수입력항목설정, 항목명, 항목값을 입력합니다.)
사용자설정목록(필수항목)	관리자가 직접 추가하는 항목과 값을 체크박스 형식으로 만들어 필드를 생성합니다, 해당 필드는 필수로 입력하여야 합니다. 입력하지 않을 시 필드가 추가된 페이지에 있는 설정들을 수정을 할 수 없습니다.(출력컬럼수설정, 항목명, 항목값을 입력합니다.)
사용자설정목록(체크박스)	관리자가 직접 추가하는 항목과 값을 체크박스 형식으로 만들어 필드를 생성합니다.(출력컬럼수설정, 항목명, 항목값을 입력합니다.)
시스템목록	시스템에 미리 설정되어있는 항목들을 이용하여 드롭다운메뉴 형식으로 만들어 필드를 생성합니다. (필수입력항목설정, 항목선택의 항목중 하나를 선택합니다.)
시스템목록(필수항목)	시스템에 미리 설정되어있는 항목들을 이용하여 드롭다운메뉴 형식으로 만들어 필드를 생성합니다, 해당 필드는 필수로 입력하여야 합니다, 입력하지 않을 시 필드가 추가된 페이지에 있는 설정들을 수정을 할 수 없습니다. (필수입력항목설정, 항목선택의 항목중 하나를 선택합니다.)
시스템목록(다중선택)	시스템에 미리 설정되어 있는 항목들을 이용하여 리스트 박스 형식으로 만들어 필드를 생성합니다. (항목선택의 항목중 하나를 선택합니다.)
시스템목록(체크박스)	시스템에 미리 설정되어 있는 항목들을 이용하여 체크박스 형식으로 만들어 필드를 생성합니다.(출력컬럼수설정, 항목선택의 항목중 하나를 선택합니다.)
사용자선택기	사용자가 'assign' 버튼을 클릭하여 사용자 이름을 검색하고 선택하는 형식의 필드를 생성합니다.
다중 사용자선택기	사용자를 다중으로 선택할 수 있는 필드를 생성합니다.
노드선택기	사용자가 'assign' 버튼을 클릭하여 IP를 검색하고 선택하는 형식의 필드를 생성합니다.
부서선택기	사용자가 'assign' 버튼을 클릭하여 부서를 검색하여 선택하는 형식의 필드를 생성합니다.(항목선택을 설정할 수 있습니다.)
파일업로드	사용자가 파일을 업로드할 수 있는 필드를 생성합니다.
보안질문 입력	사용자 추가필드에서만 선택할 수 있으며, 별도로 할당하지 않아도 사용자의 추가정보에 추가됩니다. 설정 > 사용자인증 > 사용자인증 > 아이디/비밀번호 찾기 > 보안질문설정 에 보안질문 입력 필드를 설정할 수 있습니다.

3. 생성된 필드 확인

- 노드 추가필드



-
- 장비 추가필드



구분자 생성

1. 구분자 추가

설정 > 속성관리 > 추가필드관리 > 노드, 장비, 사용자, IP신청서 > 작업선택 > 추가 (구분자) 를 선택합니다.



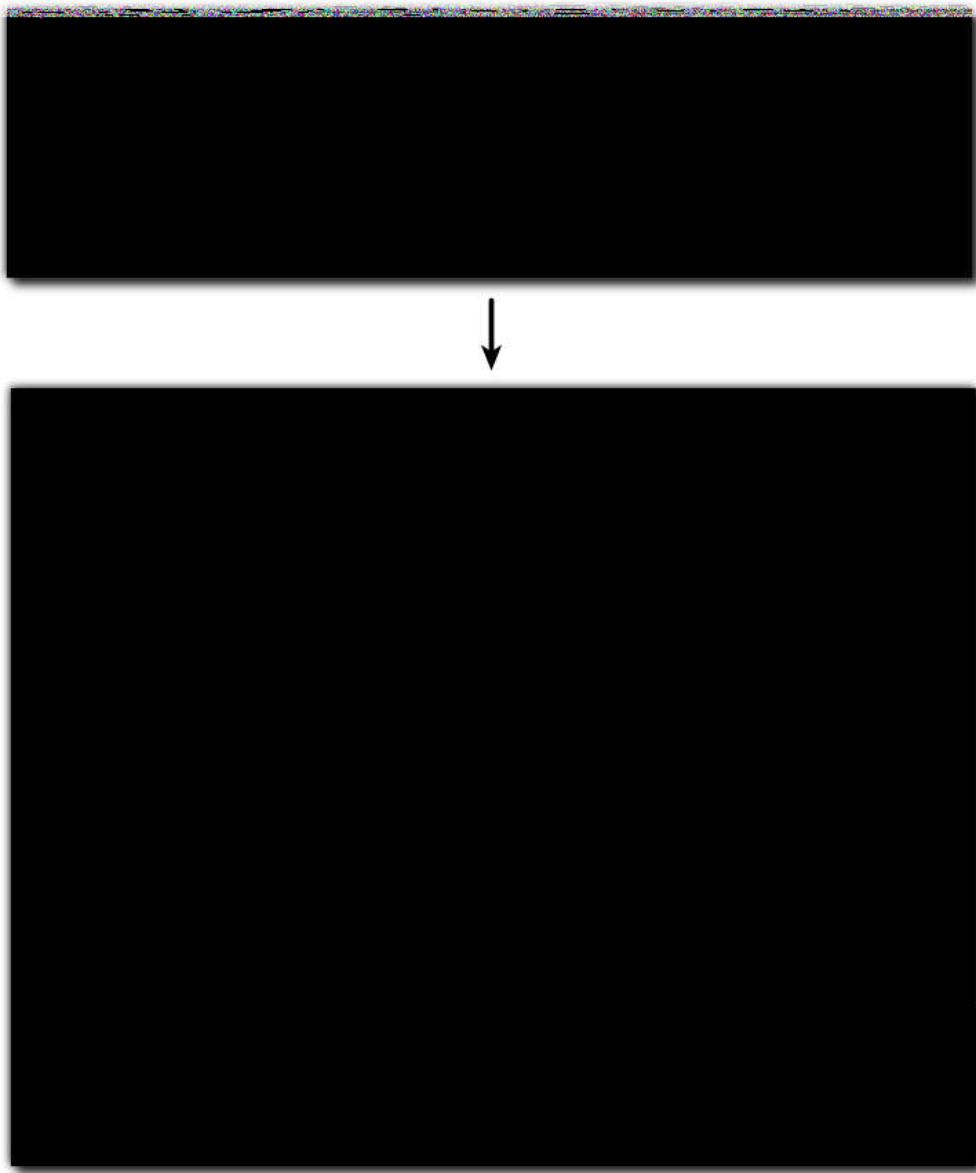
2. 구분자 설정

관리자는 필드명, 출력필드넓이, 필드설명, 순서, 입력타입 작성합니다.



항목	옵션	설명
필드명		구분자 필드를 식별할수 있는 이름을 입력합니다.
출력필드넓이		출력필드 넓이를 입력합니다.
필드설명		필드에 대한 추가적인 설명이 필요할 경우 입력합니다.
순서		필드의 순서를 입력합니다. 최상위 필드는 1입니다.
입력타입	구분선	필드와 필드를 구분하는 구분선을 생성합니다. 구분선은 점선으로 출력됩니다.
	소제목	소제목을 생성합니다. 입력한 필드명과 필드설명이 출력됩니다.

- 생성된 구분자 확인



사용자 정의 필드 삭제

관리자는 필요없는 사용자 정의 필드를 삭제할 수 있습니다.

사용자 정의 필드 삭제 진행과정은 [항목 삭제](#)를 참조 바랍니다.

용도관리

용도관리

용도관리는 사용자 및 IP 용도를 정의하고 수정하는 페이지로써, 설정은 용도관리페이지에서 할 수 있습니다.
용도관리는 사용자 및 IP 신청서를 작성할 때 설정하는 용도에 대한 페이지입니다.

- 사용자용도 : 사용자등록 신청서의 용도를 수정 및 정의할 수 있으며, 이메일 및 신청서 입력필드를 설정할 수 있습니다.
- IP 용도 : IP신규, IP반납, 장비변경, 사용자변경 신청서의 용도를 수정 및 정의 할 수 있으며, 신청서 단계별 승인 및 URL호출 등의 기능을 설정할 수 있습니다.
- [사용자용도](#)
- [IP용도](#)
- [용도별 정의 수정](#)

사용자용도

사용자용도

사용자ID가 없는 사용자가 사용자 등록할 때 설정하는 용도를 관리자가 정의하여 용도에 맞게 사용자 등록을 하며, 사용자를 용도로 구분하여 보다 쉽게 관리할 수 있습니다.

사용자용도 생성

1. 사용자용도 추가

설정 > 속성관리 > 용도관리 > 사용자용도 > 작업선택 > 추가 버튼을 클릭합니다.



2. 기본설정

ID, 이름, 설명, 순서, 신청여부를 입력합니다.



이름	설명
용도타입	해당 용도가 어느 용도의 타입인가를 나타내며, 수정할 수 없는 부분입니다.
ID	용도를 식별할 이름을 입력합니다.
이름	사용자 등록에서 용도 설정할 때 보여지는 용도 이름을 입력합니다.
설명	용도에 대한 설명을 입력합니다.
순서	정수로 기하며, 낮은 숫자일수록 우선순위가 높습니다. 더욱 자세한 내용은 정책의 순서 변경 을 참고해 주십시오.
신청여부	사용함/사용안함 옵션이 있고, 사용함 옵션 선택 시 용도 생성 시 바로 용도를 사용하며, 사용안함 옵션을 선택 시 생성하여도 바로 사용하지 않습니다. 사용하고 싶은 경우 설정 > 속성관리 > 용도관리 > 사용자용도에서 신청 항목에 있는 체크 표시를 클릭하여 활성화 합니다.

3. 처리옵션 설정

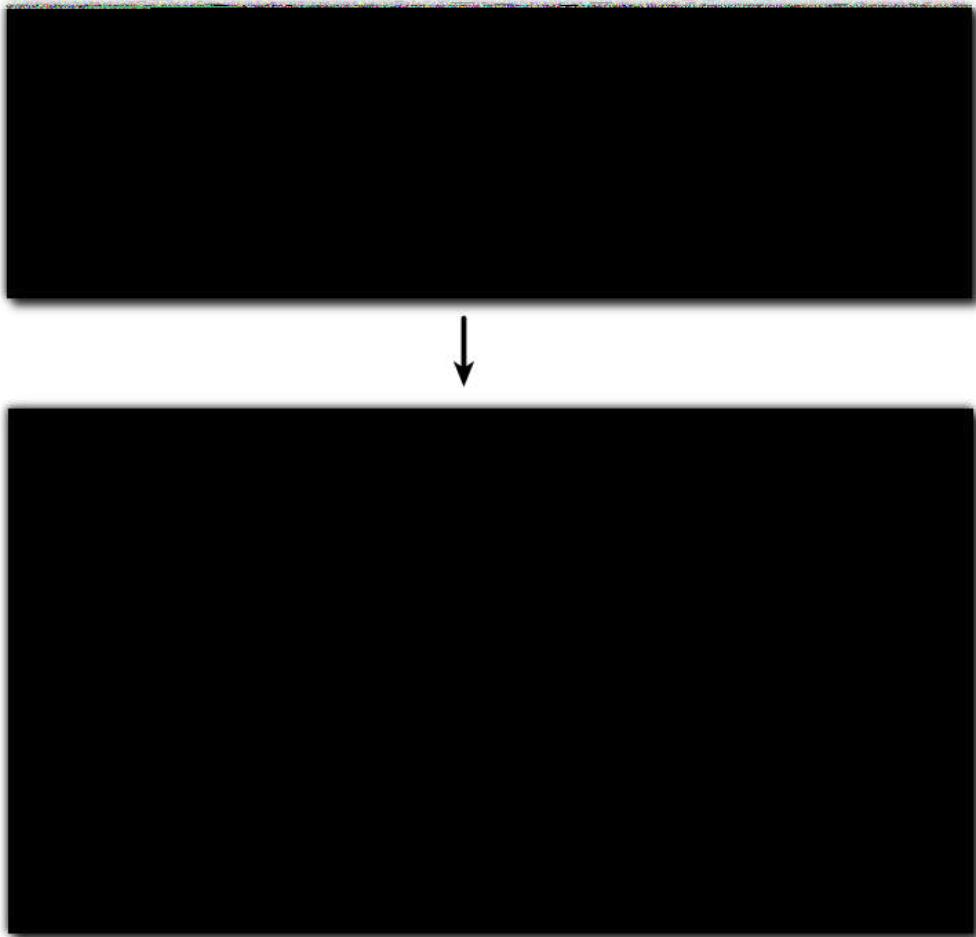
용도의 처리옵션으로 ID, 용도설명, 이메일 인증, 사용자계정 만료처리에 대한 설정합니다.



이름	옵션	설명
용도설명		용도에 대한 설명을 입력합니다. Ko의 문자는 CWP의 Language 옵션이 한국어일 경우 나타나며 en의 문자는 Language 옵션이 English일 경우에 나타납니다.
ID 패턴 제한 설정	on	ID 패턴 정규식에 정규식을 작성하고 해당 정규식에 맞게 ID를 생성하도록 제한합니다.
	off	정규식에 상관없이 ID를 생성할 수 있습니다.
ID 패턴 정규식		ID 패턴 제한 설정 옵션이 on일 경우에 활성화 되며, 정규식을 입력합니다. 입력한 정규식을 토대로 ID를 생성하여야 합니다.
ID 입력 설명문		ID입력에 대한 설명을 작성합니다. 신규사용자등록 페이지의 아이디 항목에 하단에 입력한 문구가 출력됩니다. Ko의 문자는 CWP의 Language 옵션이 한국어일 경우 나타나며 en의 문자는 Language 옵션이 English일 경우에 나타납니다.
피방문자 이메일 승인	on	등록되어 있는 사용자 및 관리자의 이메일로 신규사용자등록 승인, 거부 메시지를 전송하여 사용자가 신규사용자등록을 승인, 거부할 수 있습니다.
	off	관리자가 관리 > 신청 > 사용자신청서 > 신규등록에서 신규사용자 등록을 승인해주어야 합니다.
이메일 승인자	모두	사용자등록 알림수신설정이 되어 있는 관리자와 신규신청등록할 때 피방문자 항목에 설정한 사용자에게 신규사용자등록 승인, 거부 메시지가 전송됩니다.
	피방문자	사용자등록 할 때 피방문자 항목에 설정한 사용자에게 신규사용자등록 승인, 거부 메시지가 전송됩니다.
사용자계정 만료처리	관리자	사용자등록 알림수신설정이 되어 있는 관리자에게 신규사용자등록 승인, 거부 메시지가 전송됩니다.
	계정중지	신규사용자등록 할 때 설정한 사용기간을 만료하였을 시 해당 계정을 종지시켜 사용하지 못하도록 합니다.
계정삭제		신규사용자등록 할 때 설정한 사용기간을 만료하였을 시 해당 계정을 삭제합니다.

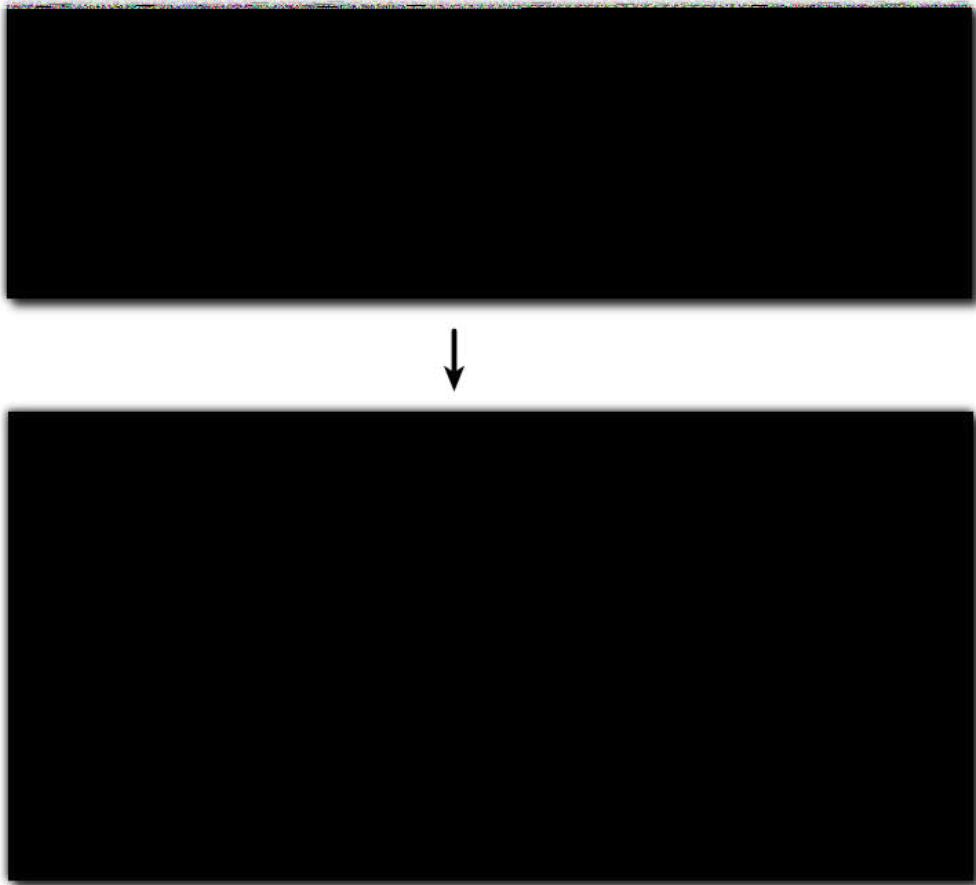
4. 용도별 신청정보필드 할당

신규사용자등록에 작성해야하는 신청정보필드를 추가 및 삭제할 수 있습니다.
신청정보필드 편집방법은 용도별 정의 수정을 참고 바랍니다.



5. 용도별 계정정보필드 할당

신규사용자등록에 작성해야하는 계정정보필드를 추가 및 삭제할 수 있습니다.
계정정보필드는 사용자 사용자정의 필드를 사용합니다.
계정정보필드 편집방법은 용도별 정의 수정을 참고 바랍니다.



IP용도

IP용도

- IP신규

IP신규 신청서 용도를 정의 및 수정할 수 있으며, 용도별로 신청서 필드를 설정할 수 있습니다.



- IP반납

IP반납 신청서 처리 방식 및 IP반납 신청서 필드를 설정할 수 있습니다.



- 장비변경

장비변경 신청서 처리 방식 및 장비변경 신청서 필드를 설정할 수 있습니다.



- 사용자변경

사용자변경 신청서 처리 방식 및 사용자변경 신청서 필드를 설정할 수 있습니다.



IP신규

IP신규

IP가 차단된 사용자가 IP신청할 때 설정하는 용도를 관리자가 정의하여 용도에 맞게 IP신청을 하며, IP를 용도로 구분하여 보다 쉽게 관리할 수 있습니다.

IP신규 생성

1. IP신규 추가

설정 > 속성관리 > 용도관리 > IP용도 > IP신규 > 작업선택 > 추가 버튼을 클릭합니다.



2. 기본설정

ID, 이름, 설명, 순서, 신청여부를 입력합니다.



이름	설명
용도타입	해당 용도가 어느 용도의 타입인가를 나타내며, 수정할 수 없는 부분입니다.
ID	용도를 식별할 이름을 입력합니다.
이름	사용자 등록에서 용도 설정할 때 보여지는 용도 이름을 입력합니다.
설명	용도에 대한 설명을 입력합니다.
순서	정수로 기하며, 낮은 숫자일수록 우선순위가 높습니다. 더욱 자세한 내용은 정책의 순서 변경을 참고해 주십시오.
신청여부	사용함/사용안함 옵션이 있고, 사용함 옵션 선택 시 용도 생성 시 바로 용도를 사용하며, 사용안함 옵션을 선택 시 생성하여도 바로 사용하지 않습니다. 사용하고 싶은 경우 설정 > 속성관리 > 용도관리 > IP용도 > IP신규 에서 신청 항목에 있는 체크 표시를 클릭하여 활성화 합니다.

3. 승인방식 설정

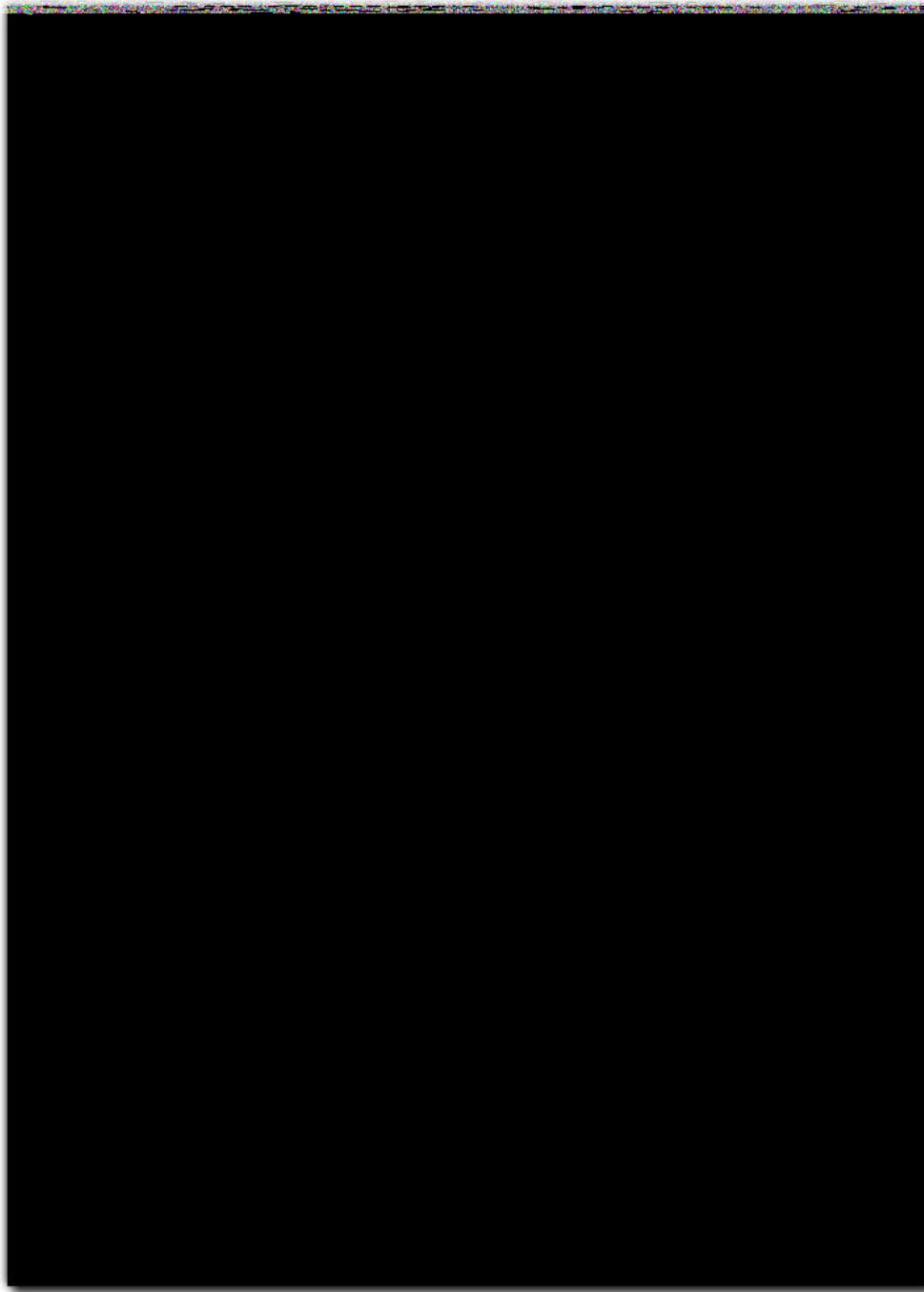
사용자가 신청한IP 승인방식을 설정합니다.



이름	옵션	설명
자동승인	사용함	사용자가 IP신청 시 관리자 승인 없이 즉시 승인되어 사용자에게 자동으로 IP를 할당합니다. 승인자 이메일 승인 옵션이 사용함으로 설정되어 있을 경우 이메일 승인 후 사용자에게 자동으로 IP가 할당됩니다.
	사용안함	사용자가 IP 신청 시 관리 > 신청 > IP신규/반납에서 관리자가 IP신청서를 승인 및 거부 할 수 있습니다.
승인자 이메일 승인	사용함	IP신청서에 승인자 항목이 추가되며, 승인자 항목에 선택된 승인자에게 IP신청서를 승인 및 거부할 수 있는 이메일이 발송됩니다. 승인자 항목에서 선택할 수 있는 사용자는 단계별 승인에 첫번째줄에 있는 사용자그룹이며, 다음줄에도 사용자그룹이 있을 경우 다음줄 사용자그룹에 포함된 사용자에게 IP반납 신청서를 승인 및 거부할 수 있는 이메일이 발송됩니다.
	사용안함	이메일 승인을 사용하지 않습니다.
승인자 이메일 전달 대상	모두전달	단계별 승인에 할당된 사용자그룹에 속하는 사용자에게 승인자 이메일을 발송합니다.
	동일부서	단계별 승인에 할당된 사용자그룹에 속하는 사용자 중 신청자와 동일한 부서의 사용자에게만 승인자 이메일을 발송합니다.
	관리자	단계별 승인에 할당된 사용자그룹에 속하는 사용자 중 관리자에게만 승인자 이메일을 발송합니다.
단계별 승인		사용자그룹을 할당합니다. 할당된 사용자그룹에 포함된 관리자는 NAC관리콘솔에 접속해 단계에 맞는 신청서를 확인 후 승인 및 거부합니다. 첫번째줄에 있는 사용자그룹이 1단계이며 다음 줄은 2단계입니다. 줄 바꿈에 따라 단계가 나뉘어집니다.

4. 처리옵션 설정

IP용도에 맞는 처리옵션을 설정합니다.



이름	옵션	설명
신청서처리 기본정책	모두허용	신청자에게 MAC/IP를 허용한 상태로 IP를 할당합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다. 첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 MAC/IP 차단모드로 설정합니다. 두번째. 정책 > 제어정책 > IP차단 관리 정책 을 사용으로 설정합니다.
	IP허용	신청자에게 IP를 허용한 상태로 IP를 할당합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다. 첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 IP 차단모드로 설정합니다. 두번째. 정책 > 제어정책 > IP차단 관리 정책 을 사용으로 설정합니다.

	MAC허용	<p>신청자에게 MAC을 허용한 상태로 IP를 할당합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 MAC 차단모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p>
	변경금지	<p>신청자에게 신청 시에 입력한 MAC으로 변경금지 정책을 적용하여 IP를 할당합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 변경금지모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p> <p>세번째. 설정 > 속성관리 > 용도관리 > IP용도 > IP신규 > 용도ID 클릭 > 용도별 신청정보 > 신규 신청 입력 필드에 MAC(IPMAPP_Mac)을 할당합니다.</p>
	충돌보호	<p>신청자에게 신청 시에 입력한 MAC으로 충돌보호 정책을 적용하여 IP를 할당합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 충돌보호모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p> <p>세번째. 설정 > 속성관리 > 용도관리 > IP용도 > IP신규 > 용도ID 클릭 > 용도별 신청정보 > 신규 신청 입력 필드에 MAC(IPMAPP_Mac)을 할당합니다.</p>
	변경금지+충돌보호	<p>신청자에게 신청 시에 입력한 MAC으로 충돌보호+변경금지 정책을 적용하여 IP를 할당합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 변경금지모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p> <p>세번째. 설정 > 속성관리 > 용도관리 > IP용도 > IP신규 > 용도ID 클릭 > 용도별 신청정보 > 신규 신청 입력 필드에 MAC(IPMAPP_Mac)을 할당합니다.</p>
	모두허용(신청PC)	<p>신청자에게 현재 사용중인 IP를 그대로 사용하게 하고 IP 및 MAC차단을 해제합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 MAC/IP 차단모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p>
	IP허용(신청PC)	<p>신청자에게 현재 사용중인 IP를 그대로 사용하게 하고 IP 차단을 해제합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 IP 차단모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p>
	MAC허용(신청PC)	<p>신청자에게 현재 사용중인 IP를 그대로 사용하게 하고 MAC 차단을 해제합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 MAC 차단모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p>
	변경금지(신청PC)	<p>신청자에게 현재 사용중인 IP를 그대로 사용하게 하고 변경금지 차단을 해제합니다. 해당 옵션을 사용하기 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 변경금지모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p>
	충돌보호(신청PC)	<p>신청자에게 현재 사용중인 IP를 그대로 사용하게 하고 충돌보호 차단을 해제합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 충돌보호모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p>
	변경금지+충돌보호(신청PC)	<p>신청자에게 현재 사용중인 IP를 그대로 사용하게 하고 충돌보호 및 변경금지 차단을 해제합니다. 해당 옵션을 사용하기 위해 다음과 같은 설정이 필요합니다.</p> <p>첫번째. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > eth클릭에서 신규노드정책 설정을 변경금지모드로 설정합니다.</p> <p>두번째. 정책 > 제어정책 > IP차단 관리 정책을 사용으로 설정합니다.</p>

승인번호 사용시 미사용IP할당	사용함	신청서처리 기본정책 옵션이 승인번호 관련 옵션으로 설정되어 있을 경우 활성화 되며, 사용함일 경우 할당받은 IP로 IP를 변경하고 CWP페이지에서 IP승인확인 버튼을 클릭하여 승인번호를 확인하여야 차단정책이 풀리며, 할당받은 IP를 사용할 수 있습니다.
	사용안함	신청서처리 기본정책 옵션이 승인번호 관련 옵션으로 설정되어 있을 경우 활성화 되며, 사용안함일 경우 CPW페이지의 IP승인확인에서 할당받은 승인번호를 입력할 시 IP변경 없이 차단정책이 풀리게됩니다.
IP호스트번호(처음)		신청자에게 처음으로 할당할 IP 설정으로, 설정한 호스트번호의 IP부터를 할당할 수 있으며 설정한 호스트번호 보다 작은 수의 호스트번호 IP는 할당할 수 없습니다.
IP호스트번호(마지막)		신청자에게 마지막으로 할당할 IP 설정으로, 설정한 호스터번호 보다 큰 수의 호스트번호 IP는 할당할 수 없습니다.
IP사용자 인증제한여부	모든사용자	IP소유자를 모든사용자로 설정합니다.
	사용자지정	IP소유자 외 다른 사용자는 IP소유자가 소유하고 있는 IP를 사용할 수 없습니다.
	노드정책준수	IP소유자와 관계없이 노드정책을 모두 준수하였을 경우 IP를 사용할 수 있습니다.
호스트명 할당	사용안함	IP를 할당할 때 호스트명을 제한하지 않습니다.
	승인시 직접입력	관리자가 IP신청서를 처리할 때 제한할 호스트명을 설정하고 설정한 호스트명에 따라 호스트명을 제한합니다. 신청자가 호스트명을 변경하지 않을 경우 네트워크 차단이 이루어 집니다.
	할당패턴입력	호스트명 할당패턴 항목에 설정한 할당패턴에 따라 호스트명을 제한합니다. 신청자가 호스트명을 변경하지 않을 경우 네트워크 차단이 이루어 집니다.
호스트명 할당패턴		호스트명 할당 항목의 옵션이 할당패턴입력 일 시 활성화 되며, +add 버튼을 클릭하여 패تون을 입력합니다. 설정한 패턴대로 호스트명을 제한합니다.
IP소유부서 변경여부	사용함, 사용안함	부서의 IP를 사용 중에 다른부서로 변경되어 사용자ID의 부서가 변경될 경우, 현재 사용하고 있는 IP를 변경된 부서에서 관리하게 됩니다.
	IP신청서 처리시만	IP신청서 처리 시에는 변경된 부서가 아닌 예전의 부서로 IP를 할당합니다.
동일MAC 노드 사용여부	사용함, 사용안함	IP신청서를 처리할 때 신청자의 MAC으로 등록되어 있는 노드들 중 MAC차단이 걸려있는 노드들의 MAC을 모두 허용합니다.
IP할당 노드그룹 지정		노드그룹을 지정하여 노드그룹에 설정되어 있는 IP를 관리자가 IP 신청서를 확인하고 IP를 할당할 때 할당합니다.
용도 사용가능한 사용자그룹		사용자그룹을 지정하여 사용자그룹에 포함되어 있는 사용자만 해당 용도의 신청서를 작성할 수 있게 합니다.
URL호출	사용함	IP신청서 승인 시 설정한 URL을 호출합니다.
	사용안함	IP신청서 승인 시 URL을 호출하지 않습니다.
URL		URL 호출 항목이 사용함일 경우 활성화 되며, IP신청서 승인 시 호출할 URL을 입력합니다.
CHARSET	EUC-KR	URL의 CHARSET이 EUC-KR일 경우 설정합니다.
	UTF-8	URL의 CHARSET이 UTF-8일 경우 설정합니다.
센서별위치정보 변경여부	변경가능	IP신청서 신청할 때 IP할당 노드그룹 지정 항목에 할당되어 있는 센서IP가 보이며 한 가지를 선택할 수 있습니다. 그외 센서는 선택할 수 없습니다. 노드그룹 지정 항목이 비어있을 시 모든 센서가 보이며 한 가지를 선택할 수 있습니다. IP신청 시 자동로그인으로 접속할 경우 IP신청서에 자동으로 노드에 맞는 센서로 사용위치가 설정됩니다. 자동로그인은 설정 > 환경설정 > IP관리 > 자동로그인 옵션에서 설정할 수 있습니다.
센서별위치정보 변경여부	변경불가	IP신청서 신청 시 모든 센서가 보이며 한 가지를 선택할 수 있습니다. IP신청 시 자동로그인으로 접속할 경우 IP신청서에 자동으로 노드에 맞는 센서로 사용위치가 설정됩니다. 자동로그인은 설정 > 환경설정 > IP관리 > 자동로그인 옵션에서 설정할 수 있습니다.

5. 용도별 신청정보

IP신청서를 작성할 때 입력하여야 하는 필드를 추가 및 삭제할 수 있습니다.



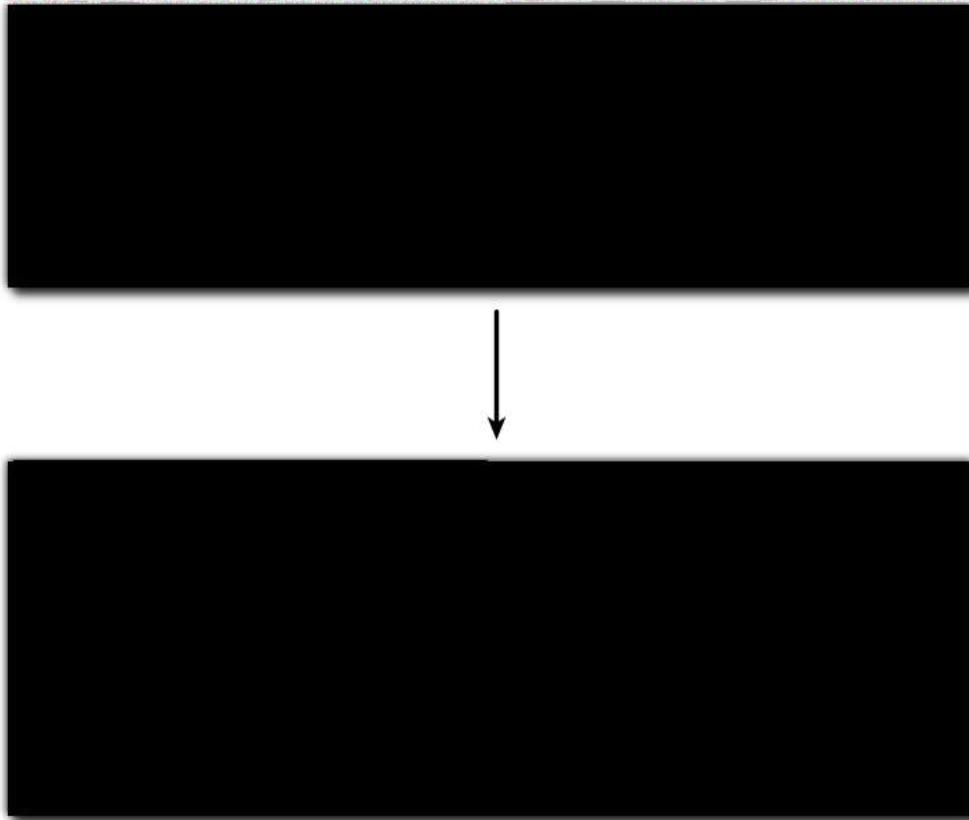
이름	옵션	설명
용도타입지정	일반용도	인증된 사용자 및 로그인을 통해 IP신청서 등록 페이지에 접속할 시 일반용도로 설정된 용도를 사용할 수 있습니다.
	방문자용도	임시로그인을 통해 IP신청서 등록 페이지에 접속할 시 방문자용도로 설정된 용도를 사용할 수 있습니다.
일반사용자 대리신청여부	사용안함	일반사용자가 대리신청할 수 없습니다.
	동일부서	일반사용자가 동일부서에 속한 사용자에 대해 IP신청을 대리로 할 수 있습니다.
	모든부서	일반사용자가 모든부서의 사용자에 대해 IP신청을 대리로 할 수 있습니다.

- 사용자 정보입력 필드

사용자 정보입력 필드는 용도타입지정 설정이 방문자용도일 경우 활성화 되며, IP신청서에 작성해야하는 사용자 정보입력 필드를 추가 및 삭제할 수 있습니다.

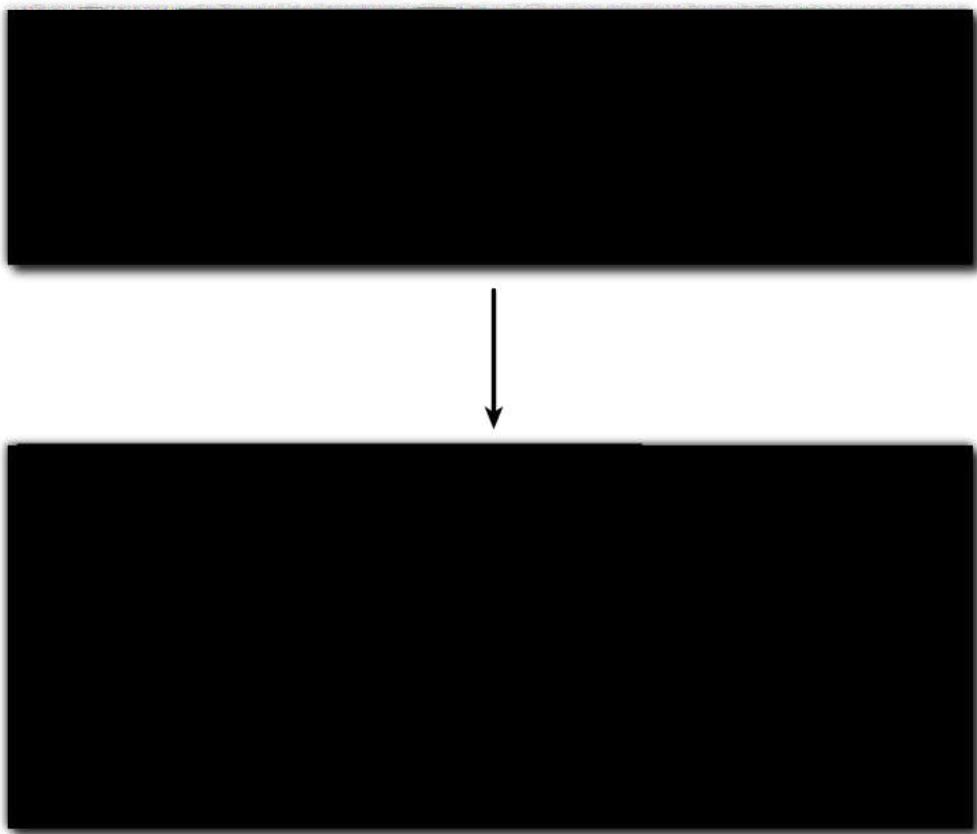
사용자 정보입력 필드는 설정 > 속성관리 > IP신청서 사용자정의 필드 를 사용합니다.

사용자 정보입력 필드 편집방법은 [용도별 정의 수정](#)을 참고 바랍니다.



- 신규 신청 입력 필드

용도타입지정 설정이 방문자용도일 경우와 일반용도일 경우 모두 활성화 되며, IP신청서에 작성해야하는 신청 정보 입력 필드를 추가 및 삭제할 수 있습니다.
신규 신청 입력 필드는 설정 > 속성관리 > IP신청서 사용자정의 필드 를 사용합니다.



IP반납

IP반납

IP반납 신청서의 필드를 추가 및 제거할 수 있으며, 단계별승인 및 이메일승인 기능을 설정할 수 있습니다.

- 승인방식

신청서 거부, 승인 방식을 설정할 수 있습니다.



이름	옵션	설명
자동승인	사용함	사용자가 IP반납 신청 시 관리자 승인 없이 즉시 승인되어 IP를 반납합니다. 승인자 이메일 승인 옵션이 사용함으로 설정되어 있을 경우 이메일 승인 후 IP가 반납됩니다.
	사용안함	사용자가 IP 반납 신청 시 관리 > 신청 > IP신규/반납에서 관리자가 신청서를 승인 및 거부 할 수 있습니다.
승인자 이메일 승인	사용함	IP반납 신청서에 승인자 항목이 추가되며, 승인자 항목에 선택된 승인자에게 IP반납 신청서를 승인 및 거부할 수 있는 이메일이 발송됩니다. 승인자 항목에서 선택할 수 있는 사용자는 단계별 승인에 첫번째줄에 있는 사용자그룹이며, 다음줄에도 사용자그룹이 있을 경우 다음줄 사용자그룹에 포함된 사용자에게 IP반납 신청서를 승인 및 거부할 수 있는 이메일이 발송됩니다.
	사용안함	이메일 승인을 사용하지 않습니다.
단계별 승인		사용자그룹을 할당합니다. 할당된 사용자그룹에 포함된 관리자는 관리 > 신청 > IP사용신청서 > 단계별승인에서 단계에 맞는 신청서를 확인 후 승인 및 거부합니다. 첫번째줄에 있는 사용자그룹이 1단계이며 다음 줄은 2단계입니다. 줄 바꿈에 따라 단계가 나뉘어집니다.

- 처리옵션

신청서 처리 후 수행하는 옵션들을 설정할 수 있습니다.



이름	옵션	설명
URL호출	사용함	IP반납 신청서 승인 시 설정한 URL을 호출합니다.
	사용안함	IP반납 신청서 승인 시 URL을 호출하지 않습니다.
URL		URL 호출 항목이 사용함일 경우 활성화 되며, IP반납 신청서 승인 시 호출할 URL을 입력합니다.
CHARSET	EUC-KR	URL의 CHARSET이 EUC-KR일 경우 설정합니다.
	UTF-8	URL의 CHARSET이 UTF-8일 경우 설정합니다.

- 신청정보

신청서에 입력하는 필드를 설정할 수 있습니다.



이름	설명
반납 신청 입력 필드	활당 버튼을 클릭하여 신청서의 입력 필드를 추가 및 제거할 수 있으며, 입력 필드는 설정 > 속성관리 > 추가필드관리 > IP신청서에서 생성할 수 있습니다.

장비변경

장비변경

장비변경 신청서의 필드를 추가 및 제거할 수 있으며, 단계별승인 및 이메일승인 기능을 설정할 수 있습니다.

- 승인방식

신청서 거부, 승인 방식을 설정할 수 있습니다.



이름	옵션	설명
자동승인	사용함	사용자가 장비변경 신청 시 관리자 승인 없이 즉시 승인되어 장비변경이 허용됩니다. 승인자 이메일 승인 옵션이 사용함으로 설정되어 있을 경우 이메일 승인 후 장비변경이 허용됩니다.
	사용안함	사용자가 장비변경 신청 시 관리 > 신청 > 장비변경에서 관리자가 신청서를 승인 및 거부 할 수 있습니다.
승인자 이메일 승인	사용함	장비변경 신청서에 승인자 항목이 추가되며, 승인자 항목에 선택된 승인자에게 장비변경 신청서를 승인 및 거부할 수 있는 이메일이 발송됩니다. 승인자 항목에서 선택할 수 있는 사용자는 단계별 승인에 첫번째줄에 있는 사용자그룹이며, 다음줄에도 사용자그룹이 있을 경우 다음줄 사용자그룹에 포함된 사용자에게 장비변경 신청서를 승인 및 거부할 수 있는 이메일이 발송됩니다.
	사용안함	이메일 승인을 사용하지 않습니다.
단계별 승인		사용자그룹을 할당합니다. 할당된 사용자그룹에 포함된 관리자는 관리 > 신청 > IP사용신청서 > 단계별승인에서 단계에 맞는 신청서를 확인 후 승인 및 거부합니다. 첫번째줄에 있는 사용자그룹이 1단계이며 다음 줄은 2단계입니다. 줄 바꿈에 따라 단계가 나뉘어집니다.

- 처리옵션

신청서 처리 후 수행하는 옵션들을 설정할 수 있습니다.



이름	옵션	설명
URL호출	사용함	장비변경 신청서 승인 시 설정한 URL을 호출합니다.

	사용안함	장비변경 신청서 승인 시 URL을 호출하지 않습니다.
URL		URL 호출 항목이 사용함일 경우 활성화 되며, 장비변경 신청서 승인 시 호출할 URL을 입력합니다.
CHARSET	EUC-KR	URL의 CHARSET이 EUC-KR일 경우 설정합니다.
	UTF-8	URL의 CHARSET이 UTF-8일 경우 설정합니다.

- 신청정보

신청서에 입력하는 필드를 설정할 수 있습니다.



이름	설명
장비변경 신청 입력 필드	할당 버튼을 클릭하여 신청서의 입력 필드를 추가 및 제거할 수 있으며, 입력 필드는 설정 > 속성관리 > 추가필드관리 > IP신청서에서 생성할 수 있습니다.

사용자변경

사용자변경

사용자변경 신청서의 필드를 추가 및 제거할 수 있으며, 단계별승인 및 이메일승인 기능을 설정할 수 있습니다.

- 승인방식

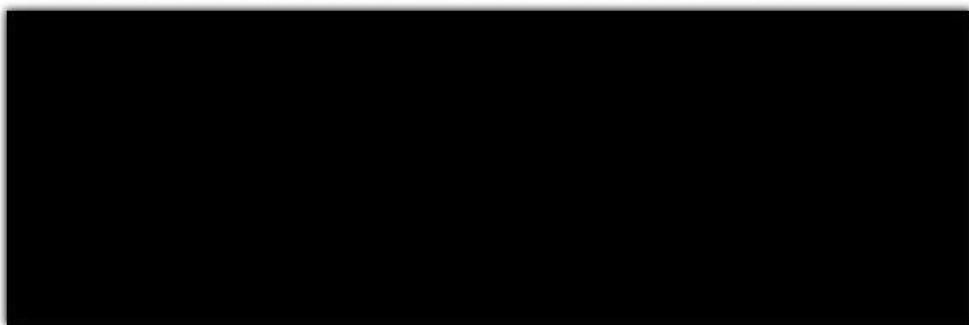
신청서 거부, 승인 방식을 설정할 수 있습니다.



이름	옵션	설명
자동승인	사용함	사용자가 사용자변경 신청 시 관리자 승인 없이 즉시 승인되어 IP의 사용자가 변경됩니다. 승인자 이메일 승인 옵션이 사용함으로 설정되어 있을 경우 이메일 승인 후 IP의 사용자가 변경됩니다.
	사용안함	사용자가 사용자변경 신청 시 관리 > 신청 > 사용자변경에서 관리자가 신청서를 승인 및 거부 할 수 있습니다.
승인자 이메일 승인	사용함	사용자변경 신청서에 승인자 항목이 추가되며, 승인자 항목에 선택된 승인자에게 사용자변경 신청서를 승인 및 거부할 수 있는 이메일이 발송됩니다. 승인자 항목에서 선택할 수 있는 사용자는 단계별 승인에 첫번째줄에 있는 사용자그룹이며, 다음줄에도 사용자그룹이 있을 경우 다음줄 사용자그룹에 포함된 사용자에게 사용자변경 신청서를 승인 및 거부할 수 있는 이메일이 발송됩니다.
	사용안함	이메일 승인을 사용하지 않습니다.
단계별 승인		사용자그룹을 할당합니다. 할당된 사용자그룹에 포함된 관리자는 관리 > 신청 > IP사용신청서 > 단계별승인에서 단계에 맞는 신청서를 확인 후 승인 및 거부합니다. 첫번째줄에 있는 사용자그룹이 1단계이며 다음 줄은 2단계입니다. 줄 바꿈에 따라 단계가 나뉘어집니다.

- 처리옵션

신청서 처리 후 수행하는 옵션들을 설정할 수 있습니다.



이름	옵션	설명

URL호출	사용함	사용자변경 신청서 승인 시 설정한 URL을 호출합니다.
	사용안함	사용자변경 신청서 승인 시 URL을 호출하지 않습니다.
URL		URL 호출 항목이 사용함일 경우 활성화 되며, 사용자변경 신청서 승인 시 호출할 URL을 입력합니다.
CHARSET	EUC-KR	URL의 CHARSET이 EUC-KR일 경우 설정합니다.
	UTF-8	URL의 CHARSET이 UTF-8일 경우 설정합니다.

- 신청정보

신청서에 입력하는 필드를 설정할 수 있습니다.



이름	설명
사용자변경 신청 입력 필드	할당 버튼을 클릭하여 신청서의 입력 필드를 추가 및 제거할 수 있으며, 입력 필드는 설정 > 속성관리 > 추가필드관리 > IP신청서에서 생성할 수 있습니다.

용도별 정의 수정

용도별 정의 수정

관리자는 용도별로 할당한 필드들의 제목, 필드설명, 필드크기, 입력타입 등 편집할 수 있습니다.

1. 수정할 정보 선택

설정 > 속성관리 > 용도관리 > 사용자용도 or IP용도 > 용도별 정의 수정에서 수정할 정보를 선택합니다.



2. 필드 선택

해당 용도에 할당한 필드만 보이며, 수정할 필드의 필드명을 클릭합니다.



3. 필드 수정

관리자는 현재 정의되어 있는 필드를 수정할 수 있습니다. 수정방법은 [추가필드관리](#)를 참고 바랍니다.



접속인증페이지(CWP)

접속인증페이지(CWP)

CWP(접속인증페이지)는 사용자의 정책 위반으로 인한 네트워크 차단시, 웹페이지로 접속하여 위반한 내용을 확인하고 해결방안을 알 수 있게 해 주는 페이지입니다.

공지사항, 페이지구성, 메시지관리, 사용자동의 페이지, 사용자정의 링크에 대한 기능들을 설정 할 수 있습니다.

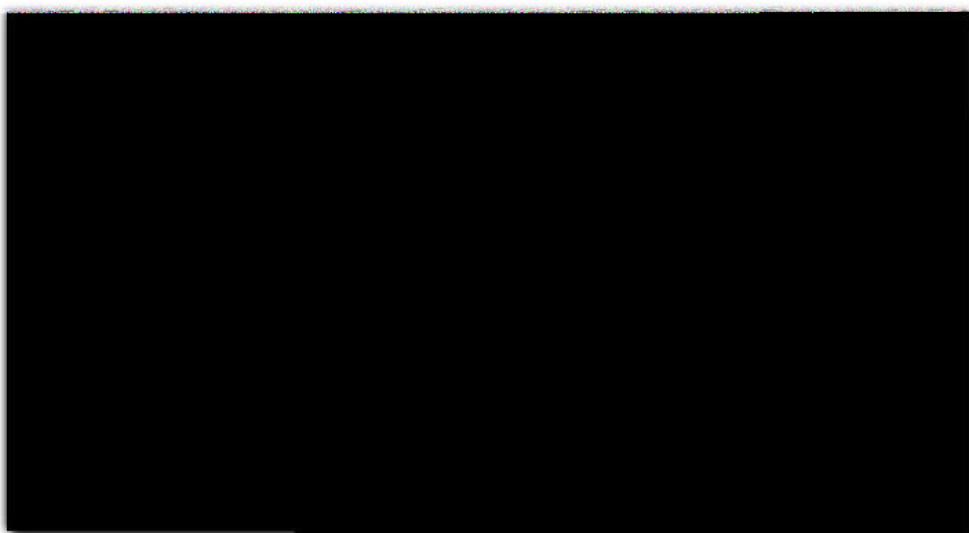
- 공지사항

관리자가 알고 싶은 내용을 공지사항 기능을 이용하여 접속인증페이지(CWP)에서 공지사항을 확인할 수 있습니다.



- 페이지 구성

접속인증페이지(CWP) 페이지의 레이아웃 및 도움말, 메시지 등을 수정할 수 있습니다.



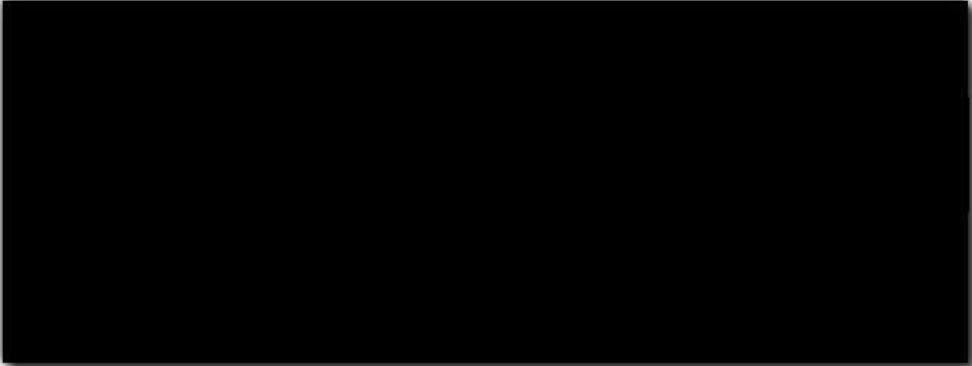
- 메시지관리

사용자에게 보여줄 알림 메세지를 수정할 수 있습니다.



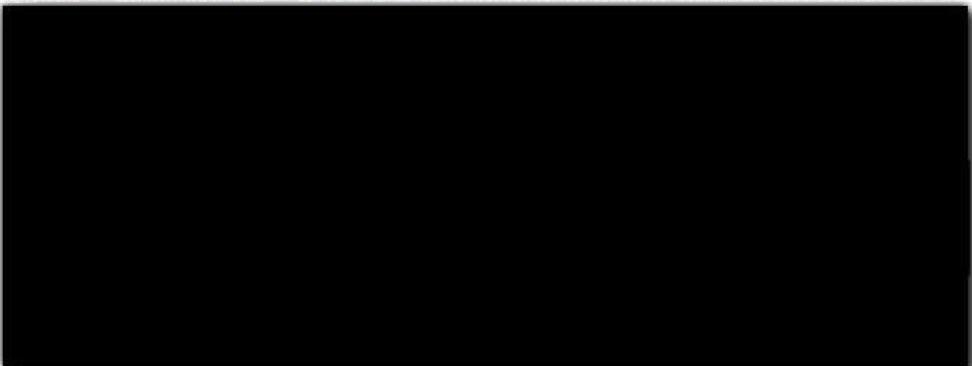
- 사용자정보

사용자 등록 시 필요한 동의 및 약관이 필요한 경우 해당 기능을 사용하여 동의페이지를 생성할 수 있습니다.



- 보안서약

보안서약이 필요한 경우 해당 기능을 사용하여 동의페이지를 생성할 수 있습니다.



- 사용자정의 버튼

접속인증페이지(CWP)에 아이콘을 추가하여 해당 아이콘을 클릭할 시 관리자가 설정한 URL로 접속할 수 있습니다.



- CWP설정

CWP 페이지에 관련된 다양한 설정을 할 수 있습니다.



디자인 템플릿

디자인 템플릿이란?

디자인 템플릿을 통해 접속인증페이지(CWP2)의 UI 구성 및 디자인을 변경할 수 있습니다.

디자인 템플릿 추가

- 설정 > 접속인증페이지(CWP) > 디자인 템플릿 > 작업선택 > 생성 을 클릭합니다.



- 생성할 디자인 템플릿의 이름, 설명을 입력 후 다음 버튼을 클릭합니다.



- 레이아웃을 설정 후 완료 버튼을 클릭합니다.



- 다음과 같이 디자인 템플릿이 추가됩니다.



-
5. 추가된 디자인 템플릿은 정책 > 노드정책에서 설정하여 적용할 수 있습니다.



디자인 템플릿

관리자는 디자인 템플릿의 컴포넌트 설정, 수정, CSS스타일, 레이아웃, 이미지업로드를 이용하여 CWP2를 custom하게 변경할 수 있습니다.



- 메인화면

메인화면은 CWP2의 변경된 부분들을 CWP2에 접속하지 않고 즉시 확인할 수 있습니다.



- 컴포넌트 설정

CWP2에 사용되는 컴포넌트들을 추가 및 삭제할 수 있습니다.



- 수정

CWP2의 컴포넌트 및 UI 구성은 source에서 수정할 수 있습니다.



- CSS스타일

CWP2의 CSS스타일을 추가할 수 있습니다.



- 레이아웃

CWP2의 레이아웃을 수정할 수 있습니다.



- 이미지 업로드

CWP2에 사용될 이미지를 업로드합니다. 업로드한 이미지는 수정, 레이아웃 탭에서 사용할 수 있습니다.



공지사항

공지사항이란?

관리자는 공지사항 기능을 이용하여 중요한 사항을 쉽게 사용자들에게 알려줄 수 있습니다.
공지사항은 접속인증페이지(CWP)에서 확인할 수 있습니다.

공지사항 추가/삭제

- 공지사항 추가
 - 1. 설정 > 접속인증페이지(CWP) > 공지사항 > 작업선택 > 생성 를 선택합니다.



-
2. 공지사항의 내용과 공지기간을 설정하고 추가 버튼을 선택합니다.



공지사항을 추가 후, 접속인증페이지에 접속하면 공지사항이 등록되어 있는것을 볼 수 있습니다.





- 공지사항 삭제

관리자는 공지사항을 삭제할 수 있습니다.

삭제방법은 [항목 삭제](#)를 참조해 주시기 바랍니다.

메시지관리

메시지관리란?

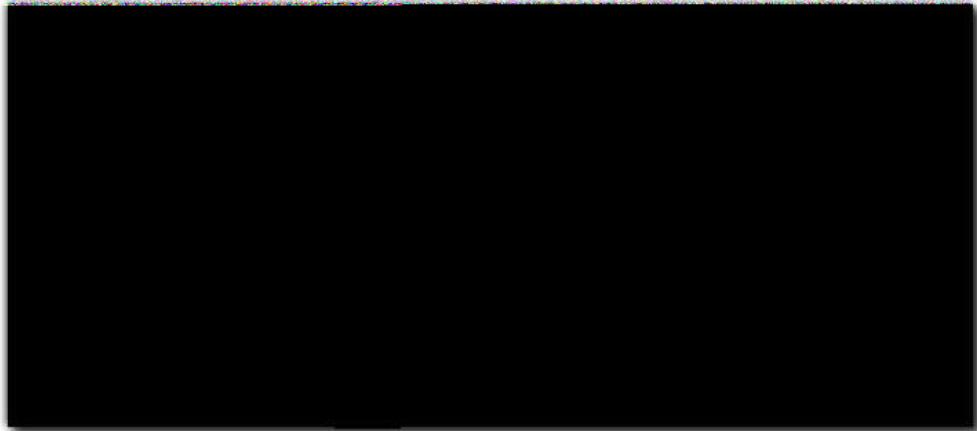
사용자에게 보여줄 메시지를 관리합니다.

사용자에게 보여주는 메시지는 사용자가 어떤 이유에 의해 제어를 받는지 나타내어 주기도 하지만, 그것이 오히려 공격자에겐 많은 정보를 제공해 공격의 시발점이 되기도 합니다.

따라서 관리자는 사용자에게 보여줄 메시지와 그렇지 않은 메시지를 잘 구분하여 설정해야 합니다.

- 메시지 사용설정

메시지는 사용체크박스 항목의 체크유무에 따라 설정을 변경할 수 있습니다.(사용항목 체크 해제시 메시지가 표시되지 않습니다.)



- 메시지 수정

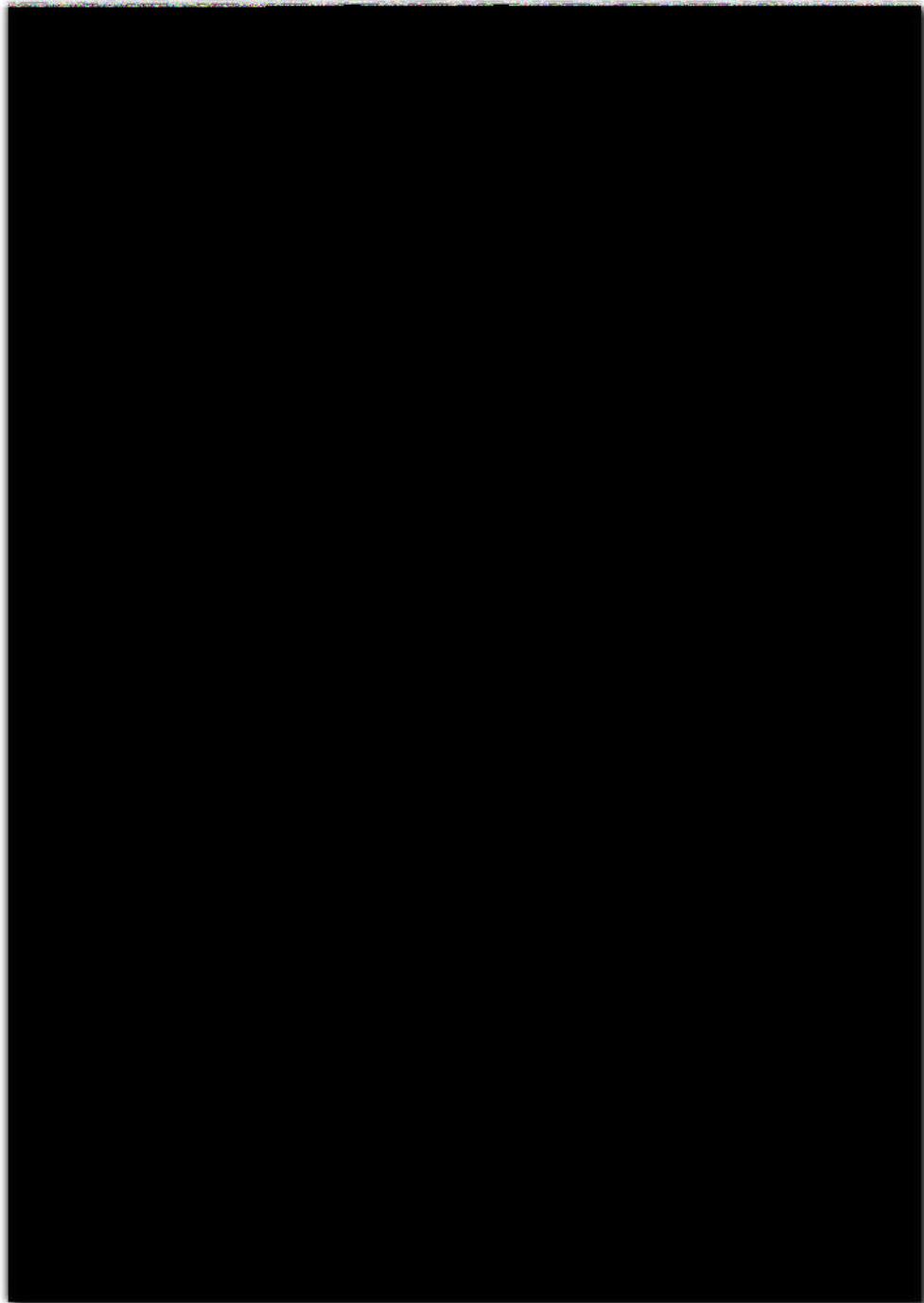
1. 메시지ID 클릭

수정하고 싶은 메시지ID를 클릭 합니다.



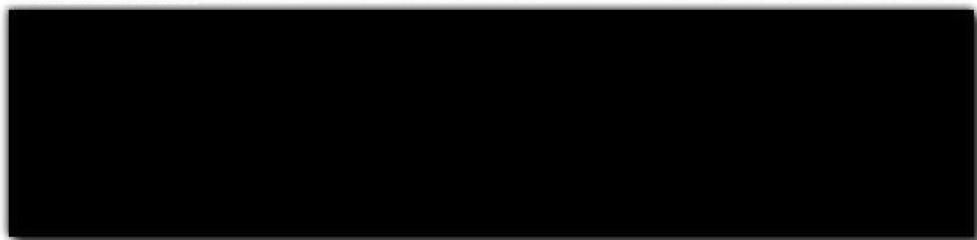
2. 메시지 수정

메시지의 내용을 수정 할 수 있으며, 적용모드를 이용하여 메시지를 출력하지 않게 할 수 있습니다.
메시지 수정 시 원본메시지 옵션이 출력되며, 원본메시지 옵션을 선택하여 원본메시지를 확인할 수 있습니다.



3. 메시지 확인

아래의 그림과 같이 메시지 내용이 바뀐걸 확인 할 수 있습니다.



동의페이지

동의페이지

동의가 필요한 서약을 사용자 등록 및 주기적으로 동의를 받고 관리할 수 있습니다.
동의페이지에는 사용자정보와 보안서약이 있으며 내용은 다음과 같습니다.

- 사용자정보

사용자가 CWP페이지에서 사용자등록 시 동의페이지를 출력하고 관리자가 필요한 정보를 사용자에게 요청할 수 있습니다.
자세한 내용은 [사용자정보](#)를 참고바랍니다.

- 보안서약

사용자에게 서약 동의를 주기적 혹은 MAC, PC가 변경되었을 시 서약 동의를 받아야할때 동의페이지를 자동으로 호출하며,
동의여부로 네트워크 제어를 할 수 있습니다.
자세한 내용은 [보안서약](#)을 참고바랍니다.

사용자정보

사용자정보란?

관리자는 사용자정보 페이지를 이용하여 사용자가 CWP페이지에서 사용자 계정을 등록할 때, 약관을 읽어보고 동의한 사용자만 계정을 등록할 수 있도록 합니다.

사용자정보 추가/삭제/순서 일괄수정

관리자는 사용자정보를 추가/삭제/순서이동 시킬 수 있습니다.

- 정책에서 사용자동의 페이지 ON

정책 > 노드정책 > 인증정책 > 사용자동록 페이지 를 ON으로 설정합니다.

정책 > 노드정책 > 인증정책 > 사용자동록 페이지 > 사용자동의 페이지 를 ON으로 설정합니다.



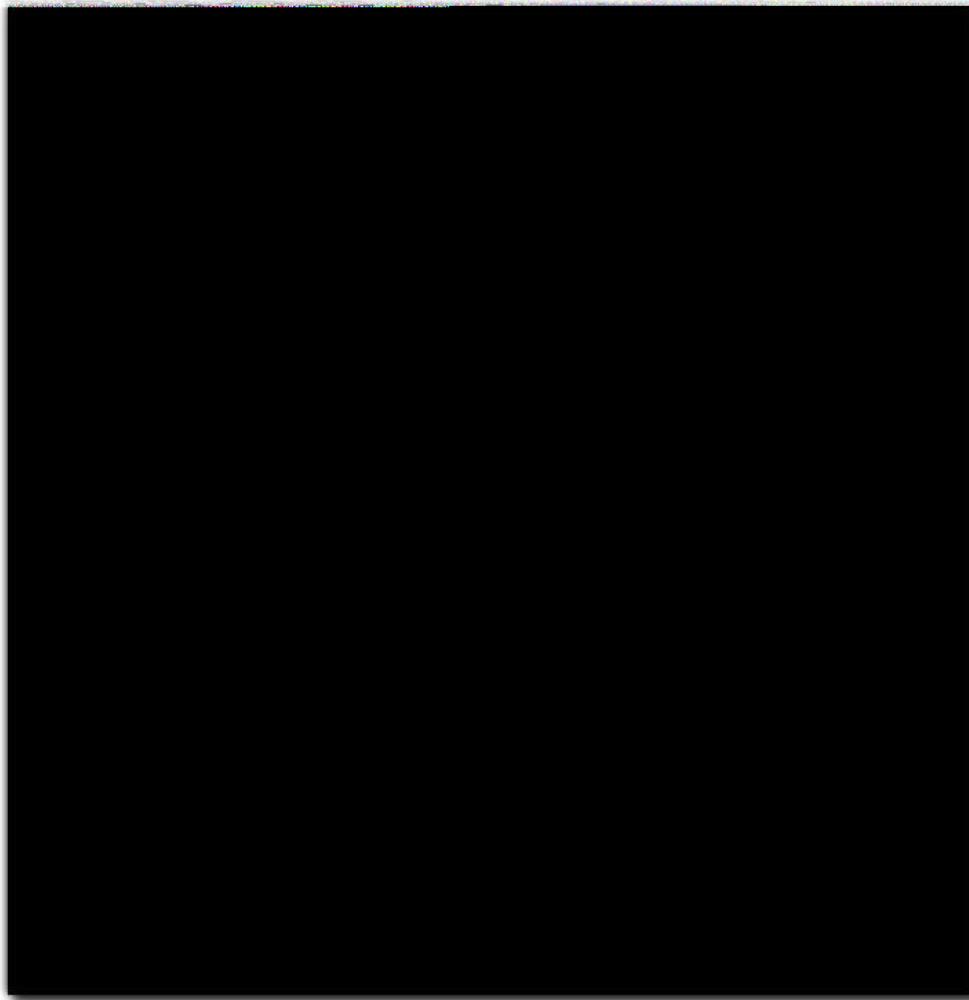
- 사용자정보 추가

설정 > 접속인증페이지(CWP) > 동의페이지 > 사용자정보 > 작업선택 > 추가 를 선택합니다.



- 사용자정보 작성

약관명, 동의설명, 순서,, 수집정보, 약관내용을 기입하고 추가 버튼을 선택합니다.



항목	내용
약관명	약관을 식별할 수 있는 이름을 입력합니다.
동의설명	동의여부를 확인하는 문구를 입력합니다.
약관내용	약관내용을 입력합니다.
수집정보	필드를 추가하여 사용자에게 정보를 요청합니다.

- 사용자정보 순서일괄수정/순서이동

사용자정보는 여러개를 만들어 여러약관에 대하여 동의를 받을 수 있습니다.
순서에따라 동의페이지가 나오는 순서가 바뀝니다. 제일 윗쪽에 위치하는 동의페이지가 첫번째로 출력됩니다.

순서의 변경에는 테이블 우측에 순서항목의 화살표를 이용하여 순서를 변경하는 방법과 작업선택 > 순서 일괄수정 을 이용하여 순서를 변경하는 방법이 있습니다.





만들어진 사용자정보는 접속인증페이지의 사용자등록 페이지에서 확인할 수 있습니다.



- 사용자정보 삭제

관리자는 필요없는 사용자정보를 삭제할 수 있습니다.

삭제방법은 [항목삭제 페이지](#)를 참조해 주시기 바랍니다.

보안서약

보안서약이란?

동의페이지를 주기적으로 호출하여 보안서약동의를 받고 관리할 수 있습니다.

보안서약 추가/삭제/순서 일괄수정

관리자는 보안서약을 추가/삭제/순서를 이동 시킬 수 있습니다.

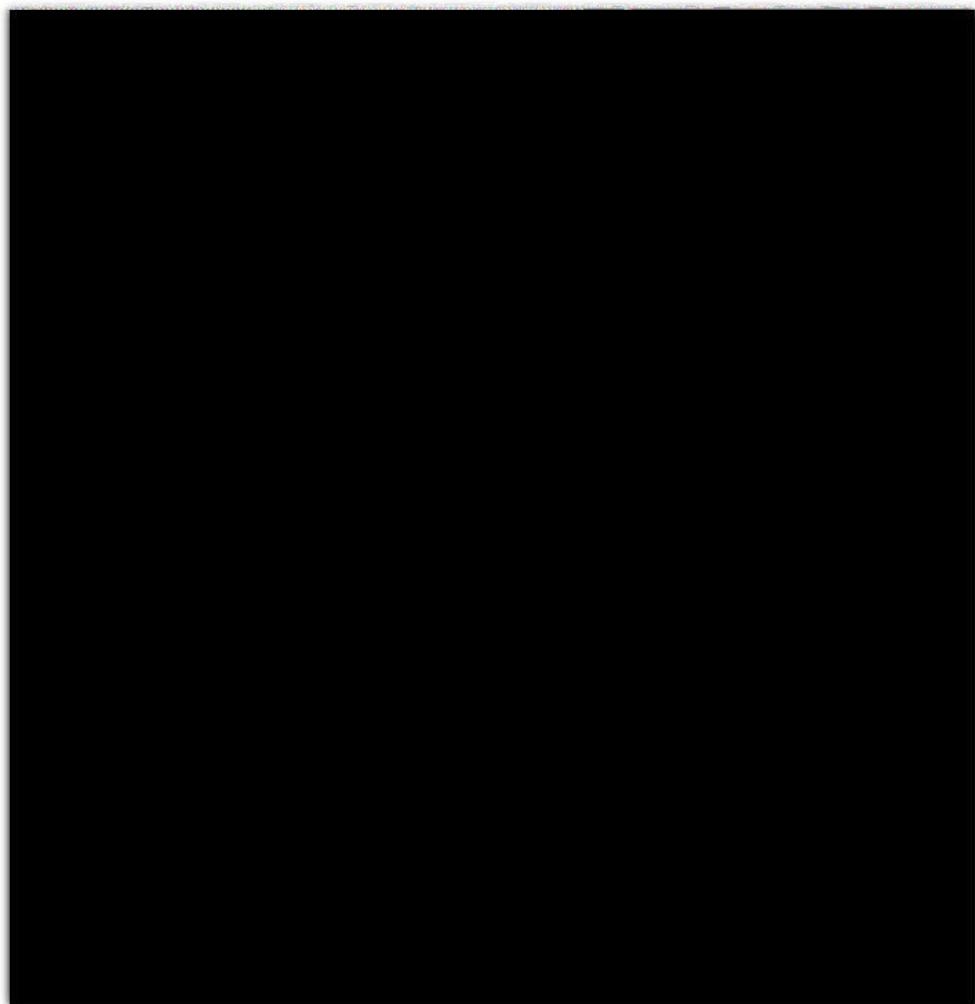
- 보안서약 추가

설정 > 접속인증페이지(CWP) > 동의페이지 > 보안서약 > 작업선택 > 추가 를 선택합니다.



- 보안서약 작성

약관명, 동의설명, 순서, 수집정보, 약관내용을 기입하고 추가 버튼을 선택합니다.



항목	내용
약관명	약관을 식별할 수 있는 이름을 입력합니다.
동의설명	동의여부를 확인하는 문구를 입력합니다.
약관제외 노드그룹	설정한 노드그룹에 포함하는 노드는 보안서약을 출력하지 않습니다.
순서	다수의 약관을 표시할 때 순서가 낮은 약관이 상위에 표시됩니다.
약관내용	약관내용을 입력합니다.
수집정보	필드를 추가하여 사용자에게 정보를 요청합니다.

- 보안서약 순서일괄수정/순서이동

보안서약을 여러개를 만들어 여러약관에 대하여 동의를 받을 수 있습니다.
순서에따라 동의페이지가 나오는 순서가 바뀝니다. 제일 윗쪽에 위치하는 동의페이지가 첫번째로 출력됩니다.

순서의 변경에는 테이블 우측에 순서항목의 화살표를 이용하여 순서를 변경하는 방법과 작업선택 > 순서 일괄수정 을 이용하여 순서를 변경하는 방법이 있습니다.



- 보안서약 삭제

관리자는 필요없는 보안서약을 삭제할 수 있습니다.

삭제방법은 [항목삭제 페이지](#)를 참조해 주시기 바랍니다.

사용자정의 버튼

사용자정의 버튼이란?

관리자는 접속인증페이지(CWP), 에이전트 트레이 아이콘에 관리자가 추가한 버튼형의 링크를 추가할 수 있습니다.

사용자정의 버튼의 추가/삭제/순서 일괄수정

관리자는 사용자정의 버튼을 추가/삭제/순서를 변경할 수 있습니다.

- 사용자정의 버튼 추가

- 설정 > 접속인증페이지(CWP) > 사용자정의 버튼 > 작업선택 > 추가 를 선택합니다.



- 기본설정

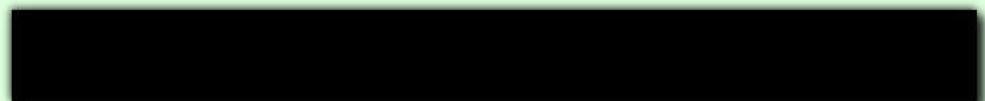
이름, 설명, 이미지 URL 등 기본정보를 기입합니다.



이미지 업로드를 클릭 시,
접속인증페이지(cwp) > 페이지구성 > 이미지업로드
페이지로 이동하여 이미지를 업로드할 수 있습니다.



아이콘으로 사용할 이미지를 업로드한 후에는 다음과 같은 형식으로 입력합니다.



3. 버튼설정

버튼타입과 표시유무를 선택합니다.



버튼타입과 버튼표시에 대한 설명은 아래 표와 같습니다.

설정항목	설정 값	설명
버튼타입	하이퍼링크	CWP 페이지에서 버튼을 클릭할 시 설정한 URL로 이동합니다.
	팝업 원도우	CWP 페이지에서 버튼을 클릭할 시 팝업 창으로 해당 URL을 띵웁니다.
	에이전트 트레이 메뉴	작업표시줄에 있는 에이전트 트레이 아이콘을 우클릭 할 시 나타나며, 해당 버튼을 클릭할 시 익스플로러 창으로 해당 URL을 띵웁니다. 매크로 : {_IP} = 로컬IP 정보 {_MAC} = 로컬MAC 정보 {_DEVICEID} = 노드의 장비 ID {_USERID} = 인증된 사용자 ID
	정보수집	CWP 페이지에서 버튼을 클릭할 시 추가한 필드에 대한 정보를 요청하는 페이지를 띵웁니다, 정보 입력 시 해당 필드에 입력한 정보가 출력됩니다.
	다운로드	CWP 페이지에서 버튼을 클릭할 시 업로드한 파일을 다운로드할 수 있습니다.
버튼표시	항상출력	접속인증페이지에 해당 버튼아이콘이 항상 표시됩니다.
	노드그룹에 포함된 경우에만 출력	접속인증페이지에 접속한 노드가 선택한 노드그룹속에 포함되어 있을때만 버튼아이콘이 표시됩니다.
	노드그룹에 포함안된 경우에만 출력	접속인증페이지에 접속한 노드가 선택한 노드그룹속에 포함되어있지 않을때만 버튼아이콘이 표시됩니다.

사용자정의 버튼 삭제

관리자는 필요없는 사용자정의 버튼 삭제할 수 있습니다.

사용자정의 버튼 삭제 진행과정은 항목 삭제를 참조 바랍니다.

CWP설정

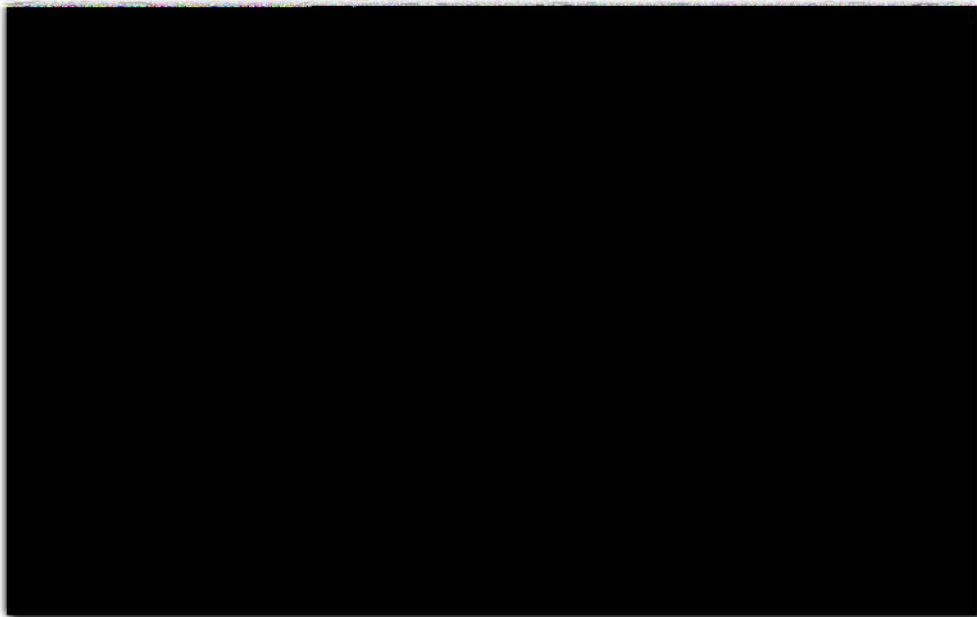
CWP설정

CWP(접속인증페이지)는 사용자의 정책 위반으로 인한 네트워크 차단시, 웹페이지로 접속하여 위반한 내용을 확인하고 해결방안을 알 수 있습니다.

CWP설정은 CWP에 관련된 설정들을 할 수 있습니다.

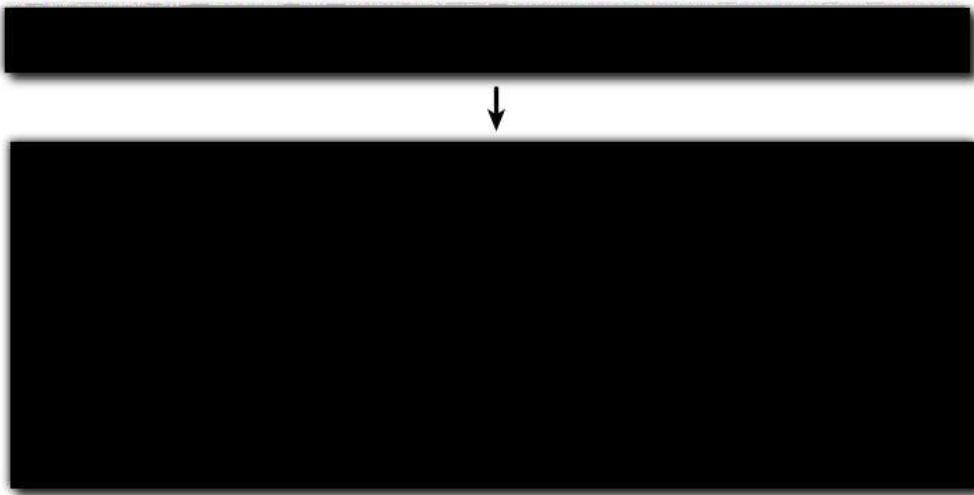
- 접속인증페이지(CWP) 설정

접속인증페이지(CWP)의 환경설정을 할 수 있습니다.



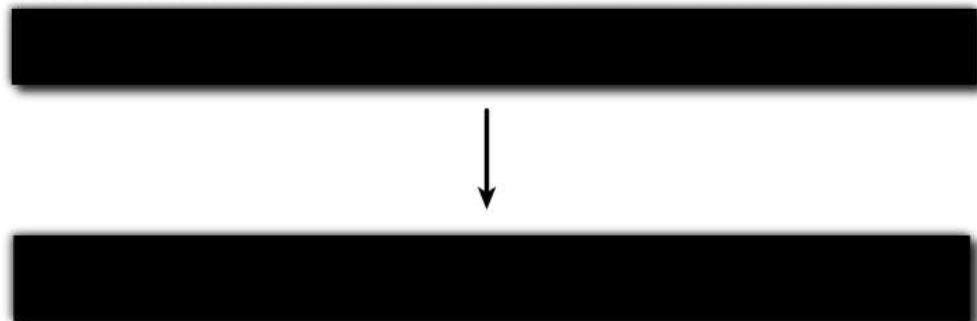
1. IP관리 메시지 우선

IP관리 메시지 우선 설정을 on으로 설정 후 IP가 차단 되어 CWP(접속인증페이지)에 접속할 시 IP 사용 신청 아이콘을 제외한 모든 아이콘이 보이지 않게 됩니다. IP 사용 신청 사용 여부는 [IP 사용신청서](#)를 참조해 주시기 바랍니다.



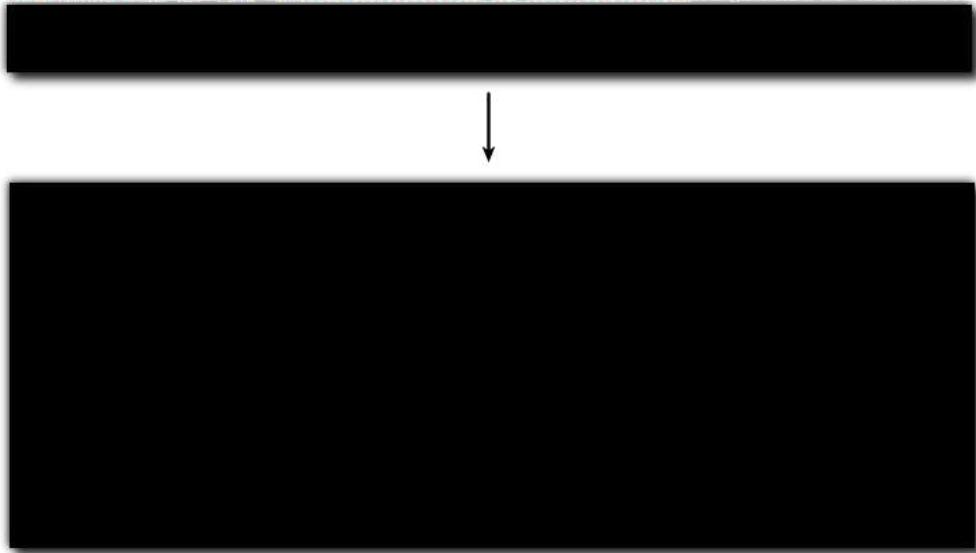
- 진행바 표시

진행바 표시 옵션을 on으로 할 경우 pc재검사버튼을 할 때 아래의 그림과 같이 PC재검사 진행바를 표시 합니다.



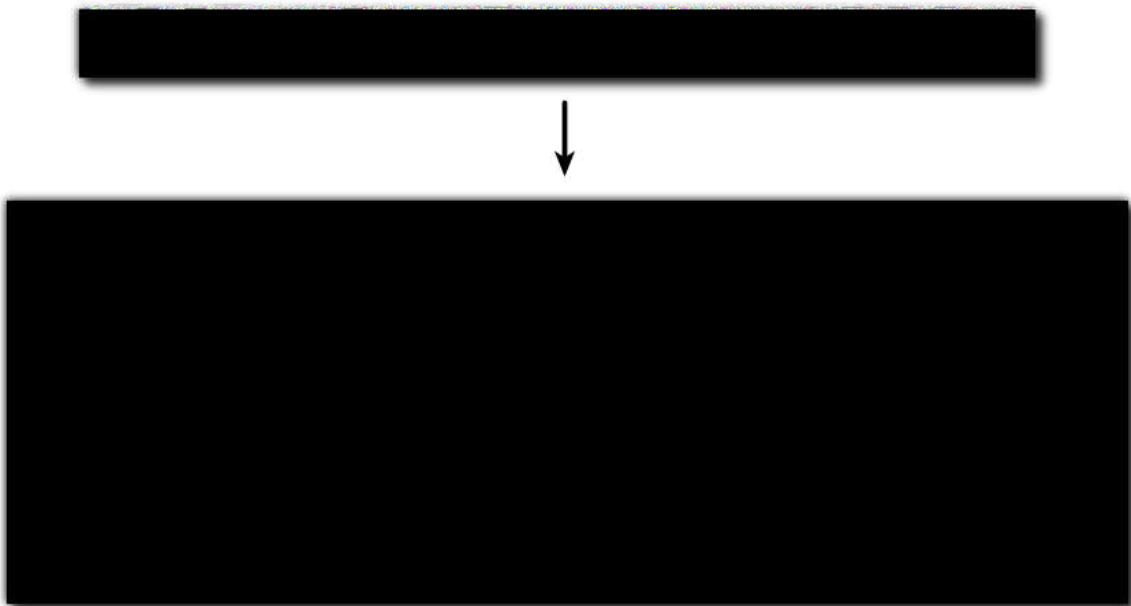
2. 지원언어

지원언어를 English 한 가지만 선택한 후 CWP(접속인증페이지)에 접속할 시 English언어만 지원하므로 모든 문자가 English으로 표시되고 한국어는 표시되지 않습니다.



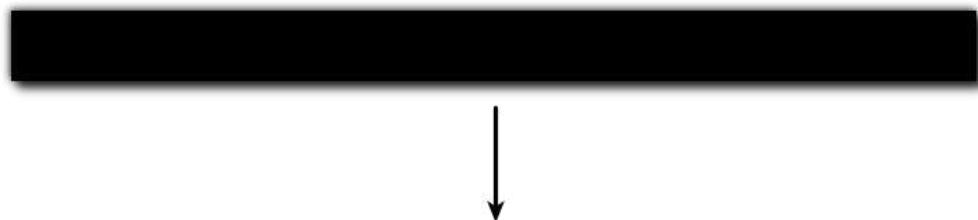
3. 타임존 변경알림

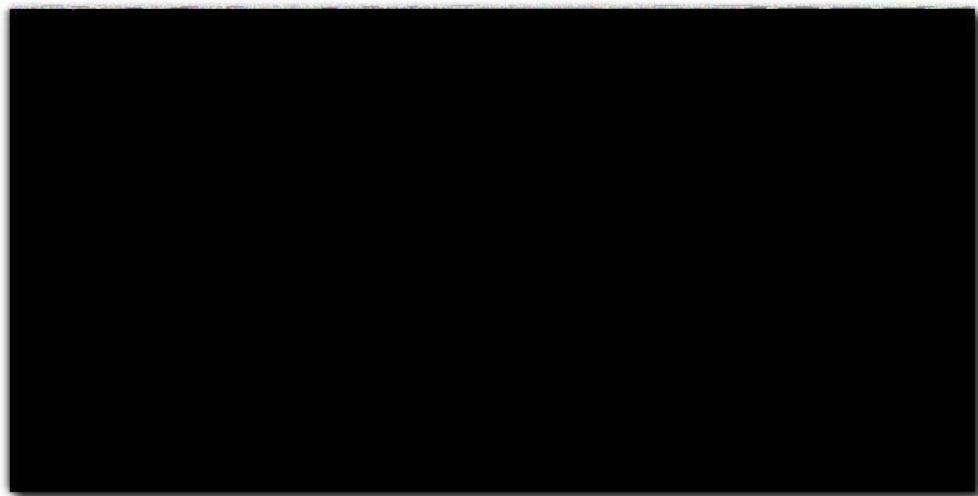
타임존 변경알림 기능이 On일 경우 사용자의 타임존과 NAC의 타임존이 다를 시 CWP 페이지에 아래와 같은 메시지를 출력합니다.



- 호스트명 변경

호스트명 변경 기능이 off인 상태에서 호스트명제한을 설정할 시 CWP(접속인증페이지)에 컴퓨터이름변경 아이콘이 보이지 않습니다. 호스트명 제한은 [노드정책](#)을 참고 바랍니다.





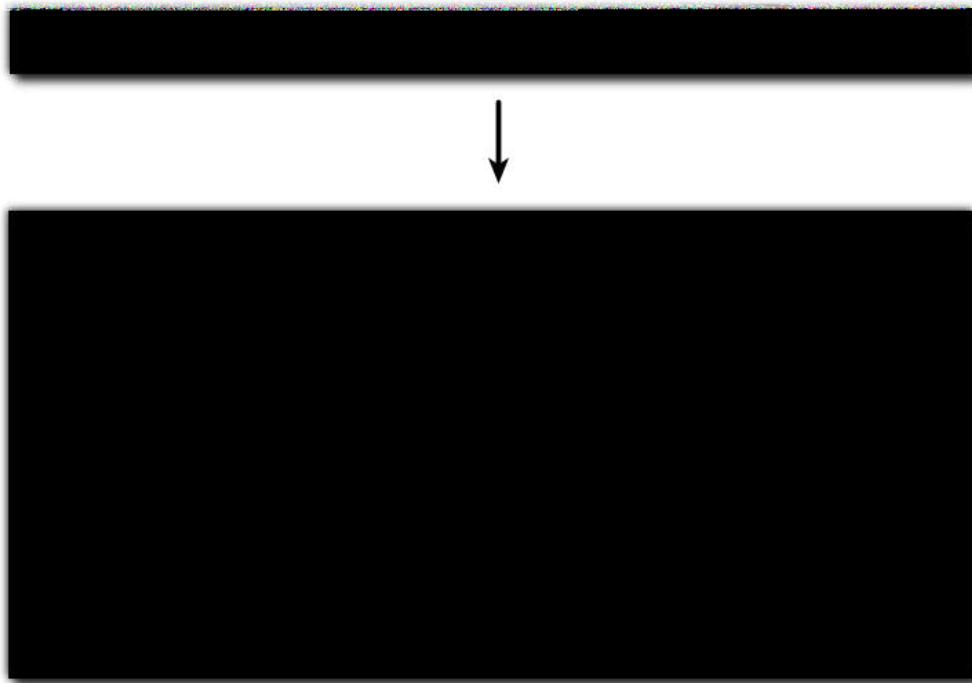
4. CWP 도메인 설정

CWP 도메인 설정은 CWP의 URL을 변경할 때 사용됩니다. 해당 기능을 사용하기 위해선 전용 DNS서버에 센터 IP를 등록 후 CWP 도메인 설정에 아래의 그림과 같이 원하는 도메인을 입력 합니다.



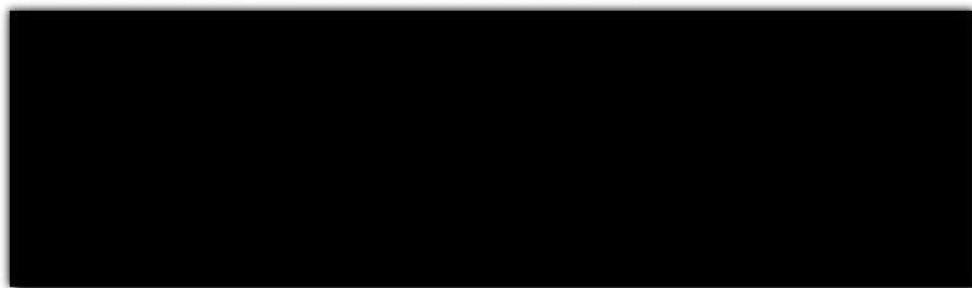
5. CWP SSL 사용

노드가 차단되어 CWP페이지로 접속될 경우 SSL 방식으로 접속합니다.



6. 세션 타임아웃

세션 타임아웃 설정이 5분으로 설정 후 CWP에 접속 후 어떠한 행위도 하지 않을 시 5분 후에 아래의 그림과 같이 자동으로 세션이 종료됩니다.



7. CWP 접근 허용 그룹

CWP 접근을 허용할 네트워크를 선택합니다. 허용 그룹에 포함되는 경우에만 CWP가 출력됩니다.

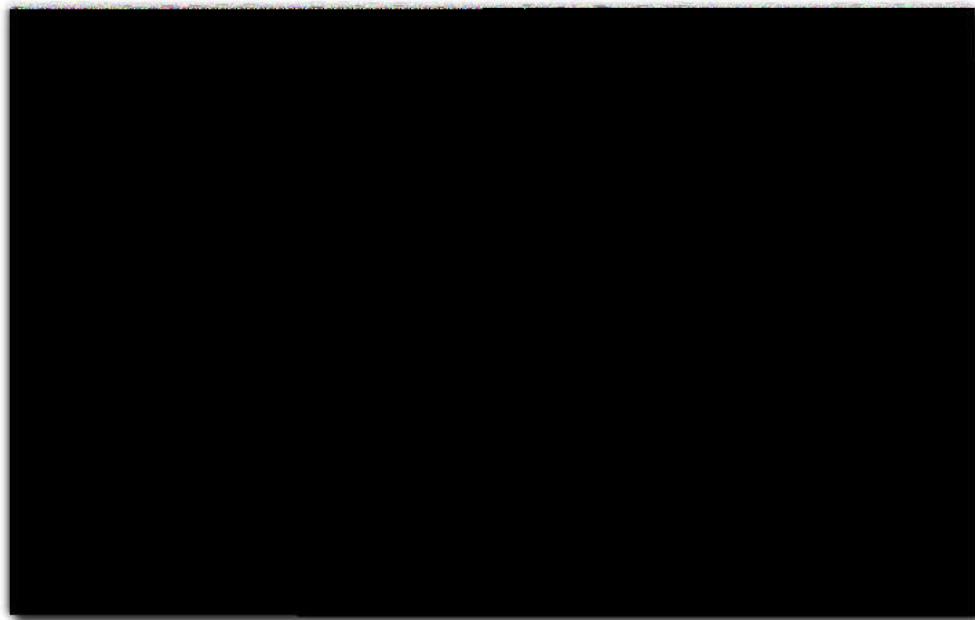


서비스

서비스

- RADIUS서버

RADIUS서버에서 RADIUS의 인증키, 접속허용그룹 등 RADIUS에 관련된 설정을 할 수 있습니다.



RADIUS 서버

RADIUS 서버

관리자는 설정 > 환경설정 > RADIUS 서버 페이지를 이용하여 RADIUS 서버에 관련된 설정을 할 수 있습니다.
RADIUS 기능이 필요한 경우 CLI에서 "RADIUS-Server enable"을 수행해야합니다.

- RADIUS Secret



설정 항목	설명
인증키	RADIUS 클라이언트의 인증키를 설정합니다. 인증키를 설정해야만 RADIUS 서버가 동작합니다. 인증키는 9~30자리 까지 설정할 수 있으며 문자, 숫자, 특수문자 모두 포함되어 있어야 합니다.
접속허용IP	RADIUS 서버에 접근 할 수 있는 IP를 설정합니다.

- RADIUS 인증서버



설정 항목	설명
포트 번호(Authentication)	인증서비스를 제공하기 위한 포트 번호를 입력합니다. 기본값 1812
EAP 인증	무선 AP 사용자 인증에서 사용되는 EAP 인증 기능을 사용할지의 여부를 선택합니다.
기본 EAP 유형(PEAP)	기본 EAP 인증 유형을 선택합니다.
격리 VLAN	RADIUS 인증 시 격리된 VLAN을 노드에 할당합니다. switch에 RADIUS 설정이 필요합니다.
VLAN 번호	격리 VLAN으로 할당할 VLAN 번호를 입력합니다.
노드 그룹	격리 VLAN을 할당할 노드 그룹을 설정합니다.
신규 노드	신규 노드를 격리 VLAN으로 할당할지 여부를 선택합니다.
VLAN 할당	RADIUS Attribute 매치 조건을 통한 지정된 VLAN을 할당 합니다.
MAC 인증	RADIUS 서버가 MAC 인증 요청을 받아들일지 여부를 선택합니다.
노드 그룹	MAC 인증 옵션이 on일 경우 활성화 되며, MAC 인증을 적용할 노드 그룹을 선택합니다.
Accounting 생성	사용자 인증 시 자체적으로 Accounting을 생성할지 여부를 선택합니다. (NAS 또는 AP가 Accounting을 지원하지 않을 경우 사용)
NAC 사용자 인증	NAC에 등록되어 있는 사용자들을 RADIUS 인증 시 허용할지 여부를 선택합니다.
Active Directory 인증 연동	Active Directory를 연동하여 인증을 허용할지의 여부를 선택합니다. AD 서버가 정상적으로 구동하지 않을 시 외부 사용자에 대한 인증이 정상적으로 수행되지 않습니다.
도메인 네임	Active Directory 서버의 도메인 네임을 입력합니다. (ex: site.com)

Domain Admin 계정 아이디	ActiveDirectory 서버의 Domain Admin 계정 아이디를 입력합니다.(초기값으로 Administrator가 입력되어 있습니다.)
Domain admin 계정 비밀번호	ActiveDirectory 서버의 Domain Admin 계정 비밀번호를 입력합니다.
외부 URL 인증연동	외부 URL에서 genianNAC 사용자 정보를 연동하여 genianNAC 사용자 ID로 외부 URL에 로그인 및 접속 할 수 있습니다.
URL	인증을 수행할 외부 URL을 입력합니다.
방식	GET,POST 중 호출방식을 선택합니다.
POST데이터	데이터를 입력합니다.(POST 방식에서만 사용)
결과검증 정규식	인증 성공을 판별할 수 있는 정규식을 입력합니다.
E-Mail 인증연동	E-Mail 서버를 연동하여 인증을 할지의 여부를 선택합니다. 해당 기능을 사용하기 위해서는 설정 > 환경설정 > 사용자인증 에서 POP3, IMAP 항목에 E-Mail 서버 정보를 설정해주어야 합니다.

- RADIUS Accounting Server

RADIUS 인증 시 별도의 NAC 사용자 인증 없이 한번에 AP를 사용할 수 있습니다. 즉 RADIUS 인증과 NAC 사용자 인증이 한번의 RADIUS인증으로 모두 처리가 됩니다.

설정 항목	설명
포트번호(Accounting)	인증서비스를 제공하기 위한 포트번호를 입력합니다. 기본값 1813
인증대체	RADIUS 인증대체를 사용할지 여부를 선택합니다.
패킷타입	처리할 Accounting 패킷의 Acct-Status-Type을 선택합니다. (Start:인증, Stop:인증해제)
노드검색방법	인증처리할 노드검색방법을 선택합니다. (MAC:Calling-Station-Id, IP:Framed-IP-Address)
적용대상	인증처리할 노드의 업다운 상태를 선택합니다.

사용자인증

사용자인증

- 사용자관리

비밀번호 정책, 휴면사용자 처리 여부 등 계정에 관련된 설정을 할 수 있습니다.



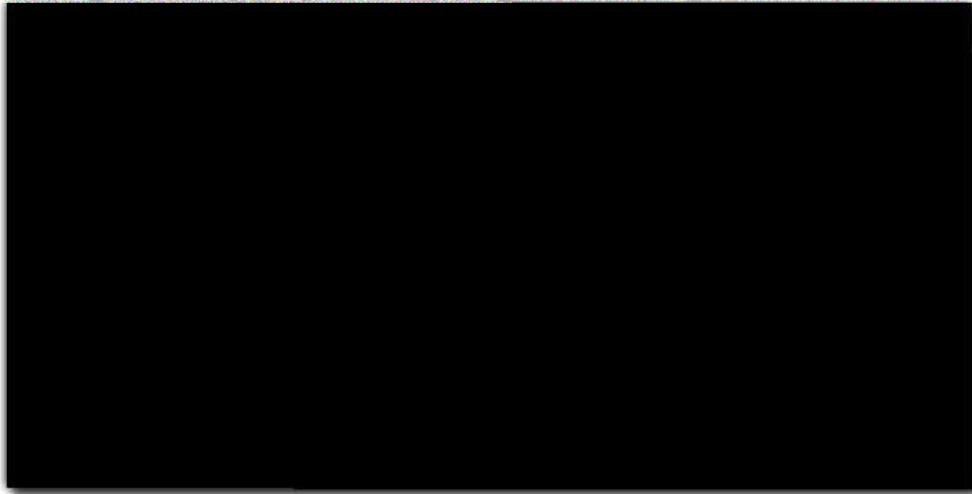
- 사용자 인증

LOAP, POP3, IMAP 인증연동 및 인증 관련 설정을 할 수 있습니다.



- 인증대체

RADIUS 인증을 NAC 인증으로 대체할 경우 관련된 설정을 할 수 있습니다.



- 사용자 정보 동기화

다른 데이터 베이스에 있는 계정 정보를 GrianNAC 데이터 베이스로 동기화 할 경우 관련된 설정을 할 수 있습니다.



- 관리역할

사용 가능한 관리역할을 확인할 수 있습니다.



사용자관리

사용자관리

사용자관리에 필요한 설정을 할 수 있습니다.

- 휴먼사용자

휴먼사용자 기준 및 중지여부를 설정 할 수 있습니다.

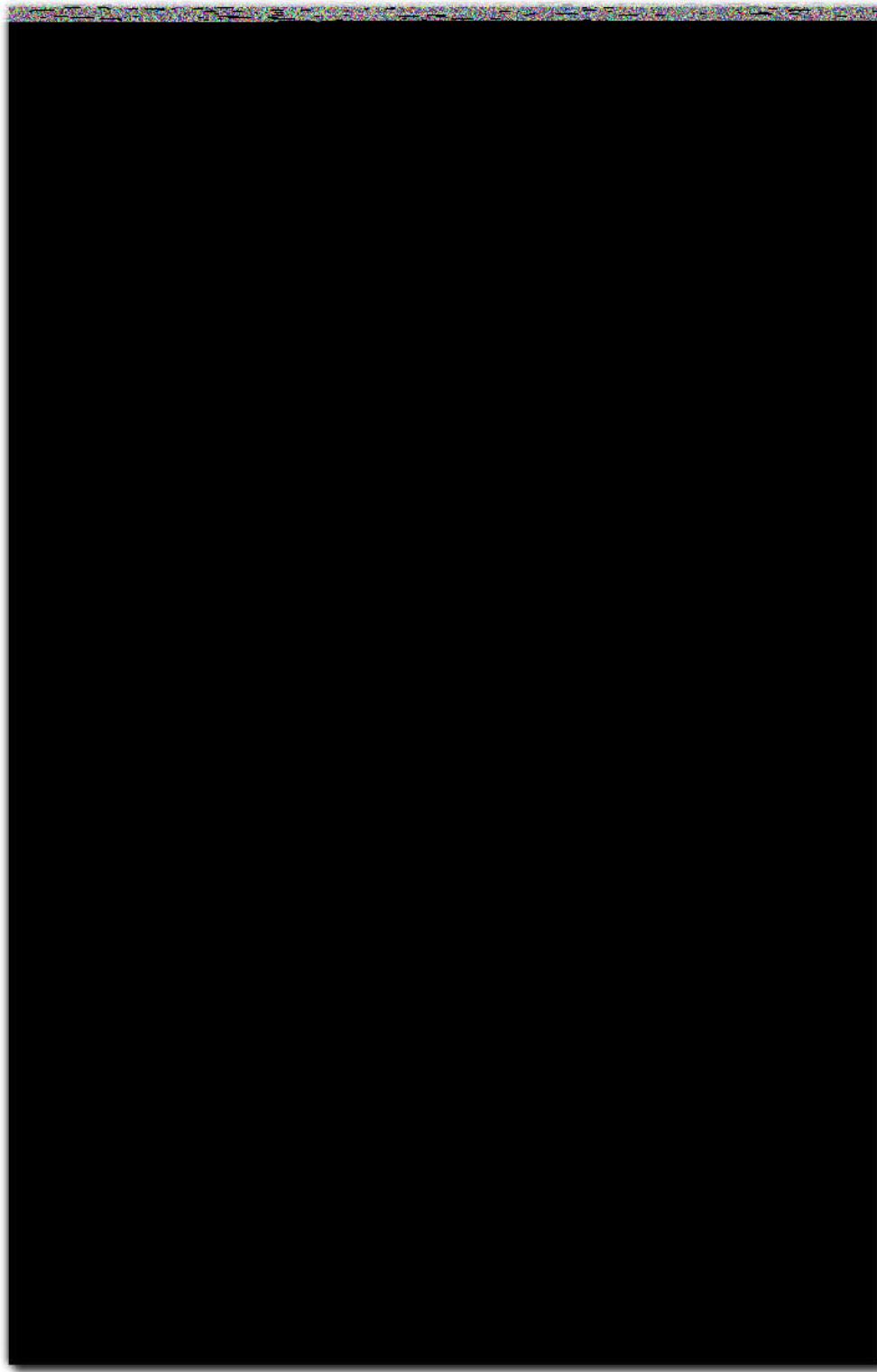


휴먼사용자에 대한 내용은 아래와 같습니다.

항목	옵션	내용
휴먼사용자중지	On, Off	장기간 로그인 기록이 없는 사용자를 사용중지상태로 전환시킬지의 여부를 선택합니다. 휴면기간의 단위에는 일, 주, 개월이 있습니다. default : 1개월 최소값 : 1일 최대값 : 없음
휴면기간	일, 주, 개월	설정한 기간동안 로그인 기록이 없을 시 휴먼사용자(사용중지)로 전환됩니다.
휴면관리자중지	On, Off	장기간 로그인 기록이 없는 관리자를 사용중지상태로 전환시킬지 여부를 선택합니다. (관리역할이 superAdmin인 계정은 제외)

- 비밀번호 정책

비밀번호 제한, 변경주기, 암호화 설정을 할 수 있습니다.



비밀번호 정책에 대한 내용은 아래와 같습니다.

항목이름	옵션	설명
비밀번호 저장방식	HMAC-SHA256	비밀번호가 HMAC-SHA256 방식으로 암호화 되어 저장 됩니다.
	Windows NT-Hash	비밀번호가 Windows NT-Hash 방식으로 암호화 되어 저장 됩니다.
최소길이	9~30 중 입력	사용자 등록할 때 비밀번호 자릿수가 입력한 값보다 미만일 경우 사용자등록을 할 수 없습니다.

최대길이	9~30 중 입력	사용자 등록할 때 비밀번호 자릿수가 입력한 값보다 초과할 경우 사용자등록을 할 수 없습니다.
문자로 시작	On, off	비밀번호를 설정할 때 첫번째 자리를 문자로 사용하여야 사용자 등록을 할 수 있습니다.
대/소문자 혼용	On, Off	비밀번호에 영문 대문자, 소문자를 사용하여야 사용자 등록을 할 수 있습니다.
문자반복 불가횟수	0, 임의 입력	비밀번호를 설정할 때 입력한 값 만큼 반복문자를 사용할 경우 사용자등록을 할 수 없습니다. 0을 입력할 시 문자반복 사용에 제한이 없습니다.
연속문자 불가횟수	0, 임의 입력	비밀번호를 설정할 때 입력한 값만큼 연속문자를 사용할 경우 사용자등록을 할 수 없습니다. 0을 입력할 시 연속문자 사용에 제한이 없습니다.
검증 정규식 사용	ON, Off	관리자가 정규식을 정하여 비밀번호를 검증할 수 있습니다.
검증 정규식	정규식 입력	검증 정규식이 ON일 때 입력 가능하며, 사용자 등록할 때 입력한 정규식을 이용하여 비밀번호를 검증 합니다.
검증 오류메시지	출력메시지 입력	사용자 등록할 때, 사용하려는 비밀번호가 검증 정규식에 맞지 않을 때 출력할 내용을 입력 합니다.
ID문자열 포함금지	On, Off	비밀번호에 ID문자열을 포함할 수 없도록 합니다.
Blacklist 단어 사용금지	On, Off	Blacklist 단어를 비밀번호에 포함할 수 없도록 합니다. Blacklist 단어들은 TXT파일로 Blacklist 파일 옵션에 업로드합니다.
Blacklist 파일	TXT 파일	업로드한 TXT 파일의 내용은 비밀번호에 포함할 수 없습니다. 업로드 가능한 최대 크기는 2GB이며 내용은 줄바꿈으로 구분합니다. 알파벳순서로 정렬되어 있어야합니다.
비밀번호변경	On, Off	주기적으로 비밀번호 변경을 권하거나 강제적으로 변경하도록 합니다.
변경주기	일, 주, 개월	비밀번호 변경 설정이 on일 때 변경주기를 설정할 수 있습니다. 변경주기는 일, 주, 개월으로 설정할 수 있으며, 사용자가 마지막으로 비밀번호를 변경 한 날짜에서 설정한 변경주기가 지나야지만 비밀번호 변경을 권하거나 강제적으로 변경하도록 합니다. default : 90일 최소값 : 1일 최대값 : 없음
변경방법	변경강제	변경주기에 설정된 주기가 됐을 시 비밀번호를 무조건 변경해야만 로그인을 할 수 있습니다.
	변경권유	변경주기에 설정된 주기가 됐을 시 비밀번호를 변경을 권유 합니다.
비밀번호만료전알림	분, 시간, 일, 주, 개월	비밀번호 변경주기 설정으로 비밀번호가 만료되기 전에 에이전트 메시지를 전송합니다.
과거비밀번호기억	0, 임의 입력	과거에 사용하던 비밀번호를 입력한 값만큼 기억하여 비밀번호 변경 시 과거에 사용하였던 비밀번호로 변경하지 못하도록 할 수 있습니다.
임시 비밀번호패턴	On, Off	임시비밀번호 발급 시 패턴문자열 항목에 설정된 매크로 패턴을 임시비밀번호로 발급합니다.
패턴문자열		사용자에게 발급할 임시비밀번호로 사용될 매크로를 설정합니다.

- 계정만료

계정만료 관련 설정을 할 수 있습니다.



계정만료에 대한 내용은 아래와 같습니다.

항목이름	옵션	설명
계정만료전알림	분, 시간, 일, 주, 개월	사용자계정에 계정사용만료 설정이 되어있을 경우 계정사용이 만료되기 전에 에이전트 메시지를 전송합니다.

- 사용자등록신청

사용자 신청 관련 설정 할 수 있습니다.



사용자등록신청에 대한 내용은 아래와 같습니다.

항목	옵션	내용
사용자 다중신청서 양식		CWP 페이지에서 다수의 사용자를 한번에 신청 시 필요한 양식을 Excel 파일로 작성하여 업로드할 수 있습니다. 업로드하지 않을 시 기본적으로 NAC에서 제공하는 양식을 사용합니다.
사용자신청 거부사유 입력	사용안함, 승인시, 거부시, 승인/거부시	관리자가 사용자신청을 거부 및 승인 시 사유를 입력하는 팝업 창을 띄웁니다.

사용자인증

사용자인증

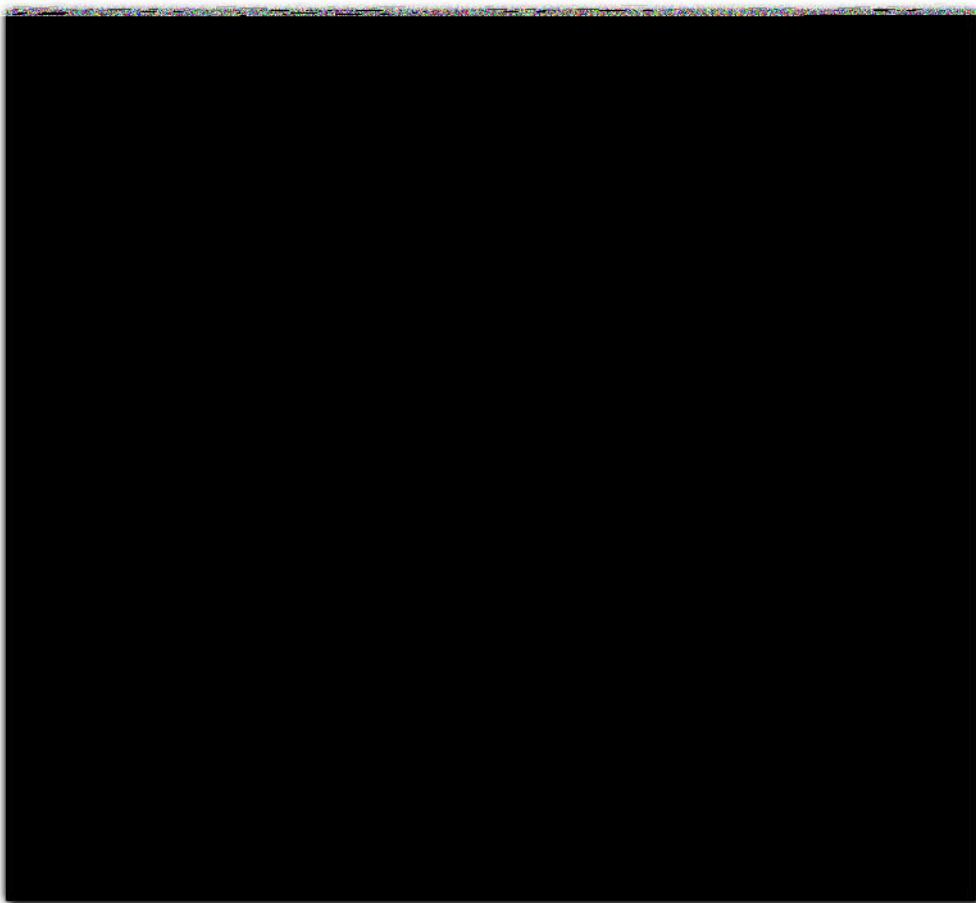
사용자인증 페이지 설정 > 환경설정 > 사용자인증 를 이용하여 사용자인증에 관한 설정을 할 수 있습니다.



인증연동 기능들을 사용할 경우 외부서버에서 NAC만 접근할 있도록 접근을 통제해야 하며, 인증연동에 필요한 항목들을 모두 충족하여야 합니다.

- **인증옵션**

인증범위, 인증허용 IP 설정, 소유자 설정등을 할 수 있습니다.



인증옵션 부분의 항목과 설명은 아래 표와 같습니다.

항목이름	설정 값	설명
인증범위	노드	인증범위가 노드일 경우, 사용자 인증시 IP와 인증값이 매핑됩니다. 인증 후, IP가 변경되면 재인증을 거쳐야 합니다.
인증허용 IP 설정	ON, OFF	사용자 인증 시 최초, 또는 인증허용 IP 설정이 존재하지 않을 경우 해당 노드의 IP가 사용자의 인증허용 IP로 설정 됩니다.
	장비	인증범위가 장비일 경우, 사용자 인증시 MAC과 인증값이 매핑됩니다. 인증 후, IP가 변경되어도 인증상태가 유지됩니다.
소유자 설정	ON,OFF	사용자 인증시 해당 IP 또는 장비의 소유자를 인증받은 사용자로 자동설정할지의 유무를 선택합니다.
설정범위	IP	노드상세정보 > IP관리 > IP정책 의 소유자를 현재 인증자로 설정합니다.
	장비	노드상세정보 > IP관리 > MAC정책 의 소유자를 현재 인증자로 설정합니다.
	IP+장비	노드상세정보 > IP관리 > IP관리/MAC정책 의 소유자를 모두 현재 인증자로 설정합니다.
재설정 여부	미설정시	소유자가 미설정 되어있을 경우 최초의 인증자로 소유자를 설정하고, 그 후에 다른 사용자가 인증하여도 소유자가 변경되지 않습니다.

	인증시마다	소유자가 설정되어 있어도, 해당 노드에 인증하는 사용자가 바뀔 경우, 현재 인증된 사용자로 소유자를 설정합니다.
사용자ID 정규식적용	정규식	사용자 인증 시 설정된 정규식 패턴에 일치하는 아이디로 인증처리를 위한 설정을 합니다.
사용자인증시 ID보호	ON, OFF	사용자인증 시 입력하는 ID가 *로 표시되며, 인증받은 ID도 *로 표시합니다.
로그아웃 사용	ON, OFF	인증사용자 옆 부분에 로그아웃 기능이 추가됩니다.
아이디/비밀번호 찾기	ON, OFF	로그인창 하단에 아이디/비밀번호 찾기 기능이 추가 됩니다.
아이디찾기	사용안함	아이디 찾기 기능을 사용하지 않습니다.
	SMS/이메일 인증 선택	사용자 ID에 등록된 휴대폰 번호와 전자우편 주소를 이용하여 휴대폰 인증과 이메일 인증을 하며, 원하는 한가지 인증 방식을 선택하여 인증을 받아 아이디를 찾을 수 있습니다.
	SMS 인증	사용자 ID에 등록된 휴대폰 번호를 이용하여 아이디를 찾을 수 있습니다.
	이메일 인증	사용자 ID에 등록된 전자우편 주소를 이용하여 아이디를 찾을 수 있습니다.
비밀번호찾기	사용안함	비밀번호 찾기 기능을 사용하지 않습니다.
	SMS/이메일 인증 선택	사용자 ID에 등록된 휴대폰 번호와 전자우편 주소를 이용하여 휴대폰 인증과 이메일 인증을 하며, 원하는 한가지 인증 방식을 선택하여 인증을 받아 비밀번호를 찾을 수 있습니다.
	SMS 인증	사용자 ID에 등록된 휴대폰 번호를 이용하여 비밀번호를 찾을 수 있습니다.
	이메일 인증	사용자 ID에 등록된 전자우편 주소를 이용하여 비밀번호를 찾을 수 있습니다.
	보안질문	비밀번호 찾기만 가능한 방식이며, 사용자 ID에 등록된 보안질문의 답을 이용하여 비밀번호를 찾을 수 있습니다.
보안질문 설정	사용자 필드	설정 > 속성관리 > 추가필드관리 > 사용자에 보안질문 입력 타입으로 설정된 필드를 보안질문으로 설정할 수 있습니다.
사용자인증정보표시	ON, OFF	사용자 인증 시 우측 상단에 사용자 이름이 표시됩니다. 표시된 사용자 이름을 클릭하여 사용자 정보를 수정할 수 있습니다.
사용자정보 노드반영	ON, OFF	사용자등록신청서 승인 시 사용자의 신청사유와 이름이 인증한 PC 노드정보의 설명과 이름에 출력됩니다.

인증연동

인증연동

외부인증서버를 이용하여 NAC 사용자 인증을 받을 수 있습니다.

- RADIUS 인증연동

RADIUS 인증연동을 사용 시 별도의 NAC 사용자 인증 없이 한번에 AP를 사용할 수 있습니다. 즉 RADIUS 인증과 NAC 사용자 인증이 한번의 RADIUS 인증으로 모두 처리가 됩니다.

RADIUS 기능이 필요한 경우 CLI에서 "RADIUS-Server enable"을 수행해야 합니다.



설정항목	설명
서버주소	RADIUS 인증 연동 시 사용할 RADIUS서버 IP주소를 입력합니다.
서버포트	RADIUS 서버 포트번호를 입력합니다.
인증키	RADIUS 서버의 인증키를 입력합니다.

- LDAP 인증연동



LDAP 인증연동에 대한 항목과 내용은 아래와 같습니다.

항목	내용
서버주소	LDAP 인증연동을 위한 서버시스템의 주소/도메인을 설정합니다.
서버포트	LDAP 서비스 포트번호를 설정합니다.
Base DN	LDAP Base DN을 설정합니다. (예 : CN = Users, DC = geni, DC = geninetworks, DC = com)
Bind DN	사용자 검색을 위한 Bind DN 값을 설정합니다, Anonymous검색이 가능할 경우 공백.
Bind Password	사용자 검색을 위한 Bind DN 비밀번호를 설정합니다.
Search Attribute	사용자 ID를 담고있는 속성값 이름(ActiveDirectory : sAMAccountName)
SSL 접속	SSL연결을 사용할지 여부를 선택합니다.
Secondary LDAP사용	LDAP 서버 인증연동이 추가적으로 필요한 경우 여부를 선택합니다.

- POP3 인증연동



pop3 인증연동에 대한 항목과 내용은 아래와 같습니다.

항목	내용
POP3 서버	POP3 사용자 연동 시 사용할 POP3 서버 주소를 입력합니다.
POP3 포트	POP3 서버 접속포트를 입력합니다. (Plain : 110, SSL : 995)
사용자도메인	인증 시 사용자ID에 첨부할 도메인명을 입력합니다. (예 : abc.com)

- IMAP 인증연동



IMAP 인증연동에 대한 항목과 내용은 아래와 같습니다.

항목	내용
IMAP 서버	IMAP 사용자 연동 시 사용할 IMAP 서버 주소를 입력합니다.
IMAP 포트	IMAP 서버 접속포트를 입력합니다. (Plain : 143, SSL : 993)
사용자도메인	인증 시 사용자 ID에 첨부할 도메인명을 입력합니다. (예 : abc.com)

- SMTP 인증연동



SMTP 인증연동에 대한 항목과 내용은 아래와 같습니다.

항목	내용
SMTP 서버	SMTP 사용자 연동 시 사용할 SMTP 서버 주소를 입력합니다.
SMTP 포트	SMTP 서버 접속포트를 설정합니다. (Plainin : 25, SSL : 465)
사용자도메인	인증시 사용자 ID에 첨부할 도메인명을 입력합니다. (예 : abc.com)

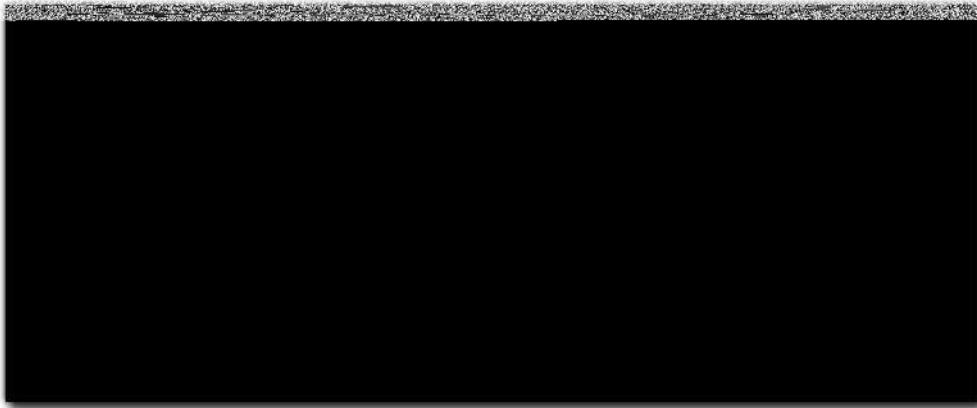
- Webhook 인증연동



Webhook 인증연동에 대한 항목과 내용은 아래와 같습니다.

항목	내용
URL	인증을 수행할 외부 URL을 입력합니다.
방식	GET,POST 중 호출방식을 선택합니다.
결과검증 정규식	인증 성공을 판별할 수 있는 정규식을 입력합니다.

- SAML2 인증연동



SAML2 인증연동에 대한 항목과 내용은 아래와 같습니다.

항목	내용
SP Entity ID	SAML 인증업체(IdP)의 SAML 설정시 Entity ID에 위의 값을 복사하여 입력하시기 바랍니다.
SP ACS URL	SAML 인증업체(IdP)에서 인증 후 인증결과를 받을 주소입니다. IdP의 SAML 설정시 ACS URL에 위의 값을 복사하여 입력하시기 바랍니다.
IdP Entity ID	SAML 인증업체(IdP)에서 제공하는 Entity ID를 입력하시기 바랍니다.
IdP SSO URL	SAML 인증업체(IdP)에서 제공하는 SSO URL을 입력하시기 바랍니다.
x509 Certificate	SAML 인증업체(IdP)에서 제공하는 X.509 Certificate 값을 입력하시기 바랍니다.

- 인증테스트



인증테스트에 대한 항목과 내용은 아래와 같습니다.

항목	내용
인증테스트	사용자 인증을 테스트해 볼 수 있습니다. 테스트 팝업창이뜨면 인증정보 저장소와 아이디 비밀번호를 입력하여 인증과정을 테스트할 수 있습니다.

정보 동기화

정보 동기화

외부에 존재하는 정보(Data base)를 GenianNAC Data DB에 동기화시키는 기능을 제공합니다. 이를 위해서 별도의 독립 실행모듈(authsync)과 실행모듈이 수행하는데 필요한 설정파일을 제공합니다.



- 정보 동기화 시 동기화하려는 ID와 GenianNAC에 있는 ID와 동일 할 시 해당 ID만 동기화 되지 않으며 GenianNAC에 있는 ID는 그대로 남아있습니다.
- 오타를 입력할 시 동기화가 되지 않을 수 있으니 주의바랍니다.

정보 동기화 추가

관리자는 동기화할 정보가 담겨있는 데이터베이스의 설정을 입력하여, 정보를 손쉽게 동기화할 수 있습니다.

설정 > 환경설정 > 정보 동기화 > 작업선택 > 추가 를 선택하고, 내용을 기입합니다.

- 기초정보

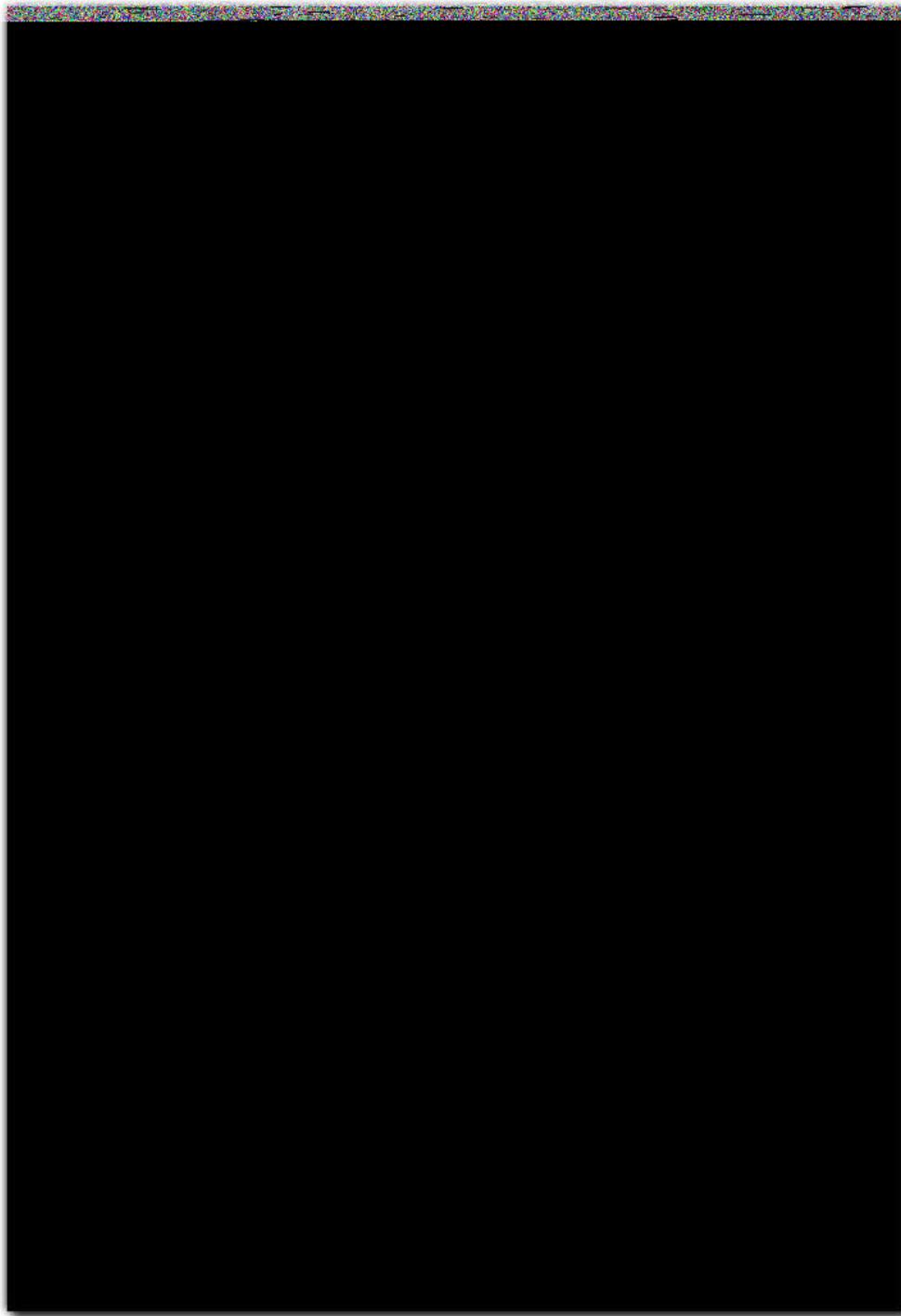
정보 동기화를 위해 필요한 기초정보를 입력합니다.

항목	옵션	내용
ID		정보 동기화를 식별할 ID를 입력합니다.
설명		주의사항이나 추가적 설명이 필요할 경우 입력합니다.
동기화 수행주기	동기화 수행안함	동기화를 수행하지 않습니다.
	매일 지정된 시각	지정시각을 설정하고 매일 설정한 시각마다 동기화를 수행합니다.
	지정된 시간마다	시간주기를 설정하고 설정한 시간주기마다 동기화를 수행합니다.
지정시각		동기화 수행주기 옵션이 매일 지정된 시각 일 경우 활성화 되며, 매일 동기화할 시각을 hh:mm 형식으로 입력합니다.
시간주기	분, 시간, 일, 주, 개월	동기화 수행 옵션이 지정된 시각 일 경우 활성화 되며, 동기화 수행 주기 시간을 설정합니다.
정책적용여부	적용함	정보 동기화를 수행합니다.
	사용안함	정보 동기화를 수행하지 않습니다.

환경변수 설정		DB타입이 서로 다를 경우 환경변수가 필요할 수 있습니다. 필요한 환경변수를 입력합니다.
사용자정의쿼리		필요한 쿼리문을 작성할 시 해당 쿼리문을 수행합니다.

- 기본정보

정보 동기화를 위한 기본 설정을 합니다.

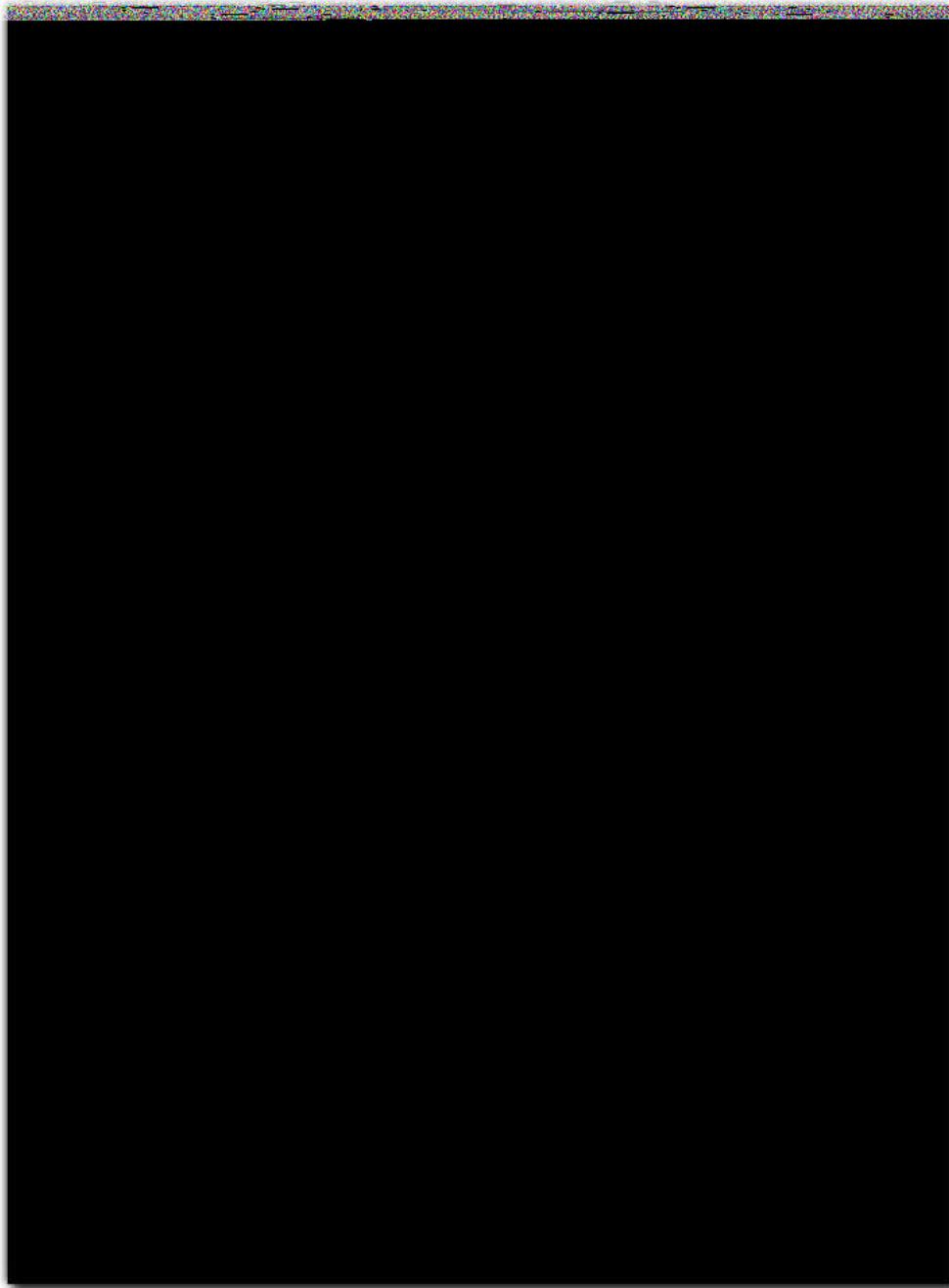


항목	옵션	내용
통신시 Charset		GENIAN DB server와의 통신시 사용할 charset지정 합니다. 예를 들어 DB타입이 CSV인경우 파일내의 한글이 euckr로 되어 있다면 euckr로 설정합니다.
DB타입	ORACLE	정보 동기화할 DB의 타입이 ORACLE일 경우 설정합니다.
	MYSQL	정보 동기화할 DB의 타입이 MYSQL일 경우 설정합니다.

	MSSQL/Sybase	정보 동기화할 DB의 타입이 MSSQL/Sybase일 경우 설정합니다.
	IBM DB2	정보 동기화할 DB의 타입이 IBM DB2일 경우 설정합니다.
	Tibero	정보 동기화할 DB의 타입이 Tibero일 경우 설정합니다.
	Altibase	정보 동기화할 DB의 타입이 Altibase일 경우 설정합니다.
	PostgreSQL	정보 동기화할 DB의 타입이 PostgreSQL일 경우 설정합니다.
	LDAP	정보 동기화할 DB의 타입이 LDAP일 경우 설정합니다.
	CSV	정보 동기화할 DB의 타입이 CSV일 경우 설정합니다.
	CSV(Upload)	정보 동기화할 DB타입이 CSV일 경우 설정합니다, CSV와 다른점은 파일을 URL이 아닌 직접 CSV 파일을 업로드하는 방식입니다.
	CUBRID	정보 동기화할 DB타입이 CUBRID일 경우 설정합니다.
	Google G Suite	정보 동기화할 DB타입이 Google G Suite일 경우 설정합니다.
DB SERVER		동기화할 DB SERVER의 IP 또는 이름을 설정합니다.
DB PORT		동기화할 DB의 PORT를 설정합니다, DB별 default PORT는 Oracle(1521), MSSQL/Sybase(1433), MySQL(3306), Tibero(8629), LDAP(389) 입니다.
DB USER		DB의 USER을 입력합니다, DB 타입이 LDAP 일 경우 DB USER에 Bind DN을 입력합니다.
DB PASSWORD		DB의 패스워를 입력합니다, LDAP일 경우 Bind DN을 입력합니다.
DB SID/NAME		DB의 NAME를 입력합니다.
TDS version		DB타입 설정이 MSSQL/Sybase 일 경우 TDS protocol version 을 선택합니다.
DB Charset		DB타입 설정이 ORACLE일 경우 활성화 되며, 연동할 ORACLE DB의 Charset을 설정합니다.
데이터소스 구분값		다수의 소스로 부터 동기화를 수행할 경우 데이터소스 구분값을 확인하여 동기화 시 다른 DB의 데이터는 삭제되지 않도록 합니다.
컬럼구분자		DB타입 설정이 CSV일 경우 활성화 되며, CSV 파일의 구분자를 입력합니다.
사용자정보파일		DB타입 설정이 CSV일 경우 활성화 되며, 외부 서버에 CSV파일이 저장되어 있을 경우 URL을 입력하여 외부 서버에 있는 CSV파일을 동기화할 수 있습니다, 해당 항목은 사용자 정보를 담고 있는 CSV파일을 동기화합니다.
사용자정보파일(업로드)		DB타입 설정이 CSV(Upload)일 경우 활성화 되며, 동기화할 CSV 파일을 업로드합니다, 해당 항목은 사용자 정보를 담고 있는 CSV파일을 동기화합니다.
부서정보파일		DB타입 설정이 CSV일 경우 활성화 되며, 외부 서버에 CSV파일이 저장되어 있을 경우 URL을 입력하여 외부 서버에 있는 CSV파일을 동기화할 수 있습니다, 해당 항목은 부서 정보를 담고 있는 CSV파일을 동기화합니다.
부서정보파일(업로드)		DB타입 설정이 CSV일 경우 활성화 되며, 동기화할 CSV 파일을 업로드합니다, 해당 항목은 부서 정보를 담고 있는 CSV파일을 동기화합니다.
직급정보파일		DB타입 설정이 CSV일 경우 활성화 되며, 외부 서버에 CSV파일이 저장되어 있을 경우 URL을 입력하여 외부 서버에 있는 CSV파일을 동기화할 수 있습니다, 해당 항목은 직급 정보를 담고 있는 CSV파일을 동기화합니다.
직급정보파일(업로드)		DB타입 설정이 CSV일 경우 활성화 되며, 동기화할 CSV 파일을 업로드합니다, 해당 항목은 직급 정보를 담고 있는 CSV파일을 동기화합니다.
노드정보파일		DB타입 설정이 CSV일 경우 활성화 되며, 외부 서버에 CSV파일이 저장되어 있을 경우 URL을 입력하여 외부 서버에 있는 CSV파일을 동기화할 수 있습니다, 해당 항목은 노드 정보를 담고 있는 CSV파일을 동기화합니다.
노드정보파일(업로드)		DB타입 설정이 CSV일 경우 활성화 되며, 동기화할 CSV 파일을 업로드합니다, 해당 항목은 노드 정보를 담고 있는 CSV파일을 동기화합니다.

- 사용자 정보

사용자 정보 동기화에 필요한 컬럼명 및 인증 관련 설정을 합니다.



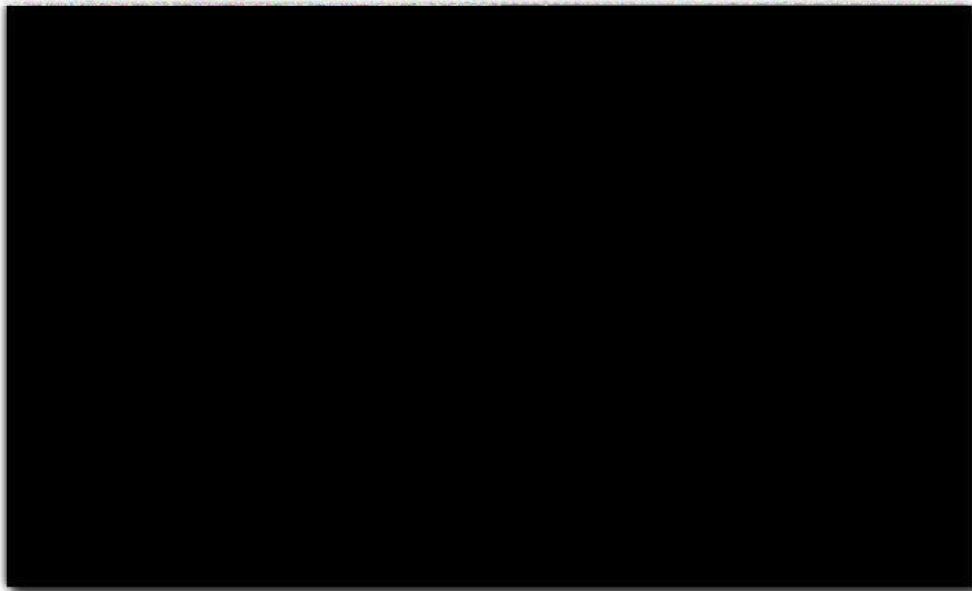
항목	옵션	내용
사용자테이블명		동기화할 사용자 정보가 담겨 있는 테이블명을 입력합니다. RDBMS의 경우 테이블이름, LDAP의 경우 Base DN, CSV인 경우는 사용하지 않습니다.
사용자조건문		동기화를 수행할 조건을 쿼리로 입력합니다. 입력한 조건을 충족한 사용자는 동기화를 수행하고 조건을 충족하지 않은 사용자는 삭제처리가 되고 동기화를 수행하지 않습니다. LDAP인 경우 filter 사용. filter 예제: (objectClass=person)
사용자ID컬럼명		사용자테이블명 항목에 입력한 테이블에서 사용자ID 정보가 들어있는 컬럼명을 입력합니다. 우측의 둘음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
사용자이름컬럼명		사용자테이블명 항목에 입력한 테이블에서 사용자이름 정보가 들어있는 컬럼 명을 입력합니다. 우측의 둘음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.

패스워드컬럼명		사용자테이블명 항목에 입력한 테이블에서 패스워드 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
원본 암호화 알고리즘		동기화 DB에서 사용하는 암호화 알고리즘을 선택합니다. GenianNAC가 지원하는 암호화 알고리즘은 MySQL PASSWORD, MD5, SHA1, SHA256, SHA384, SHA512, HMAC-SHA256, BASE64_ENCODE, Windeows NT-Hash, StoredFunction, Plain Text 입니다.
로컬 암호화 알고리즘		원본 암호화 알고리즘 설정이 Plain Text 일 경우 활성화 되며, 동기화 할 때 Plain Text인 암호를 암호화할 알고리즘을 선택합니다. GenianNAC가 지원하는 암호화 알고리즘은 MySQL PASSWORD, MD5, SHA1, SHA256, BASE64_ENCODE, Windeows NT-Hash, StoredFunction, Plain Text 입니다.
변경시각 컬럼명		사용자테이블명 항목에 입력한 테이블에서 최근 비밀번호를 변경한 시각 정보가 들어있는 컬럼 명을 입력합니다. 해당 항목을 이용할 시 변경시각 비교컬럼명 항목의 설정은 무시합니다.
변경시각 비교컬럼명		사용자테이블명 항목에 입력한 테이블에서 최근 비밀번호를 변경한 시각 정보가 들어있는 컬럼 명을 입력합니다. 동기화 되는 최근 비밀번호 변경 시각이 현재 사용자에게 등록되어 있는 최근 비밀번호 변경 시각보다 과거일 시 동기화 하지 않습니다.
패스워드암호화알고리즘컬럼명		사용자테이블명 항목에 입력한 테이블에서 패스워드암호화알고리즘 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
회사이름컬럼명		사용자테이블명 항목에 입력한 테이블에서 회사이름 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
부서이름컬럼명		사용자테이블명 항목에 입력한 테이블에서 부서이름 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
직급컬럼명		사용자테이블명 항목에 입력한 테이블에서 직급 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
전화번호컬럼명		사용자테이블명 항목에 입력한 테이블에서 전화번호 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
휴대폰컬럼명		사용자테이블명 항목에 입력한 테이블에서 휴대폰 번호 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
이메일컬럼명		사용자테이블명 항목에 입력한 테이블에서 이메일컬럼명 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
주소컬럼명		사용자테이블명 항목에 입력한 테이블에서 주소정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
설명컬럼명		사용자테이블명 항목에 입력한 테이블에서 사용자에 대한 설명 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 사용자ID를 동기화할 수 있습니다.
추가정보1~9컬럼명		사용자테이블명 항목에 입력한 테이블에서 추가적으로 필요한 정보가 들어있는 컬럼명을 입력합니다. 해당 컬럼에 동기화된 정보는 설정 > 속성관리 > 추가필드관리 > 사용자에서 사용필드를 USER_CUSTOM01~09 설정하여 필드를 생성한 후 설정 > 속성관리 > 용도관리 > 사용자용도에서 용도별 계정정보에 필드를 할당하여야 사용자 정보에서 확인할 수 있습니다. 필드 생성방법은 추가필드관리 를 참고바랍니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 추가정보를 동기화할 수 있습니다.
사용자용도	일반계정	동기화된 사용자ID의 용도가 일반계정으로 설정되어 동기화됩니다. 단 사용자 생성시에만 반영됩니다.
	임시계정	동기화된 사용자ID의 용도가 임시계정으로 설정되어 동기화됩니다. 단 사용자 생성시에만 반영됩니다.
계정수정설정	로컬계정으로설정	동기화된 사용자를 관리자가 생성한 계정처럼 사용자를 생성합니다. 수정할 수 있는 항목은 모든정보수정가능 옵션의 설정을 참고바랍니다.
	모든정보수정불가	관리자는 동기된 사용자 정보를 수정할 수 없습니다. 사용자는 직접 CWP페이지에서 사용자 인증을 받아 전화번호, 휴대폰, 전자우편 등의 사용자 추가정보를 수정할 수 있습니다.

	비밀번호수정가능	관리자는 동기화된 사용자의 비밀번호 정보를 수정할 수 있으며 그외 다른 정보는 수정할 수 없습니다. 사용자는 직접 CWP페이지에서 사용자 인증을 받아 비밀번호, 전화번호, 휴대폰, 전자우편 등의 사용자 추가정보를 수정할 수 있습니다.
	모든정보수정가능	관리자는 동기화된 사용자의 모든 정보를 수정할 수 있습니다. 사용자는 직접 CWP페이지에서 사용자 인증을 받아 비밀번호, 전화번호, 휴대폰, 전자우편 등의 사용자 추가정보를 수정할 수 있습니다.
인증IP 개수제한		동기화된 사용자 ID를 이용하여 중복 인증을 허용할 IP 개수를 설정합니다. 0으로 입력 시 어떠한 IP도 인증 가능합니다. 기본값은 0이며, 0~65535 까지 설정할 수 있습니다.
인증MAC 개수제한		동기화된 사용자 ID를 이용하여 중복 인증을 허용할 MAC 개수를 설정합니다. 0으로 입력 시 어떠한 MAC도 인증 가능합니다. 기본값은 0이며, 0~65535 까지 설정할 수 있습니다.
인증처리 IP 컬럼명		인증처리할 IP 정보들이 들어있는 컬럼명을 입력합니다. 해당 컬럼에 들어있는 IP들은 동기화를 수행할 때 자동으로 인증처리가 됩니다. 인증처리 MAC 컬럼명 설정이 되어 있을 시 IP와 MAC이 모두 맞아야 자동으로 인증처리됩니다.
인증처리 MAC 컬럼명		인증처리할 MAC 정보들이 들어있는 컬럼명을 입력합니다. 해당 컬럼에 들어있는 MAC들은 동기화 수행할 때 자동으로 인증처리가 됩니다. 인증처리 IP 컬럼명이 설정이 되어 있을 시 IP와 MAC이 모두 맞아야 자동으로 인증처리됩니다.
기본인증노드 인증해제	설정	삭제사용자처리에 따라 사용자 삭제/중지 될 경우 사용자 삭제/중지가 수행되기 이전에 해당 ID로 사용자 인증을 수행했을 때 삭제사용자처리에 따라 사용자 삭제/중지가 수행될 때 동시에 인증이 해제됩니다.
	해제	삭제사용자처리에 따라 사용자 삭제/중지 될 경우 사용자 삭제/중지가 수행되기 이전에 해당 ID로 사용자 인증을 수행했을 때 삭제사용자처리에 따라 사용자 삭제/중지가 수행되어도 인증이 해제되지 않고 남아있습니다.
삭제사용자처리	테이블에서 삭제	동기화 후 다시 동기화할 때 동기화할 DB에서 동기화된 ID를 삭제하고 동기화할 시 GenianNAC DB에 동기화되어 있던 ID가 삭제됩니다.
	사용중지 처리	동기화 후 다시 동기화할 때 동기화할 DB에서 동기화된 ID를 삭제하고 동기화 할 시 GenianNAC DB에 동기화되어 있던 ID는 사용중지 처리가 됩니다.
	아무 처리하지 않음	동기화 후 다시 동기화할 때 동기화할 DB에서 동기화된 ID를 삭제하고 동기화 할 시 GenianNAC DB에 동기화되어 있던 ID 정보를 그대로 보존합니다.
	삭제/중지 처리 유보기간	삭제사용자처리 옵션이 테이블삭제, 사용중지 일 경우 활성화되며, 설정된 유보기간이 지난 후 테이블 삭제, 사용중지 처리 됩니다.
인증해제 컬럼		GenianNAC DB의 컬럼을 지정하며 컬럼명을 작성할 시 "USER_" 부분을 제외한 나머지 부분을 작성합니다. 설정한 컬럼의 내용이 변경될 시 사용자 인증이 해제됩니다.
	설정	사용자 정보 동기화할 때 사용자 생성/변경에 대한 로그를 기록합니다.
	해제	사용자 정보 동기화할 때 사용자 생성/변경에 대한 로그를 기록하지 않습니다.
		동기화된 사용자 ID를 이용하여 인증할 때 인증을 허용할 IP를 입력합니다. 입력한 IP 외 다른 IP는 인증을 할 수 없습니다.
인증허용MAC		동기화된 사용자 ID를 이용하여 인증할 때 인증을 허용할 MAC를 입력합니다. 입력한 MAC 외 다른 MAC는 인증을 할 수 없습니다.
인증장비 개수제한		동기화된 사용자 ID를 이용하여 중복으로 인증할 디바이스의 개수를 설정합니다. 0으로 입력할 시 디바이스 개수를 제한하지 않습니다.
인증제한 예외 노드그룹		인증 제한을 예외시킬 노드그룹을 할당합니다. 할당한 노드그룹에 포함되는 노드는 IP/MAC/장비 인증제한, 인증허용 IP/MAC 옵션에 제한받지 않습니다.

- 부서정보

부서 동기화에 필요한 컬럼명을 입력합니다.



항목	옵션	내용
부서테이블명		동기화할 부서 정보가 들어있는 테이블명을 입력합니다.
부서조건문		데이터를 읽어올 데이터베이스의 사용자테이블에 대한 쿼리 WHERE 조건문을 설정합니다. LDAP인경우 filter사용. filter 예제: (objectClass=person)
출력정렬순서		부서목록이 출력될때의 정렬순서를 설정합니다. 정렬순서 정보를 가진 컬럼을 입력할 때는 반드시 문자열형이여야 하며 숫자형(int)컬럼일 경우 TRIM(TO_CHAR(컬럼명,'0000'))으로 입력하여야 합니다.
최상위부서 제외여부	해제	부서코드와 상위 부서가 같을 경우에도 해당 부서를 동기화 합니다.
	설정	부서코드와 상위 부서가 같을 경우 해당 부서는 동기화 하지 않습니다.
부서ID컬럼명		부서테이블명 항목에 입력한 테이블에서 부서 코드 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 부서를 동기화할 수 있습니다.
부서이름컬럼명		부서테이블 항목에 입력한 테이블에서 부서 이름 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 부서를 동기화할 수 있습니다.
상위부서컬럼명		부서테이블 명 항목에 입력한 테이블에서 상위 부서 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 부서를 동기화할 수 있습니다.
추가정보6컬럼명		부서테이블명 항목에 입력한 테이블에서 추가적으로 필요한 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 추가정보를 동기화할 수 있습니다.
추가정보7컬럼명		부서테이블명 항목에 입력한 테이블에서 추가적으로 필요한 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 추가정보를 동기화할 수 있습니다.
추가정보8컬럼명		부서테이블명 항목에 입력한 테이블에서 추가적으로 필요한 정보가 들어있는 컬럼명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 추가정보를 동기화할 수 있습니다.

- 직급정보

직급 동기화에 필요한 컬럼명을 입력합니다.



항목	내용
직급 테이블명	동기화할 직급 정보가 들어있는 테이블명을 입력합니다.
직급조건문	데이터를 읽어올 데이터베이스의 사용자테이블에 대한 쿼리 WHERE 조건문을 설정합니다. LDAP인경우 filter사용. filter 예제: (objectClass=person)
직급ID컬럼명	직급테이블명 항목에 입력한 테이블에서 직급 코드 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 직급을 동기화할 수 있습니다.
직급이름컬럼명	직급테이블명 항목에 입력한 테이블에서 직급 이름 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 직급을 동기화할 수 있습니다.

- 노드정보

노드 동기화에 필요한 컬럼명을 입력합니다.

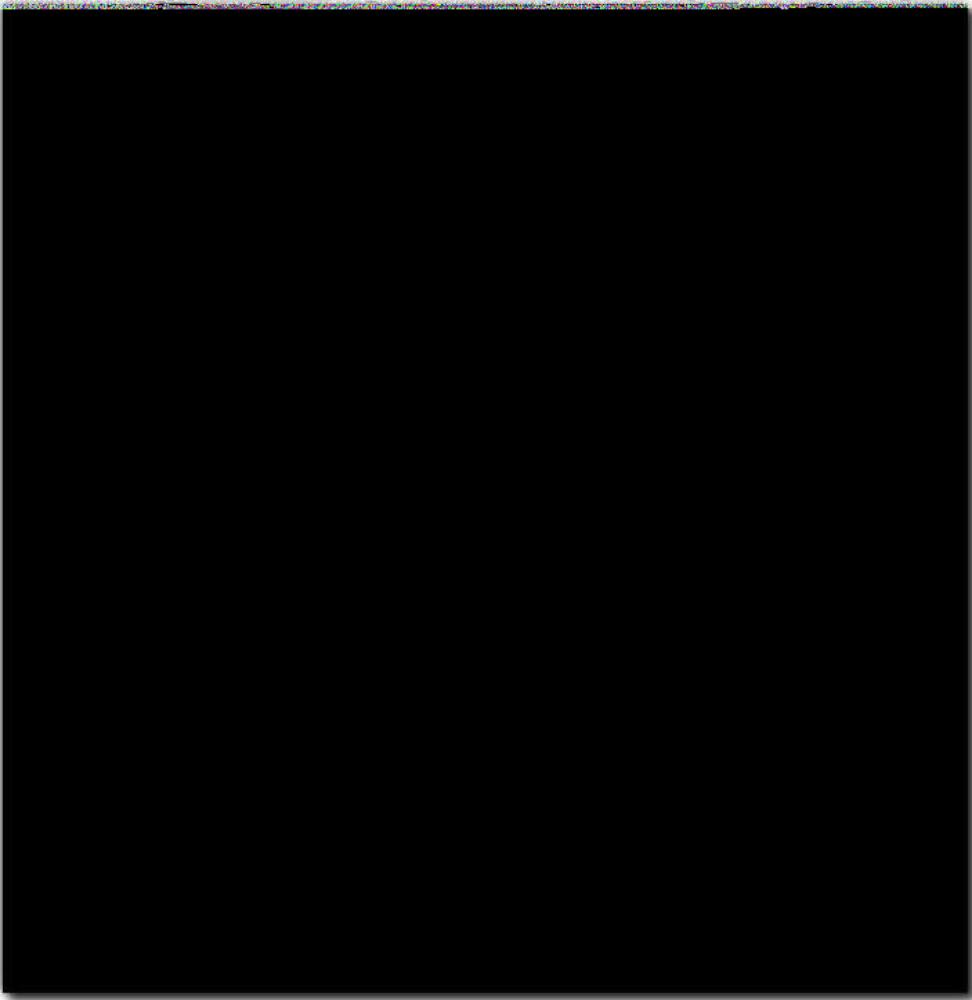


항목	내용
노드정보테이블명	동기화할 노드 정보가 들어있는 테이블명을 입력합니다.

노드정보조건문	데이터를 읽어올 데이터베이스의 노드테이블에 대한 쿼리 WHERE 조건문을 설정합니다. LDAP인 경우 filter사용. filter 예제: (objectClass=person)
IP주소컬럼명	노드정보테이블명 항목에서 입력한 테이블에서 IP주소 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 노드를 동기화할 수 있습니다.
MAC주소컬럼명	노드정보테이블명 항목에서 입력한 테이블에서 MAC주소 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 노드를 동기화할 수 있습니다.
노드이름컬럼명	노드정보테이블명 항목에서 입력한 테이블에서 노드이름 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 노드를 동기화할 수 있습니다.
노드설명컬럼명	노드정보테이블명 항목에서 입력한 테이블에서 노드설명 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 노드를 동기화할 수 있습니다.
인증사용자ID컬럼명	노드정보테이블명 항목에서 입력한 테이블에서 인증 사용자 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 노드를 동기화할 수 있습니다.
추가정보1~20컬럼명	노드정보테이블명 항목에 입력한 테이블에서 추가적으로 필요한 정보가 들어있는 컬럼명을 입력합니다. 해당 컬럼에 동기화된 정보는 설정 > 속성관리 > 추가필드관리 > 노드 에서 사용필드를 NL_CUSTOM01~20 설정하여 필드를 생성한 후 관리 > 노드 > 노드상세정보 에서 확인할 수 있습니다. 필드 생성방법은 추가필드관리 를 참고바랍니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 추가정보를 동기화할 수 있습니다.

- 장비수명주기정보

장비 정보 동기화에 필요한 컬럼명을 입력합니다.



항목	내용
장비수명주기정보테이블명	동기화할 장비수명 정보가 들어있는 테이블명을 입력합니다.

장비수명주기정보조건문	데이터를 읽어올 데이터베이스의 장비수명주기정보테이블에 대한 쿼리 WHERE 조건문을 설정합니다. LDAP인 경우 filter 사용. filter 예제: (objectClass=group)
IP주소컬럼명	동기화할 테이블에서 IP주소 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
MAC주소컬럼명	동기화할 테이블에서 MAC주소 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
제조일	동기화할 테이블에서 제조일 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
내용연수 시작일	동기화할 테이블에서 내용연수 시작일 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
구입처	동기화할 테이블에서 구입처 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
구입가격	동기화할 테이블에서 구입가격 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
책임자	동기화할 테이블에서 책임자 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
책임부서	동기화할 테이블에서 책임부서 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
일련번호	동기화할 테이블에서 일련번호 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
내용연수 만료일	동기화할 테이블에서 내용연수 만료일 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
메모	동기화할 테이블에서 장비에 필요한 메모 정보가 들어있는 컬럼 명을 입력합니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 장비정보를 동기화할 수 있습니다.
추가정보1~20컬럼명	동기화할 테이블에서 추가적으로 필요한 정보가 들어있는 컬럼명을 입력합니다. 해당 컬럼에 동기화된 정보는 설정 > 속성관리 > 추가필드관리 > 장비 수명주기 관리에서 사용필드를 NL_CUSTOM01~20 설정하여 필드를 생성한 후 관리 > 노드 > 노드상세정보에서 확인할 수 있습니다. 필드 생성방법은 추가필드관리 를 참고바랍니다. 우측의 물음표 버튼을 클릭하여 더욱 다양한 형식으로 추가정보를 동기화할 수 있습니다.

정보 동기화 삭제

관리자는 필요없는 정보 동기화를 삭제할 수 있습니다.

정보 동기화 삭제 진행과정은 [항목 삭제](#)를 참조 바랍니다.

관리역할

관리역할

최고관리자(Super Admin)는 업무분담을 위해 각기 다른 역할을 맡는 하위의 관리자들에게 관리권한을 할당할 수 있습니다. 기능별 사용권한을 제어하기 위해 각 관리역할에 맞는 권한을 부여해야합니다. 혹여, 역할에 맞지 않은 기능을 사용할 수 있는 권한은 할당하지 않도록 주의해야 합니다.

관리자는 단 하나의 관리역할을 가지며 관리역할별 권한에 의해 관리영역을 제한을 받습니다.

Genian NAC가 기본적으로 관리역할을 제공합니다.



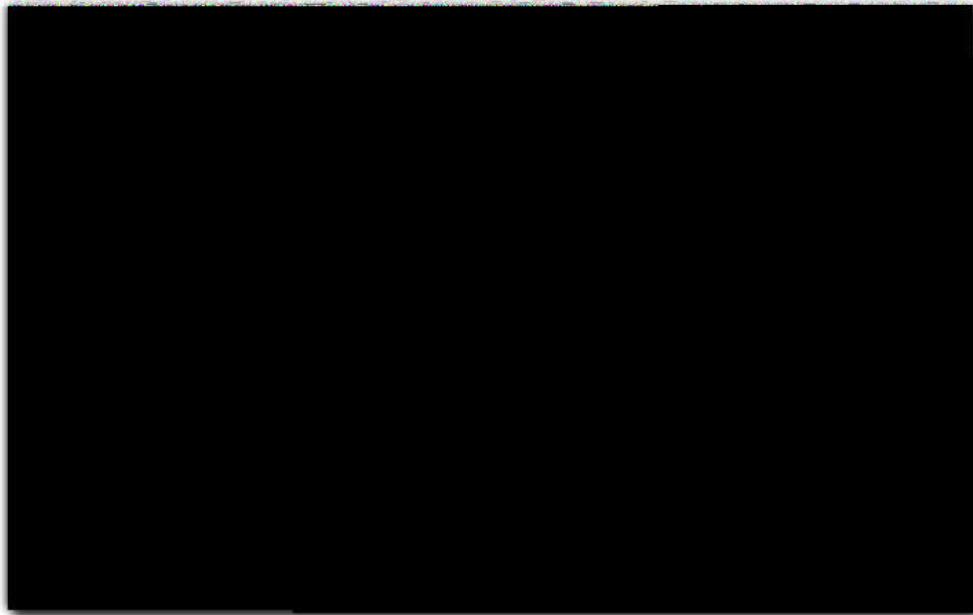
관리역할	설명
auditor	WEBUI의 관리, 감사, 정책에 대한 정보를 조회하기 위한 역할입니다. 자신의 개인정보와 위젯과 같은 조회를 위한 기능으로 제한되어 있습니다.
ipAppManager	설정 > 환경설정 > IP관리에서 IP 신청서 등록권한 옵션이 IP관리자에게만 허용을 되어 있을 경우, ipAppManager권한을 가진 관리자만이 IP신청을 할 수 있습니다.
superAdmin	가장 높은 권한이며, WEBUI의 모든 기능을 사용할 수 있습니다.

환경 설정

환경 설정

- 노드관리

SNMP, 노드정보검색 등 노드 관련 설정을 할 수 있습니다.



- IP관리

IP신청서와 사용만료된 IP/MAC처리 방법을 설정할 수 있습니다.



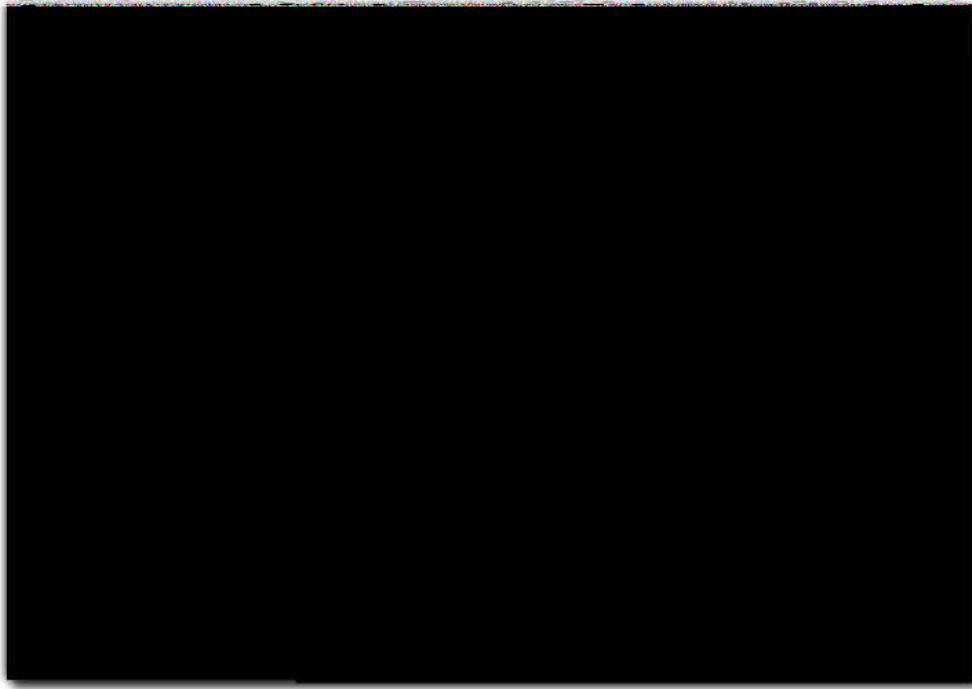
- 무선랜관리

무선랜의 감지, 자동삭제 관련된 설정을 할 수 있습니다.



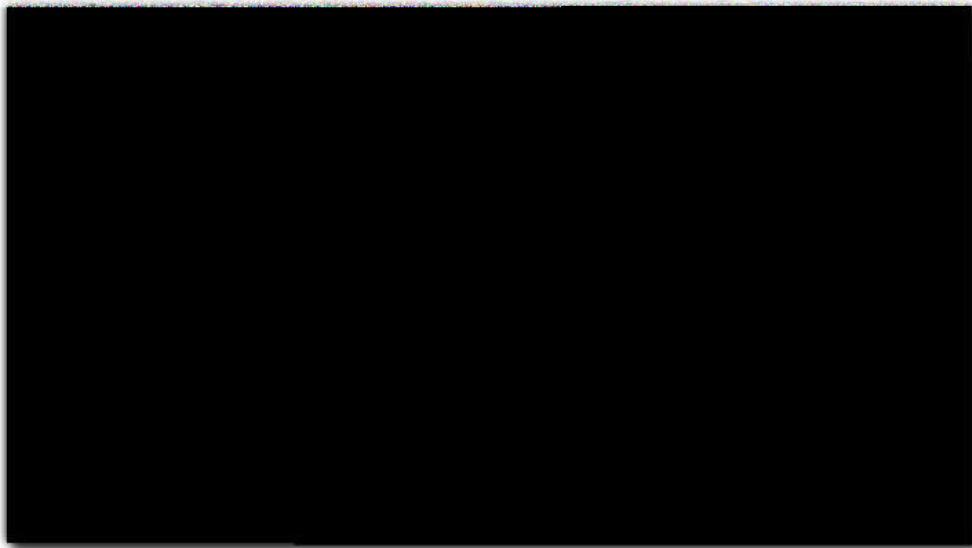
- 감사기록

감사기록 추가설정, SYSLOG 감사기록 저장 등 감사기록 관련 설정을 할 수 있습니다.



- 관리콘솔

CWP 지원언어 설정, 관리자 세션타임 아웃 등 관리콘솔 관련된 설정을 할 수 있습니다.



- 백업

백업의 수행여부, 저장에 관련된 설정을 할 수 있습니다.



- 에이전트

에이전트의 설치 과정, 에이전트 커스텀 아이콘 등록 등 에이전트에 관련된 설정을 할 수 있습니다.



- 기타설정

메일서버 등록, SMS 발신번호 설정 등 다양한 설정을 할 수 있습니다.



노드관리

노드관리

관리자는 설정 > 환경설정 > 노드관리 를 통하여 노드에관한 여러가지 설정을 할 수 있습니다.

- SNMP 검색

SNMP 이용한 노드 위치검색을 수행할지의 여부와 설정을합니다.



설정항목의 옵션과 설명은 아래 표와 같습니다.

설정항목	옵션	설명
SNMP 인증 설정	추가	SNMP 버전 2c, 3을 지원하며, SNMP 인증에 필요한 인증 정보를 설정합니다.
네트워크 정보수집	On,Off	SNMP를 통하여 스위치, 라우터의 인터페이스 정보를 수집하는 기능의 사용유무를 선택합니다, 스위치, 라우터의 인터페이스 정보는 노드 관리 뷰의 스위치,포트 항목을 통하여 확인할 수 있습니다.
검색주기	정수로 기입. 단위로는 분, 시간, 일, 주, 개월	주기로 설정된 시각마다 SNMP 검색을 수행합니다. default : 3시간 최소값 : 5분 최대값 : 1년
검색시간그룹	생성되어져 있는 시간객체	생성되어있는 시간객체 중 하나를 선택하여 선택된 시각에만 검색을 수행합니다.
검색수행	지금시작 버튼	지금시작을 클릭하면 검색주기와 검색시간그룹과는 상관없이 지금즉시 노드위치검색을 수행합니다.

- 노드정보 검색

노드IP에 대한 Reverse DNS 이름검색을 수행할지의 여부와 노드 정보수집의 스캐닝 주기 등을 설정합니다.



설정항목의 옵션과 설명은 아래 표와 같습니다.

설정항목	옵션	설명
노드 IP 이름검색	On,Off	IP주소를 통하여 호스트네임을 알아내는 리버스 DNS의 기능을 수행할지의 여부를 선택합니다.
플랫폼미탐지보고	On, Off	플랫폼 미탐지 노드가 있을때, 해당 정보를 (주)지니네트웍스에 자동전송 할지의 유무를 선택합니다.
네트워크 스캔주기	분, 시간, 일, 주, 개월	입력한 시간을 주기로 DHCP Server, UPNP, HP SLP, SIP을 스캔합니다. DHCP Server, UPNP, HP SLP, SIP 스캔 여부 설정은 시스템관리 에서 네트워크 스캔을 참고바랍니다. default : 10분 최소값 : 1분 최대값 : 1년
최초플랫폼정보 자동확인	On, Off	관리 > 노드 > 노드상세정보 > 기본정보에서 확인된 노드타입, 확인된 플랫폼 옵션에 최초 감지된 노드타입, 플랫폼 정보를 입력할지 여부를 선택합니다.

- 노드정리

수집한 노드정보들 중에 오랜기간동안 업데이트되지 않는 노드의 정보들을 삭제하는 주기를 설정합니다.



설정항목의 옵션은 아래 표와 같습니다.

설정항목	옵션	설명
IP변경노드삭제	정수로 기입. 단위로는 시간, 일, 주, 개월	노드 IP 변경 시 설정된 기간 이상 다운상태를 유지하는 과거노드 삭제 합니다. default : 3일 최소값 : 0 최대값 : 1년

- 노드등록

DHCP AutoIP(169.254.0.0/16)로 할당받은 노드를 노드로 등록할지 여부를 선택합니다.



설정항목의 옵션은 아래 표와 같습니다.

설정항목	옵션	설명
NAT IP 노드등록	On, Off	On일 경우 NAT 장비 감지시 NAT IP를 노드로 등록하고, Off일 경우 NAT 장비를 노드로 등록하지 않습니다.

- 차단설정

차단대상 노드의 WEP을 차단하기위해 차단할 HTTP포트를 설정하고, 접속인증페이지 Redirection을 적용할 User-Agent String을 설정합니다.여러개일경우 콤마로 구분합니다.



설정항목의 옵션은 아래 표와 같습니다.

설정항목	옵션
HTTP포트	차단된 노드가 입력된 HTTP포트로 접근 시 CWP페이지가 출력됩니다.
HTTPS 포트	차단된 노드가 입력된 HTTPS포트로 접근 시 CWP페이지가 출력됩니다.
User-Agent String	HTTP포트를 차단 후 User-Agent가 설정한 User-Agent String 값일 경우 CWP 페이지를 출력하고 User-Agent가 설정한 User-Agent String 값이 아닐 경우 CWP 페이지를 출력하지 않습니다.
Redirection 예외 IP	차단된 노드가 입력된 IP로 접근 시 CWP페이지를 출력하지 않습니다.

- 미사용 IP

미사용 IP를 관리그룹에 포함시킬지의 여부를 선택합니다.(ON 선택 시 미사용IP를 관리그룹에 포함시킴.)



설정항목의 옵션은 아래 표와 같습니다.

설정항목	옵션	설명
노드그룹 포함	On,Off	미사용 IP를 관리그룹에 포함시킬지의 여부를 선택합니다. 시스템 > 시스템관리 > 센서IP클릭 > 센서설정 > 미사용IP등록 옵션이 On으로 설정되어 있어야합니다. IP주소, IP관리, 센서, 정책그룹, 업/다운상태, 노드그룹 항목이 설정된 노드그룹에만 적용됩니다.
예약노드 정리	정수로 기입. 단위로는 시간, 일, 주, 개월	예약된 ip 노드가 설정된 시간 동안 사용되지 않으면 예약된 ip 노드를 삭제합니다.

포트스캔

포트스캔

해당 페이지는 각 포트번호에 해당하는 서비스명을 저장하기 위해 존재합니다.
Genian NAC는 정보수집 기능중 열려있는 포트를 수집하는 기능이 있습니다. 이때, 각 포트번호에 해당하는 서비스명은 해당 페이지에 있는 서비스명 자료를 참조하여 보여줍니다.
기본적으로 많이 쓰이는 약 150여개의 포트번호와 서비스명은 탑재되어 있으나, 꼭 표시되어야할 서비스이나 누락된 서비스는 관리자가 추가작업을 통해 서비스명이 표시되게 할 수 있습니다.

포트 생성/사용여부

관리자는 작업선택 메뉴를 통해 포트와 서비스명을 추가 및 스캔여부를 설정할 수 있습니다.

- **포트 생성**

1. 설정 > 환경설정 > 포트스캔 > 작업선택 > 생성 을 선택합니다.



2. 포트정보 입력

프로토콜과 포트번호, 서비스명을 입력합니다.



- **포트 사용여부**

1. 사용 안함으로 표시되어 있는 포트를 선택 후 설정 > 환경설정 > 포트스캔 > 작업선택 > 사용함 을 선택합니다.



-
2. 사용함으로 변경된 포트는 노드 포트 스캔 시 탐지합니다. 탐지된 포트는 노드상세정보 > 네트워크정보에 확인할 수 있으며 플랫폼 탐지에 사용됩니다.



3. 포트 스캔이 필요 없을 경우 포트를 선택 후 설정 > 환경설정 > 포트스캔 > 작업선택 > 사용안함을 선택합니다.



4. 사용안함으로 변경된 포트는 노드 포트 스캔 시 탐지하지 않으며, 노드 플랫폼 변경 및 탐지에 영향이 있을 수 있습니다.



포트삭제/수정

신규로 추가된 포트뿐 아니라 기본적으로 탑재되어있는 포트도 삭제/수정이 가능합니다.

삭제 방법은 [항목 삭제](#)를 참조해 주시기 바랍니다.

수정작업은 포트번호를 클릭하고 수정페이지로 이동하여 서비스명을 수정할 수 있습니다.



IP 관리

관리자는 IP관리 페이지 설정 > 환경설정 > IP관리 를 이용하여 IP 신청서에대한 설정과 IP 정책에 관련된 설정을 할 수 있습니다.



설정항목과 설명은 아래 표와 같습니다.

항목이름	설정 값	설명
IP사용신청	ON	IP및MAC이 차단될 때 접속인증 페이지에서 IP신청을 할 수 있도록 IP 신청아이콘을 접속인증 페이지에 생성합니다.
	OFF	접속인증 페이지에서 IP 신청을 받지 않도록 IP 신청아이콘을 접속인증 페이지에 생성하지 않습니다.
자동 로그인	ON	IP신청아이콘을 클릭할 시 IP신청페이지에 현재 인증받은 사용자ID로 자동으로 로그인합니다. 임시사용자 신청허용 옵션이 On일 시 인증을 받지 않은 사용자는 임시사용자로 자동로그인 됩니다.
	OFF	IP 사용아이콘을 클릭할 시 자동으로 로그인되지 않고 직접 아이디와 패스워드를 입력하여야 합니다.
IP신청서 거부처리	일, 주, 개월	설정한 기간이 지난 IP신청서 및 이메일 승인대기 신청서는 자동으로 거부처리 합니다. 0으로 설정할 시 해당 기능을 사용하지 않습니다.
할당대상 IP	미사용IP할당	IP 신청을 받고 IP를 할당할 때, 미사용중인 IP만 이용하여 할당합니다.
	미사용 IP 또는 차단된 IP 할당	IP 신청을 받고 IP를 할당할 때, 미사용중이거나 차단된 IP를 이용하여 할당합니다.
IP사용신청서 작동방식	부서기반	부서에 할당된 IP 대역에서 사용하지 않는 IP를 할당합니다.
	위치(센서)기반	센서가 관리하는 IP 대역에서 사용하지 않는 IP를 할당합니다.
할당대상 기준부서	사용자 부서, 신청자 부서	할당 해줄 IP를 사용할 사용자의 부서IP에서 할당 할지, IP를 신청한 사람의 부서의 IP로 할당 할지에 대한 설정 값입니다.
임시사용자 신청허용	ON	IP신청페이지의 로그인 창에 임시로그인 아이콘이 생성되며, 클릭할 시 사용자ID가 없어도 임시로그인을 하여 IP신청을 할 수 있습니다.
	OFF	IP신청페이지의 로그인 창에 임시로그인 아이콘이 생성되지 않으며, 임시로그인을 할 수 없습니다.
승인번호 인증	ON	접속인증 페이지에 IP승인확인 아이콘이 생성되며, IP신청할 때 할당 받은 승인번호를 입력하여 할당받은 IP를 사용할 수 있도록합니다.
	OFF	승인번호를 입력하는 과정 없이 바로 발급받은 IP를 사용할 수 있습니다.
IP 신청서 등록권한	모든사용자에게 허용	IP 신청을 모든사용자가 신청할 수 있습니다.
	IP 관리자에게만 허용	사용자권한이 IP 관리자(IpAppManager)인 관리자만 IP 신청서 신청이 가능합니다.
IP 신청결과 조회범위	IP 관리범위내 조회	해당 IP 관리자가 맡고있는 IP범위 내의 신청서만 결과조회가 가능합니다.
	전체신청결과 조회	전체 신청서의 신청결과 조회가 가능합니다.
	신청자 ID내 조회	신청자의 신청서만 결과조회가 가능합니다.
IP 신청 승인/거부사유 입력	사용안함	IP신청서 처리 사유를 기록하지 않습니다.
	승인시	IP신청서 승인 시, IP신청서 처리 사유를 입력할 수 있는 팝업 창이 출력됩니다. 입력한 내용은 관리 > 신청 > IP사용신청서 > 결과조회에서 처리사유 항목에서 확인할 수 있습니다.
	거부시	IP신청서 거부 시, IP신청서 처리 사유를 입력할 수 있는 팝업 창이 출력됩니다. 입력한 내용은 관리 > 신청 > IP사용신청서 > 결과조회에서 처리사유 항목에서 확인할 수 있습니다.
IP신청서 입력유지	ON	IP 신청서 작성 후 "신청서 추가" 기능을 사용 시 작성한 내용이 유지 됩니다.
	OFF	IP 신청서 작성 후 "신청서 추가" 기능을 사용 시 작성한 내용이 유지되지 않고 초기화 됩니다.
IP신청서 사용자정보 자동입력	사용안함	IP신청서의 사용자ID를 입력할 시 휴대폰, 이메일 정보가 자동으로 입력되지 않습니다.

	사용자	IP신청서의 사용자ID를 입력할 시 사용자의 휴대폰, 이메일 정보가 SMS문자통보, Email통보 필드에 자동으로 입력됩니다.
	신청자	IP신청서의 사용자ID를 입력할 시 신청자의 휴대폰, 이메일 정보가 SMS문자통보, Email통보 필드에 자동으로 입력됩니다.
IP 다중신청서 양식		엑셀을 이용하여 IP를 신청할 때 필요한 양식을 +add을 클릭하여 업로드합니다.
IP신청시스템LOGO		IP신청페이지의 로고화면을 +add을 클릭하여 업로드합니다.
Style Sheet파일		IP신청시스템 UI에 적용할 CSS파일을 업로드합니다.
IP신청서 처리결과 자동알람	<선택안함>	관리자가 관리 > 신청에서 IP신청서를 승인 및 거부 시 알람메시지가 전송되지 않습니다.
	SMS	관리자가 관리 > 신청에서 IP신청서를 승인 및 거부 시 알람메시지가 SMS으로 전송됩니다.
	Email	관리자가 관리 > 신청에서 IP신청서를 승인 및 거부 시 알람메시지가 Email으로 전송됩니다.
	SMS+Email	관리자가 관리 > 신청에서 IP신청서를 승인 및 거부 시 알람메시지가 SMS, Email 모두 전송됩니다.
알람범위	사용자	관리자가 관리 > 신청에서 IP신청서를 승인 및 거부 시 사용자에게 알람메시지가 전송됩니다.
	신청자	관리자가 관리 > 신청에서 IP신청서를 승인 및 거부 시 신청자에게 알람메시지가 전송됩니다.
	신청자+사용자	관리자가 관리 > 신청에서 IP신청서를 승인 및 거부 시 사용자, 신청자 모두에게 알람메시지가 전송됩니다.
로그인화면 문구		로그인 창 하단에 표시할 문구를 입력합니다.
로그인화면 헤더사용	ON	IP신청페이지에 헤더를 사용합니다.
	OFF	IP신청페이지에 헤더를 사용하지 않습니다.
헤더이미지		로그인화면 헤더사용 옵션이 ON일 경우에 활성화 되며, 헤더 이미지를 업로드합니다.
헤더영역 배경색		헤더영역의 배경색을 지정합니다.
사용자정의 헤더사용	ON	IP신청서 페이지 헤더부분에 HTML을 추가하여 이미지 등을 헤더 부분에 넣을 수 있습니다.
	OFF	IP신청서 페이지 헤더부분에 HTML 추가하지 않습니다.
출력높이		헤더 높이를 설정합니다.
헤더 HTML설정		IP신청서 페이지 헤더에 보일 HTML을 작성합니다.
관리화면전환	ON	IP신청서 페이지(ipmgmt3)에 로그인한 정보로 관리페이지로 추가 로그인 없이 전환하는 버튼을 출력합니다.
	OFF	IP신청서 페이지(ipmgmt3)에 로그인한 정보로 관리페이지로 추가 로그인 없이 전환하는 버튼을 출력하지 않습니다.
대상관리역할		관리화면전환 버튼을 출력할 역할을 설정합니다.

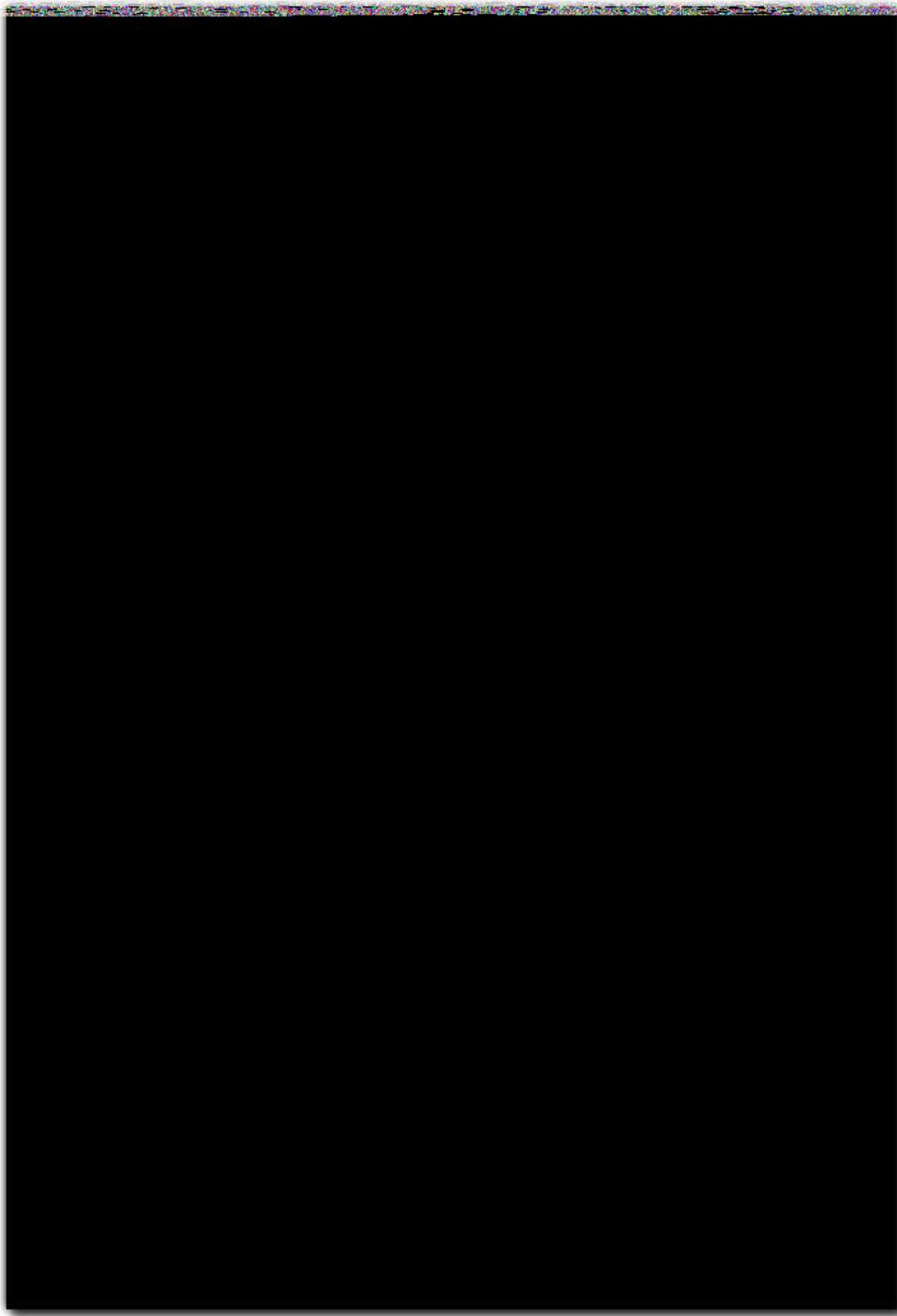
- IPM 정책



설정항목과 설명은 아래 표와 같습니다.

설정항목	설정 값	설명
IP/MAC 사용만료처리방법	삭제함	IP/MAC사용 만료 시 노드를 삭제하고, 다시 새로운 노드로 등록시켜 신규 노드정책이 적용됩니다.
	삭제안함	IP/MAC사용 만료 시 노드를 삭제하지않고, 사용만료상태로 노드를 차단시킵니다.
특수정책 우선	ON	시간제한/충돌보호/변경금지정책이 IP/MAC 차단정책보다 우선시 됩니다.
	OFF	시간제한/충돌보호/변경금지정책이 IP/MAC 차단정책보다 우선시 되지 않습니다.
동일 호스트명제한설정값 검사대상	전체센서	템플릿을 이용하여 호스트명 제한 시 센서가 탐지한 모든 네트워크에서 동일한 제한 호스트명이 존재할 경우 제한 호스트명 뒤에 숫자를 붙이게 하여 제한 호스트명을 다른 노드와 중복되지 않도록 합니다.
	현재센서	템플릿을 이용하여 호스트명 제한 시 동일한 네트워크 대역에서 동일한 제한 호스트명이 존재할 경우 제한 호스트명 뒤에 숫자를 붙이게 하여 제한 호스트명을 다른 노드와 중복되지 않도록 합니다.
노드관리 IP정책명령 사유입력	ON	관리자가 수동으로 노드에 IP정책관련 명령 시 사유를 입력할 수 있는 팝업 창이 출력됩니다. 사유는 노드의 설명 항목에서 확인할 수 있습니다.
	Off	관리자가 수동으로 노드에게 IP정책관련 명령 시 팝업 창이 출력되지 않습니다.

- IP신청시스템 화면설정



설정항목과 설명은 아래 표와 같습니다.

설정항목	내용
타이틀 문구	IP신청시스템의 타이틀에 표시될 문구를 입력합니다.
최초접속화면	IP신규신청페이지 최초 접속화면을 설정합니다.
신청시스템 메뉴	IP신규신청페이지에서 상단에 있는 공지사항, IP신규신청 등의 항목을 수정할 수 있습니다.
IP신청목록	IP신규신청페이지에서 신청서추가 기능을 이용할 때 나타나는 항목을 수정할 수 있습니다.
IP반납목록	IP반납신청페이지에서 신청서추가 기능을 이용할 때 나타나는 항목을 수정할 수 있습니다.
장비변경 목록	장비변경신청페이지에서 신청서추가 기능을 이용할 때 나타나는 항목을 수정할 수 있습니다.
사용자변경 목록	사용자변경신청페이지에서 신청서추가 기능을 이용할 때 나타나는 항목을 수정할 수 있습니다.

신청결과 목록	신청서처리결과에서 보여주는 항목을 수정할 수 있습니다.
공지사항 본문 도움말	공지사항페이지에 도움말을 작성할 수 있습니다.
IP신규신청 본문 도움말	IP신규신청페이지에 도움말을 작성할 수 있습니다.
IP반납신청 본문 도움말	IP반납신청페이지에 도움말을 작성할 수 있습니다.
장비변경 본문 도움말	장비변경페이지에 도움말을 작성할 수 있습니다.
신청서처리결과 본문 도움말	신청서처리결과에 도움말을 작성할 수 있습니다.
IP사용현황	IP사용현황에 도움말을 작성할 수 있습니다.
가져오기 본문 도움말	IP신규신청 페이지에서 가져오기 버튼을 클릭하면 가져오기페이지에 접속할 수 있으며, 가져오기페이지에 도움말을 작성할 수 있습니다.

IP신청시스템공지사항

IP신청시스템공지사항

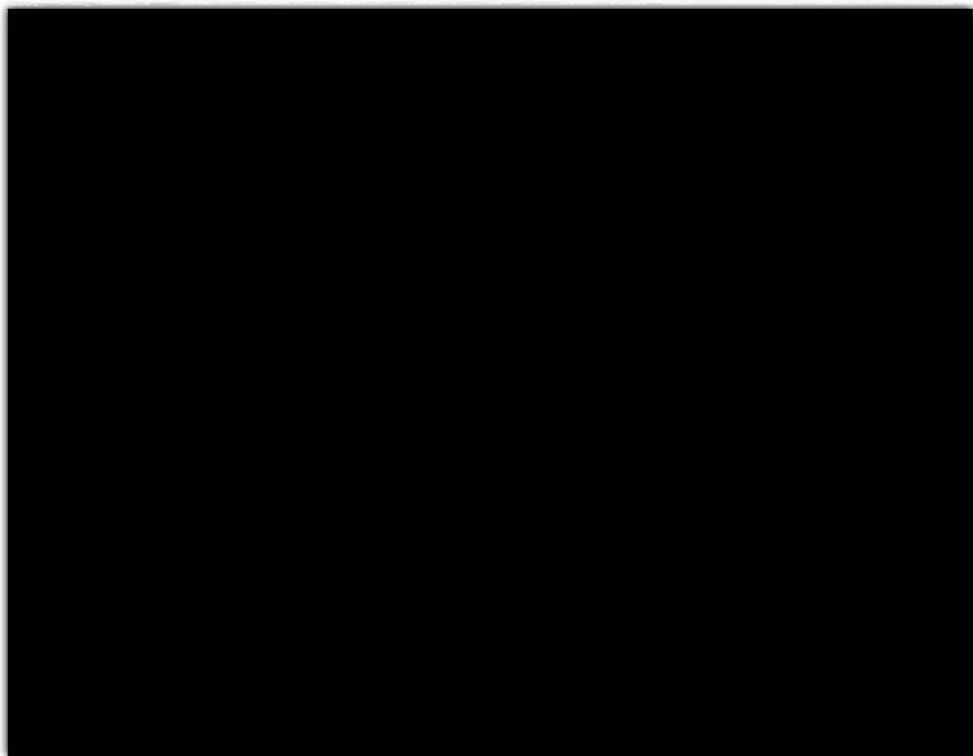
관리자는 IP신청시스템공지사항에서 공지사항을 추가하여 사용자들이 IP신청페이지에서 공지사항을 확인할 수 있도록 할 수 있습니다.
CWP 페이지에는 공지사항이 표시되지 않으며, IP신청페이지에서만 공지사항을 확인할 수 있습니다.

공지사항 생성/삭제

- 설정 > 환경설정 > IP관리 > IP신청시스템공지사항 > 작업선택 > 생성 버튼을 클릭합니다.



- 공지사항 기간, 내용을 작성하고 하단의 추가 버튼을 클릭합니다.



-
3. IP신청페이지에 접속할 시 아래의 그림과 같이 공지사항을 확인할 수 있습니다.



- 공지사항 삭제

관리자는 공지사항을 삭제할 수 있습니다.

삭제방법은 [항목 삭제](#)를 참조해 주시기 바랍니다.

무선랜관리

무선랜관리

무선랜관리 페이지 설정 > 환경설정 > 무선랜관리 를 이용하여 Genian WNAC이 수집한 무선랜 정보들을 재갱신 하는 주기를 설정할 수 있습니다.



항목들에 대한 설명은 아래 표와 같습니다.

항목 이름	설정 값	설명
무선 AP DOWN 감지	초, 분, 시간, 일, 주, 개월	무선 AP가 설정된 시간이상 감지되지 않을 경우 해당 무선 AP가 Down상태로 변경 됩니다. default : 10분 최소값 : 1분 최대값 : 1시간
무선 AP 자동삭제	일, 주, 개월	무선 AP가 설정된 기간이상 보고되지 않은 경우 해당 무선 AP를 삭제합니다. default : 3일 최소값 : 1일 최대값 : 1년
접속정보 자동삭제	일, 주, 개월	무선 AP가 설정된 기간이상 접속기록이 없을 경우 해당 무선 AP의 접속정보를 삭제 합니다. default : 3일 최소값 : 1일 최대값 : 1년
무선센서 자체 감지	On, Off	내부 네트워크에 존재하는 AP를 탐지할때 유선센서가 없을 경우 무선센서에서 자체적으로 내부 AP를 탐지합니다. Off 시 유선센서가 없을 경우 내부 AP를 탐지하지 않습니다.
내부 AP 탐지용 가상 MAC 사용	On, Off	내부 네트워크에 존재하는 AP를 탐지할때 한 개의 가상 MAC을 기준으로 내부 AP를 탐지합니다. Off 시 각 유선센서별 MAC을 무선센서로 전송하여 유선센서의 MAC을 기준으로 내부 AP를 탐지합니다.



내부 AP 탐지용 가상 MAC On일 경우

부하는 줄어들지만 단일 스위치에 다중으로 유선센서가 존재할 경우 flapping이 발생할 수 있습니다.

감사기록

감사기록

관리자는 설정 > 감사기록 페이지를 통하여 감사기록(로그)에 관한 설정을 할 수 있습니다.

- 노드 감사기록 선택

로그에 남길 추가정보를 선택할 수 있습니다. 또한 노드, 에이전트 동작상태 이력의 저장유무를 선택할 수 있습니다.



항목	옵션	설명
추가정보 저장		감사 > 로그에서 로그가 남겨질 때 체크한 정보들이 추가로 출력됩니다.
노드 동작상태 이력 저장	on, off	노드의 UP/DOWN 상태 이력을 csv 파일로 저장합니다. csv 파일은 감사 > 로그의 트리 뷰에 동작상태 트리에서 다운로드 할 수 있습니다.
에이전트 동작상태 이력 저장	on, off	에이전트의 UP/DOWN 상태 이력을 저장합니다. 이력은 감사 > 로그의 트리 뷰에 동작상태 트리에서 확인 할 수 있습니다.

- SNMP Trap 수신

SNMP Trap 이란 SNMP Agent 즉, 사용자 노드에 특정 이벤트(UP/DOWN이나 장애 등) 발생 시, 해당 노드 스스로 SNMP Manager(Genian NAC)에게 해당 사실을 알리게 됩니다.

SNMP Trap 수신 항목은 위와 같은 SNMP Trap의 사용 여부와 Community 값을 설정해 주는 항목입니다.



- Syslog 감사기록 저장

수신받은 특정 Syslog를 감사기록으로 저장할 수 있습니다.

수신받은 Syslog 중 설정한 필터에 맞는 Syslog를 감사기록으로 저장합니다.



관리콘솔

관리콘솔

관리자는 관리콘솔 페이지를 통하여 웹 콘솔의 화면과 CWP 페이지의 화면에 대한 설정을 할 수 있습니다.



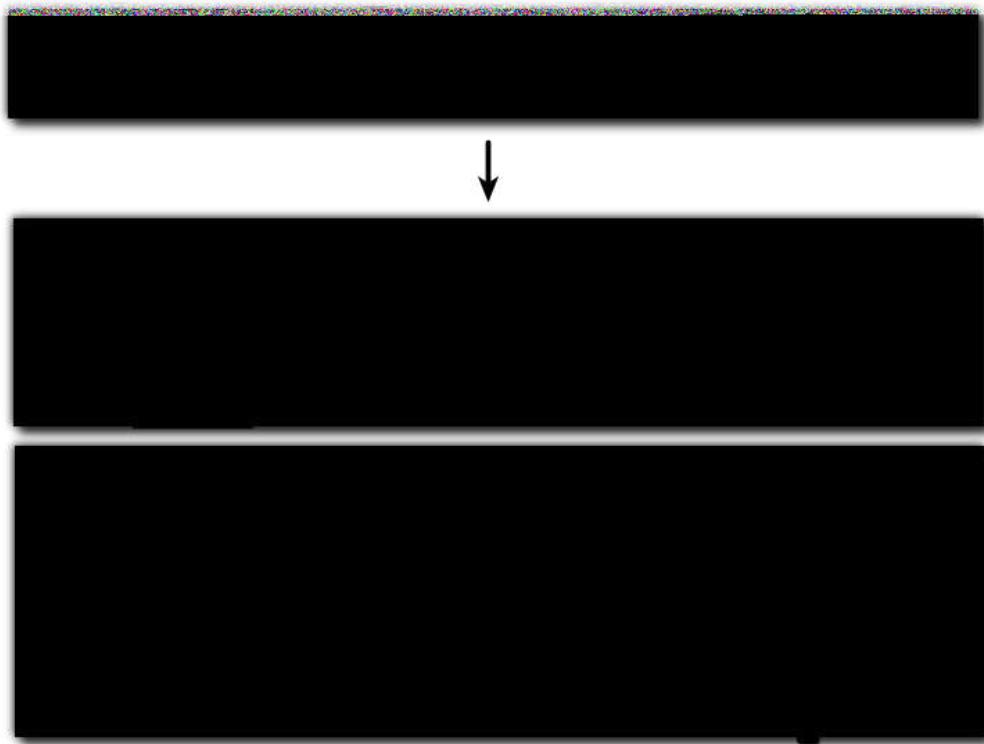
노드관리 기본대상, 노드관리 기본관점, 노드관리 기본뷰의 경우 관리자 기본 템플릿을 설정하는 것입니다.
따라서 관리자가 마지막으로 사용한 정보를 출력합니다.

- WEB 설정

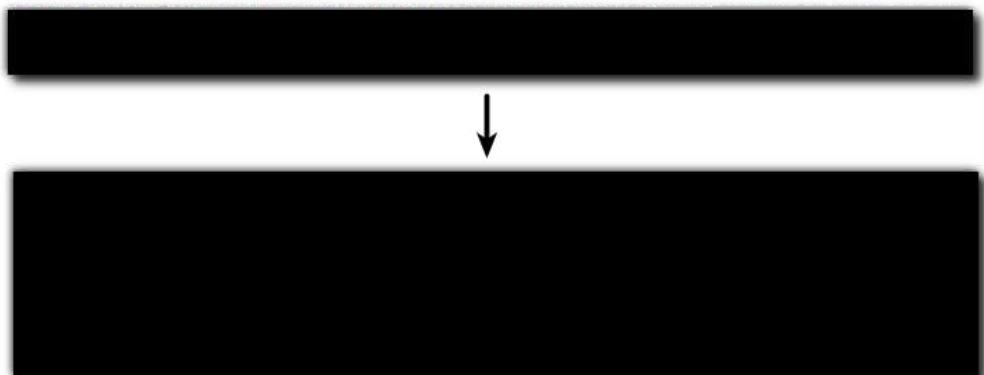
웹 콘솔의 기본화면 설정과 세션 타임아웃, 로그인정보의 출력유무 등을 설정할 수 있습니다.



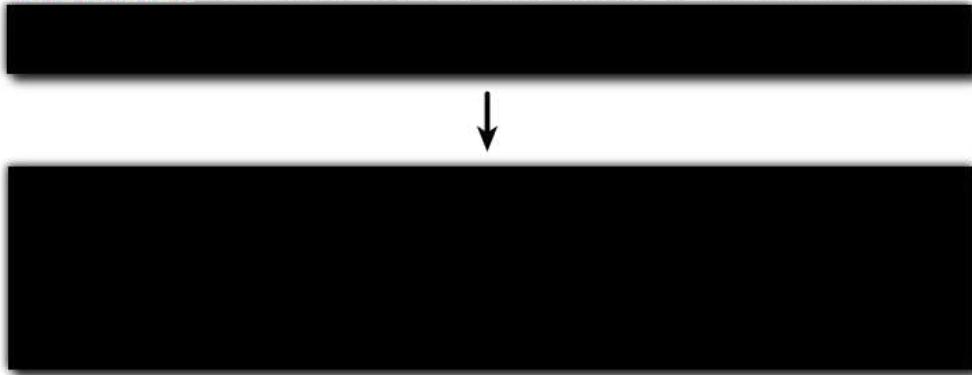
1. 타이틀 문구 변경시 변경사항은 아래와 같습니다.



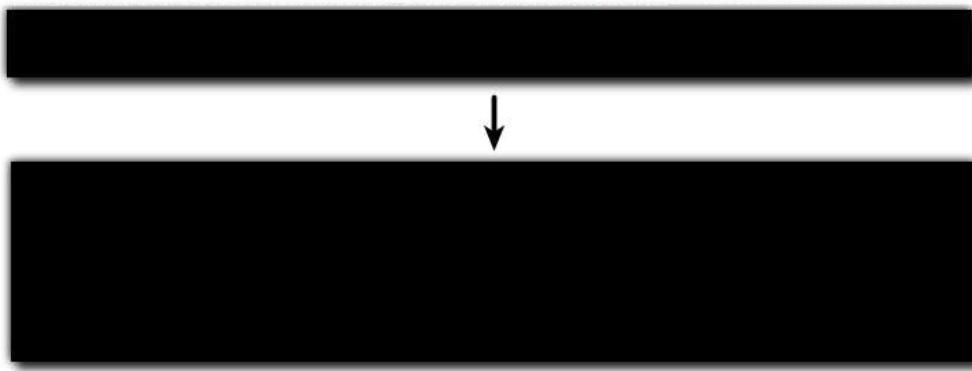
2. 노드관리 기본대상을 그룹별 IP관리로 설정 시 아래와 같이 트리 뷰의 기본 대상이 변경됩니다, 트리 뷰의 대상을 직접 다른 대상으로 변경할 시 해당 옵션이 적용되지 않고 직접 변경한 관점이 기본 대상으로 변경됩니다.



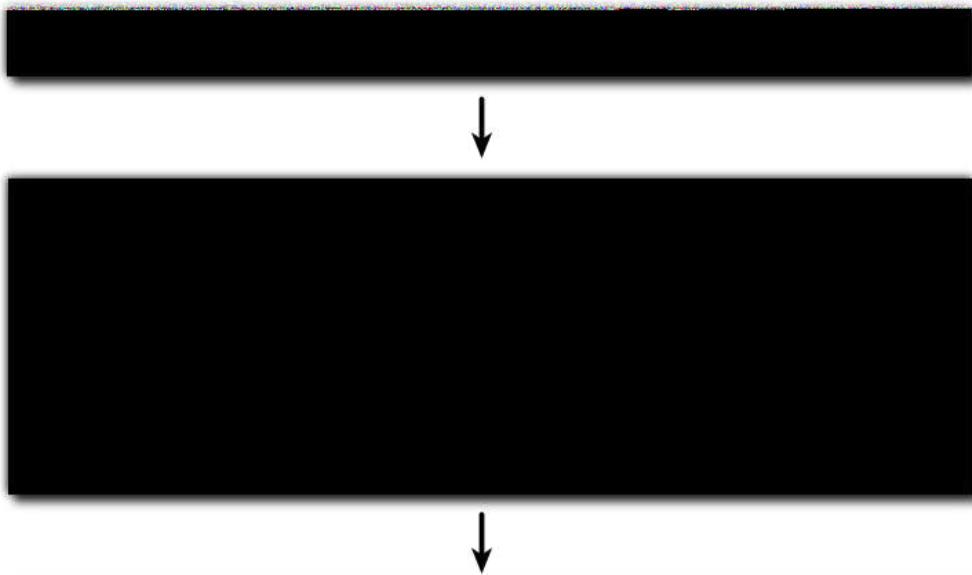
3. 노드관리 기본관점을 장비관점으로 설정 시, 아래와 같이 관리 뷰의 기본관점이 장비관점으로 변경됩니다. 노드 관리비의 관점을 직접 다른 관점으로 변경할 시 해당 옵션이 적용되지 않고 직접 변경한 관점이 기본 관점으로 변경됩니다.



4. 노드관리 기본뷰를 변경 시, 변경된 뷰가 기본뷰로 설정됩니다. 노드 관리의 뷰를 직접 다른 뷰로 변경할 시 해당 옵션이 적용되지 않고 직접 변경한 뷰가 기본 관점으로 변경됩니다.

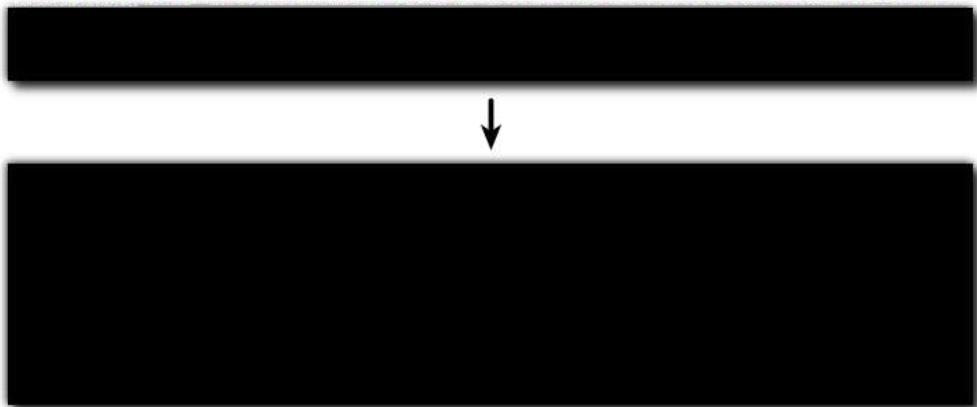


5. 관리화면 트리정렬을 수동 정렬로 설정 시, 아래와 같이 트리 뷰의 순서를 수동으로 변경할 수 있습니다. 출력명으로 설정할 경우 트리 뷰 순서를 수동으로 변경할 수 없으며 가나다 순으로 자동 정렬 됩니다.

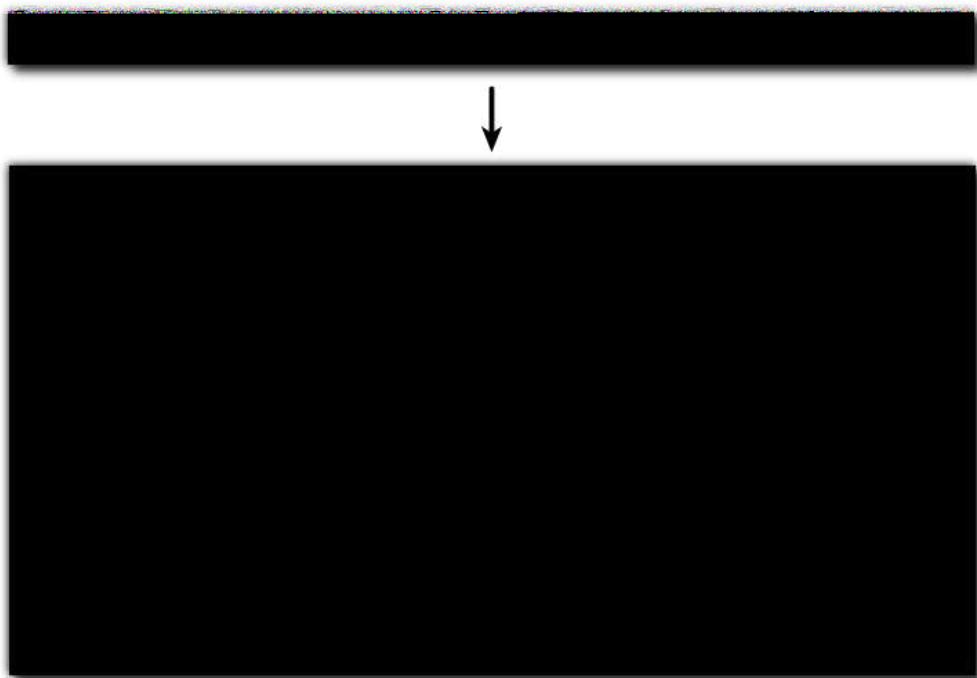




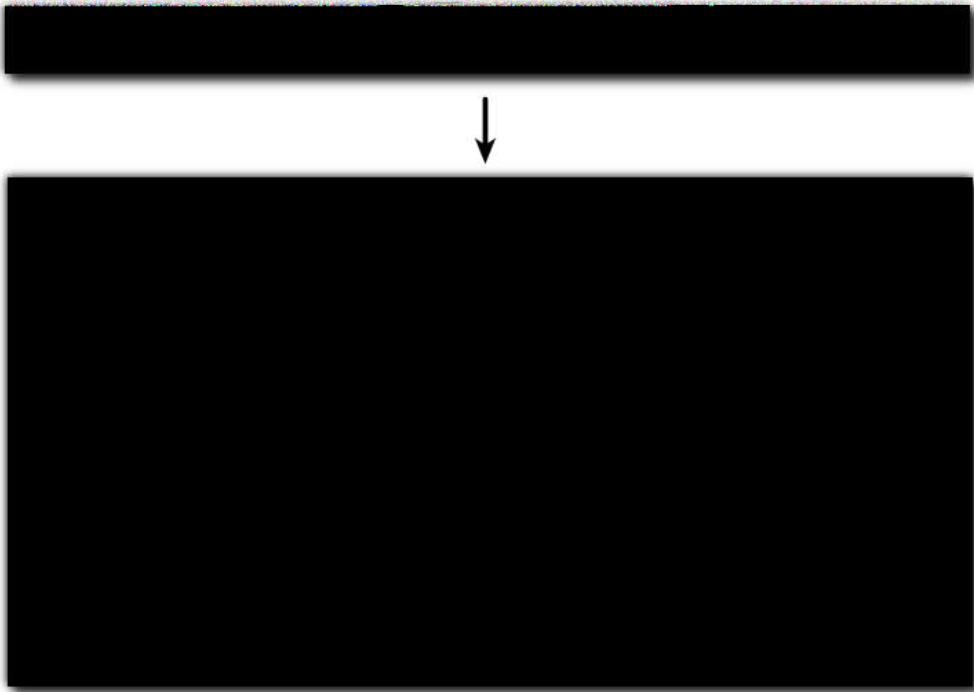
6. 노드수 미사용IP포함을 On으로 설정 시, 등록된 미사용 IP 노드가 트리 뷰에 카운트됩니다.



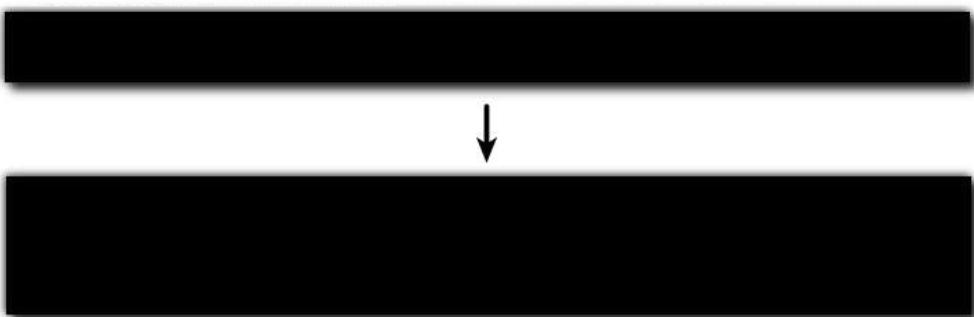
7. 화면 출력 지원언어를 설정합니다. 언어는 한국어, English를 지원합니다.



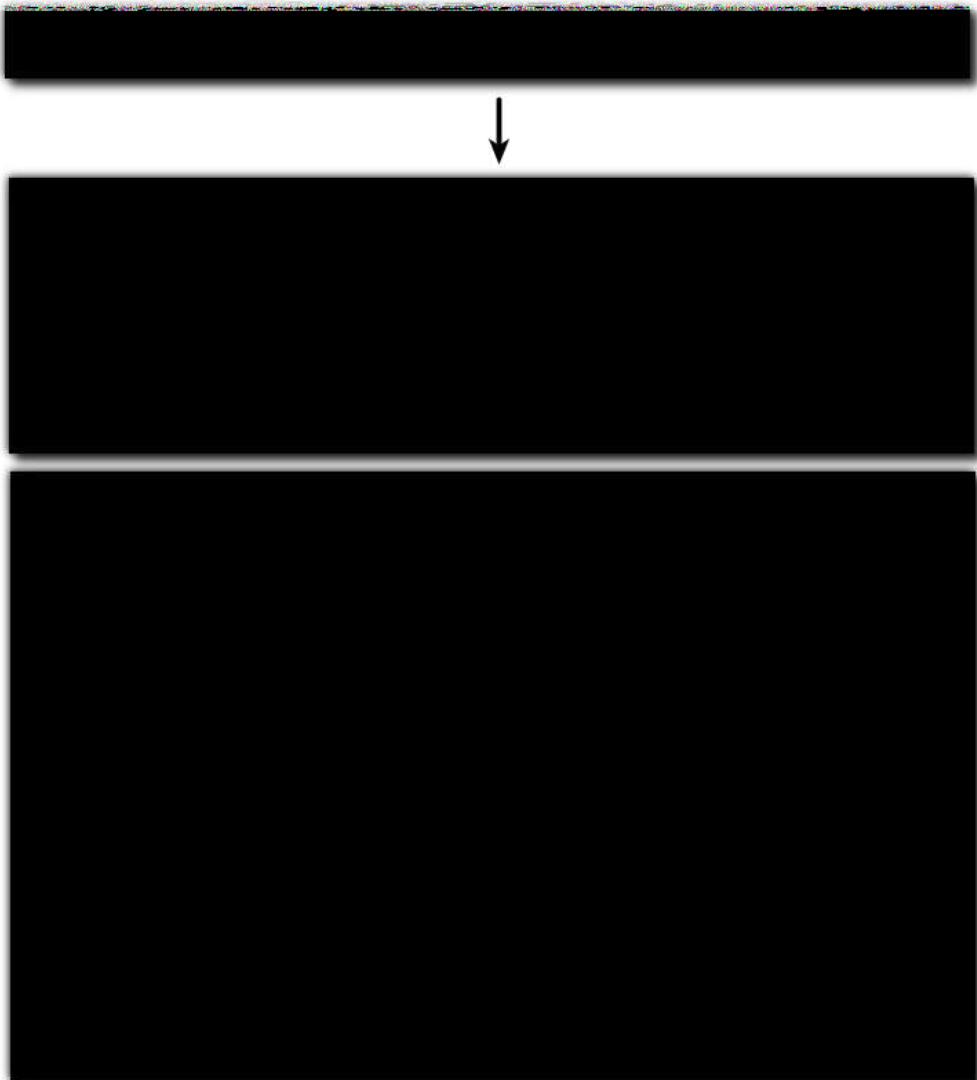
8. 관리콘솔에서 출력되는 날짜 패턴을 변경합니다.



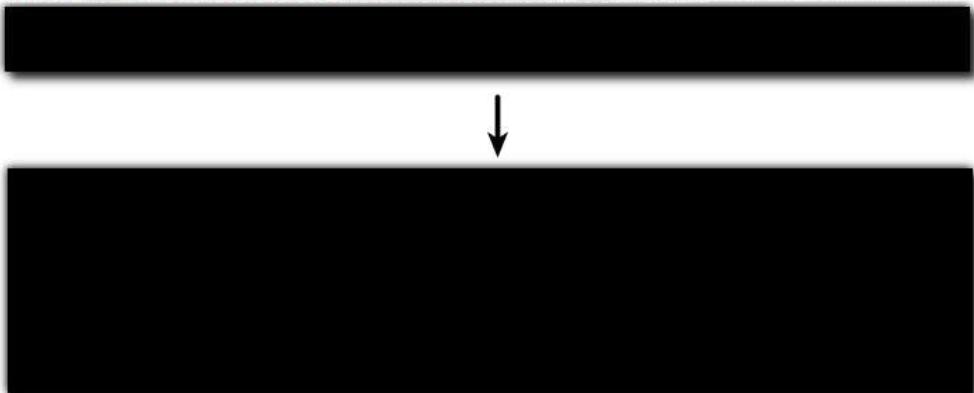
9. 관리콘솔에서 출력되는 시간 패턴을 변경합니다.



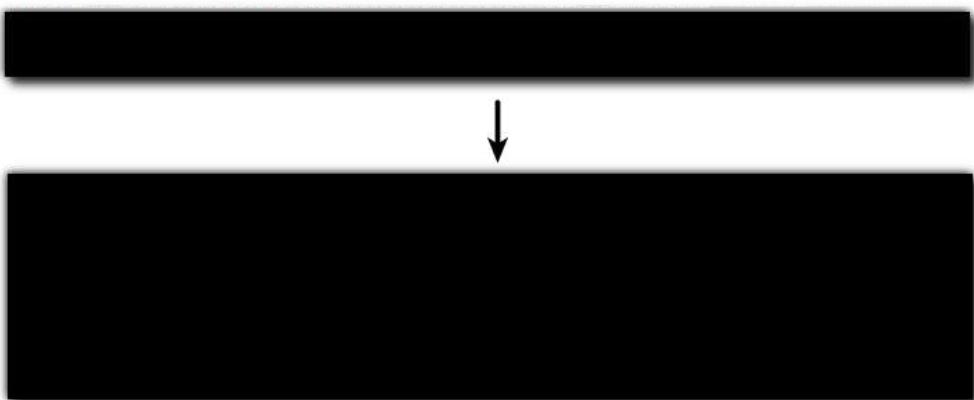
-
10. 관리콘솔에서 출력되는 로고를 업로드한 이미지로 변경합니다.



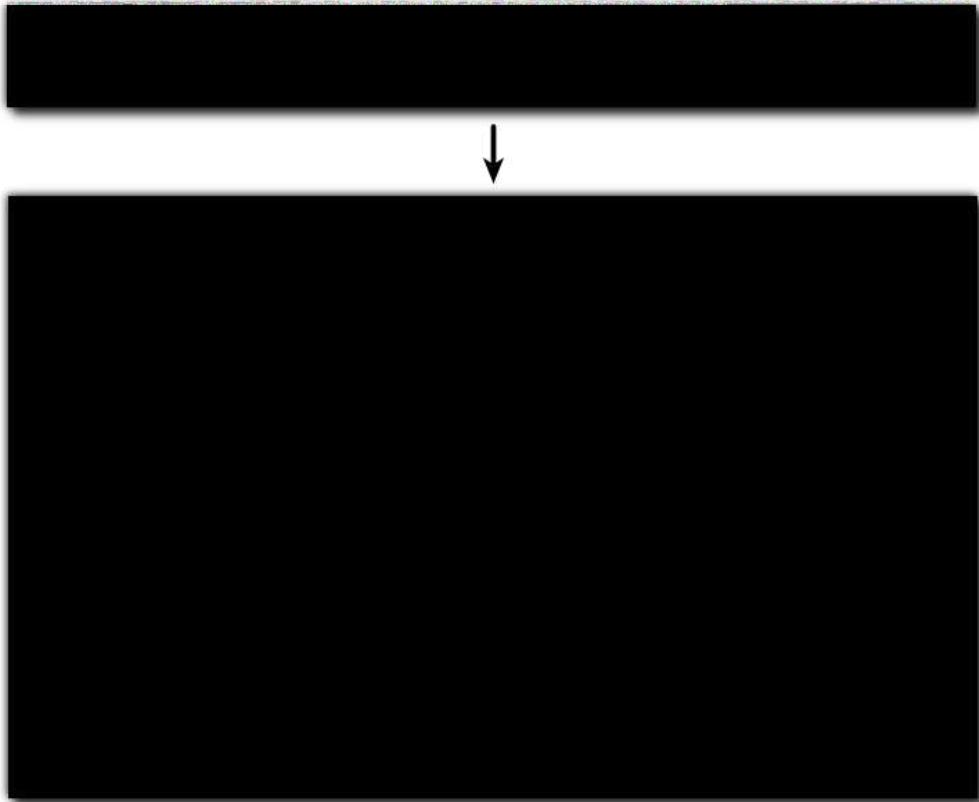
-
11. 페이지당 출력 열수를 변경 시, 변경된 열수로 기본값이 설정됩니다.



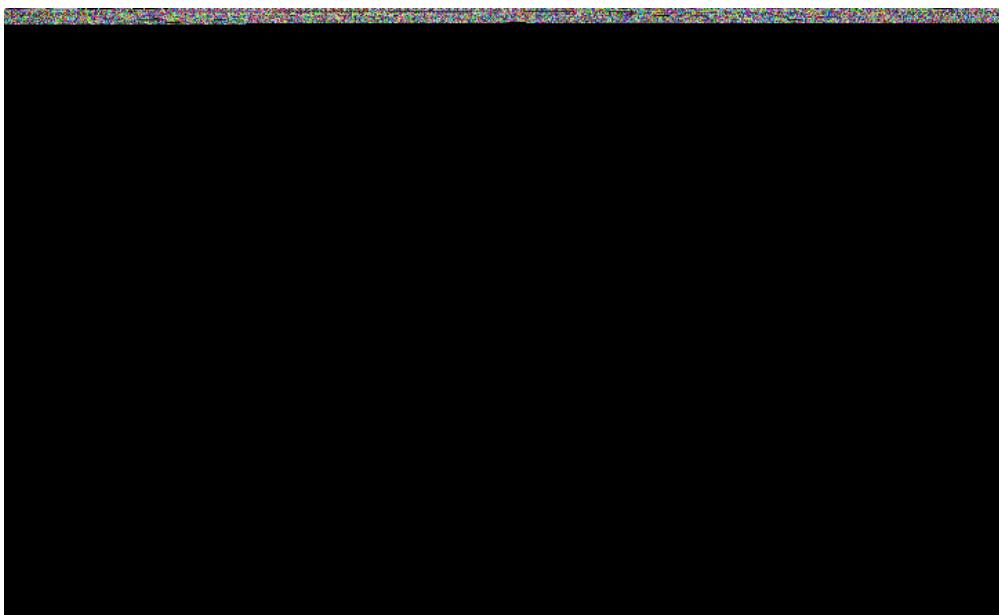
12. 세션 타임아웃 을 10분으로 설정일 시, NAC 홈페이지에서 아무것도 하지 않으면 10분 후 자동로그아웃 됩니다. 기본 값은 10분이며 최소 3분 ~ 최대 10분으로 설정할 수 있습니다.



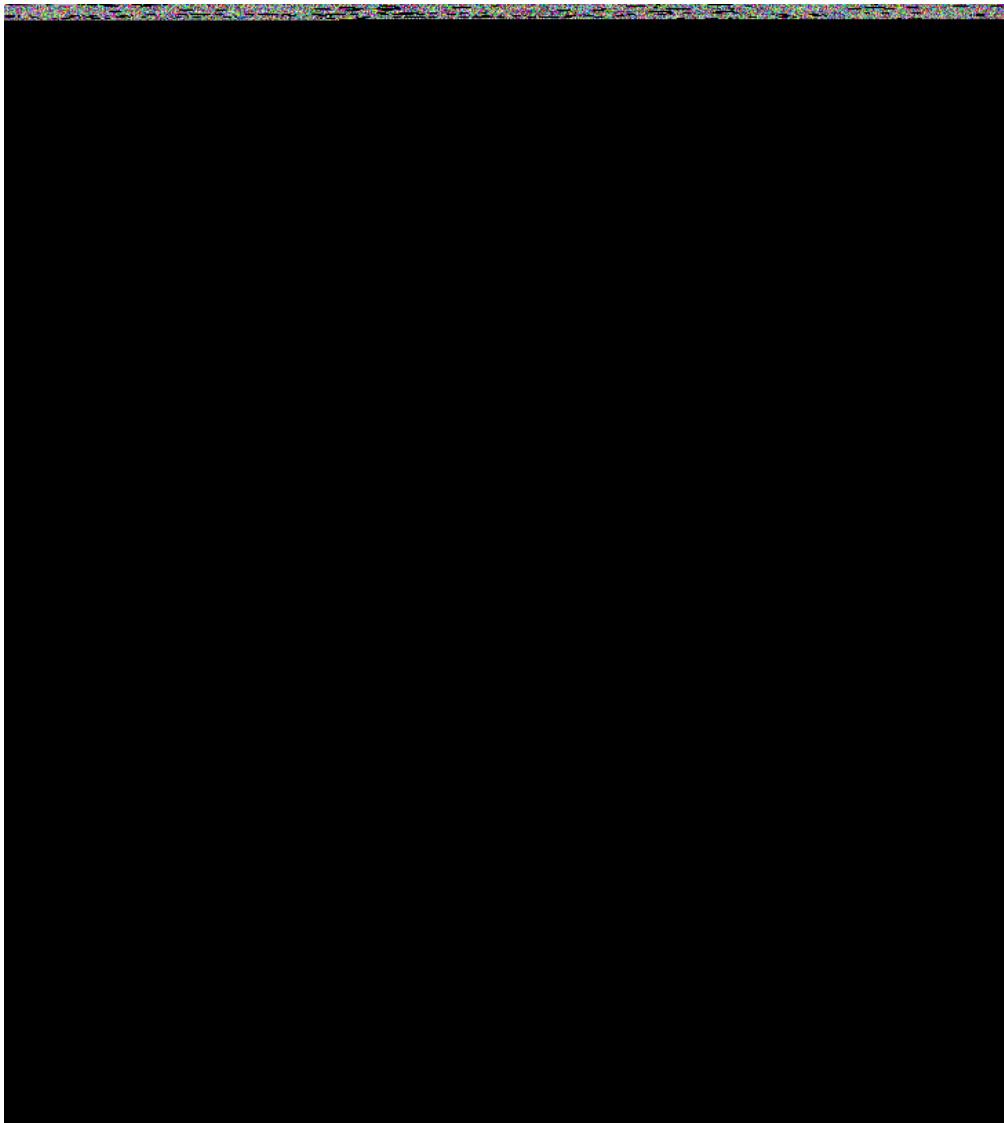
-
13. 로그인화면 문구를 HTML을 사용하여 관리자가 원하는데로 변경할 수 있습니다.



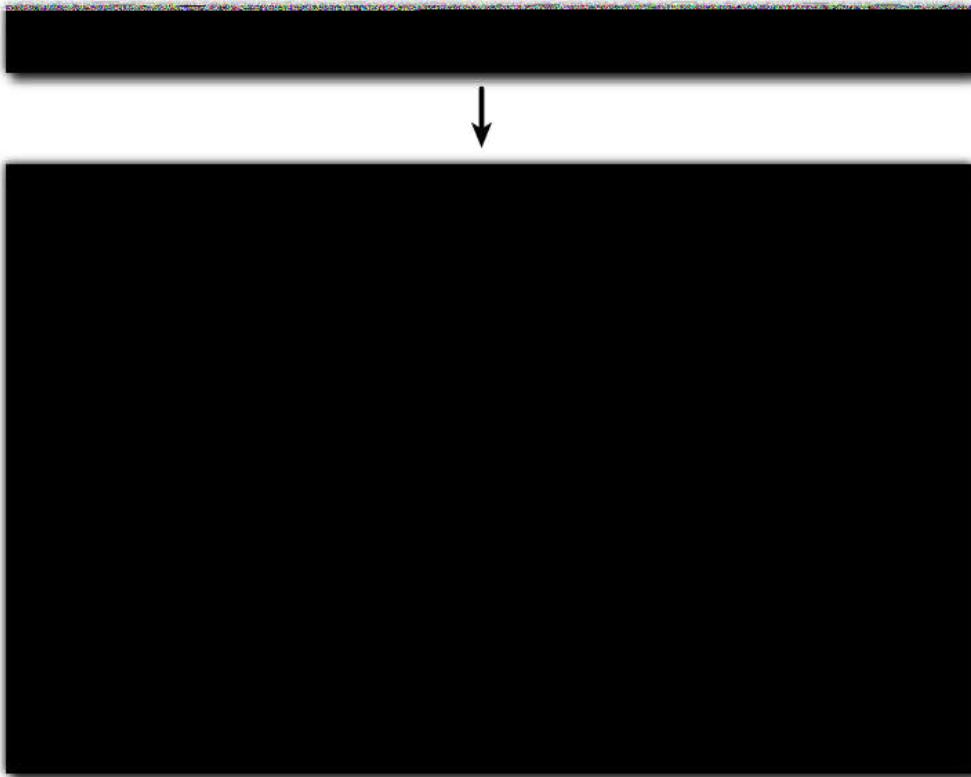
14. 2단계 인증으로 사용할 보안인증의 사용여부를 설정할 수 있습니다. 관리 > 사용자 > 관리자설정 > 2단계인증에서 2단계 인증을 설정할 수 있습니다.



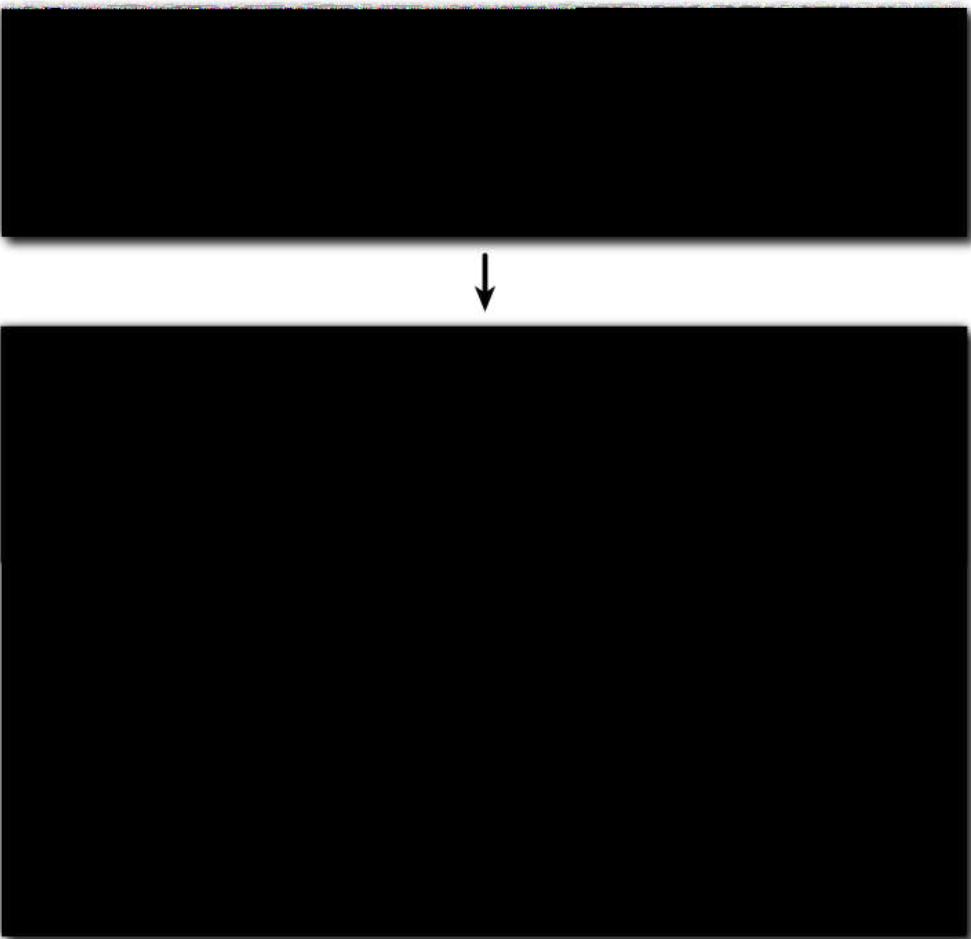
-
1. 관리자 로그인 페이지에서 관리자의 아이디 및 비밀번호 찾기 출력유무와 인증방법을 설정할 수 있습니다.



-
- 정책 > 그룹, 정책, 객체의 조건 출력 수를 설정할 수 있습니다.



- 로그인화면을 관리자가 원하는 그림과 색상으로 설정할 수 있습니다.

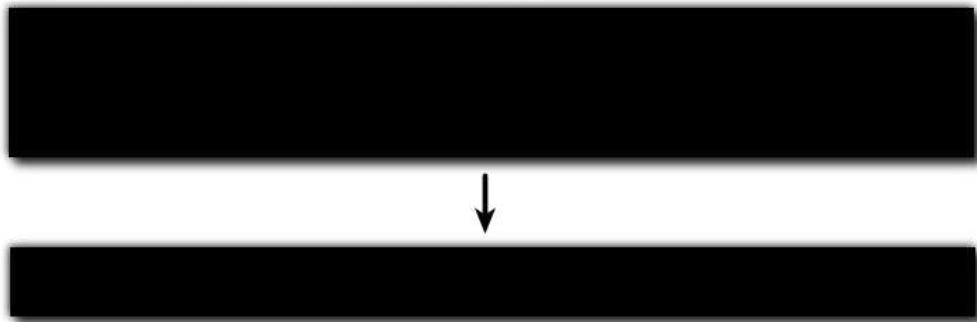


- 대시보드를 EXPORT하는 문서의 제목을 설정할 수 있습니다.



- CLI 배너

- CLI 배너에 관리자가 원하는 메시지를 입력 할 경우, Center, Sensor 장비의 CLI 접속 시 해당 메시지가 표시됩니다. CLI 접속방법은 [시스템 명령](#)을 참고바랍니다.



SSL 인증서

SSL 인증서

관리자는 서명요청서(CSR)을 이용하여 공인 SSL 인증서를 발급받아 NAC 웹 페이지에 등록할 수 있습니다.

- 1단계 : 서명요청서(CSR) 생성

호스트명, 국가코드, 회사/조직명, 이메일 입력 후 서명요청서(CSR)생성 버튼을 클릭합니다.



- 2단계 : 인증서등록

1단계에서 생성한 서명요청서(CSR)을 이용해 외부 인증서 발급기관에서 PEM 형식으로된 SSL인증서를 발급받습니다.
발급받은 인증서의 내용을 복사하여 인증서 항목에 붙여넣기를 수행하고 등록 버튼을 클릭 후 장비를 재부팅합니다.



- SSL 인증서 등록 완료

정상적으로 SSL 인증서 등록이 완료되면 다음 그림과 같이 출력됩니다.



백업

백업

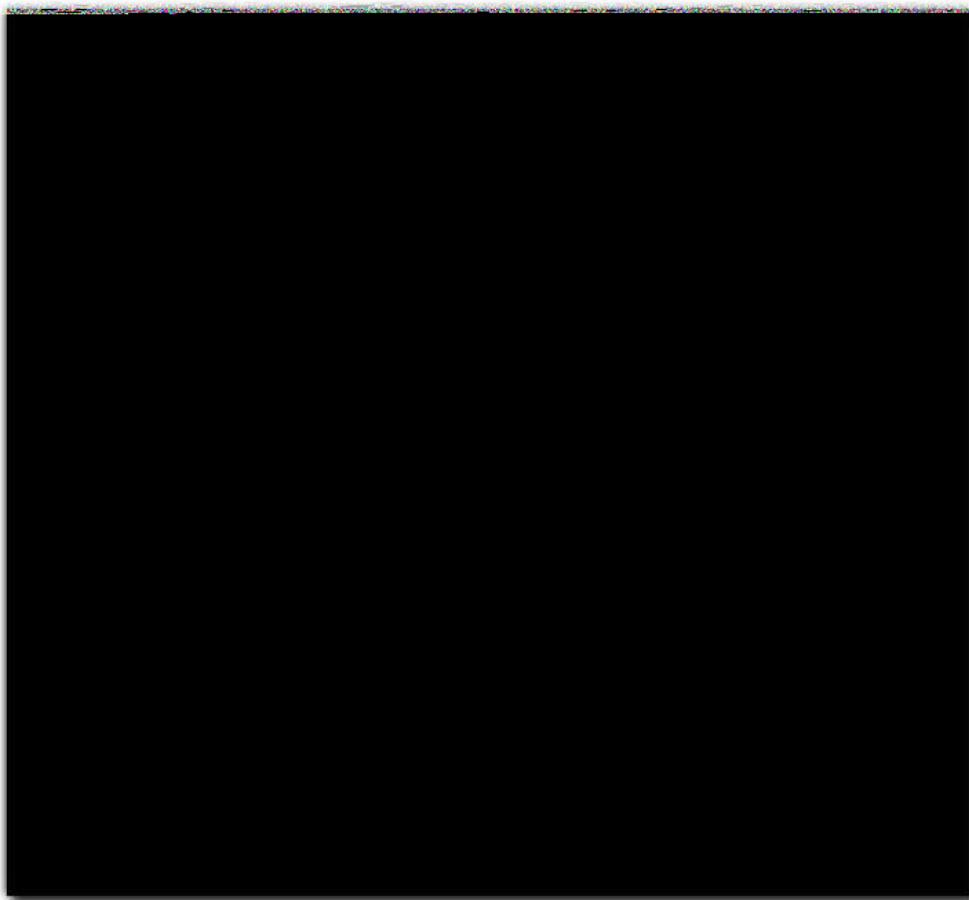
백업이란 만약의 상황에 대비하여 주기적 또는 관리자의 명령 시, 지정된 위치로 감사기록, 각종 환경설정 파일, 에이전트 파일 등을 사본을 만들어 지정된 위치에 저장해 두는 것을 말합니다.



백업을 수행하지 않을 시 장애가 발생할 때 기존에 있던 설정 및 정보, 로그를 복구할 수 없습니다.

- 백업수행

관리자는 설정 > 환경설정 > 백업 페이지를 이용하여 백업의 자동수행여부, 저장장치등을 설정할 수 있습니다.



백업 수행의 설정 내용은 아래와 같습니다.

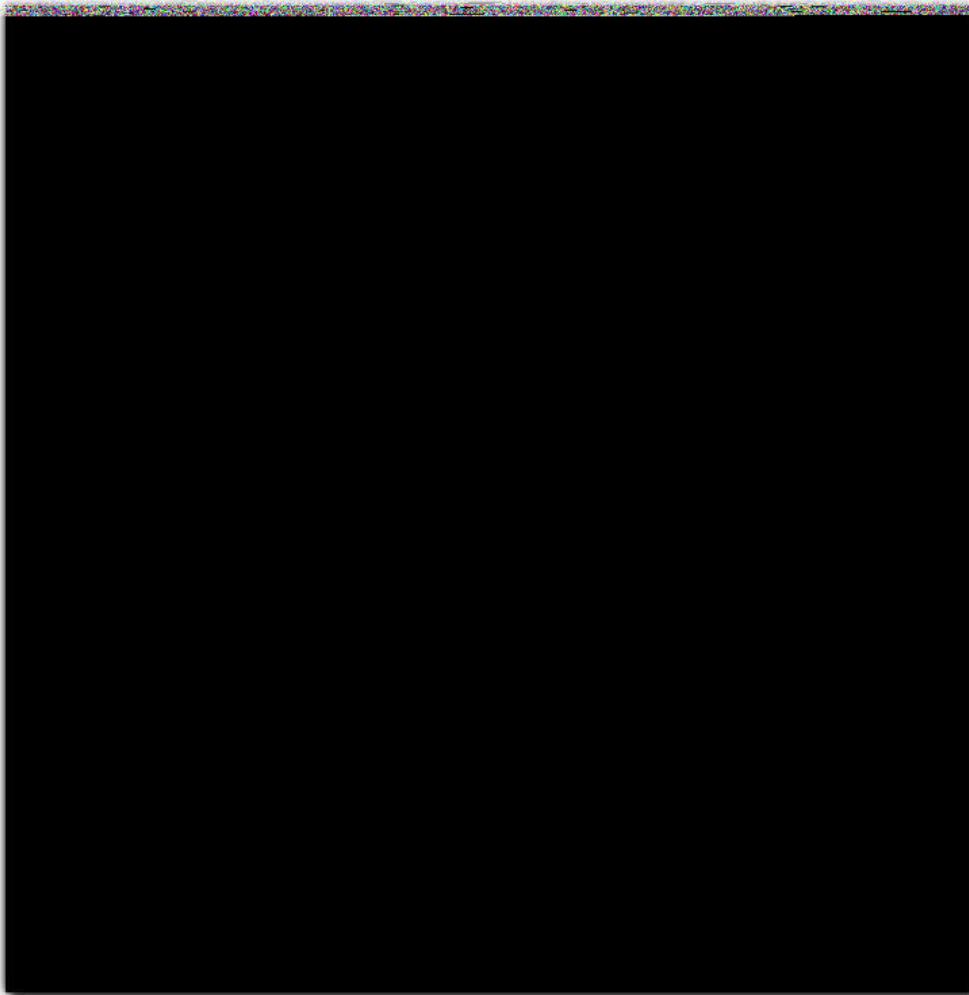
이름	옵션	내용
백업수행여부	on	백업 설정에 따라 백업을 수행합니다.
	off	백업을 수행하지 않습니다.
백업수행시각		데이터 베이스 백업작업을 수행할 시각을 설정 합니다.
여유공간보호		디스크 여유 공간을 설정합니다. 최소 10% 이상이며 설정된 비율만큼 디스크 공간은 남기며, 설정된 비율만큼에 디스크 공간이 남았을 시 가장 오래된 백업 파일을 삭제하고 백업을 수행합니다.
실행	지금시작	지금 즉시 백업을 수행합니다.
저장장치	로컬디스크	GenianNAC 장비에 백업 파일을 저장합니다. 저장된 백업파일은 시스템 명령 에서 show 명령어를 참고하시기 바랍니다.
	외부저장장치	장비에 부착된 외부저장장치에 백업 파일을 저장합니다.
	CIFS저장장치	공유 폴더(CIFS)에 백업 파일을 저장합니다.

	NFS저장장치	NFS서버에 백업 파일을 저장합니다.
	FTP SERVER	FTP 서버에 백업 파일을 저장합니다.
	SFTP SERVER	SFTP 서버에 백업 파일을 저장합니다.
사용자ID		저장 장치에 접근할때 필요한 ID를 설정합니다. 이 기능은 저장장치의 옵션이 CIFS 저장장치, FTP SERVER 경우에 설정할 수 있습니다.
사용자비밀번호		저장 장치에 접근할때 필요한 비밀번호를 설정합니다. 이 기능은 저장장치의 옵션이 CIFS 저장장치, FTP SERVER 경우에 설정할 수 있습니다.
백업파일보존여부	on	저장장치 설정이 로컬디스크 이외 일 때 활성화 되며, 로컬 외 다른 장치에 백업을 수행할 시 로컬에도 백업 파일이 남으며, 외부장치에도 백업 파일이 남습니다.
	off	저장장치 설정이 로컬디스크 이외 일 때 활성화 되며, 로컬 외 다른 장치에 백업을 수행할 시 로컬에는 백업 파일이 남지 않고, 외부장치에만 백업 파일이 남습니다.
백업저장장치경로		백업 파일을 저장할 경로를 설정합니다. 외부저장장치 설정 예: /dev/sdc1 CLI 콘솔에서 show filesystem 명령어를 입력해 주어야 저장장치가 마운트됩니다. CIFS저장장치 설정 예: \\192.168.1.73\backup NFS저장장치 설정 예: 192.168.1.73:/backup FTP SERVER 설정 예: ftp 서버에 ID/PASSWORD존재시 위 사용자ID, 사용자비밀번호란에 로그인정보를 입력합니다. 저장장치경로에는 SERVER 주소가 ftp://geni.com 이면 geni.com만 기입, 로컬디스크의 경우는 설정하지 않습니다.
백업파일 다운로드		백업목록 버튼을 클릭하여 백업파일을 확인할 수 있으며, 백업파일명을 클릭하여 백업파일을 다운로드할 수 있습니다.

에이전트

에이전트

관리자는 설정 > 환경설정 > 에이전트 페이지에서 에이전트에 관한 설정을 변경할 수 있습니다.



에이전트의 설정 내용은 아래와 같습니다.

항목 이름	설정 값	설명
설치 경로		디폴트 설치 경로에 설치하지 않고 별도의 경로에 에이전트를 설치하고 싶을 경우 별도의 설치 경로를 입력합니다.
설치전 사용자확인	ON	에이전트를 설치하기 전에 설치 여부를 창을 띠웁니다.
	OFF	에이전트의 설치 여부 상관없이 설치 합니다.
설치과정 표시	ON	에이전트를 설치진행 창을 띠어 에이전트의 설치 과정을 확인 할 수 있습니다.
	OFF	에이전트 설치진행 창을 띠우지 않고 설치 됩니다.
설치완료 메시지 표시	ON	설치과정 표시 설정이 ON으로 되어 있어야 설정 가능하며, 에이전트가 설치 완료되면 완료되었다는 창을 띠웁니다.
	OFF	에이전트가 설치 완료되었어도 설치 완료되었다는 창을 보여주지 않습니다.
설치정보 등록	ON	에이전트 설치 정보를 제어판의 프로그램 추가/제거에 등록 됩니다, 프로그램 추가/제거를 통해 에이전트를 삭제할 수 없습니다.
	OFF	에이전트 설치 정보가 제어판의 프로그램 추가/제거에 등록되지 않습니다.

자동업데이트 대상	네트워크 그룹	많은 노드들이 한번에 자동 업데이트를 할 시 NAC가 다운 될 수 있어 배포네트워크에 설정된 네트워크 그룹에 속한 노드만 자동 업데이트가 진행 됩니다. 이 기능을 통해 부하가 걸리지 않을 만큼의 노드들을 그룹으로 설정하여 많은 노드들을 나누어서 자동 업데이트를 할 수 있습니다.
서비스 대상그룹	네트워크 그룹	에이전트 서비스할 대상을 설정합니다. 서비스 이외의 대상은 에이전트가 설치되었어도 동작하지 않습니다.
내상태 확인 메뉴 표시	ON	에이전트 트레이 메뉴에서 내 상태를 확인할 수 있는 "내상태 확인" 메뉴를 표시 합니다. 해당 메뉴를 클릭할 시 CWP 페이지로 이동합니다.
	OFF	에이전트 트레이 메뉴에 "내상태 확인" 메뉴가 표시되지 않습니다.
웹브라우저	Internet Explorer	에이전트가 웹페이지를 표시하는 데 Internet Explorer 브라우저를 선택합니다.
	경로 입력	사용할 웹브라우저의 경로를 직접 입력합니다.
IE 웹브라우저 모양	표준	에이전트를 통하여 웹페이지에 접속할 경우 일반 웹페이지와 같은 창으로 접속 됩니다.
	간략	에이전트를 통하여 웹페이지에 접속할 경우 일반 웹페이지에 있는 도구, 주소창, 툴바 등이 보이지 않는 웹페이지로 접속 됩니다.
IE 웹브라우저 크기	표준	에이전트를 통하여 웹페이지에 접속할 경우 800x600 크기의 웹페이지를 팝업합니다.
	최대화	에이전트를 통하여 웹페이지에 접속할 경우 최대화한 웹페이지를 팝업합니다.
에이전트 커스텀 아이콘	add	에이전트의 트레이 아이콘에 사용될 커스텀 아이콘(ICO파일)을 업로드 합니다. 커스텀 아이콘을 설정하면 인증상태와 상관없이 항상 고정된 아이콘만 표시됩니다. X 아이콘을 클릭하여 업로드한 이미지를 삭제할 수 있습니다.
KeepAlive 전송주기	초, 분	센터와 에이전트의 통신 상태를 주기적으로 알아보기 위한 기능입니다. default : 2분 최소값 : 30초 최대값 : 10분
절전모드 재시작 시간	분, 시간	절전모드 진입 후 해당 옵션의 설정 시간을 경과했을 경우 재부팅으로 인식합니다. Windows 8은 해당 옵션에 따라 재부팅 시 재인증 기능이 동작합니다.
센터 SSL인증서 설치	ON	에이전트가 자동 업데이트 스캔을 할 시 SSL 인증서가 설치 됩니다. 인증서가 설치 될 시 NAC UI에 접속 할 때 뜨는 보안 인증서 관련 창이 더 이상 보이지 않습니다.
	OFF	자동 업데이트 스캔을 하여도 SSL 인증서가 설치 되지 않습니다.

운영체제 업데이트

운영체제 업데이트

패치를 위한 패치 업데이트 서버를 설정하고, 동기화를 위한 프록시 서버를 설정합니다.

- 패치서비스

패치파일을 검색할 업데이트 서버를 설정하고 업데이트 서버에서 패치파일을 다운로드 받을 연결방법을 선택합니다.



항목	옵션	내용
검색방법	Microsoft Windows Update	Microsoft 사이트에서 직접 Windows에 필요한 패치파일을 검색하는 방법입니다.
	WSUS	Windows Server Update Services를 지정하여 그곳에서 Windows에 필요한 패치파일을 검색하는 방법입니다.
	Offline Scan File	폐쇄망일 경우에 사용되는 옵션이며, Genian Syncer를 이용하여 MS의 최신 패치 정보를 센터에 업로드 합니다. 노드는 외부 네트워크로 접속할 필요 없이 내부에 있는 센터에 접속하여 Windows에 필요한 패치파일을 검색 합니다.
WSUS서버 IP		검색방법 설정을 WSUS으로 설정할 시 활성화 되며, Windows Server Update Services의 IP를 입력합니다.
연결방법	Microsoft/WSUS 직접연결	검색방법이 Microsoft Windows Update 또는 WSUS일 경우 선택한 서버에서 직접 패치파일을 다운로드 합니다.
	센터를 통한 연결 (다운로드)	NAC 센터를 프록시 서버로 설정 후 패치파일을 다운로드합니다. NAC 센터를 프록시로 설정 후 다운로드한 패치파일은 노드에도 설치되고 센터의 캐시서버에도 설치됩니다. 캐시서버에 설치된 패치파일은 다른 노드가 해당 패치파일이 필요할 경우 MS 또는 WSUS에 접속할 필요 없이 센터의 캐시서버에서 더욱 빠르게 다운로드 받을 수 있습니다. 해당 옵션을 사용하기 위해 패치 Proxy 서비스 설정이 되어 있어야 하며 설정 방법은 시스템관리 에서 환경설정 부분을 참고 바랍니다.
	센터를 통한 연결 (다운로드+검색)	다운로드와 검색 모두를 센터를 프록시로 설정 후 이용합니다. 센터만 외부 네트워크를 사용할 수 있는 환경일 경우 노드들이 Microsoft 사이트 및 WSUS에 접속하지 못하여 검색 및 다운로드가 불가능하게 됩니다. 하지만, 해당 옵션을 이용하여 센터를 프록시로 설정할 시 노드들이 Microsoft 사이트 및 WSUS에서 검색 및 다운로드를 할 수 있게 됩니다. 해당 옵션을 사용하기 위해 패치 Proxy 서비스 설정이 되어 있어야 하며 설정 방법은 시스템관리 에서 환경설정 부분을 참고 바랍니다.
연결방법	Apple 직접연결	접속허용 도메인 옵션에 있는 서버에서 패치파일을 검색 및 다운로드하는 방법입니다.

	NAC를 통한 연결(다운로드)	NAC 센터를 프록시 서버로 설정 후 패치파일을 다운로드합니다. NAC 센터를 프록시로 설정 후 다운로드한 패치파일은 노드에도 설치되고 센터의 캐시서버에도 설치됩니다. 캐시서버에 설치된 패치파일은 다른 노드가 해당 패치파일이 필요할 경우 업데이트 서버에 접속할 필요 없이 센터의 캐시서버에서 더욱 빠르게 다운로드 받을 수 있습니다. 해당 옵션을 사용하기 위해 패치 Proxy 서비스 설정이 되어 있어야 하며 설정 방법은 시스템관리 에서 환경설정 부분을 참고 바랍니다.
	NAC를 통한 연결(다운로드+검색)	다운로드와 검색 모두를 센터를 프록시로 설정 후 이용합니다. 센터만 외부 네트워크를 사용할 수 있는 환경일 경우 노드들이 업데이트 서버에 접속하지 못하여 검색 및 다운로드가 불가능하게 됩니다. 하지만, 해당 옵션을 이용하여 센터를 프록시로 설정할 시 노드들이 업데이트 서버에서 검색 및 다운로드를 할 수 있게 됩니다. 해당 옵션을 사용하기 위해 패치 Proxy 서비스 설정이 되어 있어야 하며 설정 방법은 시스템관리 에서 환경설정 부분을 참고 바랍니다.
Proxy 서버		프록시 서버를 설정하여 설정한 프록시 서버를 이용하여 패치파일을 다운로드 합니다. 한번이라도 다운로드한 패치파일은 Proxy 서버에 캐시로 저장하고 있어 파일이 없어도 프록시 서버를 통하여 파일 받을 수 있습니다.
접속허용 도메인		제어정책에 의해 네트워크 차단 시 업데이트를 위해 접속을 허용할 업데이트 서버 도메인을 설정합니다.

기타설정

기타설정

관리자는 설정 > 환경설정 > 기타설정 페이지를 통하여 문자셋, 메일서버, SMS 발신번호등을 설정할 수 있습니다.

- 기타 설정



기타 설정의 설정 내용은 아래와 같습니다.

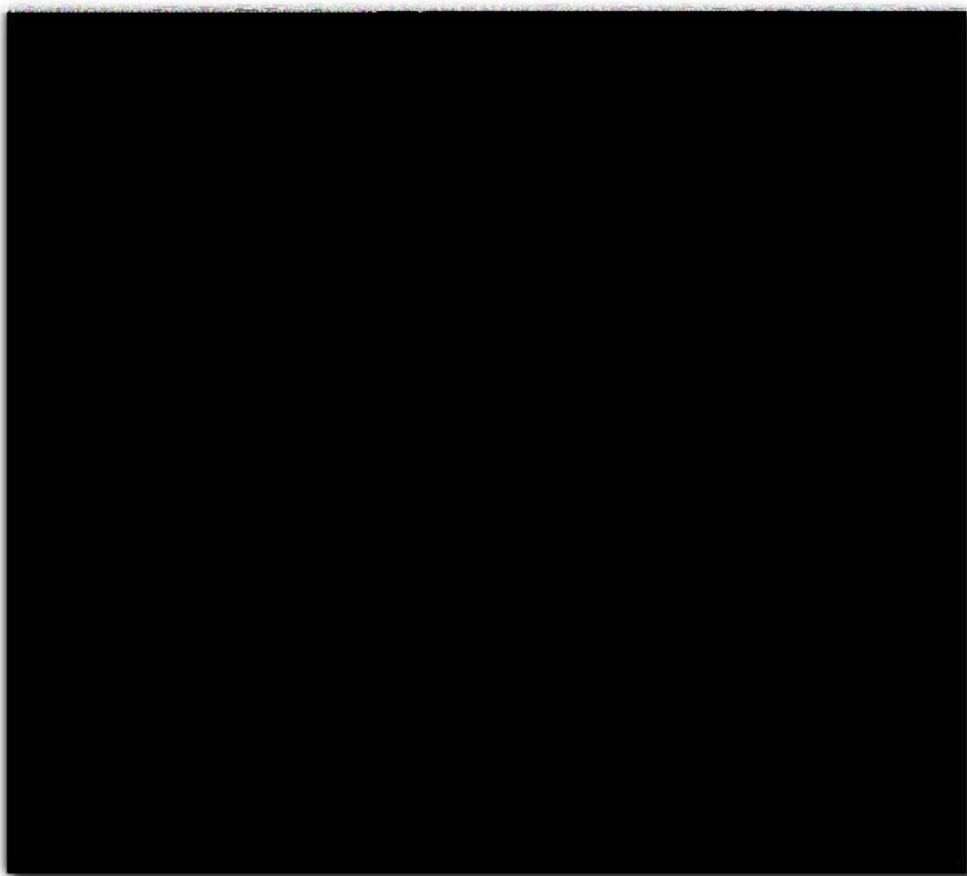
항목 이름	설정 값	설명
인터넷연결	ON	최신 업데이트, 알람 기능 등으로 인터넷을 통하여 할 수 있는 기능들을 할 수 있습니다. NAC를 폐쇠망에서 사용할 시 off로 설정합니다.
	OFF	최신 업데이트, 알람 기능, 등으로 인터넷을 통하여 할 수 있는 모든 기능을 사용하지 않습니다.
Proxy Server		사용할 Proxy Server를 설정합니다.
Proxy 예외		Proxy 예외할 주소를 설정합니다.
파일크기		관리 페이지에 파일 업로드 시 최대로 보낼 수 있는 최대 파일크기를 설정합니다. 단위 : MB
센터 Domain Name		센터의 도메인명을 설정합니다.
센터 NAT IP	IP	멀리 떨어져 있는 센터와 센서 사이에 NAT장비가 있을 시 센터와 붙어 있는 NAT장비의 IP Address를 입력하여 센터와 센서간에 통신이 가능하도록 설정합니다.
센터 NAT IP 예외대역	IP	센터 NAT IP 설정이 있을 경우 내부에 있는 노드가 센터와 통신할 때 센터 NAT IP로 통신하기 때문에 내부에 있는 노드들은 예외로 처리하여 센터와 정상적으로 통신할 수 있도록 합니다.

- 메일서버

메일 알람 기능을 이용하기 위해 메일서버 설정을 해주어야 합니다.



메일 서버 설정이 되어 있지 않을 경우 이메일 관련 기능을 사용할 수 없습니다. 이메일 관련 기능을 사용하기 위해선 메일 서버 설정이 필수로 되어 있어야 합니다.



메일 서버의 설정 내용은 아래와 같습니다.

항목 이름	설정 값	설명
메일서버	직접입력, 구글메일서버	메일 알람에 사용될 메일 서버를 선택합니다.
서버주소	메일서버 IP, 메일서버 도메인명	메일서버 IP, 도메인명을 입력 합니다.
서버포트	포트번호	메일서버의 포트를 입력 합니다.
송신자주소	이메일 주소	임의로 송신자 이메일 주소를 입력 합니다. 입력한 송신자 이메일 주소로 이메일이 전송 됩니다.
송신자이름	이름	송신자의 이름을 임의로 입력 합니다.
접속보안	SMTP(25)	암호화를 하지 않고 이메일을 전송 합니다.
	SMTP(465)	SSL 암호화하여 이메일을 전송 합니다.
	MSA/STARTTLS(587)	TLS 암호화하여 이메일을 전송 합니다.
인증사용자	ID	메일서버의 인증을 받기위해 필요한 아이디를 입력 합니다.
인증비밀번호	비밀번호	인증사용자 항목에 입력한 ID의 비밀번호를 입력 합니다.
설정테스트		수정 버튼을 클릭 후 메일설정을 토대로 메일을 전송해볼수 있습니다. 사용자가 메일을 받았을 경우 메일설정이 정상적으로 되었고, 사용자가 메일을 받지 못하였을 경우 메일설정이 잘못되었습니다.

코드 발급		메일서버 설정이 구글메일서버일 경우 활성화 되며, 송신자주소에 입력한 계정으로 로그인 후 인증코드를 발급받습니다.
구글 인증 코드		메일서버 설정이 구글메일서버일 경우 활성화 되며, 코드 발급에서 발급받은 인증코드를 입력합니다.

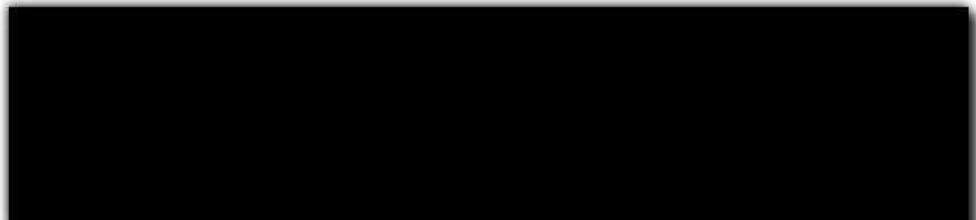
- SMS 설정



sms의 설정 내용은 아래와 같습니다.

항목 이름	설정 값	설명
SMS 서비스 종류	국내SMS	휴대폰 문자 메시지에 표시할 발신번호를 설정합니다.
	국제SMS	사용자/관리자의 국제전화번호에 국가번호가 설정되지 않은 경우 기본 국가번호로 SMS를 발송합니다.

- 운영정보 데이터 설정



운영정보 데이터의 설정 내용은 아래와 같습니다.

항목 이름	설정 값	설명
검사주기	시간, 일, 주, 개월	운영정보 데이터 버전 체크 주기를 설정합니다.
자동업데이트	ON	운영정보 데이터 버전이 최신 버전이 아닐 경우 검사주기에 자동업데이트를 수행합니다.
	OFF	시스템 > 업데이트관리 > 운영정보 데이터에서 수동으로 업데이트 할 수 있습니다.

시스템

시스템

관리자는 시스템 탭을 이용하여 시스템, 업데이트, 서비스를 관리할 수 있습니다.
설치되어 있는 장비목록을 확인할 수 있습니다.

- 시스템 : 센서, 센터, Air-Sentry에 관련된 다양한 설정과 관리를 할 수 있는 탭입니다.
- 업데이트 관리 : NAC, 에이전트, 플러그인, 데이터를 업그레이드 할 수 있는 탭입니다.
- 서비스 관리 : 정책 재적용 할 수 있고 적용중인 서비스를 일시적으로 중단할 수 있으며 웹 페이지를 재구동할 수 있는 탭입니다.
- 시스템
- 업데이트 관리
- 서비스 관리

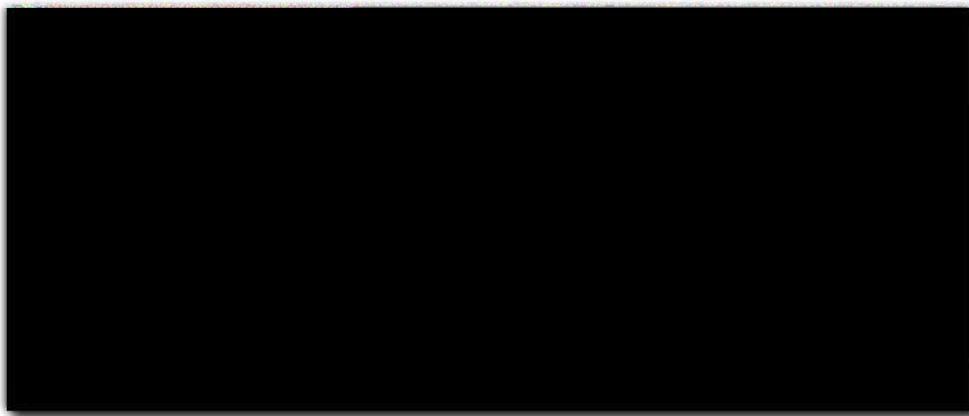
시스템

시스템

관리자는 시스템 탭을 이용하여 시스템관리, 세션관리, 라이센스를 관리할 수 있습니다.

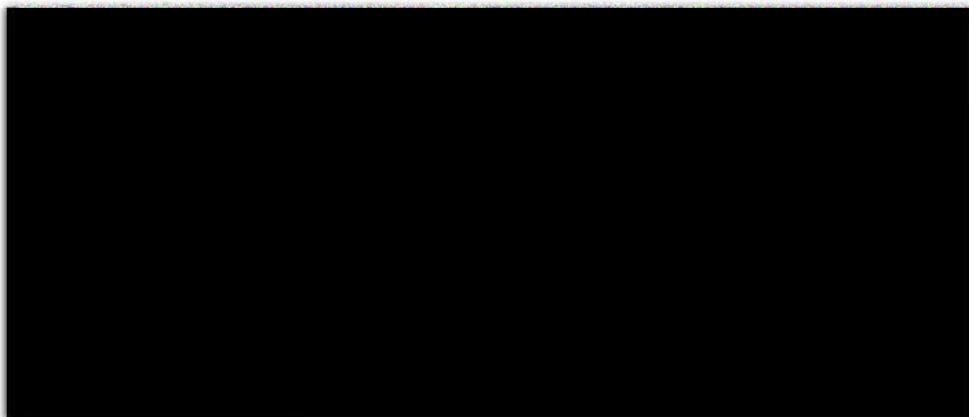
- 시스템관리

Genian 장비의 세부 시스템에 관련된 설정을 할 수 있습니다.



- 센서관리

센서 관련 설정을 다양한 방식으로 설정할 수 있으며 센서의 현황을 파악할 수 있습니다.



- 시스템초기 설정

새로운 센서장비의 초기설정을 할 수 있습니다.



- 세션관리

접속한 장비의 세션을 관리할 수 있습니다.



- 라이센스

라이센스 정보를 관리할 수 있습니다.



- 시스템관리
- 센서관리
- 시스템초기 설정
- 세션 관리
- 라이센스

시스템관리

시스템 작업선택

관리자는 시스템관리 페이지를 이용하여 시스템 상세정보확인, 센서설정, 장비재기동/삭제 등 Genian NAC의 시스템에 직접적인 설정을 할 수 있습니다.



- 장비태그설정

장비에 태그를 설정할 수 있습니다.
[노드 태그 설정](#)과 같은 설정방법이오니 참고하시기 바랍니다.

- CLI 비밀번호 변경

CLI 비밀번호 변경할 장비 선택 후 작업선택 > CLI 비밀번호 변경 을 선택하여 CLI 비밀번호를 변경합니다.



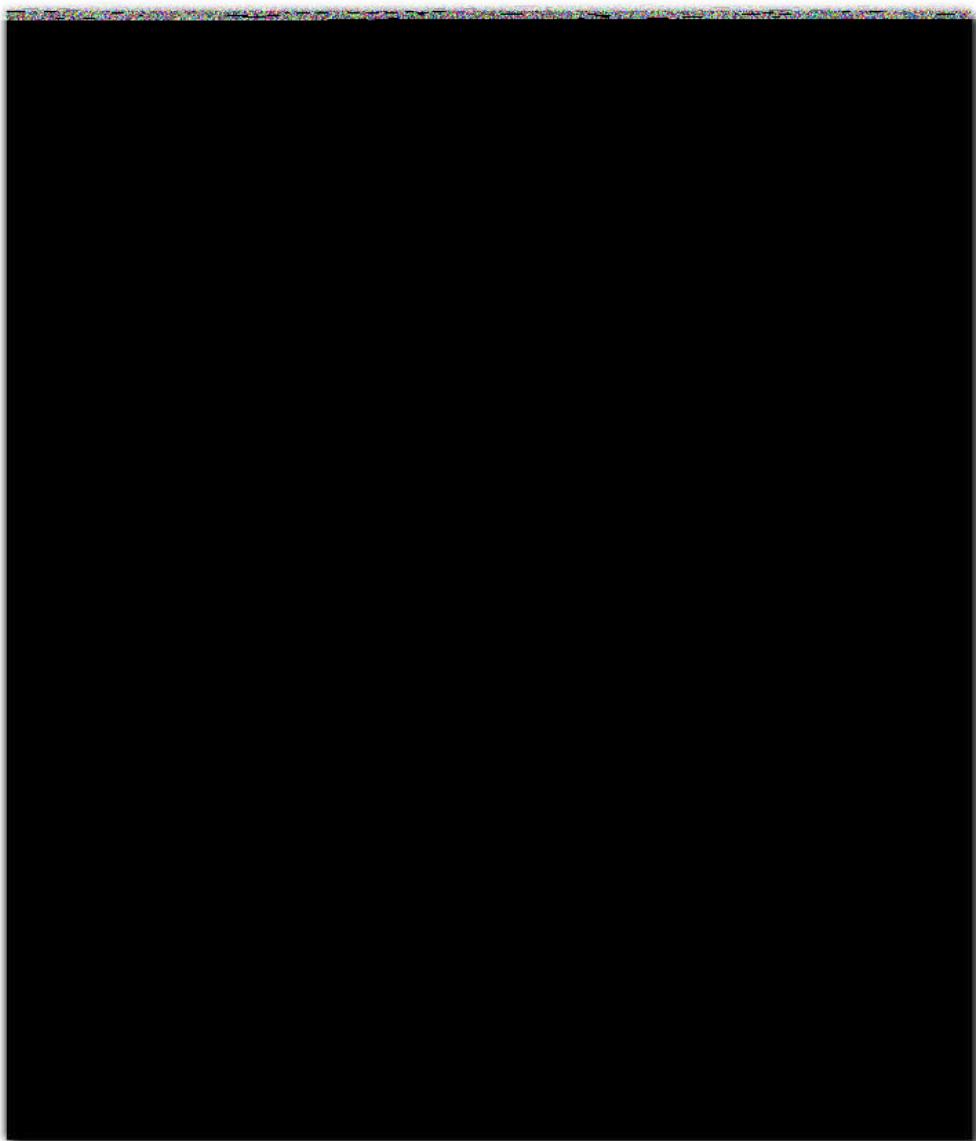
- CLI Enable 비밀번호 변경

CLI Enable 비밀번호 변경할 장비 선택 후 작업선택 > CLI Enable 비밀번호 변경 을 선택하여 CLI Enable 비밀번호를 변경합니다.



- 센서 일괄 설정

여러 센서의 센서설정을 한번에 일괄 설정할 수 있습니다.



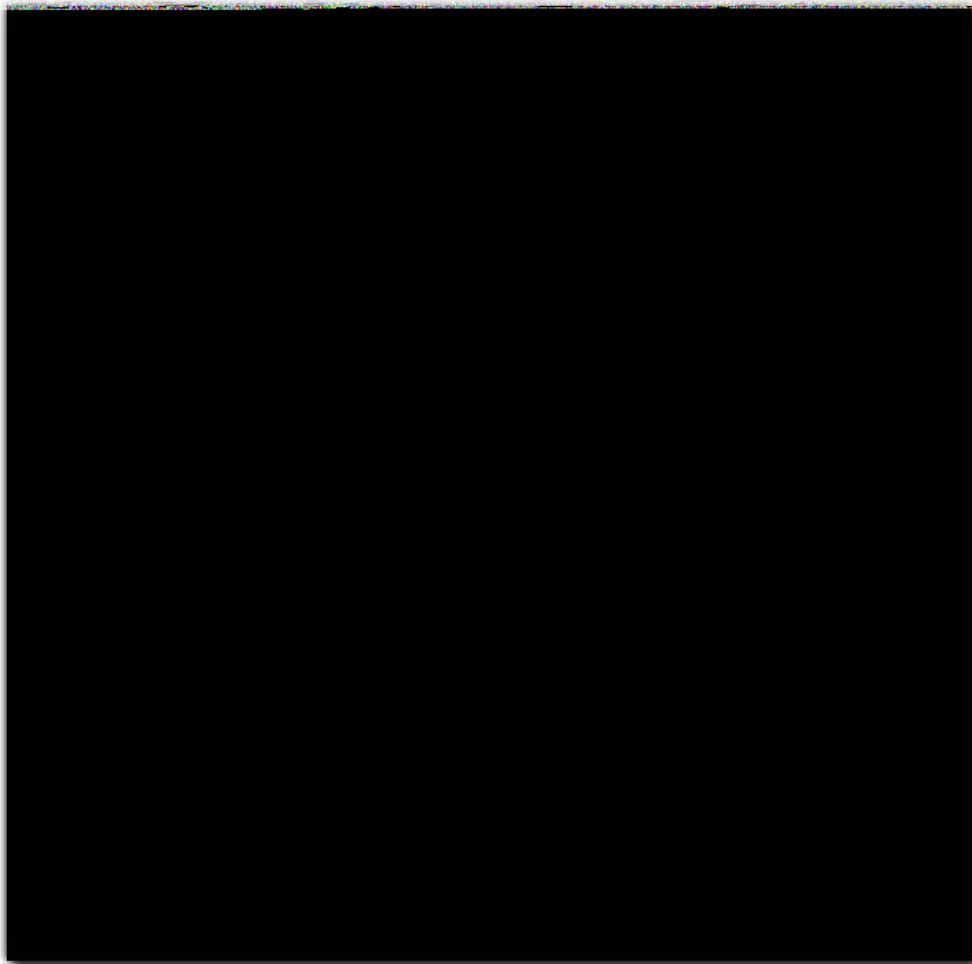
- 장비 일괄 설정

여러 센터/센서 환경설정을 한번에 일괄 설정할 수 있습니다.



- 무선센서 일괄 설정

여러 무선센서의 환경설정을 한번에 일괄 설정할 수 있습니다.



- 센서 설정 조회

여러 센서의 센서 설정을 조회 할 수 있습니다.



- 장비 설정 조회

여러 센서/센터의 환경설정을 조회할 수 있습니다.



- 무선센서 설정 조회

여러 무선센서의 환경설정을 조회할 수 있습니다.



- 장비삭제

삭제 하고싶은 장비를 선택 후 작업선택 > 장비삭제 를 선택하여 장비를 삭제합니다.

- 시스템 업그레이드

- 시스템 > 업데이트 관리 > 시스템 OS 페이지에서 이미지 파일을 업로드 합니다.

이미지 업로드 방법은 [소프트 웨어](#)를 참조해 주시기 바랍니다.

- 시스템 > 시스템 > 시스템관리 페이지로 이동하여 업그레이드할 장비를 선택하고 작업선택 > 시스템 업그레이드 를 클릭합니다.

- 이미지선택 업그레이드

이미지를 선택하여 현재 이미지의 버전에 관계 없이 upgrade 및 downgrade를 할 수 있습니다.



- 시스템 재기동

재기동 하고싶은 장비를 선택 후 작업선택 > 시스템 재기동 을 선택하여 시스템을 재기동합니다.

- 시스템 셧다운

셧다운 하고싶은 장비를 선택 후 작업선택 > 시스템 셧다운 을 선택하여 시스템을 셧다운합니다.

기본정보/시스템 정보/상태정보/IP 설정/센서설정/환경설정/제어

시스템 > 시스템 > 시스템관리 페이지에서 시스템의 IP를 선택하면 해당 IP를 사용하는 시스템의 기본정보/시스템 정보/상태정보/IP 설정/센서설정/환경설정/제어 작업을 수행할 수 있습니다.



- 기본정보

장비의 기본정보를 볼 수 있습니다. 장비의 이름과 설명을 기입할 수 있으며, 작업지시를 통하여 서브넷 노드스캔과 배포 동기화 작업을 즉시수행할 수 있습니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
장비 ID		센터가 센서를 정확하게 식별하기 위한 ID입니다.
최초등록		장비가 설치된 날짜입니다.
이름	입력	호스트명으로 등록 됩니다.
설명	입력	장비에 대한 설명을 적는곳입니다.
모델명		해당 장비의 모델명을 확인할 수 있습니다.
제품버전		현재 장비가 사용하고 있는 NAC 버전을 확인할 수 있습니다.
シリ얼		장비의シリ얼넘버를 확인할 수 있습니다.
작업지시	서브넷 노드스캔 즉시수행	해당 장비에 속해있는 노드들만 즉시 노드스캔 합니다.
	배포 동기화 즉시수행	현재 센터가 배포하고 있는 파일을 해당 장비에도 동기화 하여 해당 장비에 속해 있는 노드들도 배포 파일을 다운 받을 수 있습니다.
태그		장비에 태그를 설정할 수 있습니다.

- 시스템정보

시스템 정보를 통해 센서 정보와 센서 하드웨어, 인터페이스, 배포현황 등의 정보를 확인할 수 있으며,

시스템정보의 최근갱신시각을 확인할 수 있고 [] 을 클릭하여 시스템정보를 갱신할 수 있습니다.

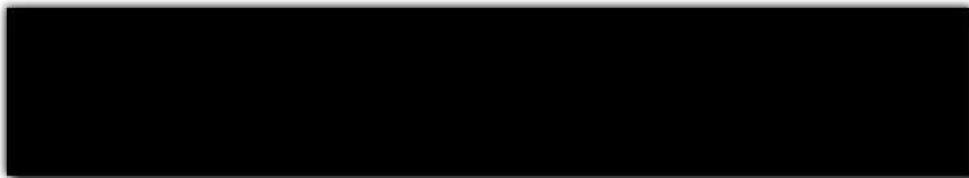


해당 페이지는 아래표와 같은 정보를 담고 있습니다.

정보	내용
센서정보	모델명, 가동시간, 디플트게이트웨이, DNS서버
CPU 정보	CPU 명, CPU 제조사, CPU 사용율, CPU 온도
메모리 정보	메모리 전체, 메모리 사용, 메모리 사용율, SWAP 전체, SWAP 사용, SWAP 사용율
저장장치정보	장치명, 총 용량, 사용된 용량, % 사용
인터페이스 정보	연결방식, 이름, MAC, IP/NETMASK, 게이트웨이, 링크, 속도, 전송방식
배포현황 정보	구분, 최근갱신시각, 최근동기화시각, 동기화상태

- 상태정보

센서의 인터페이스 상태를 확인할 수 있습니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

정보	내용
인터페이스 상태	이름, RX Bytes, RX Packets, RX Errors, RX Drops, TX Bytes, TX Packets, TX Errors, TX DROPS
Clustering 정보	IP, 마스터, 처리개수, 최초등록, 최근갱신

- IP설정

아래 그림은 IP 설정에서 eth0를 클릭한 그림입니다. 한 포트에 생성된 여러 IP 대역을 탐지할 수 있도록 설정할 수 있으며, 하니팟같은 가상 IP를 설정을 할 수 있습니다. 센서 IP와 가상IP가 부여 가능하며, 인터페이스의 마스터 주소는 콘솔을 연결하여 CLI를 통해서만 설정이 가능합니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	내용
센서 IP	한 포트에 여러 IP대역이 있을 경우, 센서 IP에 다른 대역 IP를 추가하여 추가한 IP대역의 노드를 탐지 및 제어할 수 있습니다.
가상 IP	가상 센서 IP를 생성하여 생성한 가상 센서 IP를 이용하여 패킷을 유도 합니다. 가상 센서 IP로 들어온 패킷은 가상 센서가 아닌 실제 센서가 받습니다.
가상 IP(자동설정)	가상 IP와 같은 기능이며, 센서설정 > 가상 IP 옵션에서 필요한 가상 IP만큼의 숫자를 입력할 시 입력한 숫자 만큼의 가상 IP가 자동으로 생성됩니다.

- 센서설정

센서설정을 변경하고싶은 인터페이스의 이름을 선택하여 센서설정을 변경 할 수 있습니다.



- 센서동작

센서의 동작모드와 운영모드에 대한 설정 항목입니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
센서 동작모드	None	센서 동작하지 않습니다.
	Host	센서가 동작 합니다.
	Mirror	센서가 미러모드로 동작합니다. 미러모드는 Redirection + Reject 방식으로 차단합니다.
ARP 차단 동작주기	초	차단 노드들의 arp 테이블을 설정한 주기마다 NAC MAC으로 모두 변경하여 외부네트워크로 접속하지 못하게 합니다.
ARP 차단 동작방식	Reply	차단 노드가 외부 네트워크로 접속을 하기 위해 arp를 이용할 시 arp 테이블을 변경하여 외부 네트워크로 접속하지 못합니다.
	Request	차단 노드들의 arp 테이블을 설정한 주기마다 NAC MAC으로 모두 변경하여 외부네트워크로 접속하지 못합니다.
로컬네트워크제어	on	차단 노드의 내부 네트워크를 차단 합니다.
	off	차단 노드의 외부 네트워크만 차단 합니다.

차단방법	HTTP Redirection + Drop	외부 네트워크로 접속 할려는 패킷을 중간에 NAC가 전부 폐기 합니다.
	HTTP Redirection + Reject	외부 네트워크로 접속할 때 TCP인 경우 RST 패킷을 전송하고 UDP인 경우 ICMP Port Unreachable 패킷을 전송 합니다.
미러 동작범위	Local	센서가 설치되어있는 네트워크 대역만 노드정보를 수집하고 제어합니다.
	Global	모든 IP 대역의 노드정보를 수집하고 제어합니다.
NAT IP 영역		미러모드 동작 시 실제 IP가 아닌 NAT IP로 제어할 대상 네트워크를 설정합니다. 1:1 NAT 환경에서 사용되며 NetAddress/CIDR 형식으로 여러줄로 입력 가능합니다.
센서 운영모드	Active	센서의 차단모드로써, 실제 제어를 수행합니다.
	Passive	센서의 스캔모드로써, 실제 제어를 수행하지 않습니다.
Active 동작시간	시간 객체	설정한 시간 객체를 기준으로 Active 동작 합니다.
비관리IP 제어	on	비관리노드 IP 감지 시 비관리노드 IP를 차단합니다. 센서 운영모드 옵션이 Active일 경우에만 동작합니다.
	off	비관리노드 IP가 감지되어도 비관리노드 IP를 차단하지 않습니다.
비관리IP 제어예외		비관리노드 IP 차단 시 차단을 예외할 비관리노드 IP를 NetAddress/CIDR 형식으로 입력합니다. 비관리IP 제어 옵션이 on일 경우 활성화됩니다.

2. 트래픽 모니터링

트래픽 모니터링에 대한 설정 항목입니다.

트래픽 모니터링 설정은 동작모드가 Local Mirror 모드일 경우에만 제공됩니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
수집주기	초, 분, 시간, 일, 주, 개월	노드의 트래픽 정보를 수집할 주기를 설정합니다. default : 0 최소값 : 10초 최대값 : 1일
평균계산 시간	초, 분, 시간, 일, 주, 개월	트래픽의 평균값을 설정한 시간마다 계산합니다. default : 5분 최소값 : 10초 최대값 : 1일
업데이트 최소값		단위는 KB/s이며, 설정한 값보다 낮은 트래픽인 노드는 정보를 수집하지 않습니다.
업데이트 변동폭		단위는 %이며, 설정한 값만큼의 트래픽 변동이 없을 경우, 정보를 수집하지 않습니다.
목적지별 현황수집	on	노드들이 가장 많이 접속하는 IP의 트래픽 정보를 수집합니다.
	off	노드들이 접속하는 IP의 트래픽정보를 수집하지 않습니다.
수집수량		트래픽 정보를 수집할 목적지 수량을 설정합니다. 목적지가 설정한 값보다 많을 경우 트래픽이 많은 순으로 트래픽 정보를 수집합니다.

3. 노드등록

노드등록에 관련된 설정 항목입니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
MAC당 최대등록	입력	하나의 MAC에 붙을 수 있는 노드수를 설정 합니다.
미사용IP등록	on	사용하지 않는 IP를 관리 > 노드 > 트리뷰에서 원하는센서 의 관리 뷰에 미분류 노드로 표시 합니다, Active 모드로 변경해주어야 미등록 노드를 스캔합니다.
	off	사용하지 않는 IP를 노드로 표시하지 않습니다, off일 시 IP신청시스템을 사용할 수 없으며 습니다.
IP 사용율 경고		단위는 %이며, IP 주소를 설정한 값을 초과하여 사용하였을 경우 로그에 기록 됩니다.

4. 노드정보 검사

노드정보 수집에 대한 설정 항목입니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
포트/서비스 스캔	on	센서 스캔을 진행할 때 포트 및 서비스 정보를 스캔 합니다.
	off	포트/서비스 정보를 스캔 하지 않습니다.
주기적 스캔	on	노드 정보를 주기적으로 스캔합니다, 스캔 주기는 설정 > 환경설정 > 노드관리 > 검사주기 에서 설정할 수 있습니다.
	off	노드 정보를 주기적으로 스캔하지 않습니다, 노드 최초등록 및 관리자에 의한 수동 노드스캔 명령 시에만 노드 정보를 스캔합니다.
SNMP 정보검사	on	센서 스캔을 진행할 때 SNMP 정보를 스캔합니다.
	off	SNMP 정보를 스캔 하지 않습니다.
NetBIOS 이름 검사	on	센서 스캔을 진행할 때 NetBIOS 이름 정보를 스캔 합니다.
	off	최초 스캔 및 관리자에 의해 센서 스캔할 시 NetBIOS 이름 정보를 스캔하지만 자동으로 센서 스캔을 할 때는 NetBIOS 이름 정보를 스캔하지 않습니다.

검사주기	분, 시간, 일, 주, 개월	포트/서비스, NetBIOS 이름검사 스캔을 설정한 주기마다 수행합니다. 0 입력 시 신규 노드가 등록될 때와 관리자가 수동으로 스캔을 명령을 내린 노드만 스캔을 수행합니다.
------	-----------------------	---

5. 네트워크 스캔

네트워크 관련 수집에 대한 설정 항목입니다.

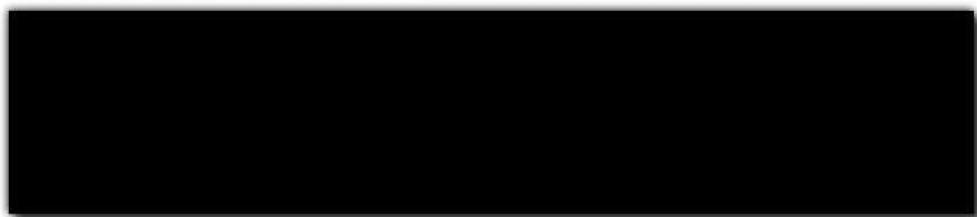


해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
DHCP Server Scan	on	센서 스캔을 진행할 때 DHCP Server 이름 정보를 스캔합니다.
	off	최초 스캔 및 관리자에 의해 센서 스캔할 시 DHCP Server 이름 정보를 스캔하지만 자동으로 센서 스캔을 할 때는 DHCP Server 이름 정보를 스캔하지 않습니다.
UPNP Scan	on	센서 스캔을 진행할 때 UPNP 정보를 스캔합니다.
	off	UPNP 정보를 스캔 하지 않습니다.
HP SLP Scan	on	센서 스캔을 진행할 때 HP SLP 정보를 스캔합니다.
	off	HP SLP 정보를 스캔 하지 않습니다.
SIP Scan	on	센서 스캔을 진행할 때 SIP 정보를 스캔합니다.
	off	SIP 정보를 스캔 하지 않습니다.

6. 노드상태 검사

노드상태 검사에 대한 설정 항목입니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
초당 상태검사 개수	입력	1초당 설정한 값만큼의 노드의 업/다운 상태를 스캔 합니다. 업/다운 상태는 노드의 전원상태를 말합니다.
MAC+IP Clone 감지	on	MAC+IP Clone을 감지 합니다. 해당 옵션을 사용하기 위해서는 MAC+IP Clone 위험감지를 생성해 주어야 합니다.
	off	MAC+IP Clone을 감지하지 않습니다.

7. 서브넷 노드스캔

서브넷에 대한 노드스캔 설정 항목입니다.

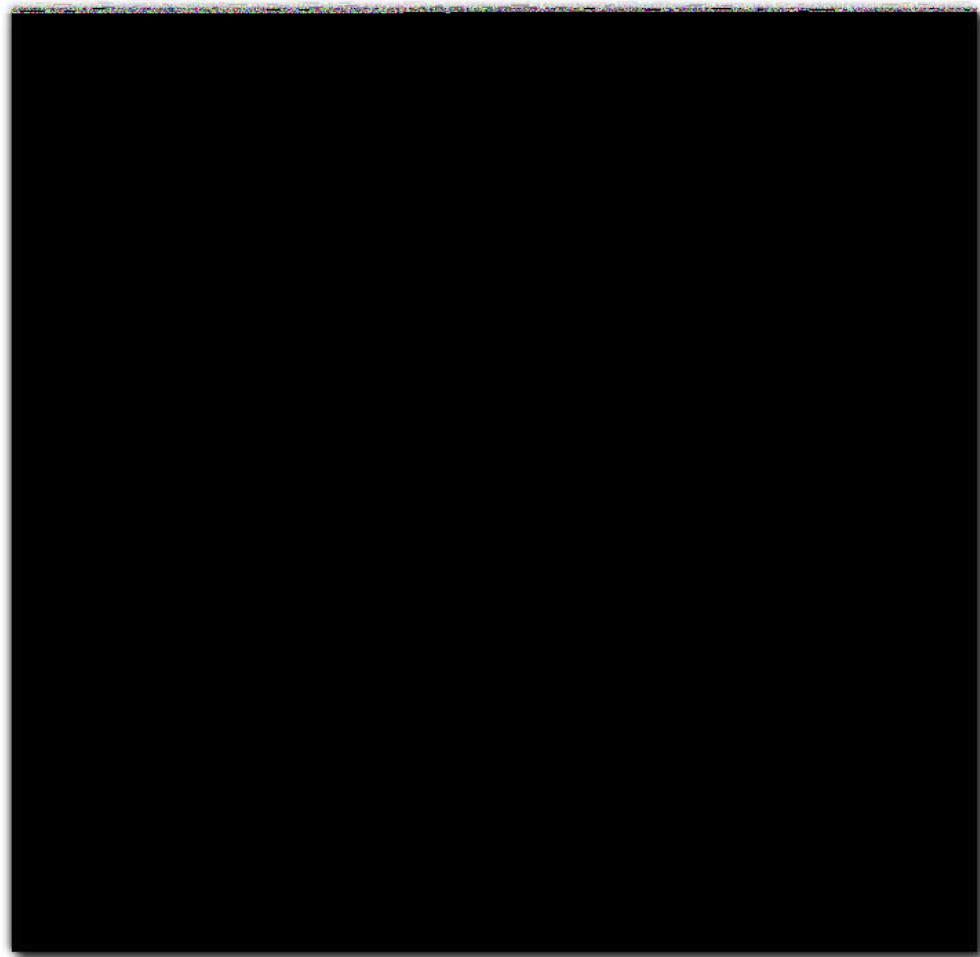


해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
수행주기	일, 주, 개월, 시간	해당 센서에 속해 있는 노드를 설정한 주기마다 스캔 합니다. default : 6시간 최소값 : 1시간 최대값 : 1년
초당 스캔개수	입력	센서 IP에 속해 있는 노드를 스캔할 때 1초당 설정한 값만큼의 노드의 수 만큼 스캔 합니다.

8. DHCP

DHCP에 관련된 설정 항목입니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
DHCP 서비스	on	센서의 DHCP 기능을 사용합니다.

	off	센서의 DHCP 기능을 사용하지 않습니다, off할 시 AirSentry에 IP를 할당하지 않으므로 AirSentry 기능이 동작하지 않을 수 있습니다.
서비스 제공방법	로컬	해당 센서 대역에 있는 노드들에 대하여 DHCP 서비스 제공합니다.
	글로벌	다른 센서의 DHCP 서버가 동작하지 않을 시 글로벌 모드의 DHCP 서버가 다른 센서의 DHCP 서버의 DB를 참고하여 DHCP 서버 역할을 합니다.
	리모트	해당 센서를 DHCP 서버로 사용하지 않고 글로벌 센서를 이용하여 DHCP 서비스를 제공받습니다.
노드 IP Pool	입력	DHCP로 사용할 IP를 입력합니다, 입력 방식으로는 개별주소(X.X.X.X), 영역(X.X.X.A-B), CIDR(X.X.X.X/16) 방식으로 작성할 수 있습니다.
대여시간		IP 대여시간을 설정합니다.
DNS 서버		DHCP로 할당할 DNS서버 주소를 설정합니다.
도메인네임		도메인 접미사를 설정합니다.
WINS 서버		WINS 주소를 설정합니다.
NTP 서버		NTP 서버 주소를 설정합니다.
센서 IP Pool	IP 입력	센서 및 Air-Sentry에 DHCP로 할당할 IP를 입력합니다, Air-Sentry는 DHCP로만 IP를 할당받을 수 있습니다.
IP 할당 금지 대상	변경 금지 위반 노드	IP변경금지를 위반한 노드는 DHCP에서 IP를 할당하지 않습니다.
	변경 금지 미설정 노드	IP변경금지를 설정하지 않은 노드는 DHCP에서 IP를 할당하지 않습니다.
DHCP노드 IP갱신	on	IP 할당 방식이 DHCP인 노드가 있을 경우, 해당 노드의 IP를 직접 할당방법으로 변경할 시 노드의 IP가 갱신 됩니다.
	off	IP 할당 방식이 DHCP인 노드가 있을 경우, 해당 노드의 IP를 직접 할당방법으로 변경할 시 다른 IP를 갖고 있지만 같은 MAC을 가진 노드가 생성 됩니다.

9. 가상 IP/IP 관리

가상 IP와 IP 정책에 관련된 설정 항목입니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
가상IP 개수	입력	센서에게 가상 IP 설정한 값만큼 자동으로 할당 합니다.
신규노드정책	MAC 차단모드	새로운 노드가 등록될 경우 MAC 차단이 이루어 집니다.
	IP 차단모드	새로운 노드가 등록될 경우 IP 차단이 이루어 집니다.
	MAC/IP 차단모드	새로운 노드가 등록될 경우 MAC/IP 차단이 이루어 집니다.
	허용모드	새로운 노드가 등록 되어도 어떠한 차단도 이루어 지지 않습니다.
	변경금지모드	새로운 노드가 등록될 경우 IP 변경 금지가 설정 됩니다, 만약 IP를 변경할 경우 네트워크 차단이 이루어 집니다.

	충돌보호모드	새로운 노드가 등록될 경우 IP 충돌 보호가 설정 됩니다. 충돌보호란 다른 사용자가 자신의 IP를 사용할 시 다른 사용자는 네트워크가 차단 되며 자신은 차단되지 않습니다.
센서 IP 충돌보호	on	해당 센서에 설정한 IP에 충돌보호 설정하여 다른 PC가 사용하지 못도록 합니다.
	off	해당 센서에 설정한 IP에 충돌보호를 하지 않습니다.

10. 기타설정

내/외부 네트워크제어 선택과 예외처리에 관련된 설정 항목입니다.

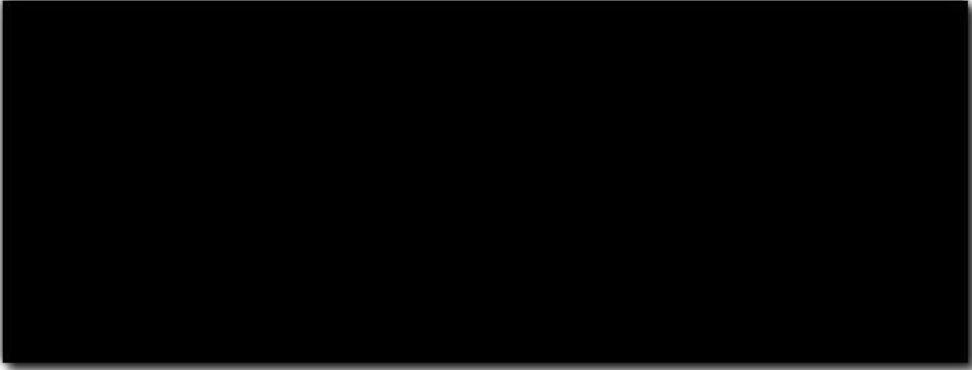


해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	내용
브릿지 MAC	출발지 MAC주소를 변경하는 브릿지장비가 있을 경우 해당 장비의 MAC을 설정합니다. (여러개일 경우 줄바꿈으로 구분)
브릿지 IP	브릿지 자신이 소유한 IP를 예외처리하기 위해서 설정합니다. (여러개일 경우 줄바꿈으로 구분)
예외처리 MAC	NAC 관리대상에서 예외처리할 MAC주소를 설정합니다. (여러개일 경우 줄바꿈로 구분)

- 환경설정

해당 페이지는 콘솔의 보안설정과 배포서비스설정, SNMP 설정 등을 할 수 있습니다.



- 보안설정

콘솔 접속에 관련된 설정을 할 수 있습니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
CLI 콘솔 접속 IP1		CLI 콘솔에 접속을 허용할 IP를 입력합니다. 입력한 IP외 다른 IP는 CLI 콘솔에 접속할 수 없습니다.
CLI 콘솔 접속 IP2		CLI 콘솔에 접속을 허용할 IP를 입력합니다. 입력한 IP외 다른 IP는 CLI 콘솔에 접속할 수 없습니다.

- 패치 Proxy 서비스설정

패치서비스를 위해 Proxy 서비스를 사용할 경우 Proxy 관련된 설정을 할 수 있습니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
사용여부	on, off	패치 검색 및 다운로드 서비스를 위한 Proxy 서비스 제공여부를 선택합니다. (50GB이상의 데이터디스크가 존재할 경우만 동작)
대상 네트워크그룹	네트워크 객체	Proxy 서비스를 적용 받을 네트워크 객체를 설정합니다. 설정하지 않을 경우 해당 센서가 관리하는 노드에 대해서만 배포 서비스를 제공합니다.

3. SNMP Agent 설정

SNMP 사용여부, 커뮤니티를 설정할 수 있습니다, SNMP 버전은 SNMP v3만 제공합니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
사용여부	on	SNMP Agent 기능 동작시킵니다.
	off	SNMP Agent 기능을 동작시키지 않습니다.
사용자명		SNMP 접속 사용자명을 설정합니다. 초기값으로 public이 설정되어있습니다.
Auth Password		접속인증을 위한 Authentication Password를 설정합니다. Auth Password는 SHA만 제공합니다.
Priv Password		데이터 암호화를 위한 Priv Password를 설정합니다. Priv Password는 AES만 제공합니다.

4. 자원경고

데이터 디스크, 메모리, CPU를 과다로 사용할 경우 관리자가 감지할 수 있도록 경고로그를 발생시키는 기능을 제공합니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	내용
데이터 디스크	설정한 % 이상의 용량을 사용하였을 시 로그에 경고 로그를 발생시킵니다. 용량은 로그에 의해 많이 사용될 수 있습니다.
메모리	설정한 % 이상의 메모리를 사용하였을 시 로그에 경고 로그를 발생시킵니다.
CPU	설정한 % 이상의 CPU를 사용할 시 경고 로그를 발생시킵니다. CPU 사용률은 5분동안의 CPU 사용률의 평균입니다.
노드수	전체 노드 수가 설정한 개수를 초과할 시 경고 로그를 발생시킵니다.

5. 날짜 및 시간

한국 외 다른 나라에서 사용할 경우 발생되는 시간차를 시스템에 적용할 수 있도록 설정할 수 있습니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
타임존	각 나라별 도시	설정한 도시의 시각을 기준으로 기능들이 동작하고, WEP에서 보여지는 시각도 설정한 도시의 시각으로 보여집니다.

6. 기타설정



항목	옵션	내용
기본문자셋	문자셋	일본어판 Windows를 사용할 경우 Windows 관련 정보를 가지고 올 때 일본어(EUC-JP)로 설정하여 일본어로 되어 있는 Widows 관련 정보를 글자 깨짐 없이 확인할 수 있습니다.

• 제어

시스템 재기동과 셧다운을 수행할 수 있습니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	내용
재기동	시스템을 종료 후 다시 시작 합니다.
셧다운	시스템을 안전하게 종료 합니다.

무선센서의 환경설정

- 무선센서 환경설정

무선센서 동작, 보안설정, 신호감도, 유효시간, AP 정보 갱신주기, 무선제어, 무선랜카드 설정을 할 수 있습니다.



해당 페이지는 아래표와 같은 정보를 담고 있습니다.

항목	옵션	내용
무선센서 운영모드	Active	무선센서를 동작시킵니다.
	None	무선센서를 동작시키지 않습니다.

CLI 콘솔 비밀번호		콘솔로 무선센서에 접속할 때의 사용할 비밀번호를 입력합니다. 보안을 위해 비밀번호는 대문자/소문자/숫자/특수문자 중 3가지 규칙 조합 및 9자리 이상의 비밀번호를 입력합니다.
SSH 접속 허용	on	SSH를 이용하여 무선센서로 접속할 수 있도록 합니다.
	off	SSH를 이용하여 무선센서로 접속하지 못하도록 합니다. default 값은 off 입니다.
최소값		단위는 dbm으로, 설정한 dbm보다 낮은 신호는 탐지하지 않습니다.
신호 변호 감지 범위		단위는 dbm으로, 최소 변동폭이 설정한 dbm 이상일 경우 dbm을 업데이트 합니다.
AP 등록 유효시간	초, 분, 시간, 일, 주, 개월	AP 감지 시 설정한 시간이 지난 후 다시 감지가 되어야만 AP로 등록 합니다. default : 30초 최소값 : 0 최대값 : 1분
AP 정보 갱신 주기	초, 분, 시간, 일, 주, 개월	설정한 시간마다 AP 정보를 갱신 합니다. default : 10초 최소값 : 10초 최대값 : 10분
접속 단말정보 갱신주기	초, 분, 시간, 일, 주, 개월	AP에 접속한 단말정보 갱신을 위한 주기를 설정합니다. default : 60초 최소값 : 10초 최대값 : 10분
Deauth 차단	on	Deauthentication 패킷을 송신하여 비인가 접속을 차단합니다.
	off	비인가 접속을 차단하지 않습니다.
차단대상 그룹		Deauth 차단 설정이 on인 경우에 활성화 되며, Deauth 차단을 설정을 적용할 무선랜 그룹을 설정합니다.
주파수 대역	2.4G	사용할 주파수 대역을 설정합니다.
무선모드	802.11bgn, 802.11bg, 802.11n	사용할 무선모드를 선택합니다.
채널	Auto, 1~13	사용할 채널을 입력합니다.

장비에 대한 성격을 나타내는 아이콘

관리자는 시스템관리 페이지에서 Logserver, RADIUS Service, Air-Sentry, Policy-Center를 확인할 수 있습니다.

- RadiusServer 동작유무를 확인할 수 있습니다.



- Logserver 동작유무를 확인할 수 있습니다.



센서관리

센서관리

관리자는 센서관리 페이지를 통해 수량이 많은 센서, 무선센서를 보다 쉽게 관리할 수 있으며, 센서, 무선센서의 설정과 현황을 쉽게 확인할 수 있습니다.



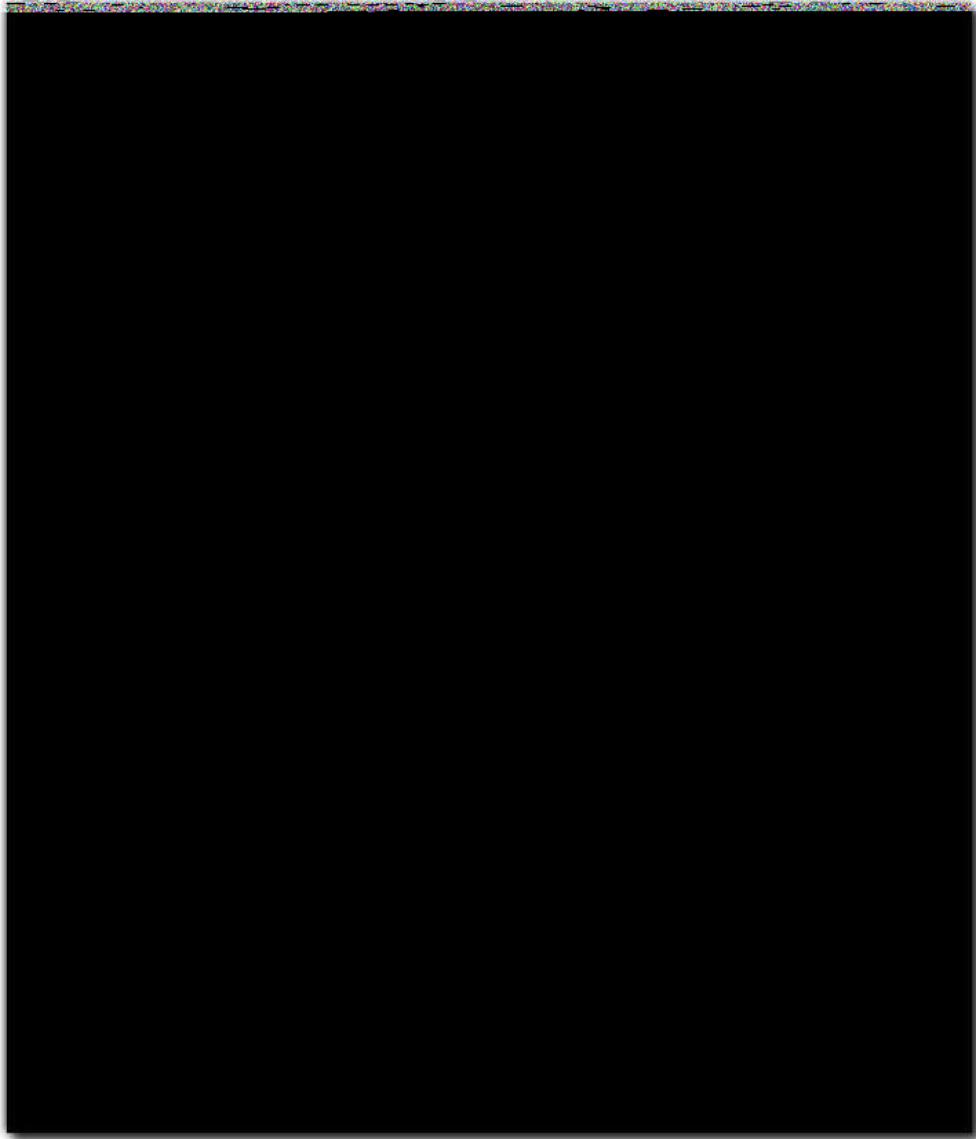
센서관리 작업선택

다수의 센서, 무선센서를 쉽게 관리하기 위해 센서를 일괄적으로 설정할 수 있는 기능들이 있어 한번의 작업으로 다수 센서를 관리할 수 있습니다.



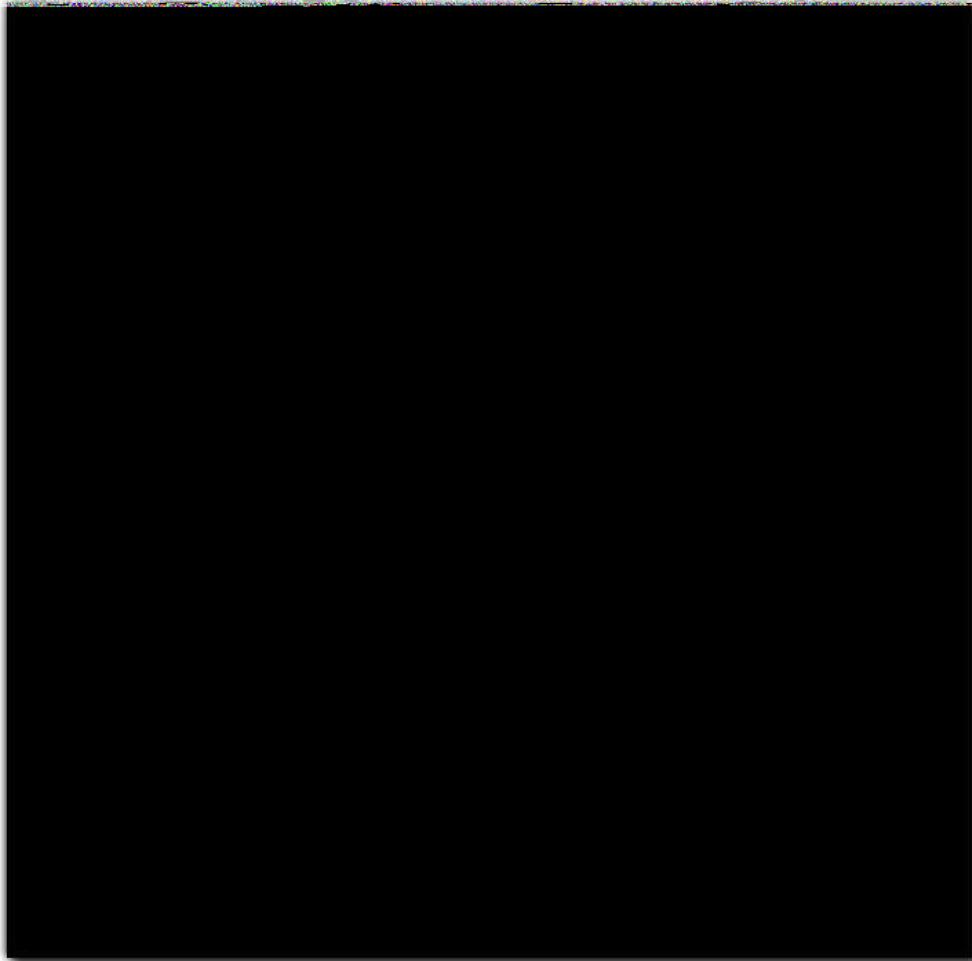
- 센서 일괄 설정

여러 센서의 센서설정을 한번에 일괄 설정할 수 있습니다.



- 무선센서 일괄 설정

여러 무선센서의 환경설정을 한번에 일괄 설정할 수 있습니다.



- 센서 설정 조회

여러 센서의 센서 설정을 조회 할 수 있습니다.



- 무선센서 설정 조회

여러 무선센서의 환경설정을 조회할 수 있습니다.



- 센서대상작업지시

여러 센서에게 작업지시를 수행하도록 할 수 있습니다.



- 센서 운영모드 일괄 설정

여러 센서의 운영모드를 변경할 수 있습니다.



시스템초기 설정

시스템초기 설정

시스템초기 설정은 환경설정, 센서, 무선센서의 초기환경을 설정하는 페이지입니다. 새로운 센서, 무선센서가 추가되었을 때 시스템기초 설정의 설정 값으로 설정 됩니다.

시스템초기 설정은 현재 사용중인 시스템에는 적용되지 않습니다.

- 환경설정 : 콘솔, 배포서비스, snmp에 관련된 설정을 할 수 있습니다.
- 센서설정 : 제어, 스캔, 센서 동작 유무에 관련된 설정을 할 수 있습니다.
- 무선센서 환경설정 : 무선센서 동작, 콘솔 비밀번호, 신호감도, 유효시간, 정보갱신주기, 무선제어에 관련된 설정을 할 수 있습니다.
- [환경설정](#)
- [센서설정](#)
- [무선센서 환경설정](#)

환경설정

환경설정

시스템초기 설정의 환경설정은 추가되는 센서의 환경설정을 초기 값으로 반영 됩니다.
시스템초기 설정의 환경설정을 변경하여 추가되는 센서의 환경설정 초기 값을 변경할 수 있습니다.

시스템초기 설정의 환경설정은 변경 방법은 기존 센서 환경설정 변경방법과 동일합니다.

센서설정

센서설정

시스템초기 설정의 센서설정은 추가되는 센서, 무선 센서의 센서설정에 초기 값으로 반영 됩니다.
시스템초기 설정의 센서설정을 변경하여 추가되는 센서, 무선센서의 센서설정 초기 값을 변경할 수 있습니다.

시스템초기 설정의 센서설정은 변경 방법은 기존 센서설정 변경방법과 동일합니다

무선센서 환경설정

무선센서 환경설정

시스템초기 설정의 무선센서 환경설정의 설정 값은 추가되는 무선 센서의 환경설정에 초기 설정으로 반영 됩니다.
시스템초기 설정의 무선센서 환경설정을 변경하여 추가되는 무선센서의 환경설정의 초기 설정을 변경할 수 있습니다.

시스템초기 설정의 무선센서 환경설정은 변경 방법은 기존 무선센서 환경설정 변경방법과 동일합니다

세션 관리

세션관리

최고 관리자(Super Admin)는 다른 관리자들의 접속현황을 확인할 수 있고, 해당 관리자의 세션을 삭제하여 연결을 끊을 수 있습니다.

세션의 삭제는 자신을 제외하고, 세션을 삭제하고싶은 관리자들을 선택한 후, 작업선택 > 삭제 를 선택하여 세션을 삭제합니다.



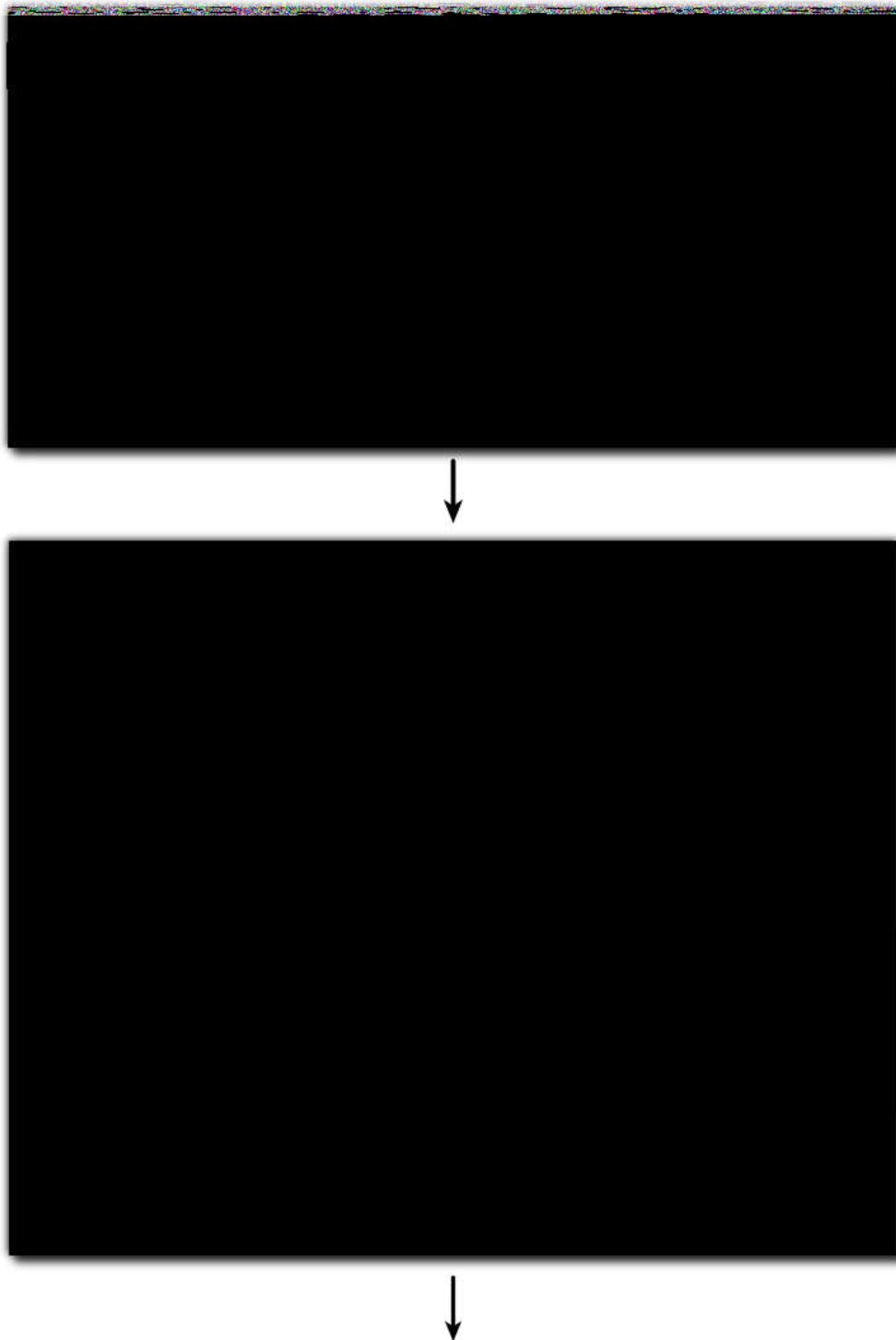
라이센스

라이센스

Genian 의 모든 제품은 라이센스를 등록해야 동작합니다.
모든 라이센스는 정상 출고된 장비에 대해서만 발급이 되며, 각 장비마다 부여된 라이센스는 다른 장비에서 사용할 수 없습니다.
라이센스에 기록된 유지보수 만료일이 지난경우에 제품은 정상동작하나 온라인 업데이트, SMS 알람기능을 사용할 수 없습니다.

- 라이센스 등록

라이센스가 등록되어있지 않을 시, 아래 그림과 같이 경고문구가 뜨며 정상작동하지 않습니다.
정상작동을 위해 해당 그림의 라이센스 등록버튼을 이용하여 라이센스를 등록하여 주십시오.





- 라이센스 발급받기

라이센스를 발급받기 위해서는 서비스사업팀에 문의하시기 바랍니다.

- 유효성 재검사

라이센스의 위반사항을 즉시 확인할 수 있으며, 위반사항을 조치 후 유효성 재검사 버튼을 이용하여 조치가 제대로 이루어졌는지 즉시 확인할 수 있습니다.

- 유지보수

유지보수의 만료일자를 나타냅니다. 유지보수 만료일자가 맞지 않을 경우 만료일 재검사 버튼을 클릭하여 확인할 수 있습니다.

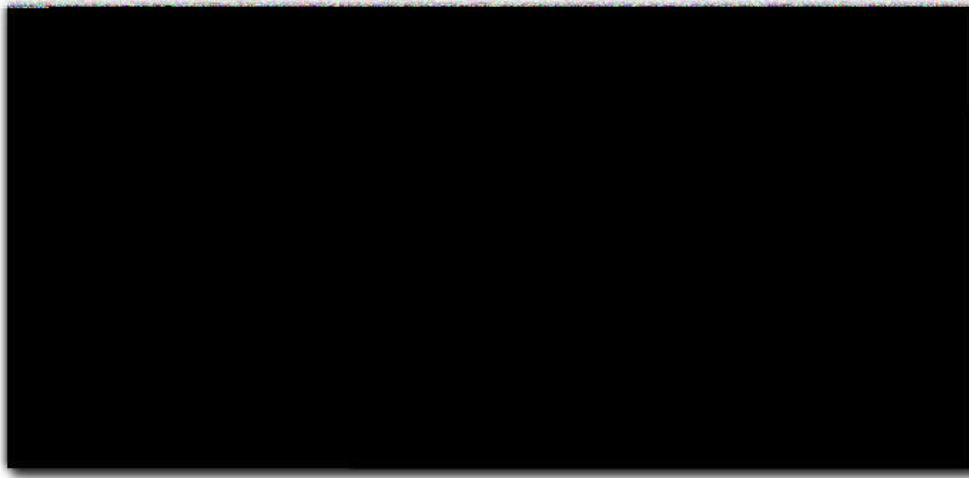
업데이트 관리

업데이트 관리

관리자는 업데이트 관리 탭을 이용하여 시스템OS, 에이전트, 플러그인, 데이터를 관리할 수 있습니다.

- 소프트웨어

Genian 소프트웨어를 업로드할 수 있습니다.



- 운영정보 데이터

CVE업데이트 정보, 운영체제 감지 데이터, 노드정보 감지데이터, 패치정보 데이터를 업데이트 할 수 있습니다.



- 소프트 웨어
- 운영정보 데이터

소프트 웨어

소프트웨어

에이전트 및 센서, 센터 업그레이드에 필요한 파일을 업로드할 수 있습니다.
업로드한 파일로 에이전트, 센서, 센터의 버전을 업그레이드 합니다.

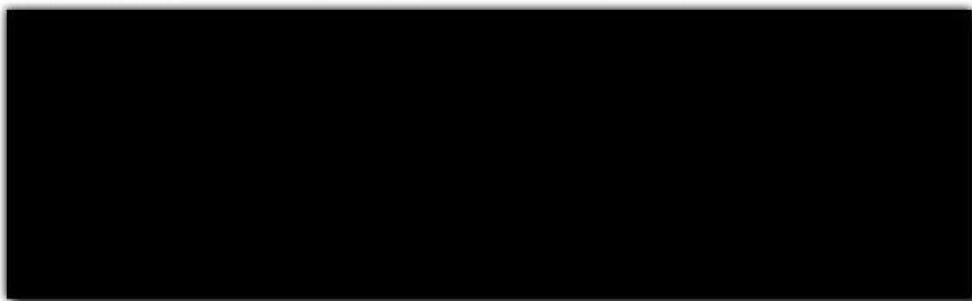
1. 수동 업로드 클릭

수동 업로드 버튼을 클릭합니다.



2. 파일 선택

업로드 팝업 창에서 파일선택 버튼을 클릭 후 업그레이드할 파일을 선택합니다.



3. 업로드

업로드 버튼을 클릭합니다. 업로드가 완료되면 자동으로 팝업 창이 종료됩니다.



4. 소프트 웨어 확인

소프트 웨어가 정상적으로 업로드 되었는지 확인합니다.



플러그인

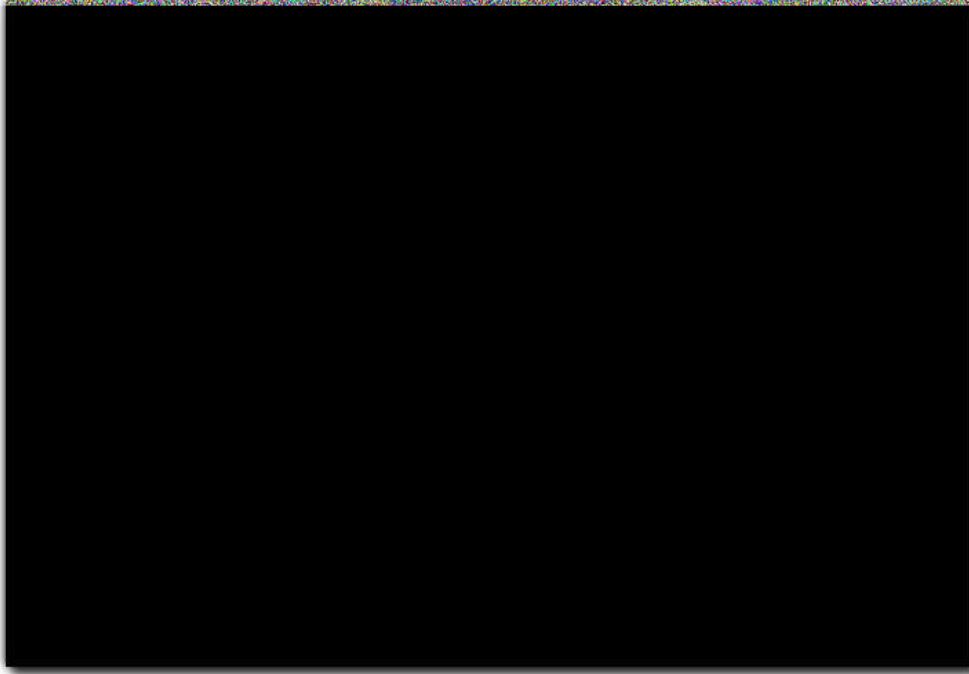
플러그인

플러그인은 사용자 내부시스템의 정보수집, 제어, 설정 값 변경을 위해, 에이전트에 의해 사용되는 부가 프로그램입니다.

플러그인 하나당 하나씩의 기능을 가지고 있고, 새로운 기능을 계속해서 추가할 수 있습니다.

플러그인에 대한 라이센스가 없을 경우 플러그인 이름이 빨간색으로 표시되며 해당 플러그인을 사용할 수 없습니다.

플러그인은 [노드액션](#) 기능을 이용하여 사용할 수 있습니다.



- ARP 관리

PC 정적 ARP를 제어하고, Anti ARP Spoofing을 수행합니다.



설정 항목	옵션	내용
Static ARP 차단	On	Static으로 설정된 ARP를 사용하지 못하도록 사용자가 수동으로 Static ARP 설정 시 Static ARP를 삭제합니다.
	Off	Static으로 설정된 ARP를 삭제 하지 않습니다.
Anti ARP Spoofing	On	ARP Spoofing 방지 기능으로 하위 옵션에서 선택한 그룹에 포함되어 있는 노드 중 충돌보호된 노드 IP와 MAC을 다른 노드의 ARP Table에 Static으로 하여 ARP Spoofing를 방지합니다.
	Off	충돌보호된 노드들의 IP와 MAC을 Static으로 ARP 설정하지 않습니다.

Node group Applies	다른 노드 ARP table에 IP와 MAC을 Static으로 적용할 그룹을 선택합니다, 총돌보호된 노드가 그룹에 포함되어 있지 않을 시 다른 노드의 ARP table에 IP와 MAC을 Static ARP로 설정하지 않습니다.
--------------------	--

- DNS 제어

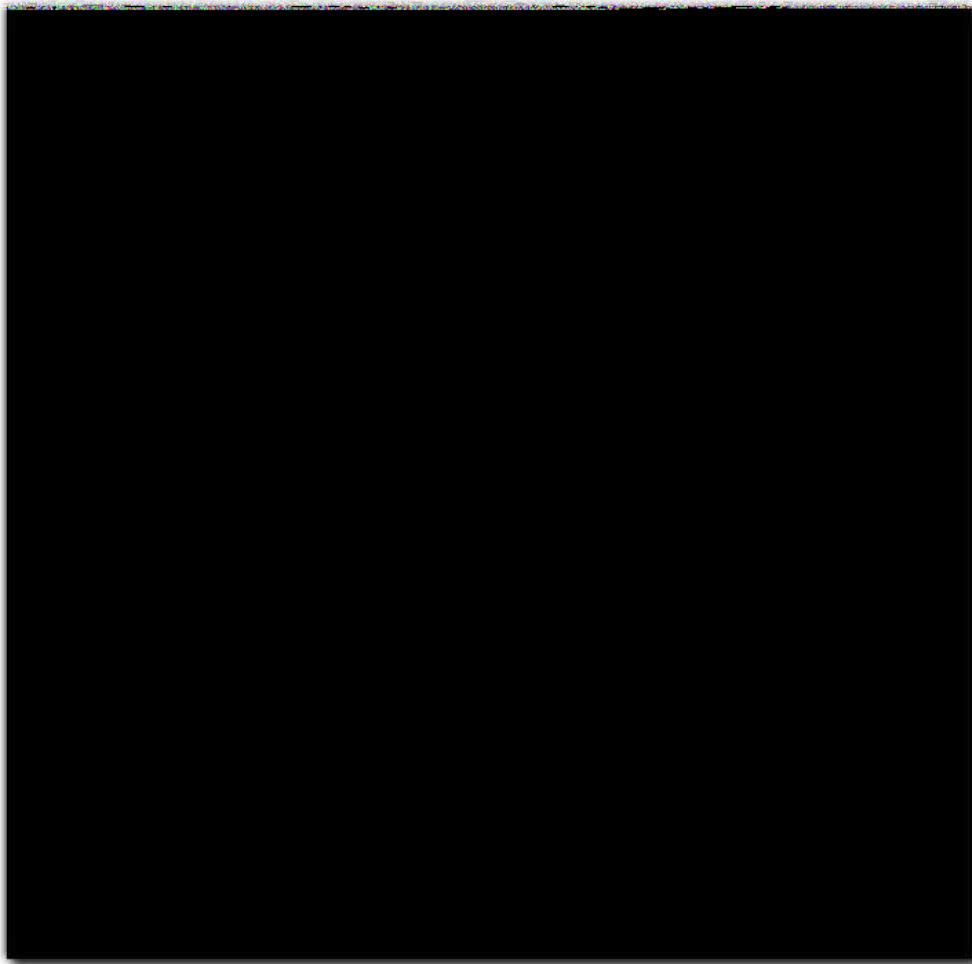
DNS 서버 및 Hosts 파일을 제어합니다.



설정 항목	옵션	내용
DNS 구성	제어안함	DNS를 제어하지 않습니다.
	자동으로 DNS 서버 주소 받기	Static IP 설정일 시 DNS를 제어 하지 않고, DHCP 설정일 시 "다음 DNS 서버 주소 사용"을 사용할 경우 강제로 "자동으로 DNS 서버 주소 받기"으로 변경합니다.
	다음 DNS 서버 주소 사용	하위옵션에서 정의한 DNS 주소로 사용자의 DNS를 제어합니다.
기본 설정 DNS 서버		DNS구성 설정이 다음 DNS 서버 주소 사용일 경우 활성화 되며, 기본 설정 DNS 서버에 적용할 DNS를 입력합니다.
보조 DNS 서버		DNS구성 설정이 다음 DNS 서버 주소 사용일 경우 활성화 되며, 보조 DNS 서버에 적용할 DNS를 입력합니다.
Hosts 파일 설정	On	하위옵션에 정의된 내용을 바탕으로 Hosts 파일을 제어합니다.
	Off	Hosts 파일을 제어하지 않습니다.
추가		Hosts 파일 설정이 On일 경우 활성화 되며, Hosts 파일에 추가할 DNS를 정의합니다.
제거		Hosts 파일 설정이 On일 경우 활성화 되며, Hosts 파일에 제거할 DNS를 정의합니다.

- IE보안옵션 제어

IE의 보안옵션을 강제화 하도록 제어합니다.



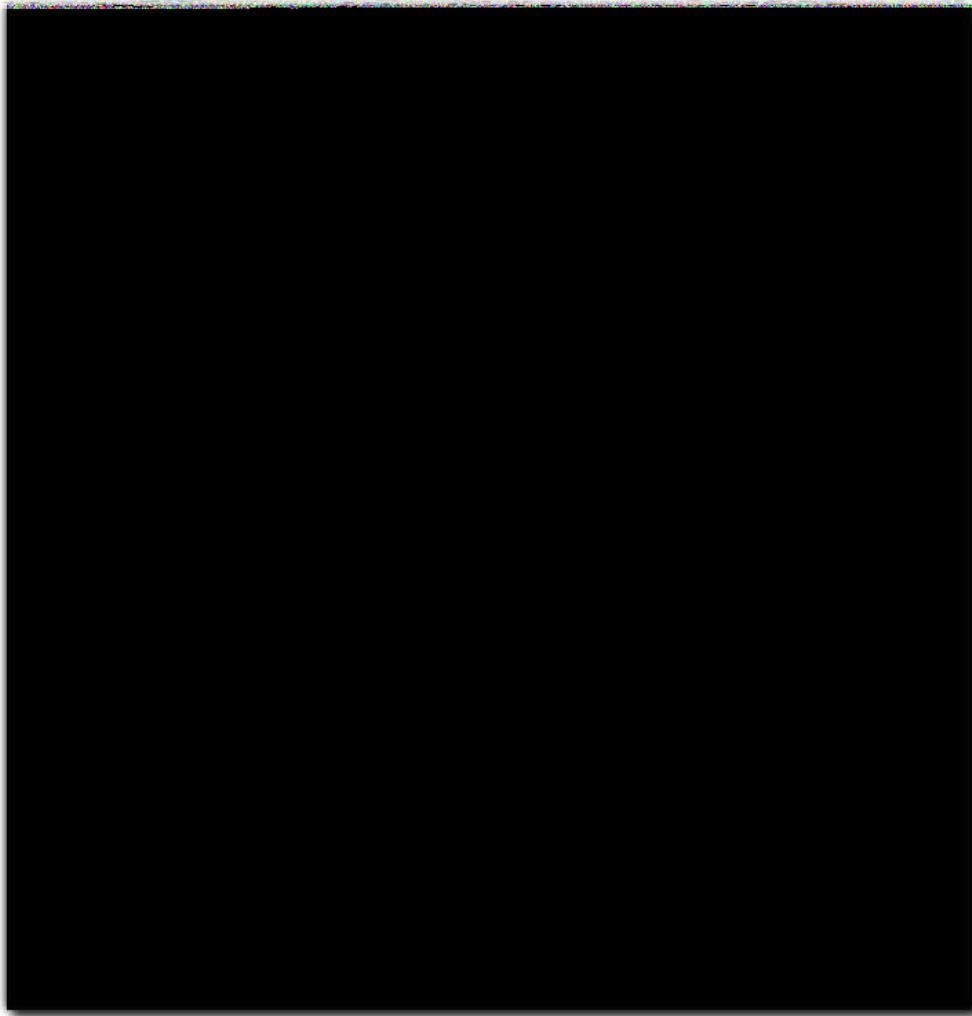
설정 항목	옵션	내용
홈 페이지		홈페이지로 제어할 사이트를 입력합니다. 입력한 주소를 홈 페이지가 되도록 제어합니다. (공란이면 제어안함)
임시인터넷파일 삭제	제어안함	"임시인터넷파일 삭제" 옵션을 제어하지 않습니다.
	강제사용	"임시인터넷파일 삭제" 옵션을 강제사용하여 브라우저를 종료 시 임시 인터넷 파일 폴더를 삭제합니다.
서명 안 된 ActiveX 컨트롤 다운로드	제어안함	"서명 안 된 ActiveX 컨트롤 다운로드" 옵션을 제어하지 않습니다.
	사용안함	"서명 안 된 ActiveX 컨트롤 다운로드" 옵션을 사용 안함으로 제어하여 서명 안 된 ActiveX를 다운로드 하지 않도록 합니다.
ActiveX 컨트롤을 자동으로 확인	제어안함	"ActiveX 컨트롤을 자동으로 사용자에게 확인" 옵션을 제어하지 않습니다.
	사용안함	"ActiveX 컨트롤을 자동으로 사용자에게 확인" 옵션을 사용 안함으로 제어하여 ActiveX 컨트롤을 자동으로 확인하지 않고 알림줄에 표시되도록 합니다.
파일 다운로드 시 자동으로 확인	제어안함	"파일 다운로드 시 자동으로 확인" 옵션을 제어하지 않습니다.
	사용안함	"파일 다운로드 시 자동으로 확인" 옵션을 사용 안함으로 제어하여 파일 다운로드시 자동으로 확인하지 않고 알림줄이 표시되도록 합니다.
팝업 차단	제어안함	"팝업 차단" 옵션을 제어하지 않습니다.
	강제사용	"팝업 차단" 옵션을 강제사용하여 팝업을 차단합니다.

신뢰할 수 있는 사이트	On	하위 옵션에서 지정한 주소를 신뢰할 수 있는 사이트로 추가 및 제거 합니다.
	Off	신뢰할 수 있는 사이트를 제어 하지 않습니다.
추가		신뢰할 수 있는 사이트 설정이 On일 경우 활성화 되며, 신뢰할 수 있는 사이트에 추가할 사이트를 입력합니다.
제거		신뢰할 수 있는 사이트 설정이 On일 경우 활성화 되며, 신뢰할 수 있는 사이트에 제거할 사이트를 입력합니다. * 입력시 모든 신뢰할 수 있는 사이트가 삭제됩니다.
서버 검증(https://)필요	제어안함	신뢰할 수 있는 사이트 설정이 On일 경우 활성화 되며, "서버 검증(https://)필요" 옵션을 제어하지 않습니다.
	강제사용	신뢰할 수 있는 사이트 설정이 On일 경우 활성화 되며, "서버 검증(https://)필요" 옵션을 강제사용하도록 제어합니다.
	사용안함	신뢰할 수 있는 사이트 설정이 On일 경우 활성화 되며, "서버 검증(https://)필요" 옵션을 사용하지 못하도록 제어합니다.
프록시 서버 사용	제어안함	프록시 설정을 제어하지 않습니다.
	사용안함	프록시를 사용 할 수 없도록 제어합니다.
	기본설정	하위 옵션에서 지정한 프록시 서버를 사용하도록 제어합니다.
	고급설정	하위 옵션에서 지정한 프록시 서버를 사용하도록 제어합니다.
주소:포트		프록시 서버 사용 설정이 "기본설정"일 경우 활성화되며, 제어할 프록시 서버 주소와 포트를 입력합니다.
http 주소:포트		프록시 서버 사용 설정이 "고급설정"일 경우 활성화되며, 제어할 프록시 서버 주소와 포트를 입력합니다.
https 주소:포트		프록시 서버 사용 설정이 "고급설정"일 경우 활성화되며, 제어할 프록시 서버 주소와 포트를 입력합니다.
ftp 주소:포트		프록시 서버 사용 설정이 "고급설정"일 경우 활성화되며, 제어할 프록시 서버 주소와 포트를 입력합니다.
Socks 주소:포트		프록시 서버 사용 설정이 "고급설정"일 경우 활성화되며, 제어할 프록시 서버 주소와 포트를 입력합니다.
로컬 주소에 프록시 서버 사용 안 함	On	프록시 서버 사용 설정이 "고급설정", "기본설정"일 경우 활성화되며, "로컬 주소에 프록시 서버 사용 안 함" 옵션을 사용하도록 제어합니다.
	Off	프록시 서버 사용설정이 "고급설정", "기본설정" 일 경우 활성화되며, "로컬 주소에 프록시 서버 사용 안 함" 옵션을 하지 못하도록 제어합니다.
프록시 서버 예외주소		프록시 서버 사용설정이 "고급설정", "기본설정" 일 경우 활성화되며, 프록시 서버로 사용하지 않을 주소를 입력합니다.
폼 자동완성	제어안함	"폼 자동완성" 기능을 제어하지 않습니다.
	사용안함	"폼 자동완성" 기능을 제어하여 폼 자동완성을 하지 않도록 합니다.
미사용 ActiveX 삭제	On	하위옵션인 미사용일에 설정한 기간동안 사용하지 않은 ActiveX를 삭제합니다.
	Off	ActiveX를 삭제하지 않습니다.
미사용일		미사용 ActiveX 삭제 설정이 "On"일 경우 활성화되며, 미사용 ActiveX를 삭제할 기준일을 입력합니다, 0을 입력할 경우 모든 ActiveX를 삭제합니다
미사용일을 알 수 없는 경우	사용안함	미사용 ActiveX 삭제 설정이 "On"일 경우 활성화되며, 미사용일을 알 수 없는 ActiveX는 삭제하지 않습니다.
	파일수정일 사용	미사용 ActiveX 삭제 설정이 "On"일 경우 활성화되며, 미사용일을 알 수 없을 경우 ActiveX 수정일을 기준으로 설정한 기준일만큼 지났을 경우 ActiveX를 삭제합니다.
Toolbar 삭제	On	IE에 설치된 모든 Toolbar를 삭제합니다.
	Off	IE에 설치된 Toolbar를 삭제하지 않습니다.
브라우저 도우미 삭제	On	IE에 설치된 모든 브라우저 도우미를 삭제합니다.
	Off	IE에 설치된 브라우저 도우미를 삭제하지 않습니다.

예외		미사용 ActiveX 삭제, Toolbar 삭제, 브라우저 도우미 삭제 옵션이 On일 경우 삭제 대상에서 예외할 ActiveX, Toolbar, 브라우저 도우미 이름을 입력합니다. 예외에 입력된 대상들은 삭제하지 않습니다.
----	--	--

- PC전원 제어

PC를 대기모드, 재부팅, 종료할 수 있도록 제어합니다.

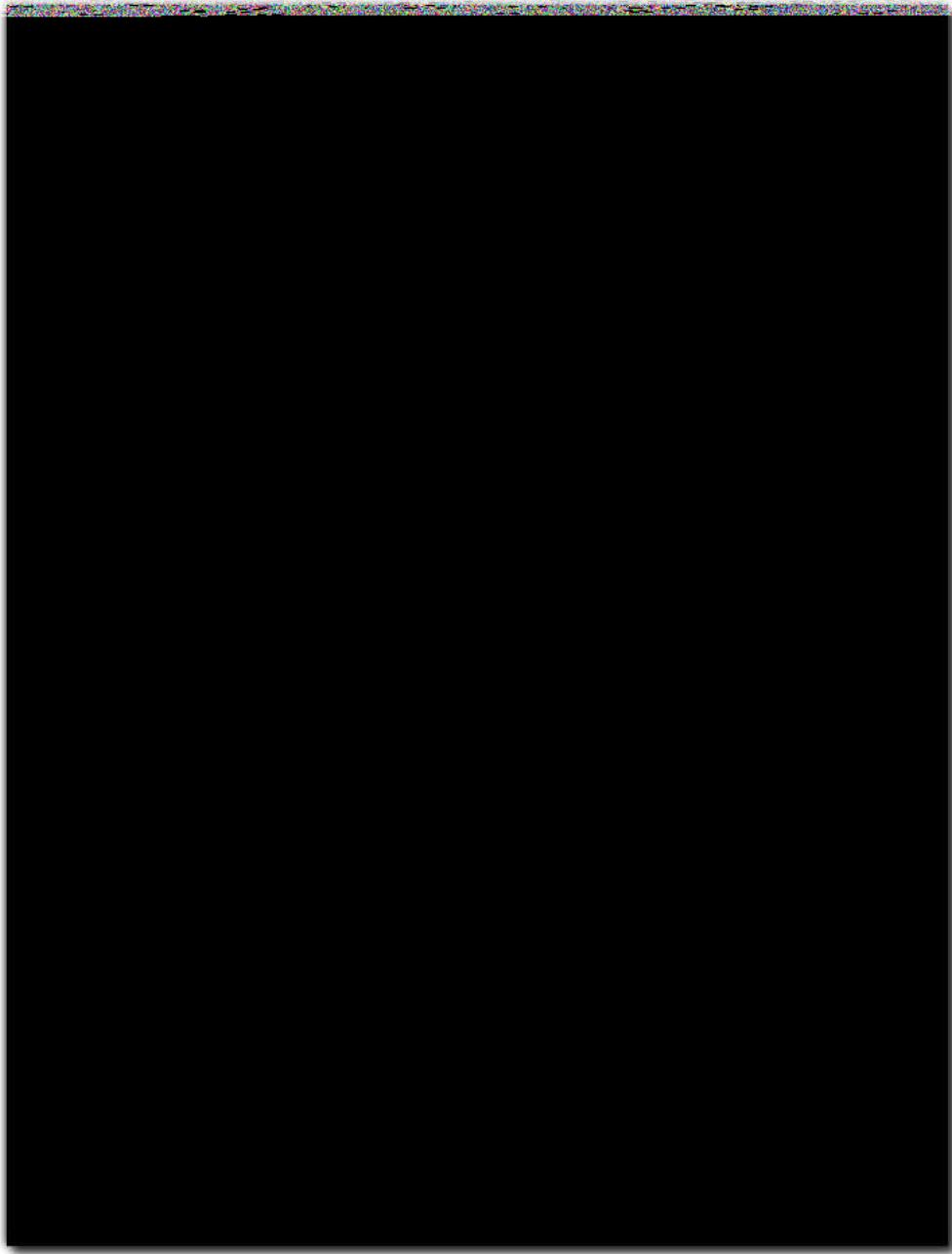


설정 항목	옵션	내용
동작방식	대기모드	대기모드로 전환하도록 제어합니다.
	재부팅	PC를 재부팅 하도록 제어합니다.
	종료	PC를 종료 하도록 제어합니다.
강제화모드	On	사용자가 제어를 취소 할 수 없도록 합니다.
	Off	사용자가 제어를 취소할 수 있도록 합니다.
대기시간		설정한 대기시간만큼 기다린 후 선택한 동작방식을 수행합니다. 대기시간 동안 팝업 창을 띄우면, 팝업 창에서 메시지 확인 및 취소, 즉시수행 작업을 할 수 있습니다.
PC가동시간		시스템의 가동시간이 설정시간 이상일 경우에만 제어를 수행합니다. 본 플러그인으로 대기모드로 변경된 후 해제되었다면 해제시점을 가동시간 0으로 여깁니다.
타이틀 표시	On	안내 메시지가 출력되는 팝업 창에 타이틀을 표시합니다.
	Off	대기시간에 팝업되는 팝업 창에 타이틀을 표시하지 않습니다.
메시지 표시 방법	HTML	사용자에게 보여줄 메시지를 입력합니다. 메시지 내용은 대기시간에 팝업되는 팝업 창에서 확인할 수 있습니다.

	이미지	사용자에게 보여줄 이미지를 업로드합니다. 이미지는 대기시간에 팝업 창에서 확인할 수 있습니다.
--	-----	--

- **TCP세션검사**

주기적으로 TCP 세션수를 수집하고, 임계치이상되는 세션수가 발견되면 네트워크 인터페이스를 차단합니다.
수집된 TCP 세션 수는 관리 > 노드 > 노드상세정보 > 네트워크정보에서 확인할 수 있습니다.



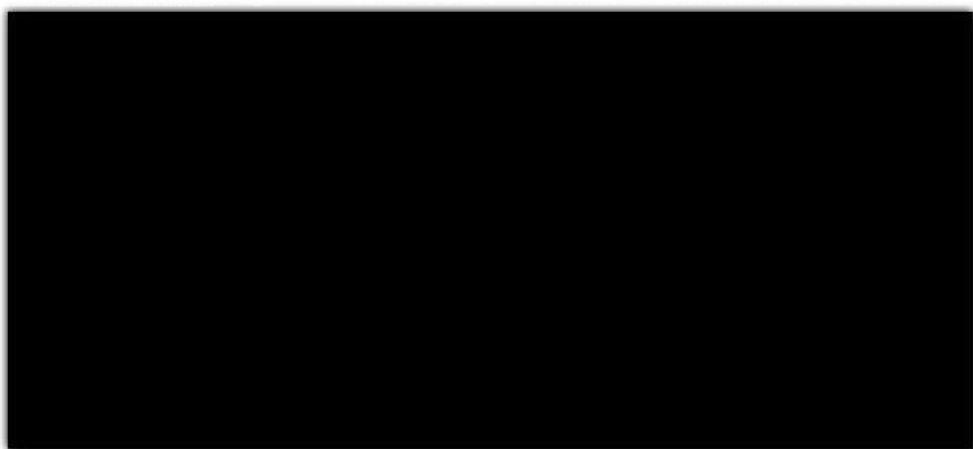
설정 항목	옵션	내용
세션정보 전송주기		사용자의 TCP 세션정보 전송주기를 설정합니다.(0 : 전송안함)
업데이트 최소비율		LISTENNING 상태를 제외한 TCP 세션 전체의 수가 이전보낸 세션수와 설정비율 이상 차이가 나면 정보를 업데이트합니다.
업데이트 최소값		세션수가 설정값 미만이면 업데이트 최소비율이 적용되지 않고 업데이트되지 않습니다.
인터넷페이스 제어	On	세션상태임계치를 정의하여 임계치 초과시 인터페이스를 차단하여, 네트워크를 사용하지 못도록 제어합니다.
	Off	인터넷페이스제어를 하지 않습니다.

전체 임계치		인터페이스 제어 설정이 On일 경우 활성화 되며, LISTENING 상태를 제외한 TCP 세션 전체 임계치가 설정 값 이상일 시 인터페이스를 차단합니다.
CLOSED 임계치		인터페이스 제어 설정이 On일 경우 활성화 되며, CLOSED 상태인 TCP 세션이 설정값 이상일 시 인터페이스를 차단합니다.
ESTABLISHED 임계치		인터페이스 제어 설정이 On일 경우 활성화 되며, ESTABLISHED 상태인 TCP 세션이 설정 값 이상일 시 인터페이스를 차단합니다.
CLOSE_WAIT 임계치		인터페이스 제어 설정이 On일 경우 활성화 되며, CLOSE_WAIT 상태인 TCP 세션이 설정 값 이상일 시 인터페이스를 차단합니다.
TIME_WAIT 임계치		인터페이스 제어 설정이 On일 경우 활성화 되며, TIME_WAIT 상태인 TCP 세션이 설정 값 이상일 시 인터페이스를 차단합니다.
SYN_SENT 임계치		인터페이스 제어 설정이 On일 경우 활성화 되며, SYN_SENT 상태인 TCP 세션이 설정 값 이상일 시 인터페이스를 차단합니다.
인터넷페이스 차단알림	사용안함	TCP 세션수가 임계치를 초과하여 인터페이스 제어되었을 때 사용자에게 차단됨을 알리지 않습니다.
	사용자메시지	정의된 사용자 메세지를 팝업 창으로 보여주어 차단됨을 알립니다.
	에이전트팝업	에이전트 팝업 창을 사용하여 장치가 차단됨을 알립니다.
사용자 메시지		인터넷페이스 차단알림설정이 사용자메시지일 경우 활성화 되며, 사용자의 인터페이스가 차단되었을때 차단됨을 알려주는 메시지를 입력합니다.

- WMI정보수집

WMI를 통하여 시스템 정보를 수집합니다.

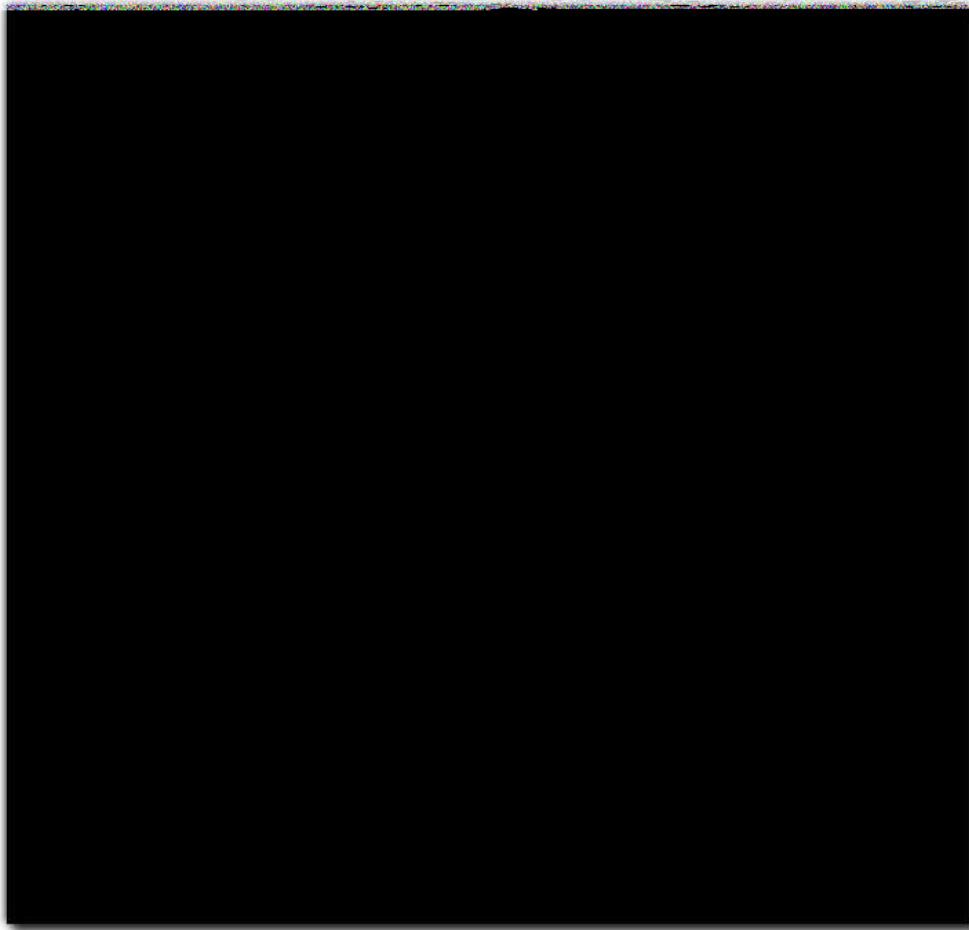
수집된 WMI 정보는 관리 > 노드 > 노드상세정보 > 시스템정보에서 확인할 수 있습니다.



설정 항목	내용
NameSpace	WMI 의 NameSpace 를 선택합니다.
WMI Query	WMI Query를 입력합니다. 여러개의 쿼리를 입력할때는 세미콜론으로 구분합니다.

- 네트워크 공유풀더

네트워크에 공유된 폴더정보를 수집하며 일정시간 이상 공유되는 폴더를 제어합니다.
수집된 공유풀더 정보는 관리 > 노드 > 노드상세정보 > 시스템정보에서 확인할 수 있습니다.



설정 항목	옵션	내용
공유풀더정보 수집	On	PC에 설정되어 있는 공유풀더 목록을 수집합니다.
	Off	PC에 설정되어 있는 공유풀더 목록을 수집하지 않습니다.
공유풀더 해제	On	PC에 설정되어 있는 공유풀더를 해제합니다.
	Off	PC에 설정되어 있는 공유풀더를 해제하지 않습니다.
공유 허용 시간		공유풀더 해제 설정이 On일 경우 활성화되며, 폴더공유 후 설정시간 동안 폴더공유를 해제하지 않습니다. 설정시간이 지났을 경우 공유풀더를 해제합니다.
읽기권한만 허용	On	공유풀더 해제 설정이 On일 경우 활성화되며, 쓰기 권한이 허용되어 있는 공유풀더 공유를 해제하고, 읽기 권한만 허용한 공유풀더는 해제하지 않습니다.
	Off	공유풀더 해제 설정이 On일 경우 활성화되며, 권한 관계 없이 공유풀더 모두 해제합니다.
Everyone권한 외 허용	On	공유풀더 해제 설정이 On일 경우 활성화되며, 공유풀더 사용자 중 Everyone가 있을 경우 공유를 해제합니다.
	Off	공유풀더 해제 설정이 On일 경우 활성화되며, Everyone권한 관계없이 공유풀더 모두 해제합니다.
관리풀더 허용	On	공유풀더 해제 설정이 On일 경우 활성화되며, Windows 관리 공유풀더를 해제하지 않습니다.
	Off	공유풀더 해제 설정이 On일 경우 활성화되며, Windows 관리 공유풀더를 해제 합니다.
공유해제알림 방법	사용안함	공유풀더 해제 시 사용자에게 해제사실을 알리지 않습니다.
	사용자메시지	정의된 사용자 메세지를 팝업 창으로 보여주어 공유풀더가 해제사실을 알립니다.

	에이전트팝업	에이전트 팝업 창을 사용하여 공유풀더가 해제사실을 알립니다.
사용자 메시지		공유해제알림 방법 설정이 사용자메시지일 경우 활성화 되며, 공유풀더가 해제되었다는 사실을 알려주는 메시지를 입력합니다.

- 네트워크정보 수집

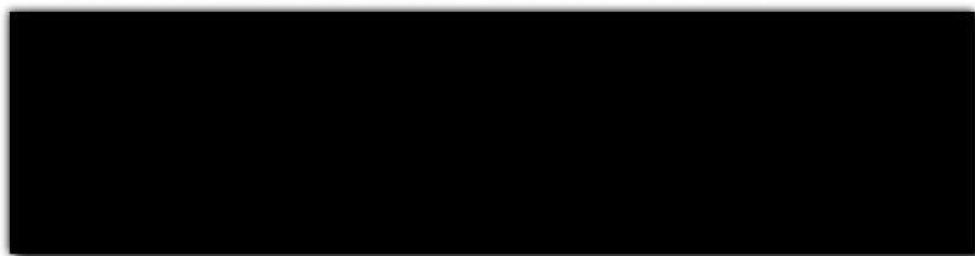
네트워크 인터페이스 정보와 탐지된 포트정보를 수집하여 노드정보에 표시합니다.
 인페이스 정보는 관리 > 노드 > 노드상세정보 > 시스템정보에서 확인할 수 있습니다.
 공유풀더 정보는 관리 > 노드 > 노드상세정보 > 네트워크정보에서 확인할 수 있습니다.



설정 항목	옵션	내용
트래픽 정보 업데이트 비율		마지막으로 전송한 트래픽량이 수집 시 트래픽량과 설정비율 이상 차이가 나면 정보를 업데이트합니다.
전송주기		인터페이스 정보 수집 주기를 설정합니다.
이동평균 시간		설정시간 동안의 평균 트래픽을 전송주기에 전송합니다. 전송주기보다 길게 설정합니다.
열린포트 정보 수집	On	열린포트 정보를 수집 합니다.
	Off	열린포트 정보를 수집하지 않습니다.

- 모니터정보 수집

로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다.



설정 항목
별도의 설정이 필요 없는 플러그인입니다.

- 모양 및 개인설정

원도우 바탕화면, 화면보호기에 대한 설정 정보를 수집 및 제어합니다.
수집된 화면보호기 정보는 관리 > 노드 > 노드상세정보 > 시스템정보에서 확인할 수 있습니다.



설정 항목	옵션	내용
화면보호기정보 수집	On	PC에서 사용되고 있는 화면보호기 설정정보를 수집합니다.
	Off	PC에서 사용되고 있는 화면보호기 설정정보를 수집하지 않습니다.
NAC 로그온 화면 표시	On	화면보호기 해제 시 NAC 인증이 해제 됩니다.
	Off	화면보호기 해제 시 NAC 인증이 해제되지 않습니다.
파일 무결성 검사주기	On	업로드한 화면보호기 파일, 바탕화면 파일 이름이 사용자가 사용하는 파일 이름과 같을 경우 사용자 파일이 화면보호기 및 바탕화면에 출력될 수 있어, 이를 방지하기 위해 주기적으로 검사하여 관리자가 업로드한 파일을 사용하도록 제어합니다.
	Off	업로드 파일과 사용자 파일에 대한 무결성 검사를 하지 않습니다.
화면보호기 제어	On	화면보호기 사용을 강제화 합니다.
	Off	화면보호기 사용을 강제화 하지 않습니다.
대기시간		화면보호기가 수행되기 까지의 시간을 설정합니다.
대기시간 고정	On	대기시간 옵션에 설정한 설정 값 보다 사용자가 설정한 시간이 짧을 경우에도 관리자가 설정한 대기시간으로 제어합니다.
	Off	대기시간 옵션에 설정한 설정 값 보다 사용자가 설정한 시간 짧을 경우 제어하지 않습니다.
원도우 로그온 화면 표시	On	화면보호기의 "다시 시작할 때 로그온 화면 표시" 옵션을 사용하도록 제어합니다.
	Off	화면보호기의 "다시 시작할 때 로그온 화면 표시" 옵션을 제어하지 않습니다.
출력내용		Genian에서 제공하는 화면보호기 사용 시 화면보호기에 입력한 메시지가 출력됩니다.

화면보호기 파일업로드		화면보호기 이미지를 업로드 합니다. 업로드 가능한 이미지 확장자는 scr입니다.
화면보호기 파일이름		화면보호기 파일 이름을 설정합니다.
사용자지정 화면보호기 허용	On	관리자가 업로드한 화면보호기 이미지가 아닌 사용자가 지정한 화면보호기 이미지도 사용할 수 있도록 합니다.
	Off	사용자가 지정한 화면보호기 이미지를 사용하지 못하도록 합니다.
바탕화면 이미지 제어	On	PC의 바탕화면 이미지를 강제설정 합니다.
	Off	바탕화면 이미지를 강제설정 하지 않습니다.
바탕화면 파일업로드		바탕화면 파일을 업로드 합니다. 업로드 가능한 이미지 확장자는 BMP입니다.
바탕화면 파일이름		바탕화면 파일 이름을 설정합니다.
바탕화면 이미지 위치	가운데	바탕화면 배열을 가운데로 제어합니다.
	바둑판식	바탕화면 배열을 바둑판식으로 제어합니다.
	늘이기	바탕화면 배열을 늘이기식으로 제어합니다.

- 무선랜제어

무선 네트워크 인터페이스에서 탐지되는 무선 AP에 대한 정보를 제공하며 허용되지 않은 AP 연결을 제한합니다.



설정 항목	옵션	내용
AP목록 수집 대상	수집안함	AP목록을 수집하지 않습니다.
	탐지된 AP	노드의 무선인터페이스에 탐지된 AP항목을 수집합니다. 수집된 AP항목은 관리 > 무선랜에서 확인할 수 있습니다.
	연결된 AP	노드의 무선인터페이스에 연결되어 있는 AP항목을 수집합니다. 수집된 AP항목은 관리 > 무선랜에서 확인할 수 있습니다.
무선AP스캔주기		설정한 시간을 주기로 무선 인터페이스에 탐지된 AP항목을 스캔합니다.
유효AP기준시간		스캔한 AP항목 중 설정한 시간동안 연속 탐지된 AP에 대해서만 유효한 AP로 간주하여 수집합니다.
연결된 AP 정보 전송	On	노드에 연결된 AP를 관리하기 위하여 AP연결 이력 정보를 수집합니다.
	Off	AP연결 이력정보를 수집하지 않습니다.
일괄정보 전송시간대		노드가 연결한 AP항목 이력을 설정한 시간대에 랜덤하게 1번 전송합니다.
최대시도 일수(일)		설정일자 동안 전송시간대에 AP 연결 이력을 전송 시도 실패 시 전송시간대 상관없이 즉시정보전송 합니다.
연결정보 유효시간		AP 연결 이력 전송 시각을 기준으로 설정한 시간 동안의 정보를 전송합니다. AP 연결 이력 전송 시각 03:00 이고 설정 시간이 1시간일 경우 02:00~03:00 동안 노드가 연결한 AP 항목 이력을 전송합니다.
AP연결제어	On	접속을 허용하지 않은 AP에 대한 연결을 차단합니다.
	Off	AP에 대한 연결 제어를 하지 않습니다.
접속허용 무선랜그룹		접속을 허용할 무선랜 그룹을 설정합니다.

차단알림	알리지 않음	접속을 허용하지 않은 AP에 접속하여 차단되었을 시 사용자에게 차단 사실을 알리지 않습니다.
	에이전트팝업	에이전트 팝업 창을 이용하여 AP 차단 사실을 알립니다.
	코드인증	AP 차단 시 코드 인증 창이 팝업되며 팝업 창에 나타나있는 에이전트 코드를 관리자에게 전달하고, 관리자는 관리 > 신청 > 에이전트 인증코드 발급에서 전달받은 에이전트 코드를 이용하여 인증 코드를 발급받습니다. 발급 받은 인증코드를 사용자에게 전달합니다.
제어유보시간		AP 연결 시 설정시간 동안 무선랜 정책을 받을 수 있도록 차단하지 않습니다. 무선랜 정책을 받을 시 설정한 시간 상관없이 차단합니다.
코드인증 메시지		팝업되는 코드 인증 창에 보여질 메시지를 입력합니다.
허용AP 자동연결	On	허용 SSID와 동일한 허용되지 않은 SSID로 연결할 시 허용 SSID로 자동으로 연결시도 합니다.
	Off	허용 SSID와 동일한 허용되지 않은 SSID로 연결할 시 허용 SSID로 자동으로 연결시도하지 않습니다.
AP모드 차단	On	노드의 무선인터페이스의 SoftAP나 무선Adhoc 기능을 활성화할 시 SoftAP, 무선Adhoc 기능을 차단합니다.
	Off	노드의 무선인터페이스의 SoftAP나 무선Adhoc 기능을 활성화할 시 SoftAP, 무선Adhoc 기능을 차단하지 않습니다.
차단알림	On	에이전트 팝업 창을 이용하여 SoftAP, 무선Adhoc 차단 사실을 알립니다.
	Off	SoftAP, 무선Adhoc 차단 사실을 알리지 않습니다.

- 무선연결관리자

Wireless Connection Manager 프로그램에 대한 옵션 및 동작을 제어합니다.

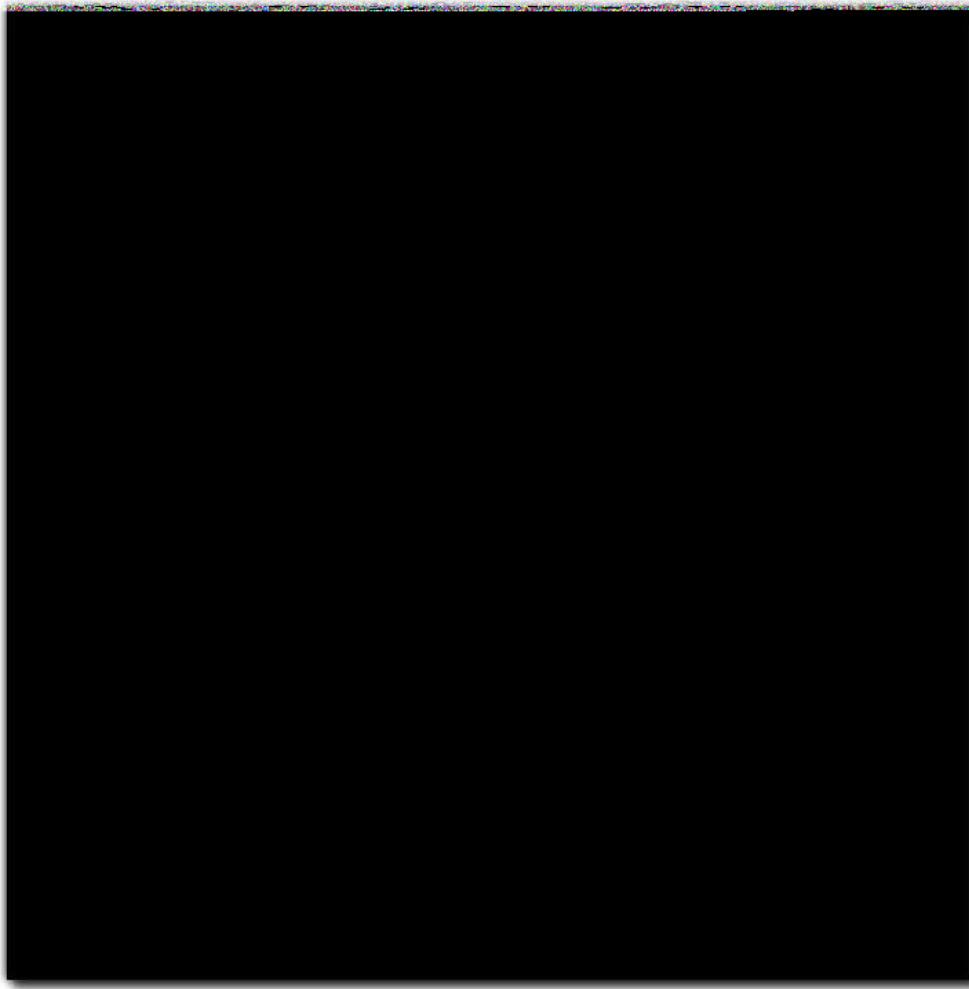


설정 항목	옵션	내용
무선프로파일		노드에 등록할 무선프로파일을 선택합니다. Client 프로파일 설정대로 노드에 무선프로파일을 등록합니다.
무선 연결 관리자 사용	On	무선연결을 간편하게 사용할 수 있도록 무선 연결 관리자(WCM)를 사용합니다.
	Off	무선 연결 관리자(WCM)을 사용하지 않습니다.

강제 실행	On	무선연결관리자 프로그램을 항상 동작하도록 강제화하고 종료하지 못하도록 합니다.
	Off	무선연결관리자 프로그램 동작을 강제화 하지 않습니다.
유선사용시 숨김	On	유선인터페이스를 사용할 경우 무선 연결 팝업 창을 자동적으로 팝업 되지 않도록 합니다.
	Off	유선인터페이스를 사용할 경우 무선 연결 팝업 창이 팝업될 경우 팝업되도록 합니다.
자동재연결	On	사용중인 AP가 끊어진 경우 지정된 프로파일 중 신호가 가장 좋은 AP로 자동 재연결을 시도합니다. 무선연결관리자의 연결해제명령으로 AP연결이 해제된 경우에는 재연결하지 않습니다.
	Off	사용중인 AP가 끊어진 경우 재연결을 시도를 하지 않습니다.
비밀번호 만료전 알림시간		무선연결 팝업 창을 통하여 연결 완료 후 비밀번호 만료가 설정기간 만큼 다가 왔을 경우 비밀번호 변경 창을 띠웁니다.
AP 선택 기능	On	연결가능한 AP를 사용자가 직접 선택하여 연결 할 수 있습니다.
	Off	연결가능한 AP 중 가장 신호가 강한 항목만 연결할 수 있도록 강제화 합니다.
아이디 설명 문자열		무선 연결 팝업 창에서 AP 접속을 위해 아이디를 입력하는 공간을 나타내는 문자열을 입력합니다.
비밀번호 설명 문자열		무선 연결 팝업 창에서 AP 접속을 위해 비밀번호를 입력하는 공간을 나타내는 문자열을 입력합니다.
아이디 저장 허용	On	최근 연결된 아이디를 다음 연결 시 자동으로 입력되게 할 것인지 선택할 수 있습니다.
	Off	최근 연결된 아이디를 다음 연결 시 자동으로 입력되게 하지 않습니다.
비밀번호 저장 허용	On	최근 연결된 비밀번호를 다음 연결 시 자동으로 입력되게 할 것인지 선택할 수 있습니다.
	Off	최근 연결된 비밀번호를 다음 연결 시 자동으로 입력되게 하지 않습니다.
자동연결허용	On	무선연결관리자 실행 시 최근 연결된 AP로 자동 연결할 것인지 선택할 수 있습니다.
	Off	무선연결관리자 실행 시 최근 연결된 AP로 자동 연결 하지 않습니다.
출력이미지 선택		무선연결 팝업 창 상단에 보여질 BMP 이미지를 업로드 합니다.
배경색상		무선연결 팝업 창 배경색을 지정합니다.
글자색상		무선연결 팝업 창 글자색을 지정합니다.
도움말		사용자에게 필요한 도움말을 작성합니다.
도움말 html 사용	On	HTML 대화상자를 사용합니다.
	Off	기본 대화상자를 사용합니다.
인증 후 실행		무선연결 성공 시 설정한 파일을 실행합니다.

- 백신정보 수집

PC에 설치되어있는 백신프로그램 정보 및 백신으로 검출된 바이러스치료로그를 실시간으로 수집합니다.

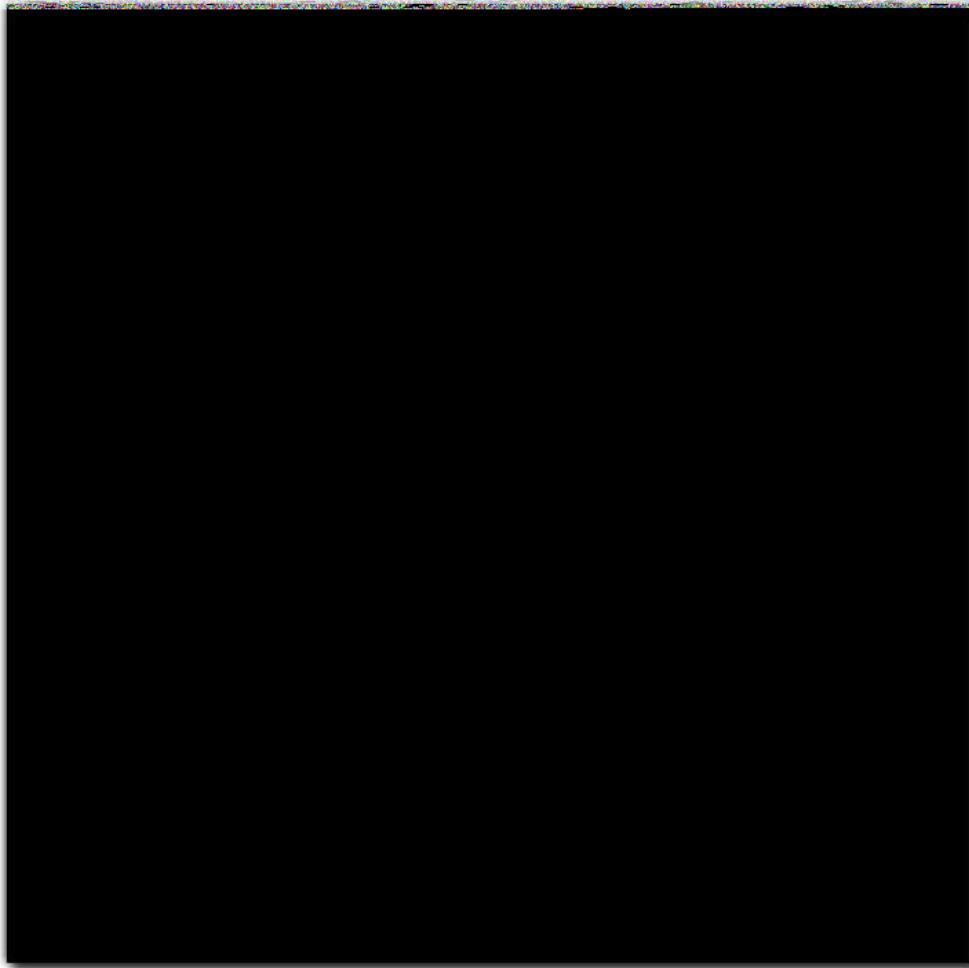


설정 항목	옵션	내용
백신정보 검사주기		백신정보를 검사하는 주기를 설정합니다.
실시간감시OFF 보류 횟수		백신업데이트와 같은 백신 작업중에는 실시간감시 설정이 On이더라도 Off로 수집 될 수 있습니다. 이러한 일시적인 Off 현상이 발생할 때는 보고되지 않도록 설정한 횟수 이상 연속으로 Off로 수집될 경우에만 실시간감시 Off 로 보고되도록 설정합니다.
백신연동	On	백신소프트웨어를 연동하여 백신소프트웨어를 제어할 수 있도록 합니다. 연동 가능한 백신 제품은 '안랩 V3', '하우리 바이로봇', '이스트소프트 알약'의 기업용 제품입니다.
	Off	백신소프트웨어를 연동하지 않습니다.
치료 감사기록	감사기록안함	백신으로 바이러스 치료 시 감사기록을 남기지 않습니다.
	감사기록함	백신으로 바이러스 치료 시 감사기록을 남깁니다.
	치료실패만 감사기록함	백신이 바이러스 치료 실패 시 감사기록을 남깁니다.
증복로그 제외시간		치료 감사기록이 한번 발생 후 똑같은 로그가 설정시간 동안 발생할 경우 감사기록하지 않습니다. 설정시간이 지난 후 똑같은 로그 발생 시 감사기록 합니다.
실시간감시 강제화	On	백신 실시간감시 사용을 강제화합니다.
	Off	백신 실시간감시 사용을 강제화 하지 않습니다.
강제검사		마지막 시각을 기준으로 설정주기마다 검사 방식 옵션에 설정된 검사 방식으로 바이러스검사를 수행합니다.

검사 방식	전체검사	백신 전체검사 혹은 정밀검사를 수행합니다.
	간편검사	백신 간편검사 혹은 빠른 검사를 수행합니다.
검사창 UI 숨기기	On	바이러스 검사 창을 띄우지 않습니다.
	Off	바이러스 검사 창을 띄웁니다.
강제업데이트		마지막 백신엔진 업데이트시각이 설정주기 이상일 때 강제로 업데이트를 수행합니다.

- 비밀번호유효성검사

윈도우 계정의 비밀번호에 대한 유효성을 검사하고 검증되지 않은 비밀번호를 안전한 비밀번호로 변경시킵니다.



설정 항목	옵션	내용
검증된 계정표시	On	비밀번호정책 및 비밀번호 변경주기 두가지 조건을 만족하여 검증 결과가 안전인 계정을 대화상자에 표시합니다.
	Off	비밀번호정책 및 비밀번호 변경주기 두가지 조건을 만족하여 검증 결과가 안전인 계정은 대화상자에 표시하지 않습니다.
비밀번호 문자열 검사방법	규칙검사	로그인 계정의 비밀번호가 설정 > 환경설정 > 사용자관리 > 비밀번호정책 을 준수하였는지 검사합니다.
	유무검사	로그인 계정 비밀번호 설정유무를 검사합니다.
	검사안함	로그인 계정 비밀번호를 검사하지 않습니다.
동작모드	변경모드	로그인 계정 비밀번호가 비밀번호 정책 및 비밀번호 변경주기에 만족하지 않을 시 비밀번호 변경 팝업 창을 띄워 비밀번호 변경을 유도합니다.
	검사모드	비밀번호 변경주기를 만족하지 않을 시 비밀번호 변경 팝업 창을 띄워 비밀번호 변경을 유도합니다.

비밀번호 변경주기		비밀번호 변경 주기를 설정합니다. 노드의 비밀번호 변경시각이 설정시간을 초과할 경우 비밀번호 검증 시 검증결과가 기간만료로 표시됩니다.
만료전알림		로그인 계정 비밀번호가 기간만료 되기 설정시간 전에 알림을 발생합니다.
비밀번호 문자열 검사방법	규칙검사	로그아웃 계정의 비밀번호가 설정 > 환경설정 > 사용자관리 > 비밀번호정책 을 준수하였는지 검사합니다.
	유무검사	로그아웃 계정 비밀번호 설정유무를 검사합니다.
	검사안함	로그아웃 계정 비밀번호를 검사하지 않습니다.
동작모드	변경모드	로그아웃 계정 비밀번호가 비밀번호 정책 및 비밀번호 변경주기에 만족하지 않을 시 비밀번호 변경 팝업 창을 띠워 비밀번호 변경을 유도합니다.
	검사모드	비밀번호 변경주기를 만족하지 않을 시 비밀번호 변경 팝업 창을 띠워 비밀번호 변경을 유도합니다.
비밀번호 변경주기		비밀번호 변경 주기를 설정합니다. 노드의 비밀번호 변경시각이 설정시간을 초과할 경우 비밀번호 검증 시 검증결과가 기간만료로 표시됩니다.
만료전알림		로그인 계정 비밀번호가 기간만료 되기 설정시간 전에 알림을 발생합니다.
검사예외ID		검사 예외시킬 로그아웃 계정의 ID를 입력합니다. 여러개 입력 시 콤마로 구분

- 사용자 알림메시지

사용자에게 알림메시지를 표시합니다.



설정 항목	옵션	내용
메시지 제목		에이전트 팝업 창에 출력될 알림 제목을 설정합니다.
클릭시 CWP접속	On	에이전트 팝업 창 클릭 시 설정한 CWP URL로 접속합니다.
	Off	에이전트 팝업 창 클릭 시 알림메시지 창을 띄웁니다.
메시지 내용		클릭시 CWP접속 설정이 Off일 경우 활성화 되며, 알림메시지 창에서 볼 수 있는 메시지 내용을 입력합니다.
CWP URL		클릭시 CWP접속 설정이 On일 경우 활성화 되며, CWP주소를 설정합니다.
클릭시 CWP접속		에이전트 팝업창 클릭시 CWP접속여부를 선택합니다, 기본적으로 보이지 않지만 http://CenterIP/ 가 입력되어 있습니다.
팝업창 고정	On	에이전트 팝업 창을 닫지 못하도록 합니다.
	Off	에이전트 팝업 창을 닫을 수 있도록 합니다.
메시지 타입	일반	일반 에이전트 팝업 창이 띄워집니다.
	경고	경고 에이전트 팝업 창이 띄워집니다.
메시지확인 알림	On	에이전트 팝업 창 클릭 시 감시기록 합니다.
	Off	에이전트 팝업 창 클릭 시 감사로그 하지 않습니다.

- 소프트웨어정보 수집

설치된 소프트웨어정보를 수집하여 노드상세정보>소프트웨어정보에 표시합니다.



설정 항목
별도의 설정이 필요 없는 플러그인입니다.

- 수행조건만 검사

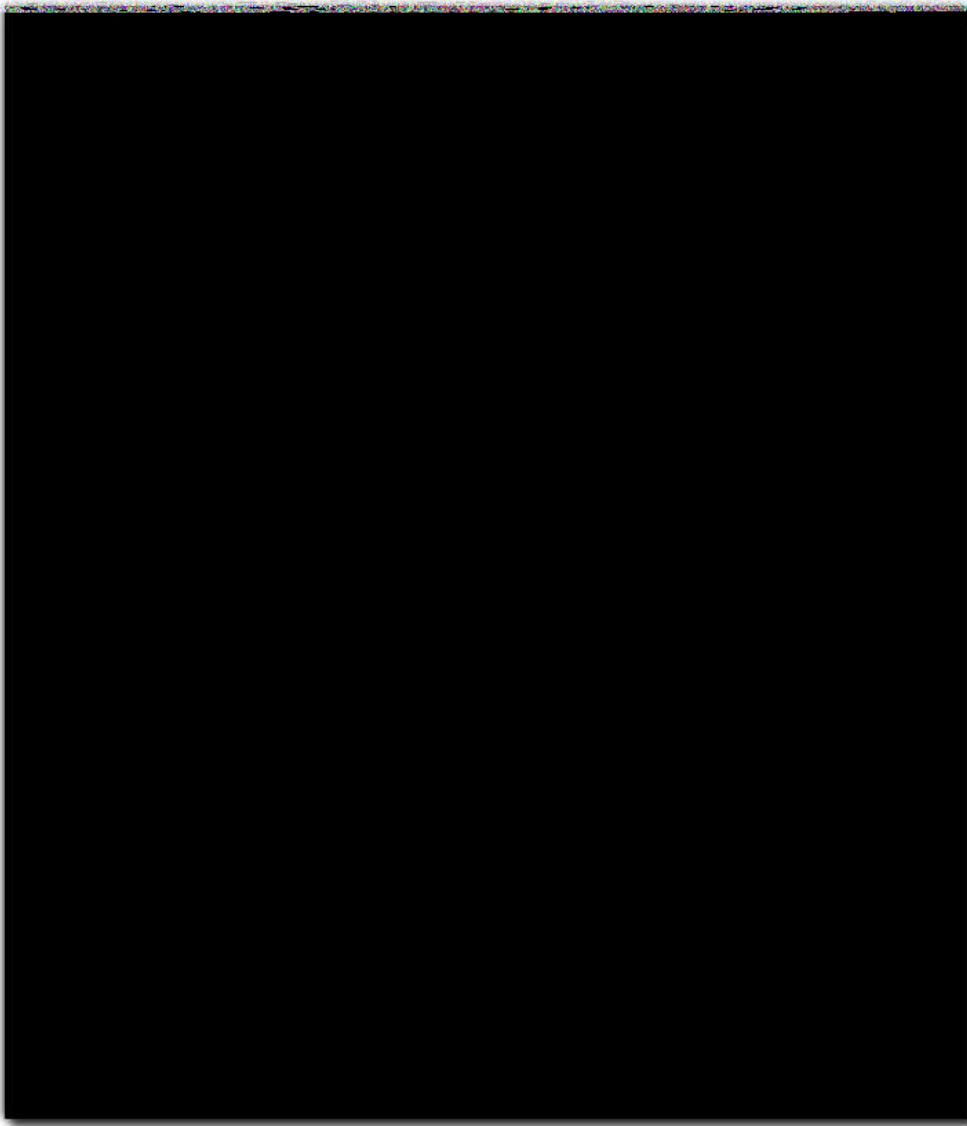
액션에 설정된 수행 조건을 체크하는데 사용하는 플러그입니다.



설정 항목
별도의 설정이 필요 없는 플러그인입니다.

- 에이전트 인증창

사용자인증 수행시 WEB페이지가 아닌 에이전트 자체 인증창을 사용합니다.

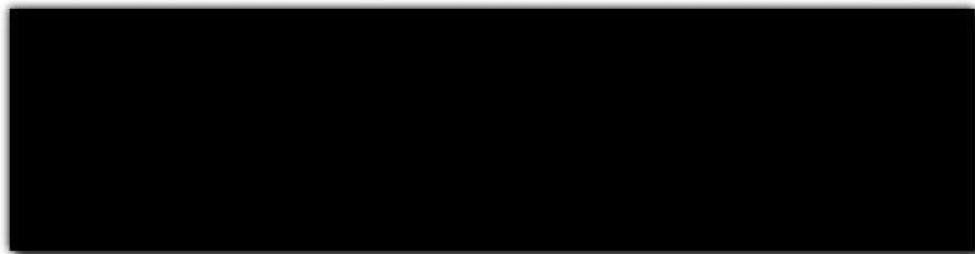


설정 항목	옵션	내용
인증방법	비밀번호	아이디와 비밀번호를 입력하여 사용자 인증을 합니다.
	지문	아이디와 지문으로 사용자 인증을 합니다.
지문인식업체		지문인식기의 제조사를 선택합니다, GenianNAC는 Suprema, Nitgen을 지원합니다.
2단계인증	사용안함	2단계인증을 사용하지 않습니다.
	지문인증	아이디와 지문으로 사용자 인증을 합니다.
지문인식업체		지문인식기의 제조사를 선택합니다, GenianNAC는 Suprema, Nitgen을 지원합니다.
이미지 사용	사용안함	Default 이미지를 사용합니다.
	로고이미지	에이전트 인증 창 로고 이미지를 업로드한 이미지로 변경합니다, BMP 파일만 업로드 가능합니다.
	배경이미지	에이전트 인증 창 배경 이미지를 업로드한 이미지로 변경합니다, BMP 파일만 업로드 가능합니다.
이미지		에이전트 인증 창에 변경할 로고 및 배경 이미지를 업로드 합니다.
입력란 시작위치		아이디, 비밀번호를 입력하는 항목이 위치를 지정합니다, 미입력 최상단에 출력되며 입력한 값만큼 최상단에서 멀어집니다.

타이틀바 표시	On	에이전트 인증 창에 타이틀바를 표시합니다.
	Off	에이전트 인증 창에 타이틀바를 표시하지 않습니다, 종료 버튼이 타이틀바에 표시되어 종료 금지 설정을 Off로 설정 해도 에이전트 인증 창을 종료할 수 없습니다.
배경색상		에이전트 인증 창의 배경색상을 입력합니다
글자색상		에이전트 인증 창의 글자색상을 입력합니다
도움말 html 사용	On	대화상자에 출력되는 도움말을 html 처리 합니다, 설정 > 접속인증페이지 > 페이지구성 > 메시지관리 > 사용자인증창 도움말에서 도움말 문구를 수정할 수 있습니다.
	Off	대화상자에 출력되는 도움말을 text처리 합니다, 설정 > 접속인증페이지 > 페이지구성 > 메시지관리 > 사용자인증창 도움말에서 도움말 문구를 수정할 수 있습니다.
종료금지	On	에이전트 인증 창을 종료할 수 없도록 합니다.
	Off	에이전트 인증 창을 종료할 수 있도록 합니다, 타이틀바 표시 설정을 On으로 설정해야 에이전트 인증 창을 종료할 수 있습니다.
전체 배경색		#000000 와 같은 형식으로 배경 색상을 지정할 시 에이전트 인증 창이 띄워질 때 에이전트 인증 창을 제외한 모든 화면을 지정한 배경 색상으로 보이도록 합니다.
잠금 해제 버튼 표시	On	로그온할 수 없을 경우 관리자에게 에이전트 인증코드를 요청하여 화면 잠금을 해제할 수 있습니다.
	Off	로그온할 수 없을 경우 화면 잠금을 해제할 수 없습니다.
인증 후 실행		인증 성공 후 설정한 파일을 실행합니다.

- 운영체제정보 수집

윈도우즈 운영체제 정보 및 윈도우즈 사용자 정보를 수집하여 노드정보에 표시합니다.

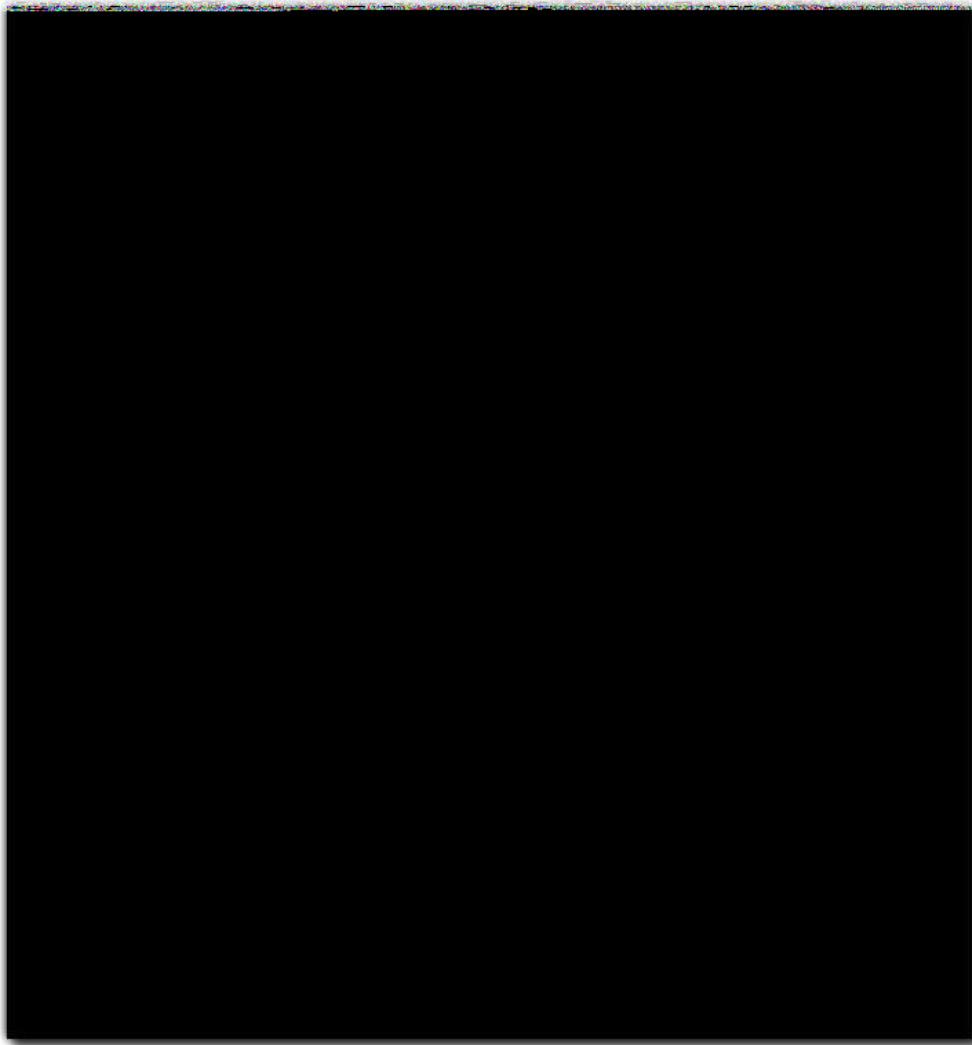


설정 항목

별도의 설정이 필요 없는 플러그인입니다.

- 원도우 보안설정

시스템에 설정된 원도우즈 방화벽, 원격데스크탑, 자동실행의 동작을 제어합니다.

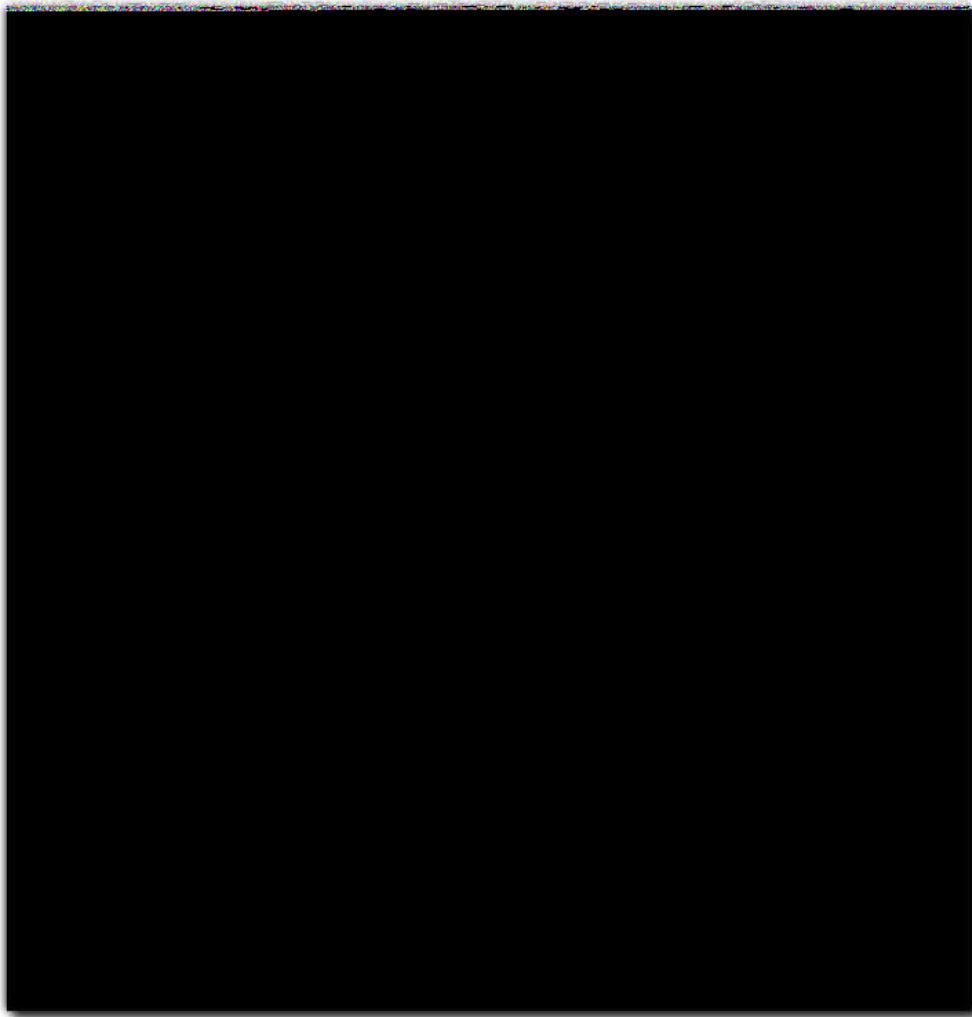


설정 항목	옵션	내용
Windows 방화벽	제어안함	Windows 방화벽 설정을 제어하지 않습니다.
	강제사용	Windows 방화벽 사용을 강제화 합니다.
원격데스크탑	제어안함	원격데스크탑 설정을 제어하지 않습니다.
	사용안함	노드를 원격데스크탑으로 사용할 수 없도록 강제 설정합니다.
자동실행	제어안함	자동 실행에 대한 제어를 하지 않습니다.
	사용안함	외부장치 연결 시 자동 실행을 수행 하지 않습니다.
CD 자동실행 차단	On	CD, DVD롬에 대한 자동 실행을 차단합니다.
	Off	CD, DVD롬에 대한 자동 실행을 차단하지 않습니다.
USB 자동실행 차단	On	이동식디스크에 대한 자동 실행을 차단합니다.
	Off	이동식디스크에 대한 자동 실행을 차단하지 않습니다.
기타장치 자동실행 차단	On	기타장치에 대한 자동 실행을 차단합니다.
	Off	기타장치에 대한 자동 실행을 차단하지 않습니다.
시간 동기화서버	제어안함	시간 동기화서버를 제어하지 않습니다.
	강제사용	하위옵션 정의한 NTP서버로 시간 동기화서버를 제어합니다.
시간 동기화서버 주소		NTP서버의 IP 및 Domain을 입력합니다.

동기화 주기		설정한 주기마다 NTP서버와 동기화 합니다.
Windows XP 예약작업	제어안함	예약작업 설정을 제어하지 않습니다.
	사용안함	예약작업 설정을 사용안함으로 제어합니다. Windows XP에서만 동작합니다.

- 원도우 업데이트

윈도우의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.



설정 항목	옵션	내용
패치관리-패치모음		패치모음을 선택합니다.
패치관리-검사주기	주기적검사	노드의 패치상태를 설정주기마다 검사합니다.
	지정시각검사	노드의 패치상태를 설정시각에 검사합니다.
주기적검사		패치관리-검사주기 설정이 주기적 검사일 경우 활성화 되며, 설정한 시간을 주기로 패치상태를 검사합니다.
지정시각검사		패치관리-검사주기 설정이 지정시각검사일 경우 활성화 되며, 선택한 시간객체의 시간동안 패치상태를 한번 검사합니다.
패치관리-화면표시	백그라운드로 설치수행	패치 시 백그라운드로 설치하여 사용자에게 패치 설치 과정을 나타내지 않습니다.
	사용자입력을 요구	패치 시 윈도우 업데이트 팝업 창을 띄워 사용자가 에이전트 팝업 창을 클릭 시 패치를 시작하고 설치 과정을 나타냅니다.
패치관리-동작모드	설치모드	노드의 패치상태 검사 및 패치모음에서 설치승인된 패치를 노드에 설치합니다.
	검사모드	노드의 패치상태를 검사합니다.
패치관리-설치시점	즉시설치	패치상태 검사 후 패치를 즉시 설치합니다.

	종료시설치	컴퓨터 종료 시 패치를 설치합니다.
	지정된시각에설치	지정된 시각에 패치를 설치합니다.
희망시간대		패치관리-설치시점 설정이 지정된시각에 설치일 경우 활성화 되며, 설정한 시간객체의 시간동안 패치상태를 한번 검사합니다.
최대시도일수(일)		설정일자동안 희망시간대에 설치를 시도하고 만일 설치를 못할 경우 희망시간대에 상관없이 즉시설치합니다.
리부팅옵션	리부팅 안함	패치 설치 후 리부팅이 필요할 시 리부팅을 하지 않습니다.
	사용자에게 알림	리부팅 수행 여부를 에이전트 팝업 창으로 알려주며, 에이전트 팝업 창을 클릭 시 리부팅을 수행합니다.
	자동리부팅	패치 설치 후 리부팅이 필요할 시 자동으로 리부팅합니다.
자동업데이트	제어안함	Windows 자동업데이트 설정을 제어하지 않습니다.
	자동설치	Windows 자동업데이트 설정을 "업데이트 자동 설치(권장)"으로 강제화합니다.
	설치전 알림	Windows 자동업데이트 설정을 "업데이트를 다운로드하지만 설치 여부는 직접 선택"으로 강제화합니다.
	다운로드전 알림	Windows 자동업데이트 설정을 "업데이트를 확인하지만 다운로드 및 설치여부는 직접 선택"으로 강제화합니다.
	사용안함	Windows 자동업데이트 설정을 "사용안함"으로 강제화합니다.
요일		자동업데이트 설정이 자동설치일 경우 활성화되며, 운영체제 자동업데이트를 수행할 요일을 선택합니다.
시각		자동업데이트 설정이 자동설치일 경우 활성화되며, 운영체제 자동업데이트를 수행할 시각을 선택합니다.

- 유선랜 인증 프로파일 설정

유선인터페이스의 802.1x 인증 설정을 강제화 합니다.

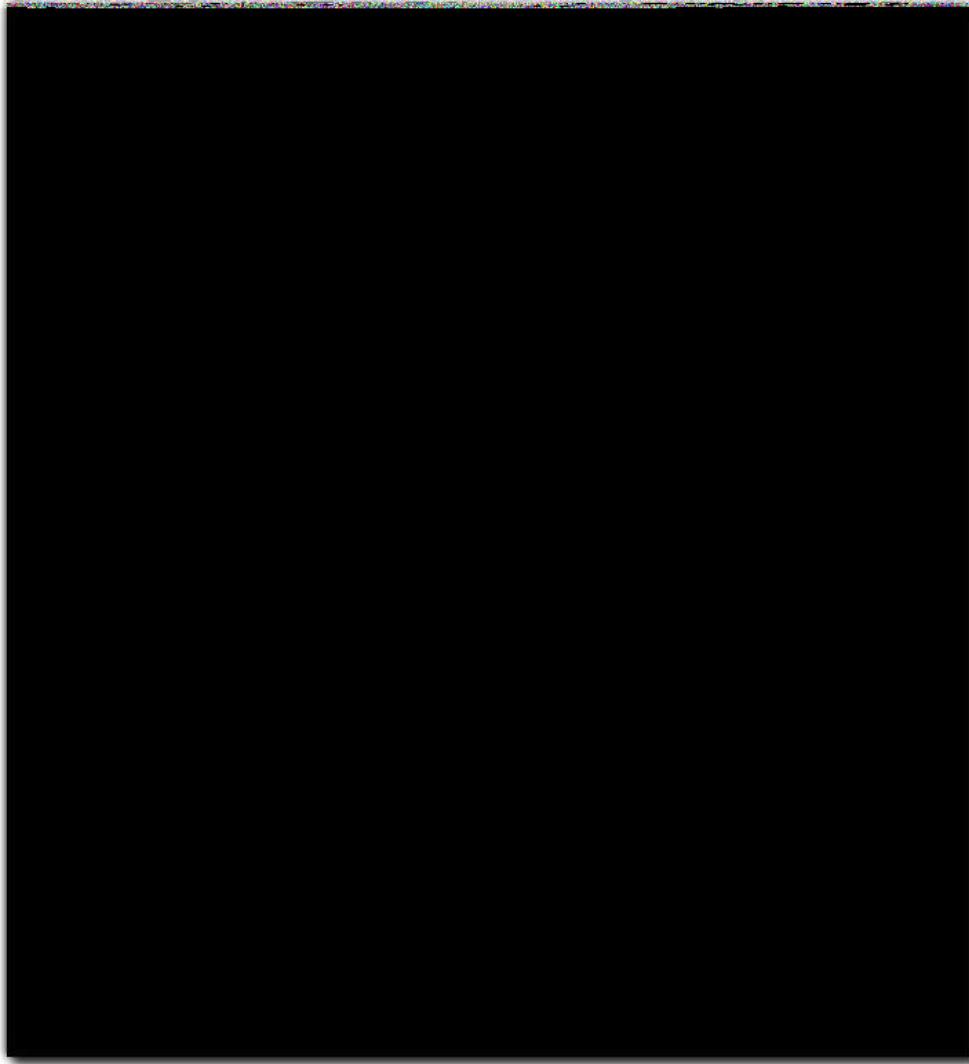


설정 항목	옵션	내용
권한 없는 네트워크 액세스로 대체	On	인증이 필요하지 않는 네트워크에 연결합니다.
	Off	인증이 필요하지 않는 네트워크로 연결하지 않습니다.
자격 증명 기억	On	인증 정보를 기억하여 이후 인증 시 아이디와 비밀번호를 입력하지 않아도 인증됩니다.
	Off	인증 정보를 기억하지 않습니다.
네트워크 인증방법		네트워크 인증정보를 선택합니다.
서버 인증서 유효성 확인	On	인증 시 인증서 유효성을 확인합니다.
	Off	인증 시 인증서 유효성을 확인하지 않습니다.
빠른 다시 연결 사용	On	빠른 다시 연결을 사용합니다.
	off	빠른 다시 연결을 사용하지 않습니다.
인증모드		인증모드를 지정합니다.
Windows로그인 정보 사용	On	자동으로 Windows 로그인 정보로 인증을 시도합니다.
	Off	Windows 로그인 정보로 인증을 시도하지 않습니다.
SSO	On	SSO를 사용합니다.
	Off	SSO를 사용하지 않습니다.
로그온 직전 수행	On	인증 직전에 SSO를 수행합니다.
	Off	인증 후에 SSO를 수행합니다.

최대 지연		최대 지연 시간을 설정합니다.
추가 대화 상자 표시	On	SSO 동안 추가 대화 상자를 표시합니다.
	Off	SSO 동안 추가 대화 상자를 표시하지 않습니다.
가상 LAN 사용	On	컴퓨터 및 사용자 인증에 별도의 가상 LAN을 사용합니다.
	Off	컴퓨터 및 사용자 인증에 별도의 가상 LAN을 사용하지 않습니다.

- 인터페이스 제어

위험이벤트 발생시 인터페이스를 사용안함으로 바꾸는 기능을 제공합니다.



설정 항목	옵션	내용
타입별 차단	제어안함	인터페이스 제어를 하지 않습니다.
	전체	노드의 유무선 인터페이스를 사용안함으로 강제화하여 네트워크를 사용하지 못하도록 합니다.
	유선	노드의 유선 인터페이스를 사용안함으로 강제화하여 네트워크를 사용하지 못하도록 합니다.
	무선	노드의 무선 인터페이스를 사용안함으로 강제화하여 네트워크를 사용하지 못하도록 합니다.
기본장치 예외	On	정책서버와 통신이 가능한 네트워크 장치는 제어대상에서 제외시킵니다.
	Off	정책서버와 통신이 가능한 인터페이스도 사용안함으로 강제화합니다.
브리지 차단	On	브리지 인터페이스를 사용안함으로 강제화 합니다. 기본장치 예외 옵션과 상관없이 제어됩니다.
	Off	브리지 인터페이스 제어를 하지 않습니다.
Promiscuous 차단	On	Promiscuous인 인터페이스를 사용안함으로 강제화 합니다. 기본장치 예외 옵션과 상관없이 차단됩니다.

	Off	Promiscuous인 인터페이스를 제어 하지 않습니다.
차단알림	사용안함	인터페이스 차단 시 사용자에게 알리지 않습니다.
	사용자메시지	인터페이스 차단 시 정의된 메시지를 팝업 창으로 띄워 사용자에게 알립니다.
	에이전트팝업	에이전트 팝업 창을 사용하여 인터페이스 차단 사실을 사용자에게 알립니다.
코드인증 사용	On	차단알림 설정이 사용자메시지일 경우 활성화 되며, 인터페이스 차단 시 코드 인증 창이 팝업되며 팝업 창에 나타나있는 에이전트 코드를 관리자에게 전달하고, 관리자는 관리 > 신청 > 에이전트 인증코드 발급에서 전달받은 에이전트 코드를 이용하여 인증 코드를 발급받습니다. 발급 받은 인증코드를 사용자에게 전달합니다. 인증코드를 통해 인터페이스를 사용할 수 있더라도 기존 인터페이스 제어 정책으로 인해 다시 차단될 수 있습니다.
	Off	인터페이스 차단 시 코드 인증 팝업 창을 띄우지 않습니다.
팝업 메시지		차단알림 설정이 사용자메시지일 경우 활성화 되며, 인터페이스 차단 시 팝업 되는 메시지 팝업 창 및 코드 인증 팝업 창에 나타날 메시지를 입력합니다.
닫기버튼 사용	On	차단알림 설정이 사용자메시지일 경우 활성화 되며, 메시지 팝업 창 및 코드 인증 팝업 창에 닫기 버튼이 활성화하여 사용자가 닫을 수 있도록 합니다.
	Off	차단알림 설정이 사용자메시지일 경우 활성화 되며, 메시지 팝업 창 및 코드 인증 팝업 창에 닫기 버튼을 비활성화하여 사용자가 닫을 수 없도록 합니다.
인터넷연결공유	허용	인터넷연결공유 설정을 제어하지 않습니다.
	차단	인터넷연결공유 설정하지 못하도록 제어합니다.

- 장치 제어

사용자 PC에서 사용금지된 장치들을 사용중지로 변경합니다.



설정 항목	옵션	내용
장치제어 방식	Disable	장치 차단 시 장치를 "사용안함" 설정하여 장치를 사용하지 못하도록 제어합니다.
	Remove	장치 차단 시 시스템에서 장치를 제거하여 장치를 사용하지 못하도록 제어합니다.
장치접근 차단팝업 사용	On	장치 차단 시 사용자에게 에이전트 팝업 창을 띄워 사용자에게 장치 차단 사실을 알립니다.
	Off	장치 차단 시 사용자에게 장치 차단 사실을 알리지 않습니다.
장치사용신청서	On	사용자가 장치사용신청서를 이용하여 제어된 장치를 사용을 할 수 있도록 합니다.
	Off	사용자가 장치사용신청을 할 수 없도록 합니다.
전체노드 사용여부	On	장치사용신청 시 신청장비 사용 대상을 전체노드 혹은 현재노드만을 선택하여 신청할 수 있습니다.
	Off	장치사용신청 시 현재노드만 신청장비를 사용할 수 있도록 합니다.
장치신청자동승인	On	장치사용신청 시 관리자 승인단계 없이 바로 자동 승인처리가 됩니다.
	Off	장치사용신청 시 자동으로 승인처리 되지 않습니다.
자동승인횟수		장치사용신청서 자동 승인횟수를 선택합니다.
자동승인횟수초기화주기		자동 승인횟수 초기화 주기를 선택합니다.
장치신청최대기간		장치사용신청 시 제어된 장치를 사용할 수 있는 최대기간을 설정합니다.
사용자암호확인	On	장치사용신청 시 사용자 비밀번호를 확인합니다.
	Off	장치사용신청 시 사용자 비밀번호를 확인하지 않습니다.

- 컴퓨터이름 변경

컴퓨터 이름을 변경하는 기능을 제공합니다.



설정 항목	옵션	내용
컴퓨터이름		제어할 컴퓨터 이름을 작성합니다. 하이픈(-)을 제외한 모든 특수문자와 공백문자를 포함할 수 없습니다. 숫자로만 된 컴퓨터이름은 사용할 수 없습니다. 매크로를 치환한 컴퓨터 이름의 길이가 영문기준 15자를 넘을 수 없습니다
리부팅방법	리부팅 안함	플러그인에 의해 컴퓨터 이름 변경 시 리부팅 하지 않습니다. 컴퓨터 이름은 리부팅 후 적용됩니다.
	사용자에게 알림	플러그인에 의해 컴퓨터 이름 변경 시 팝업 창을 띄워 리부팅 여부를 선택할 수 있습니다.
자동 리부팅		플러그인에 의해 컴퓨터 이름 변경 시 강제 리부팅합니다.

지연 시간		리부팅방법 설정이 사용자에게 알림일 경우 활성화 되며, 플러그인에 의해 컴퓨터 이름 변경 시 설정한 시간을 주기로 리부팅 수행 여부 팝업 창을 띄웁니다.
수행 계정	에이전트 기본 수행계정	에이전트 기본 계정으로 컴퓨터 이름을 변경합니다. 에이전트 계정 설정은 노드정책에서 확인할 수 있습니다.
	별도의 수행계정 설정	에이전트 기본 계정 권한으로 컴퓨터 이름을 변경하지 못할 경우 컴퓨터 이름변경을 할 수 있는 권한을 가지고 있는 계정을 설정하여 해당 계정으로 컴퓨터 이름을 변경합니다.
	아이디	수행 계정 설정이 별도의 수행계정 설정일 경우 활성화되며, AD 계정 ID를 입력합니다.
	비밀번호	수행 계정 설정이 별도의 수행계정 설정일 경우 활성화되며, AD 계정 Password 입력합니다.

- 프로그램 제거

제어판의 프로그램 제거에 등록된 프로그램중 제거 가능한 특정 프로그램을 제거합니다.



설정 항목	옵션	내용
프로그램 이름		제어판의 프로그램 제거에 등록된 프로그램중 제거할 프로그램 이름을 입력합니다.
삭제전 알림	On	프로그램 삭제전 알림 팝업 창을 띄웁니다.
	Off	프로그램 삭제전 알림 팝업 창을 띄우지 않습니다.
메시지 내용		삭제전 알림 설정이 On일 경우 활성화 되며, 팝업 창에 보여질 메시지를 입력합니다.
수행 계정	에이전트 기본 수행계정	에이전트 기본 계정 권한으로 프로그램 제거를 수행합니다. 에이전트 계정 설정은 노드정책에서 확인할 수 있습니다.
	PC에 로그인된 계정	PC에 로그인되어 있는 계정으로 프로그램 제거를 수행합니다.
	별도의 수행계정 설정	별도의 수행계정을 이용하여 프로그램 제거를 수행합니다.
아이디		수행 계정 설정이 별도의 수행계정 설정일 경우 활성화 되며, AD 계정 ID를 입력합니다.
비밀번호		수행 계정 설정이 별도의 수행계정 설정일 경우 활성화 되며, AD 계정 Password를 입력합니다.

리부팅옵션	리부팅 안함	리부팅하지 않습니다.
	사용자에게 알림	에이전트 팝업 창을 띄워 리부팅 여부를 선택할 수 있습니다.
	자동 리부팅	30초 후 리부팅 합니다. 에이전트 팝업 창 클릭 후 출력되는 팝업 창에서 리부팅을 취소 및 수행할 수 있습니다. 에이전트 팝업 창을 닫을 시 리부팅이 취소 됩니다.

- 프로세스 강제종료

액션 검사조건에 설정된 프로세스에 대해서 강제종료 기능을 수행합니다.



설정 항목	옵션	내용
차단 팝업메시지 표시	On	프로세스 강제종료 시 에이전트 팝업 창으로 표시합니다.
	Off	프로세스 강제종료 시 에이전트 팝업 창을 띄우지 않습니다.
팝업메시지내용		차단 팝업메시지 표시 설정이 On일 경우 활성화 되며, 프로세스 강제종료 시 팝업되는 메시지 내용을 입력합니다. {PROCESSNAME} 입력 시 강제종료된 프로세스 이름을 표시할 수 있습니다.

- 프린터정보 수집

컴퓨터시스템에 등록되어있는 프린터에 대한 정보를 제공합니다.



설정 항목	옵션	내용
가상 프린터 수집 제외	On	프린터수집항목 중 물리적으로 연결되어있지 않은 로컬프린터 항목을 제외시킵니다.
	Off	가상 프린터 관계 없이 프린터 정보를 수집합니다.

- 하드웨어정보 수집

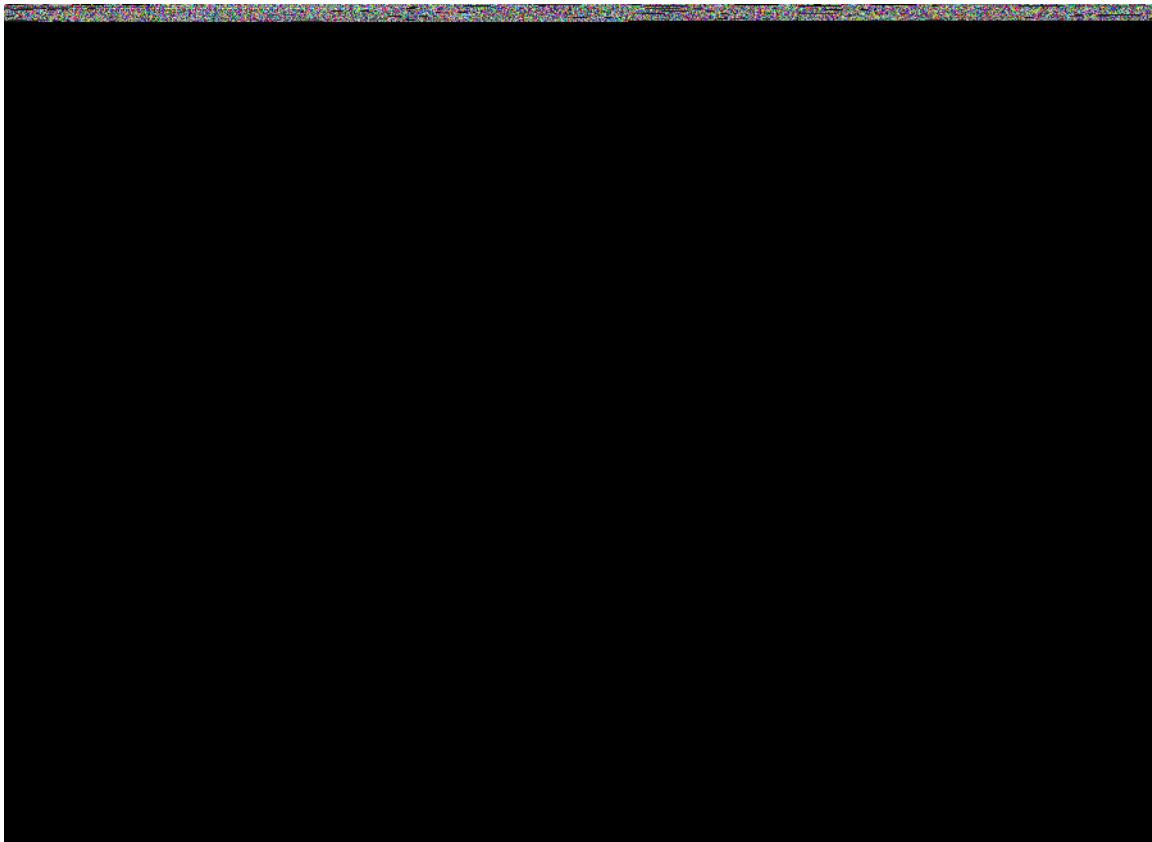
마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다.
하드웨어정보는 관리 > 노드 > 노드상세정보 > 시스템정보에서 확인할 수 있습니다.



설정 항목	내용
CPU 업데이트 최소비율	마지막으로 전송한 CPU 사용량이 수집 시 사용량과 설정비율 이상 차이가 나면 정보를 업데이트합니다. 설정비율은 전체CPU용량 기준으로 계산됩니다.
메모리 업데이트최소비율	마지막으로 전송한 메모리 사용량이 수집 시 사용량과 설정비율 이상 차이가 나면 정보를 업데이트합니다. 설정비율은 전체메모리용량 기준으로 계산됩니다.
저장장치 업데이트최소비율	마지막으로 전송한 저장장치 사용량이 수집 시 사용량과 설정비율 이상 차이가 나면 정보를 업데이트합니다. 설정비율은 전체저장장치용량 기준으로 계산됩니다.

- Malware Detector

Insights ECO 시스템과 연동하여 단말에서 발생하는 악성코드를 감지합니다.
Malware 정보는 _관리 > 노드 > 노드상세정보 > Malware 탭에서 확인할 수 있습니다.



설정 항목	내용
정보수집 동의	플러그인을 사용하기 위해서는 정보수집에 대한 사용자의 동의가 필요합니다.
수집제외경로	Malware 감지에 필요한 정보 수집에서 제외할 폴더 경로를 설정합니다.

플러그인 작업선택

관리자는 플러그인에서 작업선택 기능을 이용하여 플러그인 업로드 및 삭제를 할 수 있습니다.

- **플러그인 업로드**

플러그인 업로드를 위해 시스템 > 업데이트 관리 > 소프트 웨어 > 플러그인 > 작업선택 > 플러그인 업로드 를 클릭합니다.



플러그인 파일은 gpf 형식이며 파일 선택 버튼을 클릭하여 gpf 형식의 파일을 선택한 후 업로드 버튼을 클릭하여 플러그인을 업로드할 수 있습니다.



- **플러그인 삭제**

필요 없는 플러그인을 선택 후 시스템 > 업데이트 관리 > 플러그인 > 작업선택 > 플러그인 업로드 를 클릭합니다.
플러그인 삭제가 되지 않을 시 [항목 삭제](#)를 참고 바랍니다.



운영정보 데이터

운영정보 데이터

Genian NAC는 NMAP 혹은 여러 가지 쿼리를 이용하여 노드의 정보를 수집합니다.

간혹 얻을수 있는 정보가 한정된 경우 노드정보, 운영체제 등의 정보를 유추하는데, 이 때 사용되는 것이 GPDB와 NMDB입니다.

이는 오랜 시간 동안 운영체제와 노드정보에 대해 축척해 놓은 Genian 만의 데이터베이스입니다.

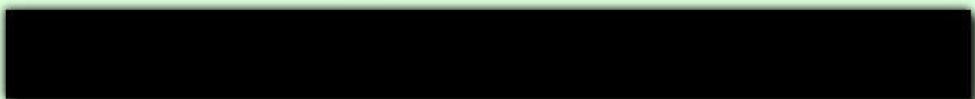
GPDB와 NMDB는 탐지가 안되거나 잘못 탐지된 부분에 대한 오탐보고를 전송하면 관련 사항이 수정되어 반영됩니다. 업데이트는 매일 수행됩니다.

해당 운영정보 데이터 페이지는 업데이트되는 GPDB와 NMDB의 정보를 받아오는 역할을 수행합니다.

또한, 업데이트 검사 버튼을 이용하여 운영체제 감지 데이터, 노드정보 감지 데이터, 패치 정보 데이터를 검사하여 최신 데이터가 아닐 경우 최신 데이터로 업데이트 할 수 있습니다.



업데이트를 수행하는 경우 인터넷이 되는 상황에서 수행해야 합니다.
따라서 설정 > 환경설정 > 기타설정에서 인터넷 연결을 On한 후에 진행하시기 바랍니다.



서비스 관리

서비스 관리

관리자는 서비스 관리 탭을 이용하여 서비스제어 기능을 수행할 수 있습니다.

- 서비스제어

모든 정책에 대한 적용, 서비스 동작 및 중지를 수행할 수 있습니다.



서비스 제어

서비스 제어

서비스 제어 페이지를 통하여 모든 정책의 적용, 네트워크 및 시스템에 적용중인 서비스를 일시적으로 중단할 수 있습니다.



항목	내용
정책적용	현재 설정되어 있는 모든 정책을 즉시 적용 합니다.
현재 서비스가 동작중입니다	중지 버튼을 클릭 할 시 네트워크 및 에이전트 제어를 중단합니다.
웹어플리케이션 재구동	관리콘솔, CWP, IP신청시스템 중 하나의 웹어플리케이션을 선택하여 선택한 웹어플리케이션을 재구동 합니다.

접속포트

접속포트

GenianNAC 제품에 서비스별로 사용되는 Port Number 정보를 제공합니다. 해당 정보를 참고하여 방화벽 설정 등 작업에 참고할 수 있습니다.

RADIUS서비스를 제외한 서비스별 Port Number는 CLI에서 변경할 수 있습니다.



감사

감사

관리자는 감사탭을 통하여 노드나 장비들에 발생되는 모든 내용의 기록을 확인할 수 있습니다.

- [로그](#) : CLI 입력한 명령어, 변경된 설정, 노드의 변경된 정보 등의 기록하며 기록을 확인할 수 있는 템입니다.
- [리포트](#) : 쿼리문을 통하여 원하는 자료를 리포트로 만들 수 있으며, 노드 수를 리포트로 생성하여 그래프로 확인할 수 있는 템입니다.
- [로그](#)
- [리포트](#)

로그

로그란?

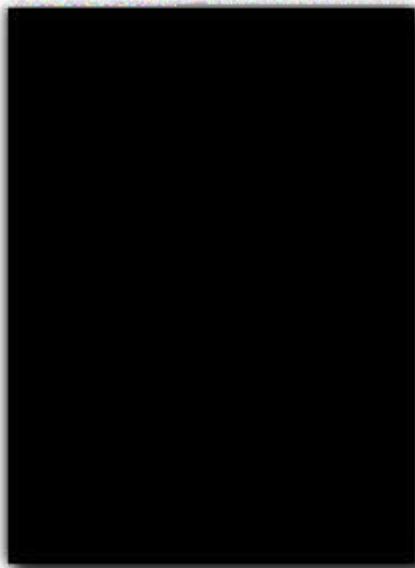
로그란 장비의 운영과정에서 발생하는 거의 모든 내용들(장비의 장애발생, 불법적인 접근 시도, 정책변경, 작업수행 결과 등)이 발생시간 등과 함께 기록된 자료입니다.

관리자는 로그를 통하여 긴급 상황에 대하여 신속히 대처할 수 있고, 로그 검색을 통하여 노드들의 패턴을 파악하여 효율적으로 정책을 수립할 수 있습니다.

로그

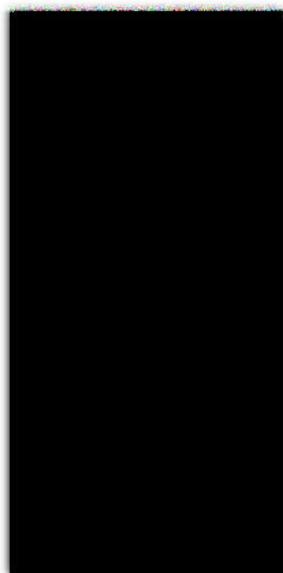
- 트리 뷰

저장된 필터를 트리로 보여주며, 필터에 존재하는 다양한 기능 설정 유무를 확인 확인할 수 있습니다.
또한, RADIUS 설정 및 동작이력 설정 시 RADIUS 인증 로그와 노드의 동작이력 확인할 수 있습니다.



- 필터 뷰

관리자는 필터를 이용하여 특정 로그를 검색할 수 있으며,
해당 필터로 검색된 로그가 발생 시 알람 및 태그 설정 등 다양한 설정을 할 수 있습니다.



- 타임차트 뷰

관리자는 로그를 막대그래프 형식으로 나타낸 타임차트 뷰를 확인하여 직관적으로 로그를 확인할 수 있습니다.



- 로그 뷰

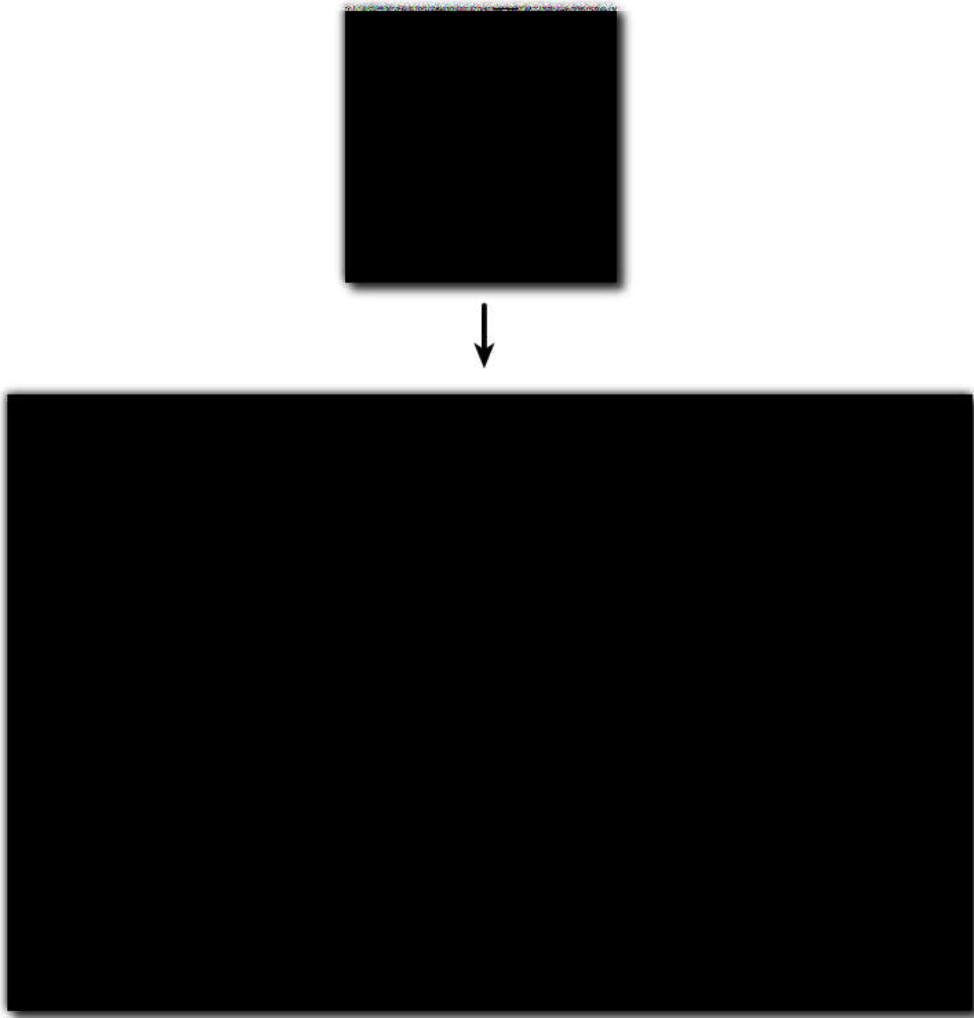
로그를 확인할 수 있으며, 필터를 설정하여 관리자가 원하는 로그만 확인할 수 있습니다.
또한, 로그모니터, 내보내기, 노드바구니에 담기 기능을 이용하여 다양한 작업을 수행 할 수 있습니다.



트리 뷰

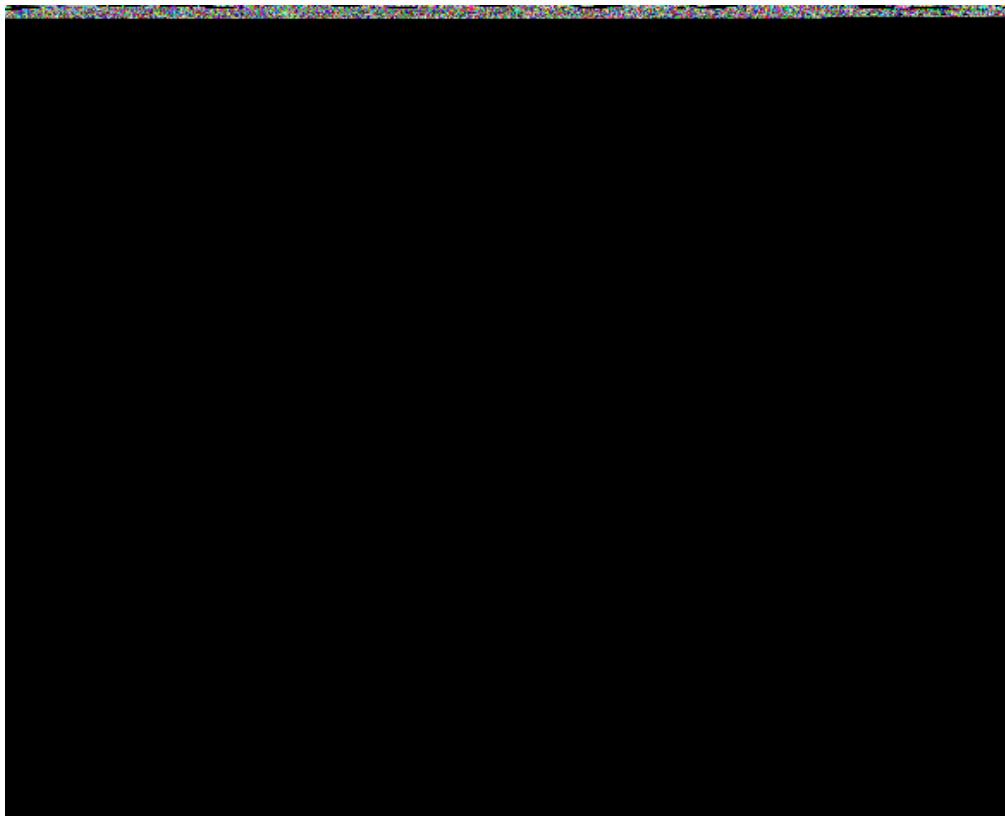
- 로그 검색

현시간에서 과거 일주일간의 로그가 로그 뷰에 출력되며, 필터 뷰를 이용하여 관리자가 원하는 로그만을 출력할 수 있습니다.



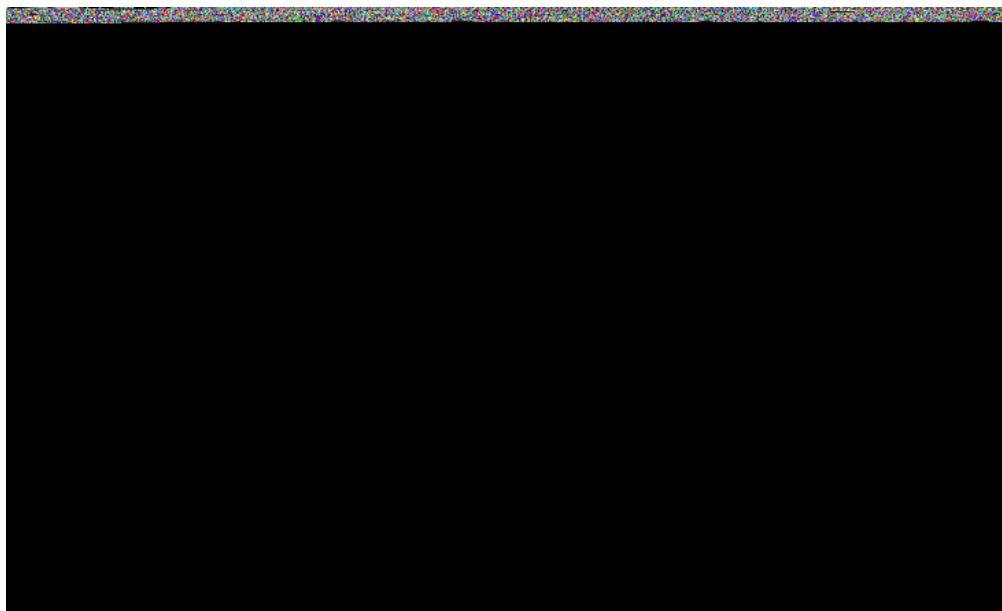
- 검색필터

저장한 필터를 확인할 수 있으며, 저장된 필터를 트리 뷰에 추가할 수 있고, 대시보드의 위젯으로 띄울 수 있습니다.
그 외 알람, SYSLOG 전송, SNMP Trap전송, URL호출 옵션 사용 유무를 확인할 수 있습니다.



- 필터선택

검색필터 관리 뷰의 로그이름을 선택하면 해당 로그 검색 페이지로 이동하여 로그를 로그필터의 수정이 가능합니다.



- 필터 설정

관심 필터 설정을 아래와 같이 토글 형식으로 변경할 수 있습니다.



관심필터의 설정에 따른 변경사항은 아래와 같습니다.

설정 항목	변경 사항
관심필터	 로그 트리 뷰에 해당 필터가 검색필터 하위에 추가되어 표시됩니다.

- 필터 알람내역

해당 필터에 알람, SYSLOG, SNMP, URL 알람이 설정되어 있는지 확인 할 수 있습니다.



- RADIUS

RADIUS Server를 활성화 시 RADIUS Server에 접근한 노드들에 대한 로그를 확인할 수 있습니다.



필터 뷰

필터를 통하여 원하는 항목의 로그만을 추출하고, 많이 사용하는 필터는 저장하여 언제든 해당 필터의 내용을 다시 볼 수 있습니다.
필터는 종류, 기간, 항목검색, 고급검색 등으로 로그를 분류할 수 있습니다.

- 종류

감사로그와 UP/DOWN로그 중 선택한 종류만 로그 뷰에서 확인할 수 있습니다. UP/DOWN로그는 저장된 동작상태 이력을 로그 뷰에서 보여주는 기능입니다.

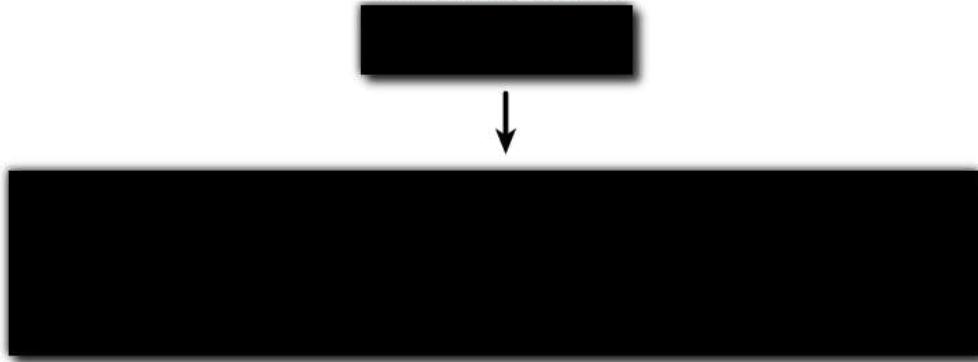
동작상태 이력 저장은 설정 > 환경설정 > 감사기록 > 동작상태 이력 저장(노드, 에이전트) 항목이 On일 시 저장됩니다.



- 기간

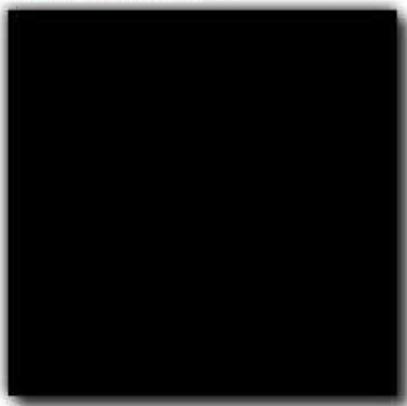
현재 날짜와 로그가 발생한 시각을 기준으로 오늘, 어제, 1주, 1개월, 1년, 전체, 사용자입력 중 선택하여, 선택한 날짜에 발생된 로그만 추출할 수 있습니다.

관리 뷰에서 필터에서 선택한 기간이 표시되며 화살표를 이용하여 기간단위 만큼 앞, 뒤로 이동이 가능합니다.



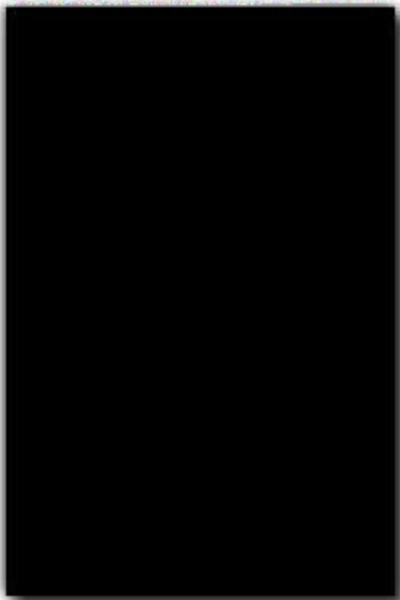
- 항목검색

IP, MAC, 사용자ID, 사용자명, 설명에 관리자가 원하는 조건을 입력하여 검색이 가능합니다.



- 고급검색

고급검색을 통하여 더욱 세분화된 조건으로 원하는 로그를 쉽게 추출할 수 있습니다.
조건에는 로그종류, 로그ID, 관리장비명, 부가정보, 부서명이 있으며,
로그종류와 로그ID 선택 가능항목은 아래 표에 열거된 내용과 같습니다.

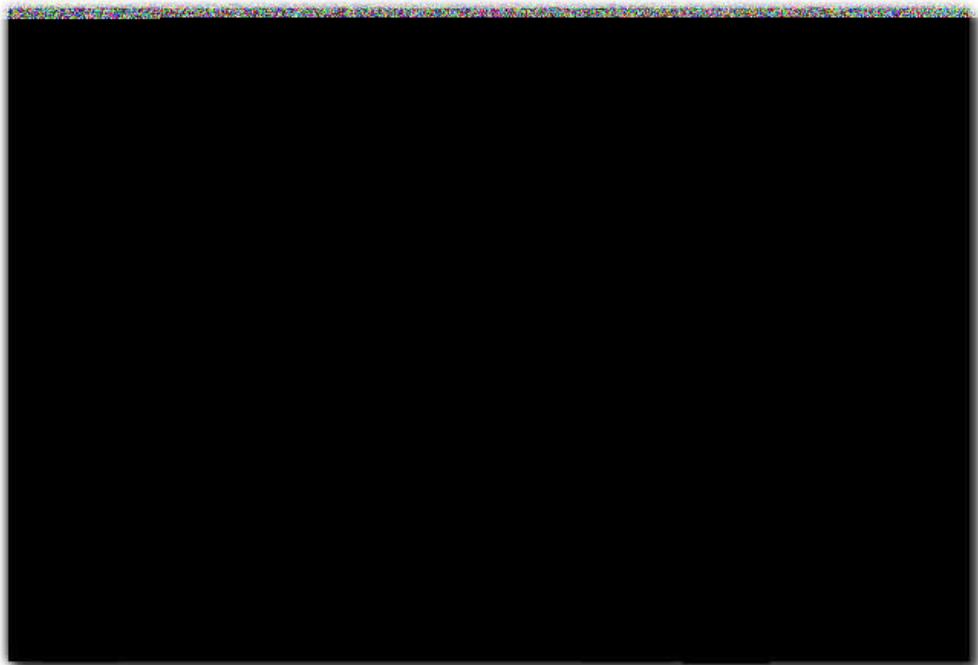


로그종류	에러, 위험, 경고, 알림
로그ID	AGENT사용시작, AGENT사용종료, CLI, DHCP, GENIAN장비, IP사용관리, IP사용시작, IP사용종료, Start, Stop, SYSLOG, 관리자접속, 그룹, 네트워크정보, 네트워크제어, 노드관리, 노드정보, 데이터동기화, 데이터무결성, 데이터베이스, 동작상태변경, 라이센스사용관리, 리포트, 매체사용관리, 무선랜AP, 무선랜관리, 무선센서정보, 바이러스치료(성공, 실패, 완료), 비정상노드, 사용자관리, 설정변경, 소프트웨어정보, 시스템관리, 시스템정보, 쓰기차단, 쓰기허용, 알람, 업데이트, 에이전트, 에이전트액션, 에이전트인증코드, 운영체제 업데이트 동기화, 운영체제 업데이트 서비스, 위험관리, 읽기차단, 읽기허용, 정책, 정책변경

- 필터 저장

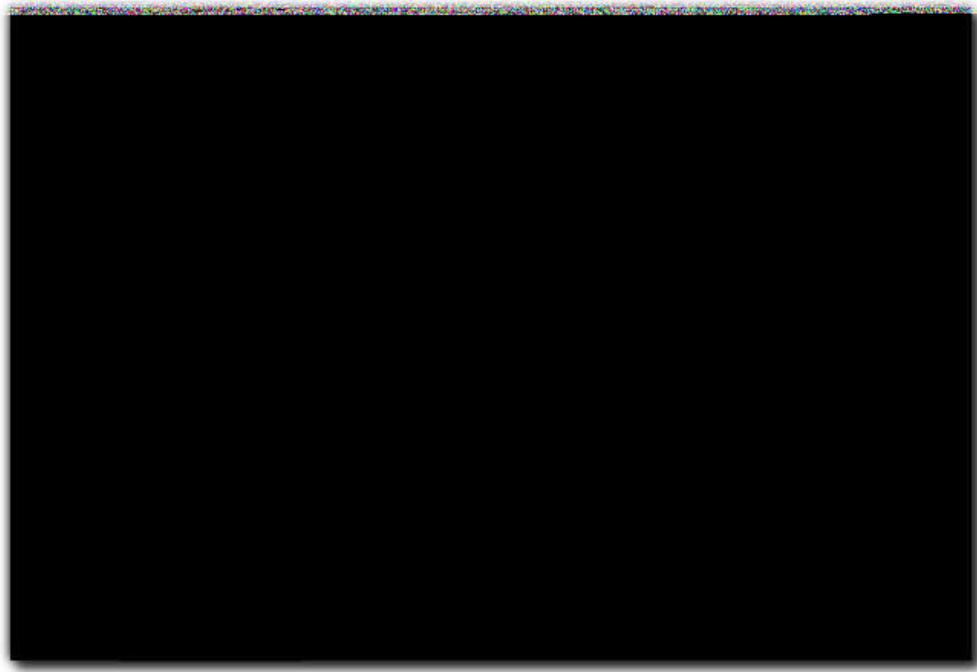
- 검색

원하는 로그종류와 로그ID를 선택합니다.



2. 저장

검색 후 결과가 로그 뷰에 정상적으로 출력되면 해당 필터를 저장합니다.



3. 신규필터 설정

알람 서비스는 해당 로그가 발생하면 관리자에게 알람을 전송하는 서비스이며, 알람 서비스에는 알람전송(SMS, Email), SYSLOG 전송, SNMP Trap, URL 호출 서비스가 있습니다. 이외에, 태그의 설정을 할 수 있습니다.



알람종류	설정 값과 설명
알람전송	알람수신 관리자, 알람수신 관리역할, 단문메시지(SMS,Email 제목), 장문메시지(Email 내용)이 들어갑니다. 알람수신 관리자와 관리역할은 OR 조건으로 설정되며, 메시지는 각 관리자 정보에 저장된 연락처 또는 메일주소로 전송됩니다. 또한 메시지의 내용에는 매크로를 이용한 템플릿을 정의하여 사용할 수 있습니다.
SYSLOG 전송	서버주소, 전송포트, SYSLOG 메시지가 전송될 문자형식인 CHARSET(EUC-KR, UTF-8)을 설정합니다.
SNMP Trap 전송	서버주소, Community, SNMP 메시지가 전송될 문자형식인 CHARSET(EUC-KR, UTF-8)을 설정합니다.
Webhook	URL, 메시지가 전송될 문자형식인 CHARSET(EUC-KR, UTF-8)을 설정합니다. SYSLOG나 SNMP Trap을 사용할 수 없을 때 사용하는 기능으로 로그 발생 시, 설정한 URL 페이지를 호출하여 로그가 발생했다는 신호를 보냅니다.
태그	할당으로 설정 시 해당 로그 필터에 로그가 기록될 시 기록된 로그의 IP, MAC, 사용자, 노드에 관리자가 지정한 태그를 지정할 수 있으며, 해제로 설정 시 해당 로그 필터에 로그가 기록될 시 지정한 태그가 해제됩니다. NONE으로 설정 시 해당 기능을 사용하지 않습니다.

- 옵션에 따른 결과

- 관심필터, 출력컬럼에 따른 결과

아래 그림과 같이 관심필터에 체크를 하고 필터를 생성하면, 트리 뷰에 해당 필터가 생성되며, 로그모니터에도 해당 로그탭이 생성됩니다. 출력컬럼 중 선택 항목에 있는 컬럼은 로그 뷰에 출력되며, 사용가능 항목에 있는 컬럼은 로그 뷰에 출력되지 않습니다.



관심필터



출력컬럼



- 알람전송

알람수신 관리자와 알람수신 관리역할을 설정하고(알람수신 관리자는 각 알람을 받을 각 관리자를 따로 지정할 수 있고, 알람수신 관리역할을 설정하게 되면 해당 권한을 가진 관리자들 모두에게 알람이 가게됩니다.), 메시지 내용을 설정합니다. 전화번호는 관리 > 사용자 > 해당 ID 선택 > 관리자 설정 에 발신번호에 입력되어 있는 전화번호로 메시지가 전송 됩니다.



타임차트 뷰

• 타임차트 뷰

관리자는 타임차트를 확인하여 검색한 기간 동안의 로그를 차트로 확인할 수 있습니다. 또한 타임차트 뷰를 드래그하여 드래그 한 영역의 기간의 로그를 로그 뷰로 확인할 수 있습니다.

타임차트는 stacked, logarithmic으로 두 가지 종류가 있으며 stacked는 로그를 차트로 만들며, 로그의 종류에 따라 차트에 보여지는 색상이 다릅니다.

로그의 종류는 우측 Legend view에 나타나 있으며, 로그의 위험정도를 파악하여 ERROR, ANOMALY, WARN, INFO으로 나눕니다. 로그 종류를 클릭할 시 차트에 해당 로그 종류가 보이지 않게 됩니다.

logarithmic은 stacked에서 보여준 차트를 대수눈금 즉, 상대적으로 로그량이 적어 보이지 않던 로그를 자세히 보여줍니다.

타임차트에 보여지는 막대를 클릭할 시 해당 막대를 구성한 로그를 확인할 수 있습니다.

분석 차트는 검색한 기간 동안의 로그를 가장 많이 발생시킨 IP TOP10, 로그ID, 인증사용자 TOP10 등의 정보를 파이 차트와 바 차트로 나타내어 관리자가 로그를 더욱 식별하기 쉽게 할 수 있도록 할 수 있는 기능입니다.



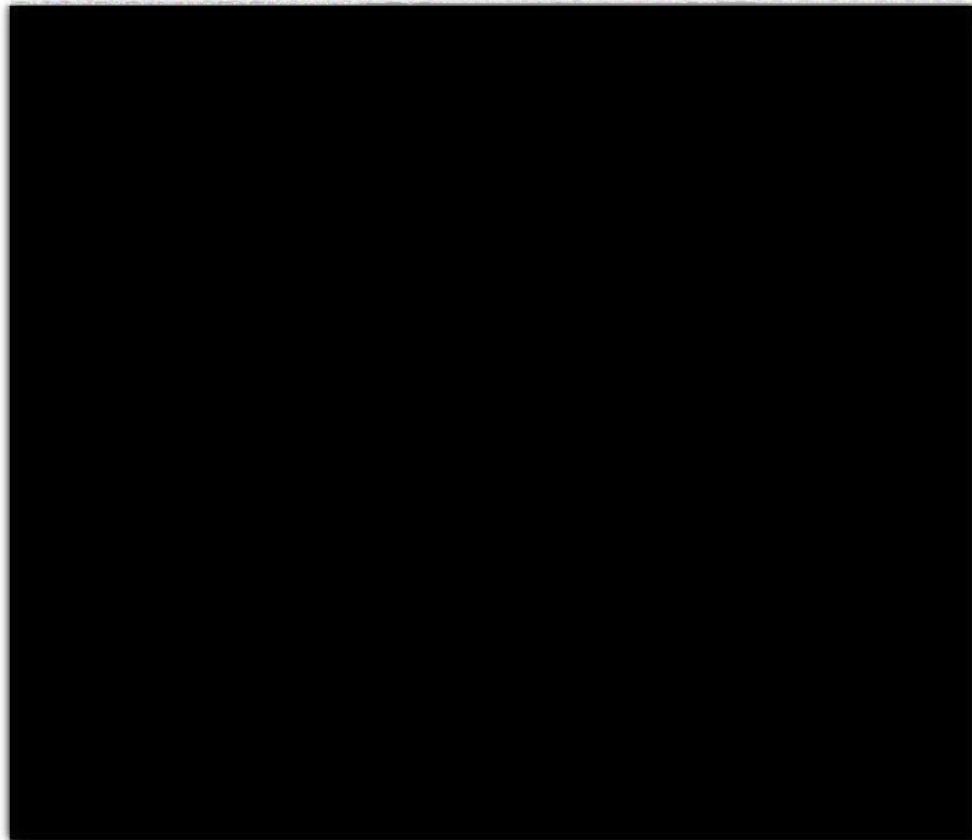
- 분석 차트

분석차트는 관리자가 로그를 식별하기 쉽게 하기 위해 로그종류, 로그ID, 로그를 발생시킨 IP TOP 10 과같은 로그를 파이차트와 바차트로 나타내어줍니다.

분석차트에 나타난 차트들을 클릭할 시 해당 로그를 테이블 형식으로 확인할 수 있습니다.

관리자는 로그 검색 버튼을 클릭 시 로그를 검색하던 페이지로 이동하게 됩니다.

분석차트는 관리자가 검색한 로그를 바탕으로 차트를 나타냅니다.



로그 뷰

- 로그 뷰

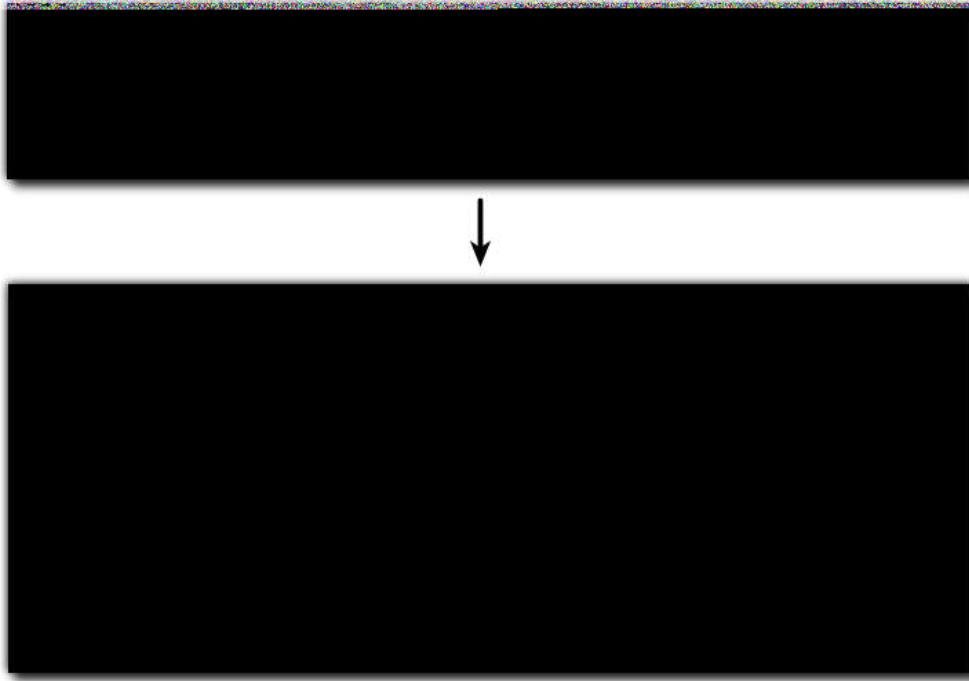
NAC는 NAC에 관련 모든 Action을 로그로 기록합니다. 로그 뷰는 관리자가 NAC 관련 로그를 확인할 수 있는 뷰입니다. 관리자는 로그 뷰를 통해 history를 확인할 수 있으며, 문제가 발생 시 보다 구체적인 내용을 로그를 통해 확인할 수 있습니다.



항목	설명
시간	로그가 발생한 시각을 나타냅니다. 클릭 시 감사로그를 상세히 조회할 수 있는 로그상세 팝업 창이 출력됩니다.
로그종류	로그의 종류를 나타내며, 위험 수준을 나타내기도 합니다.
로그ID	발생한 로그의 주제입니다.
관리장비명	등록 노드가 로그를 발생 시 해당 노드의 관리장비의 IP를 나타냅니다.
IP	로그를 발생시킨 IP를 나타냅니다.
MAC	로그를 발생시킨 MAC을 나타냅니다.
사용자ID	사용자인증 받은 노드가 로그 발생 시 사용자 ID를 나타냅니다.
사용자명	사용자인증 받은 노드가 로그 발생 시 사용자명을 나타냅니다.
부서명	로그를 발생시킨 노드의 소속된 부서를 나타냅니다.
설명	로그의 자세한 내용입니다.
추가정보	추가 정보가 설정 시 설정한 추가정보가 출력 됩니다. 추가 정보 설정은 감사기록을 참고 바랍니다.

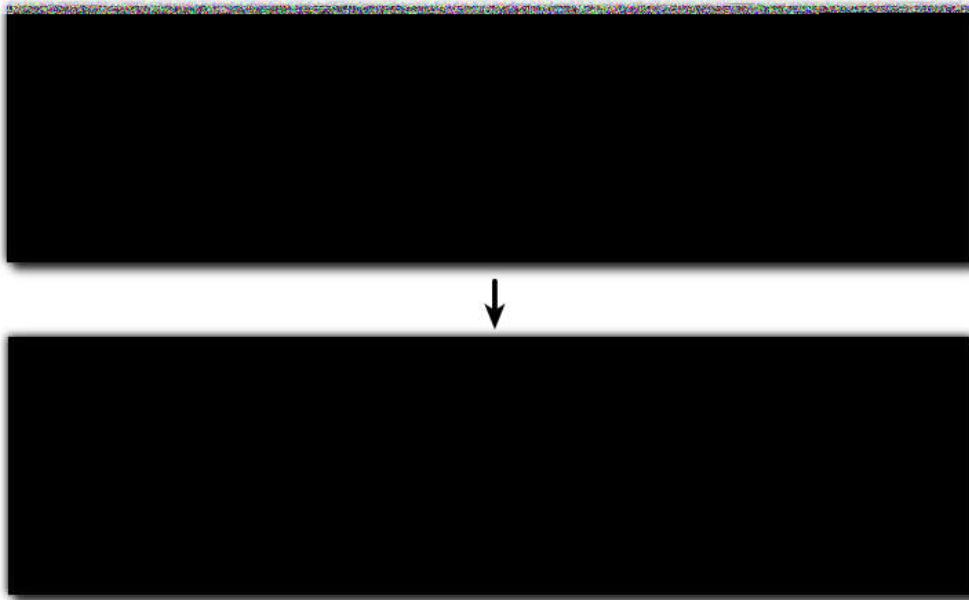
- 내보내기

관리자는 검색한 로그를 내보내기 기능을 이용하여 xlsx 확장자 파일로 출력할 수 있습니다.
확장자는 설정을 통해 xls으로 변경하여 출력할 수 있습니다. 설정 방법은 관리콘솔을 참고 바랍니다.



- 실시간 모드

관리자는 테이블창에 있는 실시간 모드를 이용하여 실시간으로 올라오는 로그를 확인할 수 있습니다.
또한, 로그 정보 업데이트 주기를 설정할 수 있고, 팝업 기능을 이용해 실시간 로그를 팝업 창에서 확인 할 수 있습니다.



리포트

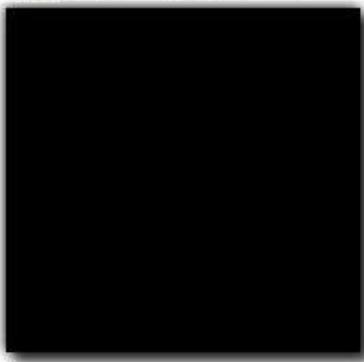
리포트란?

리포트란 관리자가 원하는 정보를 보기 쉽게 차트와 테이블로 보여주는 기능입니다.
관리자는 리포트를 이용하여 데이터를 문서화하여 보관하거나 보고 할 때 효율적으로 이용 할 수 있습니다.
리포트의 종류는 주이 리포트와 쿼리 리포트가 있습니다.

트리 뷰

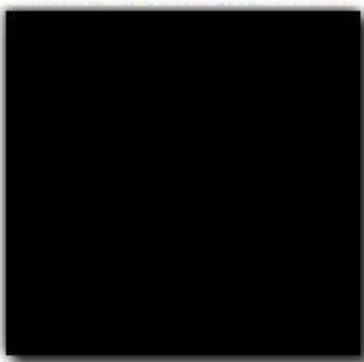
- 리포트 정의

리포트를 추가 삭제할 수 있고, 리포트 명을 클릭하여 리포트의 설정값을 수정할 수 있습니다



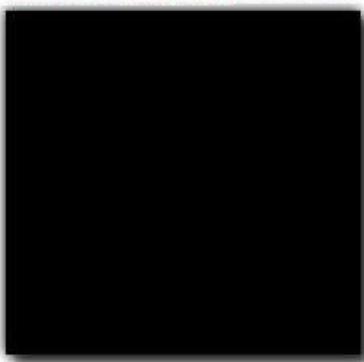
- 리포트 목록

리포트를 추가 할 시 표시한 부분에 리포트 이름이 추가 되며 리포트 이름을 클릭 시 리포트의 결과를 확인할 수 있습니다.



- 자동 리포트

기본으로 제공되는 노드그룹, 로그필터, 무선랜그룹 리포트를 정기적으로 메일로 받아 볼 수 있습니다.



관리 뷰

- 관리 뷰

등록된 리포트를 나타내어 주며 리포트명을 클릭하여 해당 리포트의 정의를 수정할 수 있습니다.



쿼리 리포트

쿼리 리포트

관리자는 쿼리 리포트 기능을 이용하여, 관리자가 원하는 쿼리문(SQL문)에 대한 결과값을 리포트형식의 엑셀파일로 출력할 수 있습니다.
쿼리 리포트는 쿼리문을 설정하여 리포트를 정의하고, 정의된 리포트에서의 파일생성 작업으로 리포트가 만들어집니다.

쿼리 리포트 추가

1. 쿼리 리포트 추가

감사 > 리포트 > 리포트 정의 > 작업선택 > 추가 를 선택하여 리포트를 설정하는 페이지로 이동합니다.



2. 기본정보 입력

리포트를 식별할 제목과 설명을 기입하고 리포트 적용유무, 자동생성 사용유무를 선택 합니다.



항 목	내 용
리 포 트 타 입	리포트 타입을 나타냅니다.
리 포 트 제 목	사용하려는 리포트 제목을 입력합니다.
리 포 트 설 명	추가 하려는 리포트의 설명을 입력합니다.
적 용 모 드	추가 하려는 리포트의 사용유무를 설정합니다.
자 동 생 성	원하는 날짜와 시간을 지정하고 그 시간에 리포트 파일을 생성하는 합니다.

3. 리포트 자동생성

쿼리 리포트의 자동생성부분이 사용함으로 선택 할 경우 입니다.



항 목	내 용
지정시각 구분	매일+시각, 지정일+시각, 날짜+시각, 요일+시각, 주/요일+시각 이 있으며, 자신이 원하는 날짜에 맞게 선택합니다.
지 정 일	지정시각 구분에서 지정일+시각을 선택 하였으면, 활성화 되고, 지정일+시각을 설정하면 설정한 지정일에 리포트가 생성됩니다.
날 짜	지정시각 구분에서 날짜+시각을 선택 하였으면, 활성화 되고, 날짜+시각을 설정하면 설정한 날짜에 리포트가 생성됩니다.
요 일	지정시각 구분에서 요일+시각을 선택 하였으면, 활성화 되고, 요일+시각을 설정하면 설정한 요일에 리포트가 생성됩니다.
주	지정시각 구분에서 주/요일+시각을 선택 하였으면, 활성화 되고, 주+시각을 설정하면 설정한 주에 리포트가 생성됩니다.
주 중 요 일	지정시각 구분에서 주/요일+시각을 선택 하였으면, 활성화 되고, 주중요일+시각을 설정하여 설정한 주중요일에 리포트가 생성됩니다.
시 각	파일이 생성될 시각을 설정합니다.

4. 리포트 출력파일

리포트 데이터를 출력할 파일 타입을 설정 합니다.
EXCEL(xls)로 리포트 데이터를 출력할 시 EXCEL 97~2003 버전이 설치되어야 리포트 데이터를 확인할 수 있으며,
EXCEL(xlsx)일 경우 excel 2007 이상 버전이 설치되어 있어야 확인할 수 있습니다.



5. 수행쿼리 입력

모든 USER의 ID와 NAME를 나타내는 SQL쿼리문 입니다. 쿼리 리포트는 SQL쿼리문을 이용하여 필요한 자료를 얻고, 쿼리 리포트를 정의 합니다.



6. 쿼리 리포트 파일 생성

감사 > 리포트 > 작업선택 > 리포트파일생성을 클릭하여 작성한 SQL쿼리문의 데이터를 엑셀 파일로 생성합니다.



7. 쿼리 리포트

입력한 SQL쿼리문의 USER ID와 USER NAME을 엑셀파일로 나타냅니다.



쿼리 리포트 삭제

관리자는 필요 없는 쿼리 리포트를 삭제 할 수 있습니다
쿼리 리포트 삭제 과정은 [항목 삭제](#)를 참조 바랍니다.

노드 리포트

노드 리포트

관리자는 노드 리포트를 이용하여 노드 그룹과 전체노드의 전체, 동작, 에이전트 설치, 동작 에이전트 노드 수에 대한 정보를 차트와 테이블로 표현하여 보여줍니다.

노드 리포트를 이용하여 노드 수를 파악하기 쉽고 한눈에 볼 수 있어 관리할 때 유용하게 활용할 수 있습니다.

노드 리포트 추가

1. 노드 리포트 추가

감사 > 리포트 > 리포트 정의 > 작업선택 > 노드리포트 추가 를 선택하여 리포트를 설정하는 페이지로 이동합니다.



2. 기본정보 입력

리포트를 식별할 제목과 설명을 기입하고 위젯 사용유무, 리포트 적용유무, 출력 기간을 설정합니다.



항 목	내 용
리 포 트 타 입	리포트 타입을 나타냅니다.
리 포 트 제 목	추가하려는 리포트의 제목을 입력합니다.
리 포 트 설 명	추가하려는 리포트의 설명을 입력합니다.
적 용 모 드	추가 하려는 리포트를 사용유무를 설정하는 것입니다.
자 동 생 성	원하는 날짜와 시각을 지정 시 설정한 시각에 리포트 파일을 생성합니다.

3. 수집 대상/차트 설정

리포트의 수행 주기를 정하고 수집대상을 정합니다. 차트 타입은 선, 면, 막대 차트 중 하나를 선택하고 차트의 색상을 정합니다. 모든 설정이 완료되면 색상버튼 아래에 있는 추가버튼을 클릭하여 리포트 설정을 추가하고 하단에 있는 추가버튼을 클릭하여 리포트를 추가합니다.

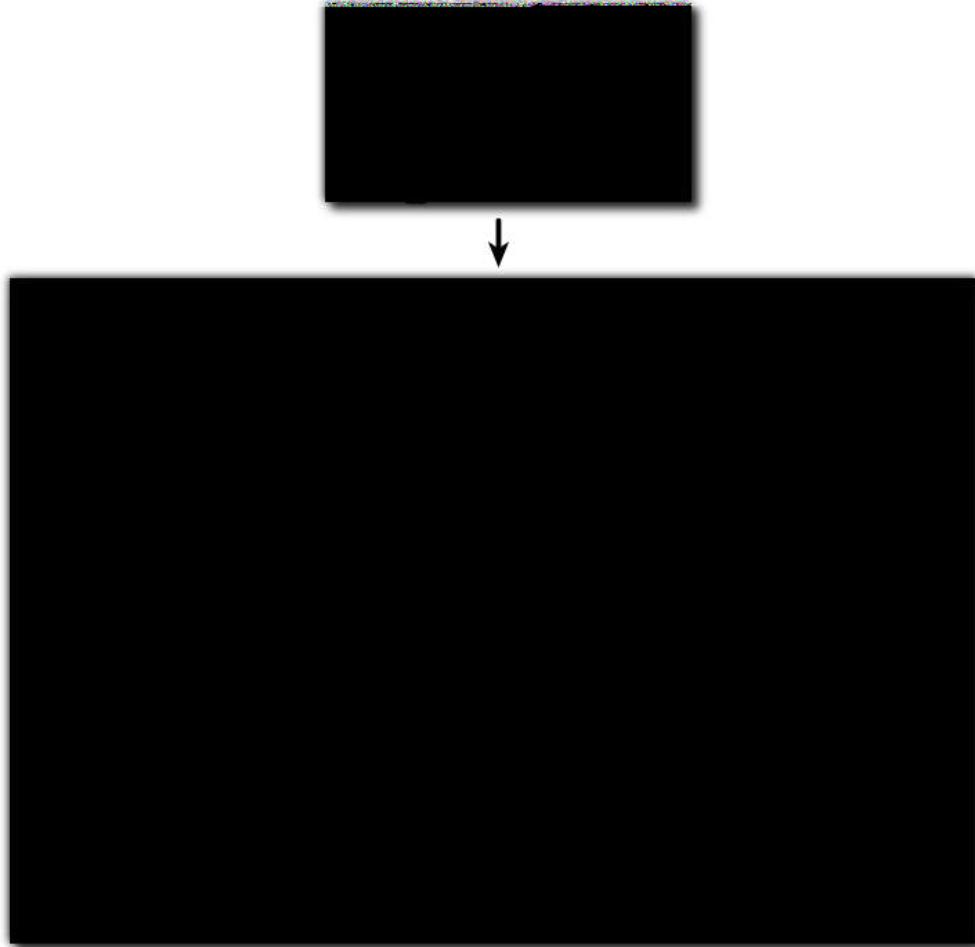


항 목	내 용
수 집 대 상	노드그룹과 전체노드 중 하나를 선택합니다.
대 상 설 정	노드그룹으로 선택할 경우 나타나는 부분으로 리포트에 작성될 노드를 노드그룹에 만들어져 있는 그룹을 통해 선별합니다.
항 목	전체 노드수, 동작 노드수, 에이전트설치 노드수, 동작에이전트설치 노드수 중 하나를 선택하면 전체노드와 노드그룹을 통해 선별된 노드들 중에 선택한 아이템에 맞는 노드의 갯수가 리포트에 작성됩니다.
출 력 명	차트의 출력되는 막대, 선, 면으로 표시되는 차트의 이름을 선택하는 부분입니다.
설 명	수집대상의 설명을 입력 합니다.
차 트 타 입	선그래프, 막대그래프, 면그래프 중 사용 할 차트를 선택합니다. 리포트에 선택한 차트로 데이터를 표시합니다.
차 트 색 상	차트의 색상을 선택합니다.
감사기록	주기마다 검사하여 변동 값이 설정값 보다 크거나 임계 값이 설정값을 초과 시 감사 > 로그에 기록됩니다.

노드 리포트 확인

1. 차트

수집한 자료를 차트로 나타내며, 평균, 최대값 옵션을 이용하여 평균과 최대값을 확인할 수 있습니다.



항 목	내 용
기 간 선 택	날짜가 적혀있는 상자를 클릭하여 날짜를 설정 후 변경 버튼을 클릭하여 설정한 기간의 정보를 차트로 나타냅니다.
일 간	당일 0시 부터 현재시간 까지의 정보를 차트로 나타냅니다.
주 간	현재시각에서 7일 전의 정보를 차트로 나타냅니다.
월 간	현재시각에서 30일 전의 정보를 차트로 나타냅니다.

2. 테이블

차트와는 다른 형태인 테이블로 확인 할 수 있으며, 내보내기 기능을 이용하여 csv파일로 다운로드 받을 수 있습니다.
평균, 최대값 옵션을 이용하여 평균과 최대값을 확인할 수 있습니다.



기간 설정

항 목	내 용
기 간 설 정	날짜가 적혀있는 상자를 클릭하여 날짜를 설정 후 변경 버튼을 클릭하여 설정한 기간의 정보를 테이블로 나타냅니다.
일 간	당일 0시 부터 현재시간 까지의 정보를 테이블로 나타냅니다.
주 간	현재시각에서 7일 전의 정보를 테이블로 나타냅니다.
월 간	현재시각에서 30일 전의 정보를 테이블로 나타냅니다.

노드 리포트 삭제

관리자는 필요 없는 노드 리포트를 삭제 할 수 있습니다.
노드 리포트 삭제 과정은 [항목 삭제](#)를 참조 바랍니다.

로그 리포트

로그 리포트

관리자는 로그 리포트 기능을 이용하여, 관리자가 원하는 로그를 리포트형식의 엑셀파일로 출력할 수 있습니다.
로그 리포트는 로그필터를 이용하여 리포트를 정의하고, 정의된 리포트에서의 파일생성 작업으로 리포트가 만들어집니다.
로그필터는 감사 > 로그에서 생성할 수 있습니다.

로그 리포트 추가

1. 로그 리포트 추가

감사 > 리포트 > 리포트 정의 > 작업선택 > 로그리포트 추가 를 선택하여 리포트를 설정하는 페이지로 이동합니다.



2. 기본정보 입력

리포트를 식별할 제목과 설명을 기입하고 리포트 적용유무, 자동생성 사용유무를 선택 합니다.



항 목	내 용
리 포 트 타 입	리포트 타입을 나타냅니다.
리 포 트 제 목	사용하려는 리포트 제목을 입력합니다.
리 포 트 설 명	추가 하려는 리포트의 설명을 입력합니다.
적 용 모 드	추가 하려는 리포트의 사용유무를 설정합니다.
자 동 생 성	원하는 날짜와 시각을 지정 시 설정한 시각에 리포트 파일을 생성합니다.

3. 리포트 자동생성

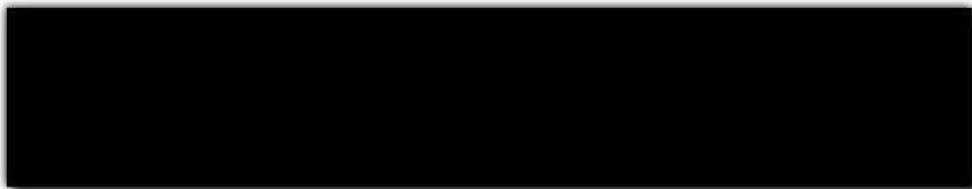
노드 리포트의 자동생성부분이 사용함으로 선택 할 경우입니다.



항 목	내 용
지정시각 구분	매일+시각, 지정일+시각, 날짜+시각, 요일+시각, 주/요일+시각 이 있으며, 자신이 원하는 날짜에 맞게 선택합니다.
지 정 일	지정시각 구분에서 지정일+시각을 선택 하였으면, 활성화 되고, 지정일+시각을 설정하면 설정한 지정일에 리포트가 생성됩니다.
날 짜	지정시각 구분에서 날짜+시각을 선택 하였으면, 활성화 되고, 날짜+시각을 설정하면 설정한 날짜에 리포트가 생성됩니다.
요 일	지정시각 구분에서 요일+시각을 선택 하였으면, 활성화 되고, 요일+시각을 설정하면 설정한 요일에 리포트가 생성됩니다.
주	지정시각 구분에서 주/요일+시각을 선택 하였으면, 활성화 되고, 주+시각을 설정하면 설정한 주에 리포트가 생성됩니다.
주 중 요 일	지정시각 구분에서 주/요일+시각을 선택 하였으면, 활성화 되고, 주중요일+시각을 설정하여 설정한 주중요일에 리포트가 생성됩니다.
시 각	파일이 생성될 시각을 설정합니다.

4. 로그필터 설정

리포트에 정의할 감사로그필터를 설정합니다.



항 목	내 용
감사로그필터	리포트에 정의할 로그필터를 설정합니다. 로그필터는 감사 > 로그에서 생성할 수 있습니다.
출력파일	리포트의 데이터를 다운로드 받을 확장자를 설정합니다.

5. 노드 리포트 파일 생성

감사 > 리포트 > 트리 뷰 > 생성한 리포트 > 작업선택 > 리포트파일생성 을 클릭하여 설정한 리포트를 다운로드 받을 수 있는 파일로 생성합니다.



6. 로그리포트

로그리포트를 다음과 같이 확인할 수 있습니다.



로그 리포트 삭제

관리자는 필요 없는 로그 리포트를 삭제 할 수 있습니다
로그 리포트 삭제 과정은 [항목 삭제 페이지](#)를 참조 바랍니다.

대시보드 리포트

대시보드 리포트

관리자는 대시보드 리포트를 이용하여 대시보드 탭에 있는 위젯 데이터를 지정된 시각에 PDF, Word, PowerPoint 타입의 파일로 이메일을 전달받을 수 있습니다.

주기적으로 위젯 데이터를 이메일로 확인할 수 있어 네트워크의 급격한 변화 및 노드의 변동사항을 빠르게 확인할 수 있고 이전 위젯 데이터를 비교하여 현 상황에 대해 효과적으로 파악할 수 있습니다.

대시보드 리포트 추가

1. 대시보드 리포트 추가

감사 > 리포트 > 리포트 정의 > 작업선택 > 대시보드 리포트 추가 를 선택하여 리포트를 설정하는 페이지로 이동합니다.



2. 기본정보 입력

리포트를 식별할 제목과 설명을 기입하고 리포트 적용유무, 자동생성 사용유무를 선택 합니다.



항 목	내 용
리 포 트 타 입	리포트 타입을 나타냅니다.
리 포 트 제 목	사용하려는 리포트 제목을 입력합니다.
리 포 트 설 명	추가 하려는 리포트의 설명을 입력합니다.
적 용 모 드	추가 하려는 리포트의 사용유무를 설정합니다.
자 동 생 성	원하는 날짜와 시각을 지정 시 설정한 시각에 리포트 파일을 생성합니다.

3. 리포트 자동생성

노드 리포트의 자동생성부분이 사용함으로 선택 할 경우입니다.



항 목	내 용
지정시각 구분	매일+시각, 지정일+시각, 날짜+시각, 요일+시각, 주/요일+시각 이 있으며, 자신이 원하는 날짜에 맞게 선택합니다.
지 정 일	지정시각 구분에서 지정일+시각을 선택 하였으면, 활성화 되고, 지정일+시각을 설정하면 설정한 지정일에 리포트가 생성됩니다.
날 짜	지정시각 구분에서 날짜+시각을 선택 하였으면, 활성화 되고, 날짜+시각을 설정하면 설정한 날짜에 리포트가 생성됩니다.
요 일	지정시각 구분에서 요일+시각을 선택 하였으면, 활성화 되고, 요일+시각을 설정하면 설정한 요일에 리포트가 생성됩니다.
주	지정시각 구분에서 주/요일+시각을 선택 하였으면, 활성화 되고, 주+시각을 설정하면 설정한 주에 리포트가 생성됩니다.
주 중 요 일	지정시각 구분에서 주/요일+시각을 선택 하였으면, 활성화 되고, 주중요일+시각을 설정하여 설정한 주중요일에 리포트가 생성됩니다.
시 각	파일이 생성될 시각을 설정합니다.

4. 세부 설정

리포트의 세부설정 및 알람을 설정합니다.



항 목	내 용
대시보드탭	대시보드 리포트에 정의할 대시보드 탭을 설정합니다.
출력파일	대시보드 리포트 생성 시 파일 타입을 설정합니다. 파일 타입은 PDF, Word, Powerpoint이 있습니다.
메일수신	대시보드 리포트 생성 시 관리자 이메일로 생성된 대시보드 리포트 파일이 첨부되어 메일이 전송됩니다. 관리자 이메일은 관리자계정 > 관리자설정 > 이메일 을 참조합니다.

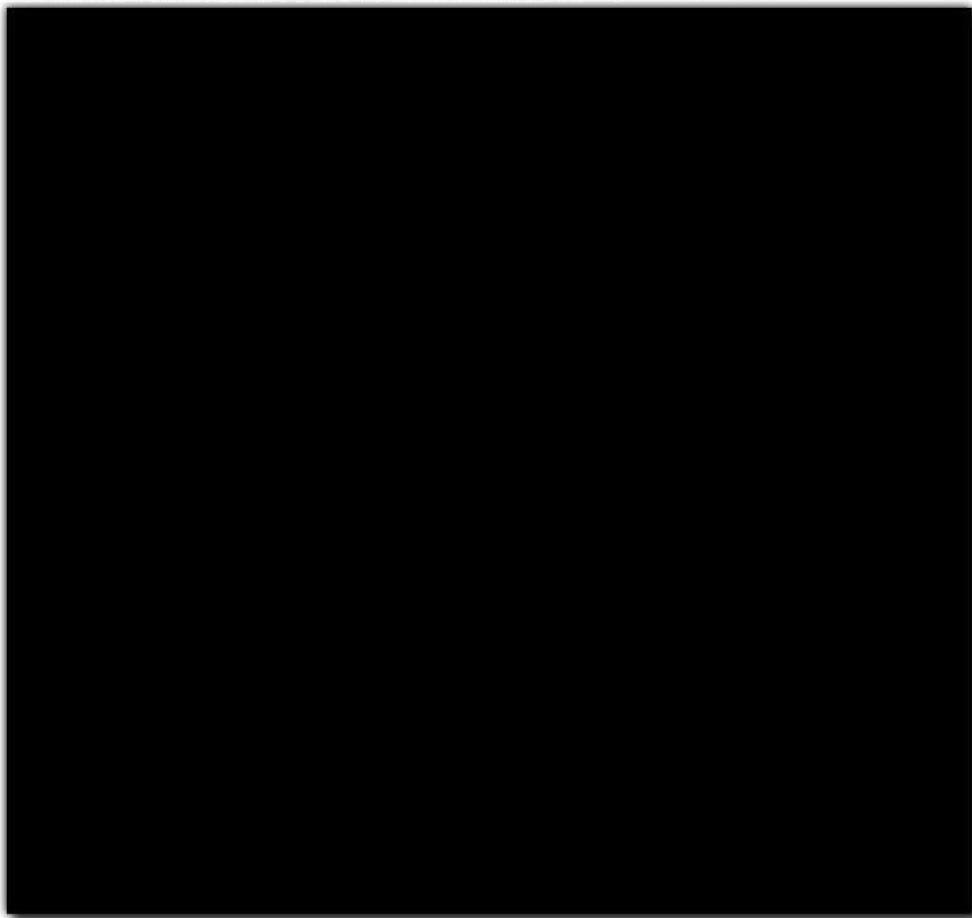
5. 대시보드 리포트 파일 생성

감사 > 리포트 > 트리 뷰 > 생성한 리포트 > 작업선택 > 리포트파일생성을 클릭하여 설정한 리포트를 다운로드 받을 수 있는 파일로 생성합니다.



6. 대시보드 리포트

대시보드 리포트를 다음과 같이 확인할 수 있습니다.



자동 리포트

자동 리포트

리포트 정의 하위 트리에 존재하는 노드그룹, 로그필터, 무선랜그룹 세 가지 리포트를 관리자 및 관리역할에 따라 주기적으로 자정 기준으로 작성된 리포트를 이메일로 받아 볼 수 있습니다.

자동 리포트는 리포트를 이메일로 받을 수 있어 NAC WEB에 접속 여부 상관없이 이메일을 통해 네트워크 상황을 확인할 수 있습니다.

자동 리포트 생성

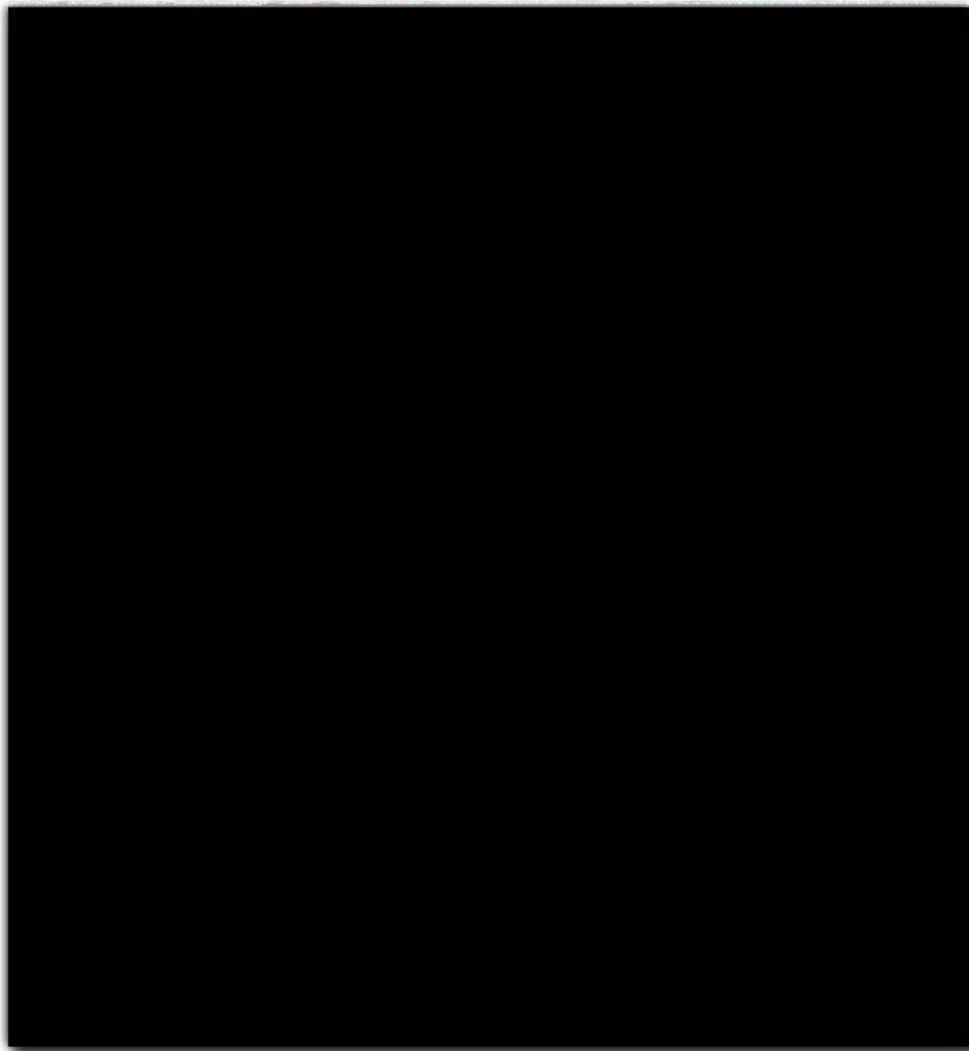
1. 자동 리포트 생성

감사 > 리포트 > 자동 리포트 > 작업선택 > 생성 를 선택하여 자동 리포트를 설정하는 페이지로 이동합니다.



2. 자동 리포트 설정

이름, 설명, 이메일로 리포트를 받을 관리자 및 관리역할, 이메일로 받을 리포트, 이메일 받을 시각을 설정합니다.



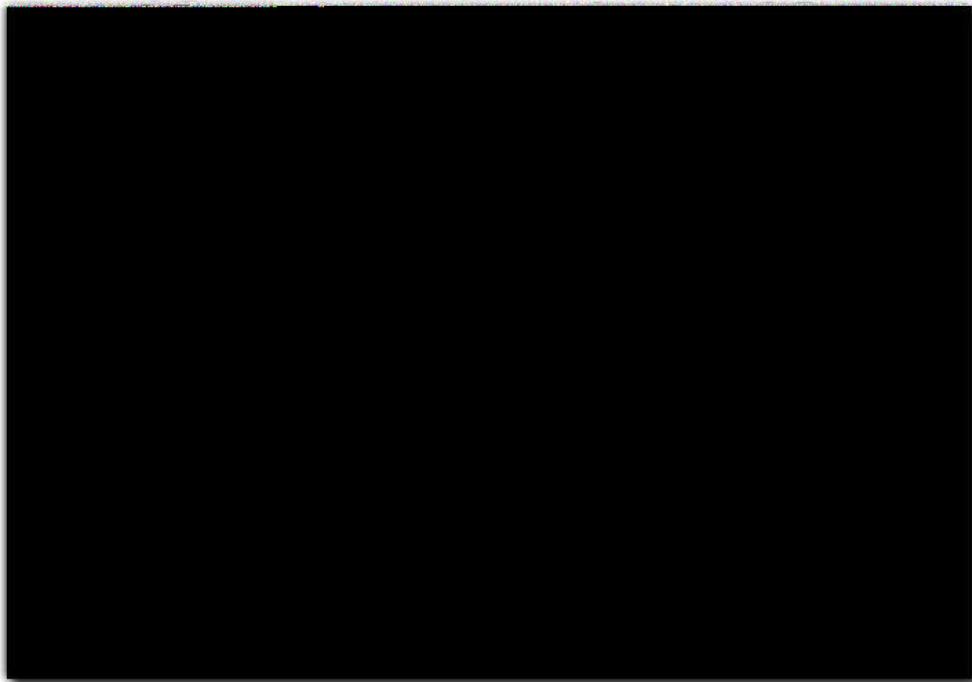
항목	설명
이름	추가하려는 자동 리포트의 제목을 입력합니다.
설명	추가하려는 자동 리포트의 설명을 입력합니다.
수신	관리자, 관리역할을 선택할 수 있으며 관리자의 경우 선택된 관리자만 리포트를 받을 수 있으며 관리역할의 경우 선택된 관리역할을 할당받은 관리자 모두 리포트를 받을 수 있습니다.
리포트	이메일로 받을 리포트를 선택합니다.
자동생성	이메일 받을 시각을 설정합니다. 사용안함일 경우 리포트를 이메일로 전송하지 않습니다.
지정시각 구분	매일+시각, 지정일+시각, 날짜+시각, 요일+시각, 주/요일+시각 이 있으며, 자신이 원하는 날짜에 맞게 선택합니다.
지정일	지정시각 구분에서 지정일+시각을 선택 하였으면, 활성화 되고, 지정일+시각을 설정하면 설정한 지정일에 리포트가 생성됩니다.
날짜	지정시각 구분에서 날짜+시각을 선택 하였으면, 활성화 되고, 날짜+시각을 설정하면 설정한 날짜에 리포트가 생성됩니다.
요일	지정시각 구분에서 요일+시각을 선택 하였으면, 활성화 되고, 요일+시각을 설정하면 설정한 요일에 리포트가 생성됩니다.
주	지정시각 구분에서 주/요일+시각을 선택 하였으면, 활성화 되고, 주+시각을 설정하면 설정한 주에 리포트가 생성됩니다.
주중요일	지정시각 구분에서 주/요일+시각을 선택 하였으면, 활성화 되고, 주중요일+시각을 설정하여 설정한 주중요일에 리포트가 생성됩니다.

시각

파일이 생성될 시각을 설정합니다.

3. 자동 리포트 확인

이메일로 받은 자동 리포트는 자정을 기준으로 데이터를 확인할 수 있습니다.



자동 리포트 삭제

관리자는 필요 없는 자동 리포트를 삭제 할 수 있습니다.
자동 리포트 삭제 과정은 [항목 삭제](#)를 참조 바랍니다.

CLI

CLI

CLI 모드에서 사용할 수 있는 시스템 명령과 환경설정방법을 작성합니다.



CLI(Command Line Interface)

컴퓨터 운영체계나 응용프로그램과의 사용자 인터페이스입니다.

사용자는 프롬프트가 나타나면 정해진 줄 위에 명령어를 입력하고, 시스템으로부터 이에 대한 응답을 받은 다음, 또다시 다른 명령어를 입력하는 식으로 진행된다.

윈도우 운영체계에서 MS-DOS로 빠져나가면, 도스 프롬프트가 나타나는데, 여기서 CLI 응용의 예를 볼 수 있다.

- 시스템 명령
- 장비 환경설정

시스템 명령

• CLI 명령

- 인가된 관리자가 Genian NAC를 사용하기 위해 필요한 IP설정, 게이트웨이설정 등의 기초 설정을 수행하여 WEBUI에 접속하기 위한 환경을 설정할 수 있습니다.
- 관리자가 시스템에 설치된 Serial인터페이스로 접속하거나 SSH(Secure Shell)의 원격접속서비스를 이용하여 터미널에뮬레이터를 이용해서 접속할 수 있습니다.
- 접속된 사용자는 인가된 관리자 여부를 확인 받기 위해 설정된 암호를 입력하여 접속할 수 있습니다.
- 크게 명령모드와 설정모드로 구분되며 명령모드는 시스템의 상태를 확인하거나 백업 또는 테스트 등의 명령을 수행할 수 있는 모드를 말하며 설정모드는 CLI에서 제공하는 여러 설정 값을 생성하거나 수정, 삭제할 수 있는 상태를 말합니다.
- CLI에 인증을 통하여 접속하게 되면 CLI는 "genian>" 이라는 프롬프트를 출력한 뒤 관리자로부터의 명령입력을 대기합니다. 이 명령입력상태가 일반모드이고 이 상태에서 명령모드에 사용 가능한 명령들을 입력함으로 원하는 기능을 수행시킬 수 있습니다.
- 관리모드로 변경하기 위해서는 일반모드에서 "enable" 명령을 입력 후 Password를 입력합니다. 관리모드로 전환되면 프롬프트는 "genian#" 로 변경됩니다.
- 설정모드로 변경하기 위해서는 명령모드에서 "configure terminal" 명령을 입력합니다. 설정모드로 전환되면 프롬프트는 "genian(config)" 로 변경됩니다.
- 설정모드를 종료하기 위해서는 프롬프트에서 "exit" 명령을 수행하면 됩니다.

• 시스템 명령 목록

genian>	일반모드	genian#	관리모드	genian(config)#	설정모드
exit	cli 서비스 종료	exit	CLI 서비스 종료	exit	CLI 서비스 종료
help	명령 도움말	help	명령 도움말	help	명령 도움말
history	명령 이력보기	history	명령 이력보기	history	명령 이력보기
quit	서비스 종료	quit	서비스 종료	quit	서비스 종료
clear	화면소거	configure	설정 모드 전환	no	설정 값 지우기(한 항목만)
enable	관리 모드 전환	clear	화면소거, dhcp, arp 제거	clear	하먼소거, dhcp, arp 제거
ping	네트워크 테스트	clock	시스템 시각 수동설정	add host	호스트 추가
show	시스템 정보 조회	disable	이전 모드 전환	admin-acl	관리자 접속 가능 IP 설정
traceroute	네트워크 테스트	do	백업 데이터관리기능	bonding	본딩 설정
		geniup	시스템 업그레이드	consoleadmin	CLI 콘솔 아이디 및 패스워드 설정
		halt	시스템 종료	device-id	deviceID 설정
		kill	프로세스 종료기능	data-server	데이터베이스 설정
		ping	네트워크 테스트	delete	호스트삭제
		reboot	시스템 재부팅	dist-server	PMS 패치파일 배포 포트 설정
		restart	서비스 재기동	enable	enable 계정 수정
		show	시스템 정보 조회	force-passive	항상 Passive모드로 동작
		shutdown	서비스 종료	healthcheck	센서 vlan 동작 모드 설정
		traceroute	네트워크 테스트	hostname	CLI의 name 설정
				interface	네트워크 인터페이스 설정
				ip	ip환경 설정
				log-server	로그 서버 설정
				management-server	http/https 포트 설정
				node-server	외부 정책서버 설정
				ntp	외부시각 동기화 설정
				sensor	정책이벤트 포트 설정
				show	설정 값 조회

				ssh	ssh 포트 설정
				superadmin	슈퍼어드민 설정
				system-locale	시스템 로케일 설정
				syslog	syslog 설정
				procmon	HA failover 설정

시스템명령 상세설명

CLI 서비스 접속

CLI 모드로 들어가기 위하여 하이퍼터미널을 이용하거나 SSH 접속을 제공하는 통신 프로그램을 이용하여 Policy Center 나 Network Sensor로 접속합니다.

하이퍼터미널로 장비 접속하는 방법에 대해서는 [제품 콘솔 접속](#)을 참고 바랍니다.

SSH접속을 하기 위해서는 Policy Center나 Network Sensor에 설정되어 있는 IP주소로 포트번호 3910번으로 접속한 후 설정되어있는 아이디와 패스워드를 입력하여 인증을 통과합니다.

CLI 서비스 종료

CLI 모드를 종료하기 위한 명령을 제공합니다.

```
genian# exit or quit
```

명령모드에서는 'exit'와 'quit' 모두 같은 결과를 가져오지만 설정모드에서 두 가지 명령이 다르게 나타납니다.
설정모드 빠져 나와 명령모드로 가기 위해서는

```
genian(config)# exit
```

터미널을 완전히 종료하기 위해서는

```
genian(config)# quit
```

명령을 수행할 수 있습니다.

명령 도움말 기능

사용자의 편의를 위해서 CLI에서 제공되는 모든 명령을 정리하여 보여주는 기능을 제공합니다. 명령문과 함께 쓰이는 파라미터와 그에 대한 설명이 보입니다.

```
genian# help
genian(config)# help
```

프롬프트에 "?" 를 입력하면 파라미터를 생략하고 명령문과 명령문에 대한 설명만 제공됩니다.

명령 이력보기 기능

사용자가 콘솔에 접속한 시점부터 CLI명령을 수행한 이력을 보여주는 기능을 제공합니다.
conf Terminal(genian(config)#) 모드에서 사용 가능합니다.

```
genian# history
Command history:
 0. history
 1. conf t
 2. history
 3. gfjg
 4. exit
 5. clear arp
 6. show configuration
 7. history
```

설정모드 들어가기

명령모드에서 설정모드로 변경합니다.

```
genian# configure [ COMMAND ]
```

COMMAND	PARAMETERS	용도
Terminal	-	명령시마다 적용을 수행하는 설정모드
batch	-	즉시적용을 하지 않고 설정만 수정하는 설정모드

화면 소거기능

보이는 콘솔창 화면을 깨끗이 소거합니다.

```
genian# clear [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
dhcp lease	[all], [ip address]	'show dhcp lease' 명령어로 확인할 수 있는 dhcp의 현황을 삭제합니다.
arp	[interface]	arp 테이블을 초기화합니다, arp 테이블은 'show arp' 명령어로 확인할 수 있습니다.
screen	-	콘솔창 화면을 깨끗이 합니다.

이전 모드 전환

관리 모드에서 일반 모드로 전환합니다.

```
genian# disable  
genian>
```

관리 모드 접속

일반 모드에서 Password 입력 시 관리 모드로 접속할 수 있습니다, 초기 Username, Password는 CLI Username, Password랑 동일하며 이후 설정 모드의 enable 명령어로 Username, password를 변경할 수 있습니다.
Username이 admin일 경우 Username이 출력되지 않습니다.

```
genian> enable  
Password:  
genian#
```

백업 데이터 관리기능

데이터베이스 및 시스템 설정의 백업을 수행하고 백업된 데이터를 복구하는 기능을 제공합니다.

```
genian# do [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
backup	-	현재 데이터베이스 및 설정을 백업
cdbackup	-	가장 최신 백업데이터를 CDR로 백업
cdrestore	-	CD에 저장된 백업 데이터로 복구
initdisk	[DEVICE PATH]	외장 디스크 초기화를 수행
restore	[BACKUPNAME]	백업한 데이터로 복구, 백업 파일의 이름 확인방법은 'show backup'명령어로 확인할 수 있습니다.

예제1> 데이터베이스 백업을 수행합니다.

```
genian# do backup
Are you sure to backup database (y/N): y
Start backup...Finished.
genian#
```

예제2> 백업한 데이터를 복구합니다.

```
genian# do restore ALDER-14483-20090416-104429 ALL
Are you sure to restore backup database (y/N): y
Stopping services...
Stopping Service...done
Restoring database...
Starting services...
Starting Service...done
genian#
```

시스템 소프트웨어 업그레이드 기능

remote Sensor를 업그레이드 하는 명령어로 remote sensor가 Policy Center정비로부터 센서이미지를 받아와 remote sensor의 업그레이드를 수행합니다.

센서이미지는 WebUI에서 업로드하여야 하며, 현재 제품 버전보다 높은 이미지가 업로드 되어야 합니다.

remote sensor의 CLI에서 사용하는 명령어입니다. Policy Center의 CLI에서는 사용할 수 없는 명령어이며 'node-server ip' 명령어로 Policy Center의 IP가 설정되어 있어야 합니다.

```
genian# geniup
```

- 업그레이드 파일 업로드 설명 : 시스템이미지를 업로드 하는 방법에 대한 설명은 'ch 8-2' 에 상세히 제공되오니 참고하시기 바랍니다.

예제1> Network Sensor의 CLI 명령으로 시스템을 업그레이드 합니다.

```
genian# geniup

System software upgrade from [http://10.200.6.1/upgrade/]

Current Version : GN300-SENSOR-release-14483-090410

Target Version : GN300-SENSOR-release-14500-090415

Do you want to upgrade this target version ? (y/N): y

Do you want to restart system after upgrade ? (Y/n): y

Downloading latest image .... done

Splitting image file ..... done

Updating kernel ..... done

Updating product ..... done

Syncing ..... done

System software upgrade finished. Now restart system.....

Shutdown System .....
```

시스템 종료 기능

실행되고 있는 Genian NAC를 종료 시키는 명령입니다. 재구동을 위해서는 장비의 전원 버튼을 직접 눌러주어야 합니다.

```
genian# halt
```

예제1> 시스템을 종료시킵니다.

```
genian# halt
Are you sure to halt system (y/N): y
Shutdown System .....
```

프로세스 종료기능

Genian NAC Policy에서 구동되고 있는 프로세스를 종료시키는 명령입니다.

```
genian# kill [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
pname	[process name]	process name으로 프로세스를 종료시킴, 실행중인 프로세스는 'show processes' 명령어로 확인할 수 있습니다.
pid	[process id]	process ID로 프로세스를 종료시킴, 실행중인 프로세스는 'show processes' 명령어로 확인할 수 있습니다.

예제1> centerd 프로세스를 종료시킵니다.

```
genian# kill pname centerd
8475 00:00:00 centerd
Are you sure to kill process (y/N): y
genian#
```

네트워크 테스트 기능

시스템에서 외부 시스템에 대해서 네트워크 테스트를 수행하기 위한 ping 명령과 traceroute 명령을 제공합니다.

```
genian# ping [ IP Address ]
genian# traceroute [ IP Address ]
```

시스템 시각 수동설정 기능

시스템의 시각을 수동으로 설정하는 명령어 입니다.

```
genian# clock [ COMMAND ] 2013-07-15/13:27:53
Mon Jul 15 13:27:53 KST 2013
```

COMMAND	PARAMETERS	용도
set	YYYY-MM-DD/hh:mm:ss	시스템 시각을 설정합니다.

시스템 재부팅 기능

시스템을 재부팅 한 후 Genian NAC 서비스를 시작하기 위한 기능을 제공합니다.

```
genian# reboot
```

서비스 재기동 기능

시스템의 재부팅 없이 Genian NAC전체 서비스를 재기동하기 위한 기능을 제공합니다.

```
genian# restart
```

시스템 정보 조회기능

시스템의 각종 상태 및 정보 값을 조회하기 위한 출력명령을 제공합니다.

```
genian# show [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
arp	-	ARP테이블을 출력합니다.
backup	-	백업된 데이터베이스 목록을 출력합니다.
configuration	-	시스템에 설정한 목록을 출력합니다.
dhcp lease	[all]	GenanNAC dhcp에서 할당해준 IP를 사용하는 IP, MAC, Expire, Interface 목록을 출력합니다.
	[ip]	GenanNAC dhcp에서 할당해준 IP를 사용하는 사용자의 dhcp ip address를 입력하면, 해당 ip의 IP, MAC, Expire, Interface 목록을 출력합니다.
	[mac]	GenanNAC dhcp에서 할당해준 IP를 사용하는 사용자의 dhcp mac address를 입력하면, 해당 mac의 IP, MAC, Expire, Interface 목록을 출력합니다.
	[interface]	인터페이스의 이름(eth0 등)을 입력하면, 해당 인터페이스에서 GenanNAC dhcp를 사용하는 사용자의 IP, MAC, Expire, Interface 목록을 출력합니다.
filesystem	-	디스크 정보를 출력합니다.
hosts	-	호스트 테이블을 출력합니다.
interface	[interface]	네트워크 인터페이스 정보를 출력합니다.
logging		로그ID가 GENIAN장비로 등록되는 로그 중에서 가장 최신 로그만 출력합니다.
memory	-	메모리 정보를 출력합니다.
nodeinfo	[ip address]	입력한 ip가 받고 있는 제어정책과 차단유무(TOXIC)에 대한 정보를 출력합니다.
processes	-	구동중인 프로세스 정보를 출력합니다.
route		라우팅 테이블을 출력합니다.
superadmin	-	superadmin권한을 가진 아이디 정보를 출력합니다.
time	-	현재 시스템의 시각을 출력합니다.
uptime	-	시스템이 구동중인 시간정보를 출력합니다.
version	-	시스템소프트웨어 버전정보를 출력합니다.
cpu	-	cpu 정보를 출력합니다.

서비스 종료 기능

시스템의 전원을 내리기 위한 서비스 종료 수행 명령을 제공합니다.

```
genian# shutdown [ COMMAND ]
```

COMMAND	PARAMETERS	용도
service	-	해당 장비에서 동작중인 모든 서비스를 종료시킵니다. 재구동을 위해서는 장비의 전원 버튼을 직접 눌러주어야 합니다.

예제1> 장비에서 동작중인 모든 서비스를 종료시킵니다.

```
genian# shutdown service
Stopping Service...done
Recovery poisoning nodes...
Stopping Service...done
done
genian#
```

설정 값 삭제 기능

설정명령어 앞에 'no'를 붙여 명령을 내리면 명시된 설정명령어에 해당하는 설정 항목을 제거합니다.

```
genian(config)# no [ CLI Command ]
```

예제1> 168.126.63.1로 설정된 네임서버 설정 값을 제거합니다.

```
genian(config)# no ip name-server 168.126.63.1
genian(config)#
```

본딩 설정 기능

여러 개의 NIC 을 논리적으로 한 개의 NIC 으로 묶습니다.

```
genian(config)# bonding [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
size	[Number]	설정 개수만큼 본딩을 사용할 수 있습니다.
parameters	[DBSERVERADDR]	본딩에 관련된 설정을 할 수 있습니다. http://blog.naver.com/songariq?Redirect=Log&logNo=80033576867 참고 하시기 바랍니다.

설정 값 모두 지우기 기능

현재 설정되어있는 모든 값을 초기화 시키는 기능을 제공합니다. IP 관련 설정이 초기화 되어 CLI에 접속할 수 없게 됩니다. 이때는 장비와 직접 콘솔로 연결하여야 합니다.

```
genian(config)# clear
```

예제1> 설정되어있는 모든 값을 제거합니다.

```
genian(config)# clear
Are you sure to delete all configuration (y/N): y
genian(config)#
```

ssh 포트 변경기능

ssh 통신에 사용될 포트를 변경하는 명령어입니다.
Default port는 3910 입니다.

```
genian(config)# ssh [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
port	[Port]	ssh 포트 설정

예제1> ssh 포트를 22로 설정합니다.

```
genian(config)# ssh port 22
genian(config)#
```

슈퍼어드민 추가하기

WebUI에서 슈퍼어드민권한을 갖는 계정을 추가하는 기능을 제공합니다. 슈퍼어드민 권한을 가진 사용자가 있을 경우 해당 명령어로 슈퍼어드민을 생성할 수 없습니다.
슈퍼어드민의 비밀번호는 보안을 위해 비밀번호는 대문자/소문자/숫자/특수문자 중 3가지 규칙 조합 및 9자리 이상의 비밀번호를 입력합니다.

```
genian(config)# superadmin [ admin ID ] [ password ] [e-mail]
```

예제1> 아이디 admin, 비밀번호 genian123, 이메일 test@gennetworks.com 의 슈퍼어드민을 추가합니다.

```
genian(config)# superadmin admin Web123! test@gennetworks.com
genian(config)#
```

호스트 추가하기

hosts파일에 호스트 항목을 추가하는 명령입니다.

```
genian(config)# add hosts [ IP address ] [ hostName ]
```

예제1> 222.122.15.10 번 IP주소를 gennetworks.com 이라는 호스트명으로 지정합니다.

```
genian(config)# add host 222.122.15.10 gennetworks.com
genian(config)#
```

호스트 삭제하기

hosts파일에서 호스트 항목을 삭제하는 명령입니다.

```
genian(config)# delete [ IP address ] [ hostName ]
```

예제1> IP주소 222.122.15.10로 등록되어있는 gennetworks.com 이라는 호스트명을 삭제합니다.

```
genian(config)# delete hosts 222.122.15.10 geninetworks.com
genian(config)#

```

DeviceID 설정하기

DeviceID를 설정하는 명령입니다.
DeviceID는 Policy Center에서 Network Sensor를 식별하는 값입니다.
변경된 DeviceID는 장비의 재부팅 후에 설정 값이 적용됩니다.

```
genian(config)# device-id [ DeviceID ]
```

예제1> Network Sensor의 Device ID를 86be50f0-b21e-1001-8022-0090fb090f45로 설정합니다.

```
genian(config)# device-id 86be50f0-b21e-1001-8022-0090fb090f45
genian(config)#

```

데이터베이스 설정기능

데이터베이스 서비스 구동 여부 및 데이터베이스의 username, password를 설정합니다.

```
genian(config)# data-server [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
enable		시스템 자체에 데이터베이스를 구동
ip	[DBSERVERADDR]	외부의 데이터베이스를 사용
port	[port]	데이터베이스의 포트를 설정
password	[DB Password]	데이터베이스의 패스워드를 설정합니다. 패스워드는 8~30자리, 영문자포함, 숫자 포함 하여야 설정
username	[DB username]	데이터베이스의 사용자명을 설정
dbname	[DB name]	데이터베이스의 이름을 설정
replica	enable serverid [Server ID] username [Username] password [Password] dbname [DBname] masterhost [Master IP]	replication 설정

예제1> 데이터베이스의 패스워드를 genian123으로 설정합니다.

```
genian(config)# data-server password pass123!
genian(config)#

```

PMS패치파일 배포 포트 변경기능

PMS패치파일을 배포 시 사용될 포트를 변경하는 명령어입니다.
Default Port는 8000입니다.

```
genian(config)# dist-server [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
Port	[Port]	PMS패치파일 배포 포트 설정

예제1> PMS패치파일 배포 포트를 8005으로 설정합니다.

```
genian(config)# dist-server port 8005
Stopping Service...done
Starting Service...done
genian(config)#
```

항상 Passive 모드로 동작하기 기능

Genian NAC 동작모드를 passive모드로만 동작하도록 설정하는 기능을 제공합니다. UI에서 센서 설정을 Active으로 변경하여도 passive모드로만 동작 합니다.

```
genian(config)# force-passive enable
```

센서의 vlan의 동작 모드 설정 기능

센서에 vlan의 동작 모드를 설정하는 기능입니다.

```
genian(config)# healthcheck mode [ COMMAND ]
```

COMMAND	PARAMETERS	용도
strict		여러 vlan 중 하나의 vlan이 동작하지 않으면 모든 vlan이 fail safe 모드가 됩니다.
alternate		여러 vlan 중 하나의 vlan이 동작하지 않아도 다른 vlan은 정상적으로 동작 합니다. 설정하지 않을 시 해당 모드가 default로 동작합니다.

CLI name 설정 기능

CLI모드에 접속할 시 나타나는 genian#을 변경할 있는 기능입니다.

```
genian(config)# hostname [CLI neme]
```

예제1 >

```
genian(config)# hostname admin
Stopping Service...done
Starting Service...done
admin(config)#
```

네트워크 인터페이스 설정기능

설정모드에서 시스템에 장착된 네트워크 인터페이스의 IP관련 속성과 서비스 동작을 설정하는 기능입니다.

```
genian(config)# interface [ Interface ] [ COMMAND ] [ PARAMETERS ]
```

COMMAND	PARAMETERS	용도
address	[ADDR] [MASK]	IP와 Subnet mask설정
duplex	[auto full half]	전송방식 설정
gateway	[GWADDR]	게이트웨이 IP설정
management-server	enable	보안관리 인터페이스(WEBUI) 구동설정
node-server	enable	정책서버(CTD) 구동설정
radius-server	enable	radius서버 구동설정
speed	[10 100 1000 auto]	속도 설정
vlan	[VLANID]	VLAN 설정
ha	group [GROUPID] linkupdelay [delayTime] no-virtual-mac nopreempt priority [PRIORITY] timeout virtual-ip	이중화 구성

예제1> 센서의 Interface 0번에 아이피를 10.200.6.1로 설정합니다.

```
genian(config)# interface eth0 address 10.200.6.1 255.255.255.0
```

```
Stopping Service...done
```

```
Interface eth0 Bringing Up IP 10.200.6.1 Netmask 255.255.255.0
```

```
Starting Service...done
```

```
genian(config)#
```

IP환경 설정기능

IP환경설정은 시스템 전체적으로 적용되는 TCP/IP관련 환경설정을 위한 명령입니다.

```
genian(config)# ip [ COMMAND ] [ PARAMETERS ]
```

COMMAND	PARAMETERS	용도
default-gateway	[GWADDR]	디폴트 게이트웨이 설정
name-server	[DNSERVERADDR]	도메인 네임서버(DNS) 설정
domain-name	[DOMAIN]	도메인 접미사 설정
route	[NETADDR] [MASK] [GWADDR]	고정 라우팅 테이블 설정

예제1> 디폴트 게이트웨이를 10.200.6.254로 지정합니다.

```
genian(config)# ip default-gateway 10.200.6.254
genian(config)#

```

log 서버 설정기능

elasticsearch(로그서버)구동을 위한 명령어 입니다.

```
genian(config)# log-server [COMMAND] [PARAMETERS]
```

COMMAND	PARAMETERS	용도
ip	[CTD IP]	외부 로그 서버 IP 설정
http-port	[Port]	로그 서버와 Center의 통신 포트 설정 Default port : 9200
tcp-port	[Port]	로그 서버와 clustering의 통신 포트 설정 Default port : 9300
cluster-name	[Name]	로그 서버 이름 설정
cluster-peers	[IP]	로그 서버 clustering 설정
enable		로그서버 구동

http / https 포트 변경기능

http, https 통신(Web)에 사용될 포트를 변경하는 명령어입니다.

Web 접속 시 변경된 포트로 접속해야합니다.

https 포트 변경 시 리모트 센서의 soap 접속 포트를 동일하게 변경해야하며, 노드의 에이전트를 재설치해야 합니다.

http, https의 Default port는 80, 443 입니다.

```
genian(config)# management-server [COMMAND] [PARAMETERS]
```

COMMAND	PARAMETERS	용도
http-port	[Port]	http 포트 설정
https-port	[Port]	https 포트 설정

예제1 > http 포트를 8080으로 https 포트를 445로 설정합니다.

```
genian(config)# management-server http-port 8080
Stopping Service...done
Starting Service...done
genian(config)# management-server https-port 445
Stopping Service...done
Starting Service...done
genian(config)#

```

외부 정책 서버(CTD) 설정기능

Network Sensor는 Policy Center와 연결되어 동작합니다. Network Sensor는 Policy Center와 동일 시스템에 존재하여 동작 할 수도 있지만 네트워크 구성에 따라 서로 다른 시스템에 구동되어 동작 될 수 있습니다. 이럴 경우 Network Sensor는 Policy Center의 접속 주소를 알아야 하고 이를 위해 다음과 같이 외부 Policy Center의 접속주소를 설정하는 명령을 제공합니다.

```
genian(config)# node-server [COMMAND] [ PARAMETERS ]
```

COMMAND	PARAMETERS	용도
bind-address	[IP]	tcp soapserver 설정
event-port	[port]	Center KeepAlive 전송 포트 설정
ip	[CTD IP]	외부 정책 서버의 IP를 이용하여 설정
host	[CTD host name]	외부 정책 서버의 host name을 이용하여 설정
port	[CTD port]	외부 정책 서버의 port 설정

예제1> Network Sensor에서 Policy Center의 IP를 10.200.6.1로 설정합니다.

```
genian(config)# node-server ip 10.200.6.1
Stopping&nnbsp; Service ... done
Starting&nnbsp; Service ... done
genian(config)#
```

외부시각 동기화(NTP) 설정기능

시스템의 시간을 외부의 신뢰할 수 있는 시간 값과 동기화 하기 위한 NTP(Network Time Protocol)서버 설정기능을 제공합니다. NTP서버가 잘못 설정될 경우 모든 기록들에 대한 시간이 잘못 되어 기록될 수도 있으며, 외부 인증 서버에서 인증서를 이용한 기능을 사용할 때 정상적으로 동작하지 않을 수 있습니다.

```
genian(config)# ntp [COMMAND] [PARAMETERS]
```

COMMAND	PARAMETERS	용도
server	[IP] / [DOMAIN NAME]	NTP SERVER 설정

예제1> ntp 서버를 10.200.6.254로 지정합니다.

```
genian(config)# ntp server 10.200.6.254
genian(config)#
```

이벤트를 Sensor로 전송하는 포트 변경기능

Center에서 Sensor로 이벤트 전송 시 사용되는 포트를 변경하는 명령어입니다.
Default Port 명령어는 3871 입니다.

```
genian(config)# sensor [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
---------	------------	----

event-port	[Port]	Center에서 Sensor로 이벤트 전송 포트 설정
------------	----------	-------------------------------

예제1> Center에서 Sensor로 이벤트 전송 포트를 3872로 설정합니다.

```
genian(config)# sensor event-port 3872
Stopping Service...done
Starting Service...done
genian(config)#+
```

설정 값 조회기능

설정 값 및 호스트테이블을 조회하기 위한 출력명령 기능을 제공합니다.

```
genian(config)# show [COMMAND]
```

COMMAND	PARAMETERS	용도
configuration		시스템에 설정한 목록을 출력합니다.
hosts		호스트 테이블을 출력합니다.

CLI 콘솔 아이디 비밀번호 변경기능

CLI 콘솔에 접속하기 위해 필요한 아이디와 비밀번호를 변경할 수 있는 기능을 제공합니다.

```
genian(config)# consoleadmin [CLI ID] [PASSWORD]
```

예제1> CLI 콘솔의 아이디를 test으로 변경하고 패스워드를 consol!@3 으로 변경합니다.

```
genian(config)# consoleadmin test consol!@3
```

```
genian(config)#+
```

시스템 로케일 설정

시스템 로케일은 WEP UI에서 보여지는 Language를 모두 영문으로 변경하고, 로그 또한 영문으로 나타나게 할 수 있는 기능을 제공합니다.

```
genian(config)# system-locale
```

COMMAND	PARAMETERS	용도
ko		감사로그를 한글로 기록합니다. 해당 옵션을 설정하지 않아도 default로 로그는 한글로 나오게 됩니다.
en		감사로그를 영문으로 기록하고 database enable 명령어 입력 전에 system-local en 설정 후 database enable 할 시 default로 한글로 생성되는 정책, 그룹 등이 모두 영문으로 생성됩니다.

SYSLOG 설정기능

디스크 없는 센서로 전송하는 SYSLOG를 Disable할 수 있는 기능을 제공합니다.

```
genian(config)# syslog [ COMMAND ] [ PARAMETER ]
```

COMMAND	PARAMETERS	용도
disable		SYSLOG disable 설정
tcp-port	[Port]	syslog tcp 전송 포트 설정 Default port : 6514
udp-port	[Port]	syslog udp 전송 포트 설정 Default port : 514

관리자 접속 가능 IP 설정

관리WEBUI에서 관리자 계정으로 로그인할 수 있는 IP를 설정할 수 있는 기능을 제공합니다.
admin-aci 명령어로 설정한 IP는 관리 > 사용자 > 해당 관리자 > 관리자 설정 > 관리WEBUI 접속 IP1 / MAC1에 설정됩니다.

```
genian(config)# admin-acl [ admin ID ] [ IP ]
```

예제1 > admin 관리자로 로그인할 수 있는 IP를 172.29.56.15으로 설정합니다.

```
genian(config)# admin-acl admin 172.29.56.15
genian(config)#
```



enable 계정 설정

일반 모드 enable 명령어로 관리 모드에 접속할 때 입력하는 Username, Password를 변경할 수 있습니다.

```
genian(config)# enable test pass123!@
genian(config)#
```

장비 환경설정

시스템 명령어를 이용해서 Genian NAC 콘솔에 접속하여 환경에 필요한 설정을 합니다.

```
genian# configure terminal
genian(config)# interface eth0 address 172.29.52.1 255.255.255.0
genian(config)# interface eth0 gateway 172.29.52.254
genian(config)# interface eth0 management enable
genian(config)# interface eth0 node-server enable
genian(config)# ip default-gateway 172.29.52.254
genian(config)# ip name-server 168.126.63.1
genian(config)# data-server username DBadmin
genian(config)# data-server enable
genian(config)# log-server cluster-name Logadmin
genian(config)# log-server enable
genian(config)# superadmin [ Username ] [ password ] email@geninetworks.com
```

영문 NAC WEP UI 환경을 사용할 시 아래의 설정을 합니다.

```
genian# configure terminal
genian(config)# interface eth0 address 172.29.52.1 255.255.255.0
genian(config)# interface eth0 gateway 172.29.52.254
genian(config)# interface eth0 management enable
genian(config)# interface eth0 node-server enable
genian(config)# ip default-gateway 172.29.52.254
genian(config)# ip name-server 168.126.63.1
genian(config)# system-locale en
genian(config)# data-server username DBadmin
genian(config)# data-server enable
genian(config)# log-server cluster-name Logadmin
genian(config)# log-server enable
genian(config)# superadmin [ Username ] [ password ] email@geninetworks.com
```



- 예시에 사용된 superadmin ID와 Password는 사용하지 마시고, 비밀번호 정책에 맞게 적용하여 사용하시기 바랍니다.
- 설정을 초기화 하고 싶을 경우 아래의 명령어를 이용하여 설정을 초기화합니다. 설정을 초기화할 시 IP관련 설정이 초기화 되어 CLI에 접속할 수 없게 됩니다. 이때는 장비와 직접 콘솔로 연결하여야 합니다.

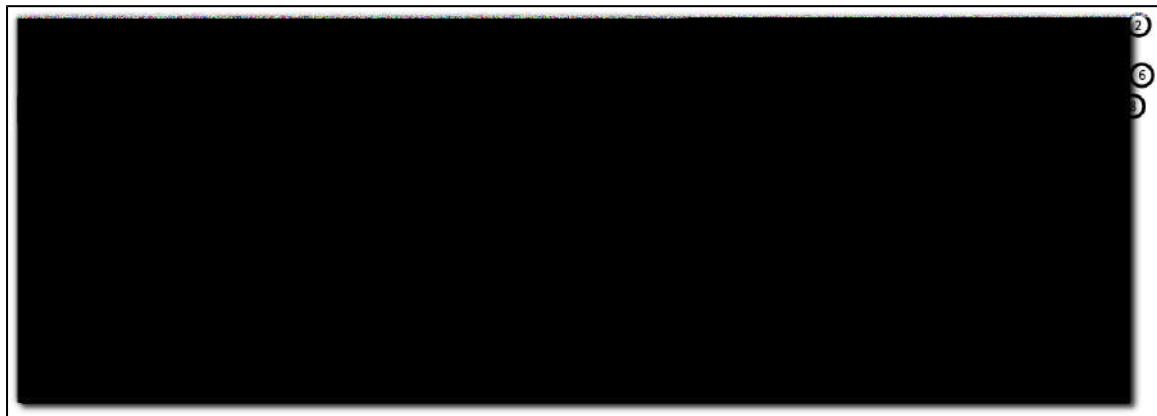
```
genian# conf terminal
genian(config)# clear
```

위와 같이 기본적인 환경설정을 하면 WebUI 콘솔로 접속이 가능합니다.
각 명령어에 대한 내용은 CLI > [시스템 명령](#) 을 참고합니다.

대시보드

대시보드

관리자는 대시보드의 위젯을 통하여 한눈에 사용자 노드의 정보들을 파악할 수 있습니다.



- ① : 메뉴 탭
원하는 메뉴를 고를 수 있는 메뉴 탭입니다.
- ② : 빠른 검색
IP, MAC 등 만을 가지고 별도의 다른 정보 없이 빠른 검색을 할 수 있는 빠른 검색창입니다.
- ③ : 로그인 정보
관리자가 로그인한 ID와 로그아웃 버튼, 관리자를 설정할 수 있는 버튼이 있습니다.
- ④ : 현재시각
현재 시각을 나타냅니다.
- ⑤ : 세션 만료시간
관리자 계정의 세션 만료시간을 나타내며, 로그인 후 만료시간 동안 아무런 작업이 없을 경우 자동로그아웃됩니다.
자동로그아웃 1분전 세션만료경고 팝업창이 출력되며, 해당 팝업창에서 로그인시간을 연장할 수 있습니다.
- ⑥ : 새로 고침
새로 고침 버튼입니다.
- ⑦ : 위젯 내보내기
현재 선택한 탭의 위젯을 PDF, DOCX, PPTX으로 내보내기 할 수 있습니다.
- ⑧ : 대시보드 설정버튼
위젯 & 탭 추가와 탭 삭제 & 수정이 가능합니다.
- ⑨ : 현황 탭
탭의 이름과 그에 대한 위젯을 보여줍니다.
- ⑩ : 위젯 뷰
관리자가 추가한 위젯을 보여줍니다.

위젯

위젯 추가 & 탭 추가 / 수정 / 삭제

관리자는 설정버튼을 이용하여 관리자의 관심항목에 따라 위젯 추가, 탭 추가/수정/삭제를 할 수 있습니다.

- 설정 버튼 메뉴



- 위젯 추가

위 설정버튼 메뉴 중, 위젯추가 버튼을 선택하면 위젯추가 팝업이 뜹니다.

위젯추가 팝업에서 원하는 위젯을 찾은 후, 대시보드에 추가 버튼을 누릅니다.



- 위젯삭제

관리자는 필요 없는 위젯을 삭제할 수 있습니다.

톱니바퀴 모양을 선택 후 삭제버튼을 누릅니다.



- 위젯 설정

관리자는 위젯을 타이틀과, 갱신주기를 설정할 수 있습니다.

톱니바퀴 모양을 선택 후 설정 버튼을 클릭하여 해당 위젯의 타이틀과 화면갱신주기를 설정할 수 있습니다.



- 탭 추가

관리자는 위 설정버튼 메뉴 중, 탭 추가 버튼을 이용하여 원하는 항목의 위젯만 모아놓은 탭을 만들 수 있습니다.



- 템 수정

관리자는 위 설정 버튼 메뉴 중, 템수정 버튼을 이용하여 템의 이름 및 레이아웃을 수정할 수 있습니다.



- 템 삭제

관리자는 위 설정 버튼 메뉴 중, 삭제 버튼을 이용하여 원하는 템을 삭제할 수 있습니다.



- 템 순서 변경

관리자는 위 설정 버튼 메뉴 중, 템 순서 변경 버튼을 이용하여 템 순서를 변경할 수 있습니다.

템 순서는 가장 위쪽에 있는 템이 가장 왼쪽에 나열되는 형식으로 변경 원하는 템을 선택 후 드래그 하거나 좌측의 화살표 버튼을 이용하여 순서를 변경할 수 있습니다.



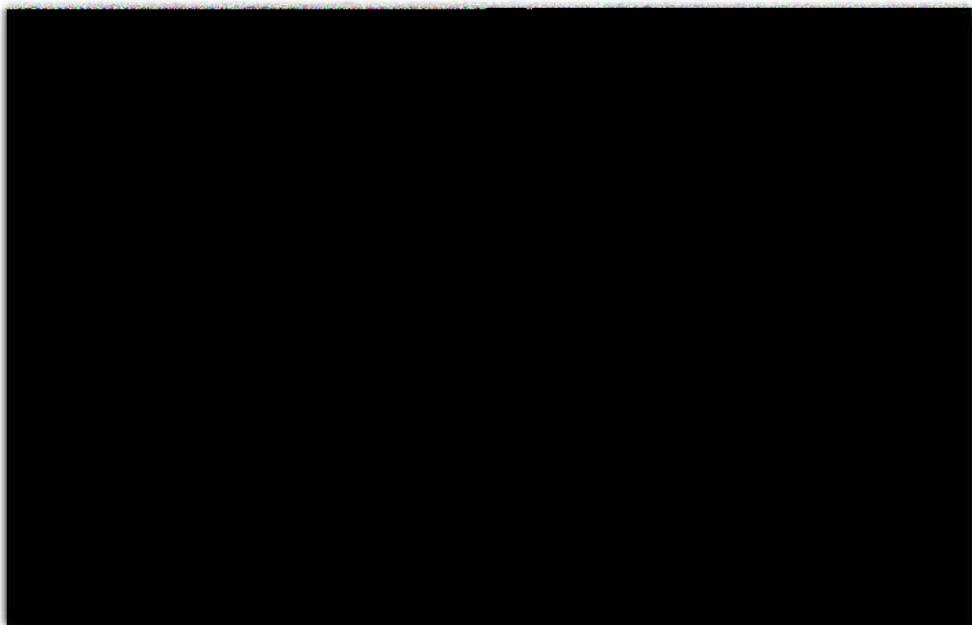
- 대시보드 초기화

관리자는 위 설정 버튼 메뉴중, 대시보드 초기화 버튼을 이용하여 대시보드에 있는 위젯, 탭을 Default로 설정할 수 있습니다.



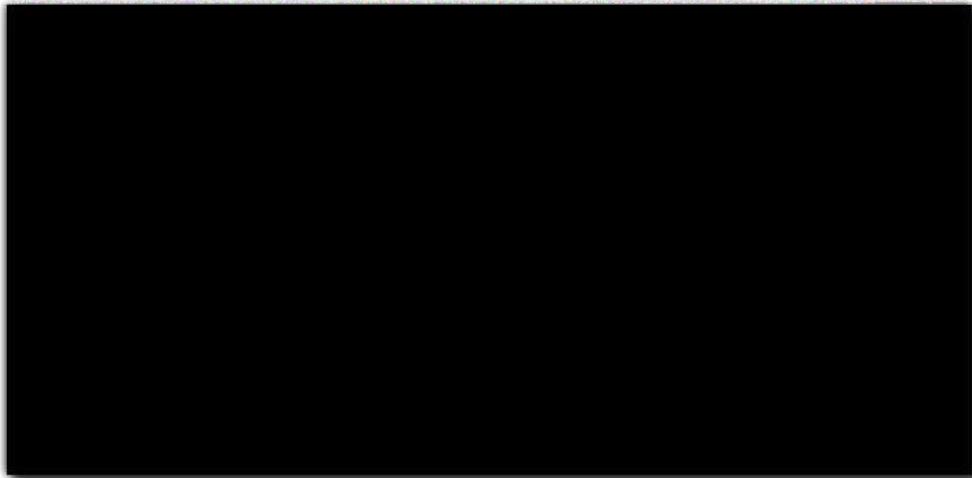
- 전체화면으로 보기

관리자는 위 설정 버튼 메뉴중, 전체화면으로 보기 버튼을 이용하여 대시보드를 전체화면으로 볼 수 있습니다. Esc 버튼으로 전체화면 모드를 종료할 수 있습니다.



- Sensor Map

탭 추가 시 탭 종류를 센서맵으로 설정하여 Sensor Map을 추가할 수 있습니다.
Sensor Map이란 Map에 센서별로 위치를 지정하여 가시적으로 센서 위치를 확인할 수 있고
센서별 노드 수, 그룹에 포함된 노드 수를 확인할 수 있어 센서별 관리가 편리해집니다.



1. 센서 배치

Sensor Map 우측 상단에 센서리스트를 클릭 후 센서 IP를 드래그하여 Map에 배치합니다.



2. 홈 저장

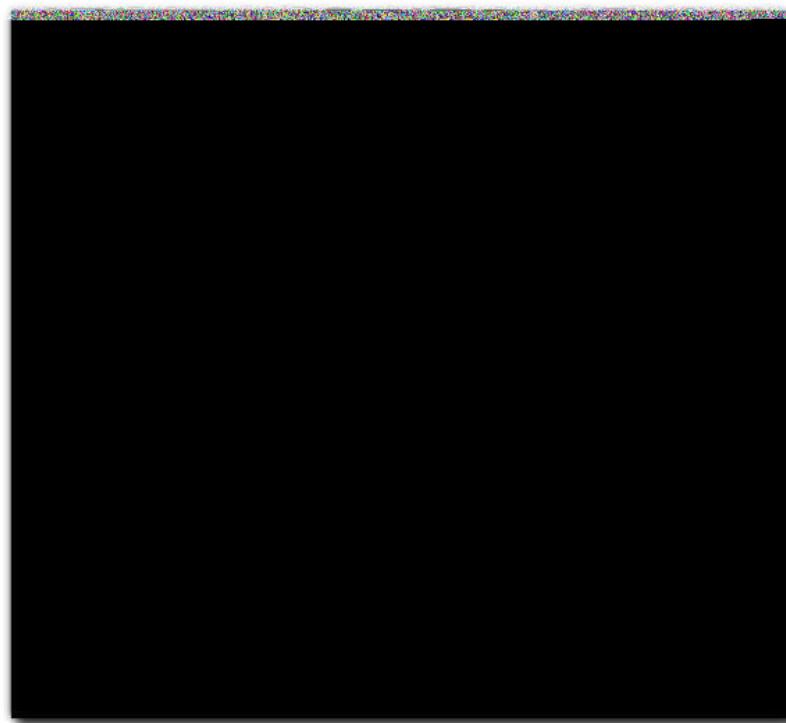
Sensor Map 우측 상단에 톱니모양을 클릭 후 홈 저장을 클릭할 시 현재 보고 있는 Map의 위치와 줌을 저장하여 좌측 상단의 홈 버튼을 클릭할 시 저장한 홈의 위치로 이동합니다.



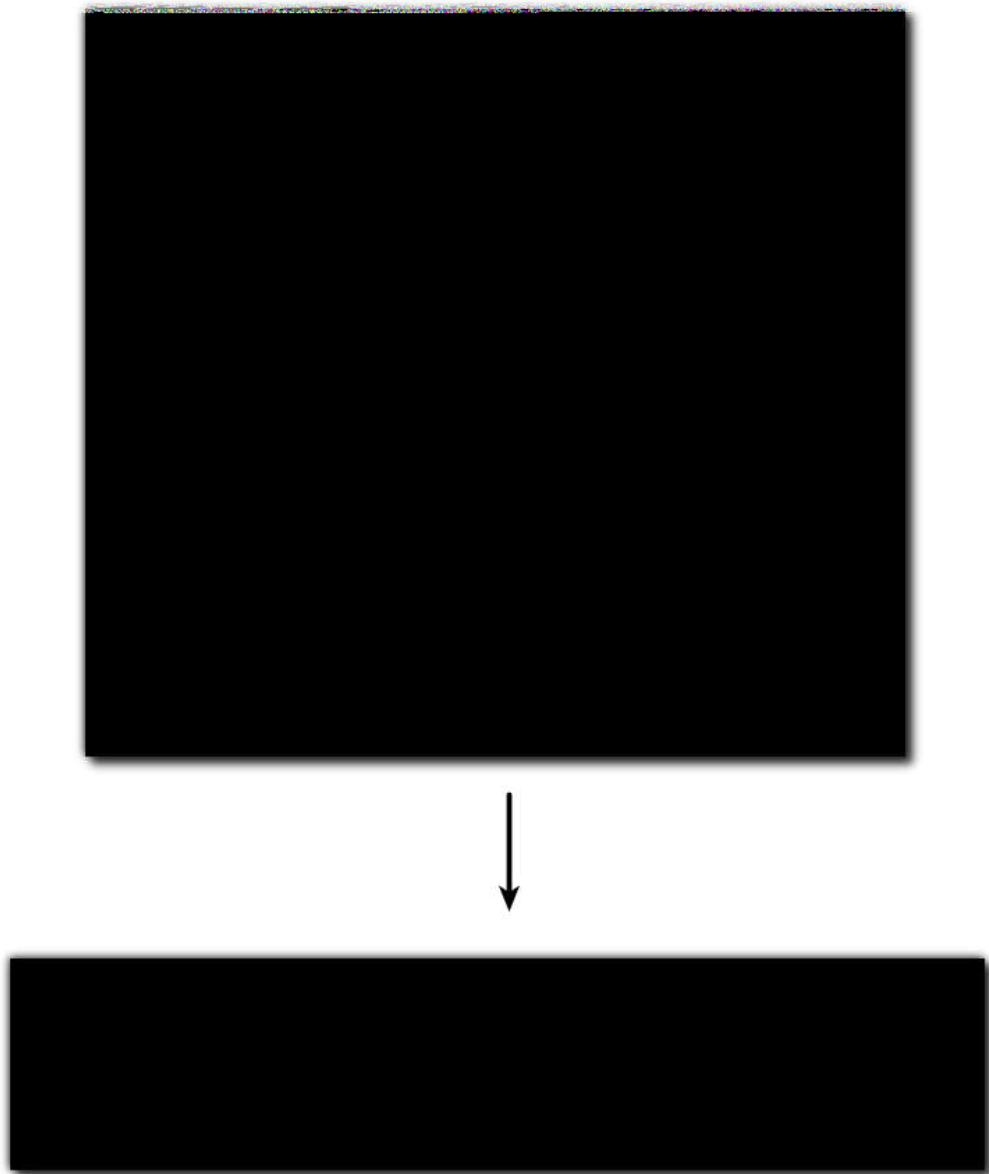
3. 관심노드그룹

Sensor Map 우측 상단에 톱니모양을 클릭 후 관심노드그룹을 클릭하여 Map에 표시되어 있는 센서 아이콘에 표시될 노드그룹을 설정합니다.

이벤트 항목에 노드그룹을 추가할 시 다음 그림과 같이 확인할 수 있습니다. 숫자를 클릭할 시 그룹에 포함된 노드를 확인할 수 있습니다.



상세 항목에 노드그룹을 추가 후 센서아이콘을 클릭하면 다음 그림과 같이 확인할 수 있습니다. 숫자를 클릭할 시 그룹에 포함된 노드를 확인할 수 있습니다.



4. 설정

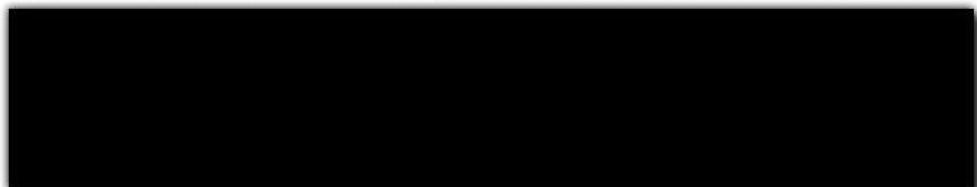
Sensor Map 우측 상단에 톱니모양을 클릭 후 설정을 클릭하여 Map에서 보여주는 노드그룹 정보 갱신주기 및 센서 클러스터링 범위를 설정할 수 있습니다.



항목	설명
클러스터링 범위	센서 아이콘이 클러스터링 되는 범위를 설정합니다.
주기	센서 아이콘에 표시되는 노드그룹 정보의 갱신 주기를 설정합니다.

5. 부가기능

좌측 상단에 세개의 아이콘이 있으며 각각의 기능은 홈 위치 이동, 현재 접속한 위치, Map 검색 기능입니다.



항목	설명
①	장소의 명칭을 검색 시 해당 위치로 이동됩니다.
②	저장한 홈 위치로 이동됩니다
③	현재 접속한 위치를 Map으로 확인할 수 있습니다.