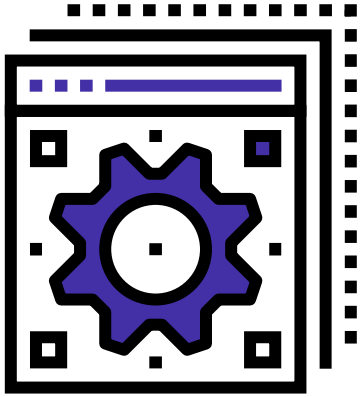
NAC EDU Chapter 4

WebUI - 감사

CONTENTS

감사

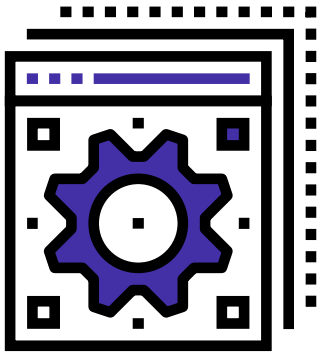


로그

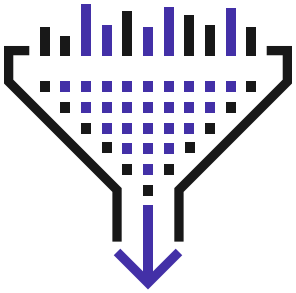
리포트

로그

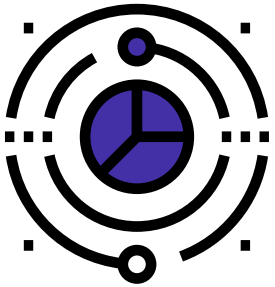
로그



로그 검색

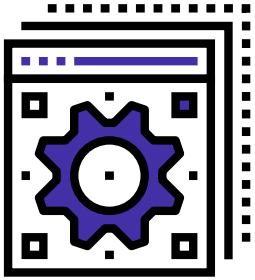


검색 필터



Radius

로그_로그 검색

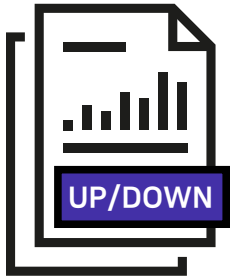


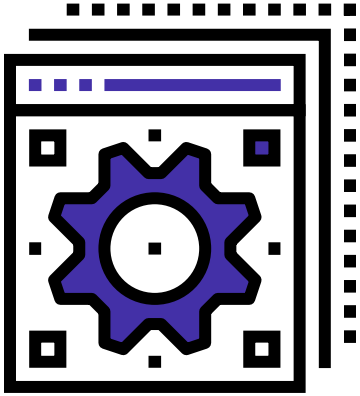
로그 검색

필터 항목	상세 내용
IP	로그를 검색할 대상 IP를 입력합니다.
MAC	로그를 검색할 대상 MAC을 입력합니다.
사용자 ID	로그를 검색할 사용자 ID를 입력합니다.
사용자 명	로그를 검색할 사용자 명(이름)을 입력합니다.
부서명	로그를 검색할 사용자 부서명을 입력합니다.
관리 장비 명	로그를 검색할 센서 이름(관리 장비 명)을 입력합니다.
추가정보	로그에 추가된 추가정보를 입력합니다. (추가 정보는 “설정 > 환경 설정 > 감사 기록”에서 설정 가능)
설명	로그를 검색할 설명을 입력합니다.
로그 타입	4가지 로그 타입을 선택합니다.
로그 ID	로그를 구분한 ID를 지정합니다.

로그_로그 검색

Genian NAC

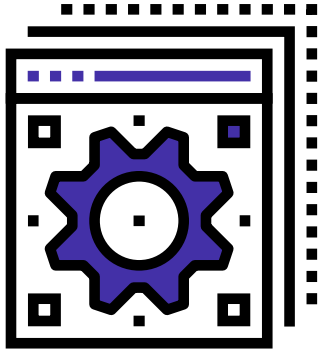




로그

로그_로그 검색

Genian NAC



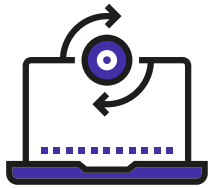
로그 검색 / Radius

검색 필터 저장

이름
설명
출력 컬럼

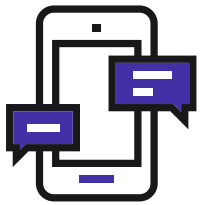
로그_로그 검색

로그 발생

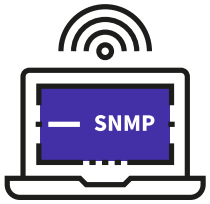


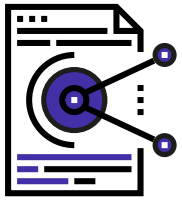
연동 기능 및
외부 전송

알람 전송
Syslog 전송
SNMP Trap 전송
Webhook
태그



관리자 알림





외부 전송

로그_검색 필터

Genian NAC

이벤트 ID	이벤트 명	상세 내용
402	AGENT 사용 시작	KEEPALIVE 를 통한 AGENT UP 관련 로그
452	AGENT 사용 종료	KEEPALIVE 를 통한 AGENT DOWN 관련 로그
120	CLI	CLI Command 수행 관련 로그
124	DHCP	DHCP 할당 관련 로그
101	GENIAN장비	Genian 장비 설정 변경 관련 로그
910	IP 사용 관리	IP 관리정책 관련 로그
401	IP 사용 시작	노드 동작상태 UP 관련 로그
451	IP 사용 종료	노드 동작상태 DOWN 관련 로그
140	SYSLOG	외부에서 전송되는 Syslog 관련 로그
900	관리자 접속	WebUI 관리자 접속 관련 로그

로그_검색 필터

Genian NAC

이벤트 ID	이벤트 명	상세 내용
110	그룹	그룹 Assigned / Removed 관련 로그
132	네트워크 정보	열린 포트, 서비스, 공유 정보 등 네트워크 정보 관련 로그
122	네트워크 제어	노드의 네트워크 설정 제어 관련 로그
100	노드 관리	신규 노드, 비 관리 노드 등록, 삭제 관련 로그
103	노드 정보	노드 타입, 연결 방식, 접속 AP 감지 및 변경 관련 로그
121	데이터 동기화	정보 동기화 관련 로그
104	데이터베이스	Database 백업 및 Error 관련 로그
102	동작상태 변경	네트워크 센서 동작상태 관련 로그
912	리포트	리포트 생성 관련 로그
123	무선랜 AP	AP모드 동작 시 최대 SSID 개수(8개)를 초과시 발생 로그

로그_검색 필터

Genian NAC

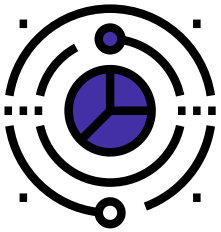
이벤트 ID	이벤트 명	상세 내용
134	무선랜 관리	SSID 관련 삭제 로그
133	무선센서정보	무선센서에서 수집정보 변경 관련 로그
300	비 정상 노드	위험관리로 탐지되는 비정상노드와 IP관리에서 비 정상 노드 탐지 로그
908	사용자 관리	Local 사용자 계정에 생성,수정 관련 로그
904	설정 변경	WebUI 설정 변경 관련 로그
906	시스템 관리	시스템 무결성 및 플러그인 업데이트
131	시스템 정보	Agent 수집하는 단말 시스템 정보 관련 로그
119	알람	외부 호출 서비스 실패 관련 로그
118	업데이트	운영 정보 데이터 업데이트 관련 로그
1007	에이전트	에이전트의 상태 및 장치 제어 관련 로그

로그_검색 필터

Genian NAC

이벤트 ID	이벤트 명	상세 내용
111	에이전트 액션	수행되는 에이전트 액션 결과값 관련 로그
1009	에이전트 인증코드	신청항목에서 발급된 에이전트 삭제 인증코드 로그
107	운영체제 업데이트 동기화	Windows 업데이트 목록 추가 관련 로그
108	운영체제 업데이트 서비스	업데이트 서버에서의 검색 서비스 관련 로그
114	위험관리	위험관리에 탐지된 대상 로그
116	인증	사용자 인증 관련 로그
109	정책	개별 단말에 노드 정책, 제어 정책 할당 / 변경 관련 로그
902	정책변경	정책에 생성, 변경 관련 로그

로그_로그검색_Radius

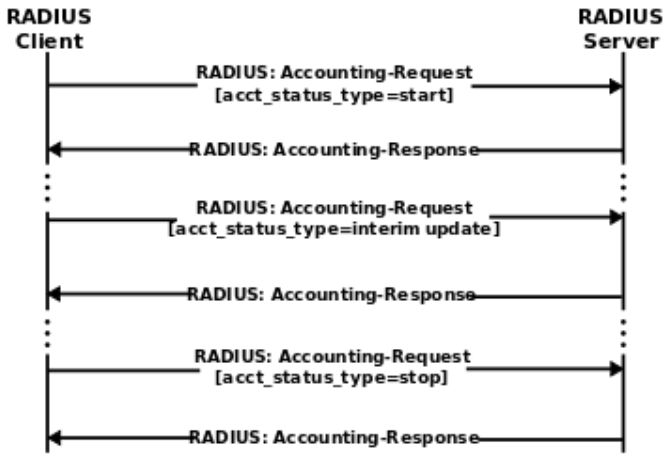


Radius

필터 항목	상세 내용
사용자 명	로그를 검색할 사용자 명(이름)을 입력합니다.
NAS IP	네트워크 액세스 서버 IP를 입력합니다.
NAS Port Type	사용자 인증 시 NAS의 물리적인 포트 타입을 선택합니다.
NAS Port	사용자 인증 시 NAS 물리적인 포트 번호를 입력합니다.
MAC	로그를 검색할 MAC을 입력합니다.
SSID	로그를 검색할 SSID를 입력합니다.
로그 타입	4가지 로그 타입을 선택합니다.
로그 ID	로그를 구분한 ID를 지정합니다.

로그_검색필터_Radius

Genian NAC



이벤트 ID	이벤트 명	상세 내용
552	Interrim-update	Radius Accounting Acct_status_type = interim-update 정보 관련 로그
501	start	Radius Accounting Acct_status_type = start 정보 관련 로그
551	stop	Radius Accounting Acct_status_type = stop 정보 관련 로그
553	Radius	Radius Request 패킷 vendor specific attribute 정보 관련 로그

리포트

리포트

리포트

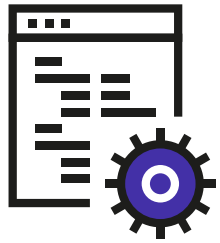
리포트_노드 리포트

리포트_로그 리포트

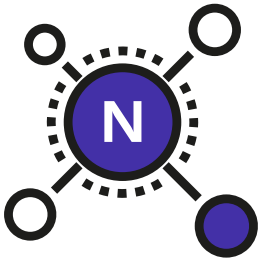
리포트_무선랜 리포트

리포트_사용자 정의

Genian NAC



쿼리 리포트



노드 리포트

로그 리포트

대시보드 리포트

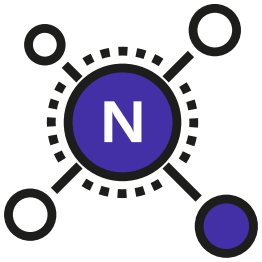
리포트_사용자 정의_쿼리 리포트

Genian NAC

생성 주기 설정
(최소 30분)

리포트_사용자 정의_노드 리포트

Genian NAC



노드 리포트

생성 주기 설정
(최소 30분)

감사 기록 설정
(임계값 / 변동값)

리포트_사용자 정의_로그 리포트

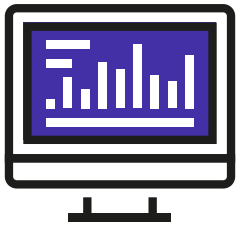
Genian NAC

로그 리포트

생성 주기 설정
(최소 30분)

리포트_사용자 정의_대시보드 리포트

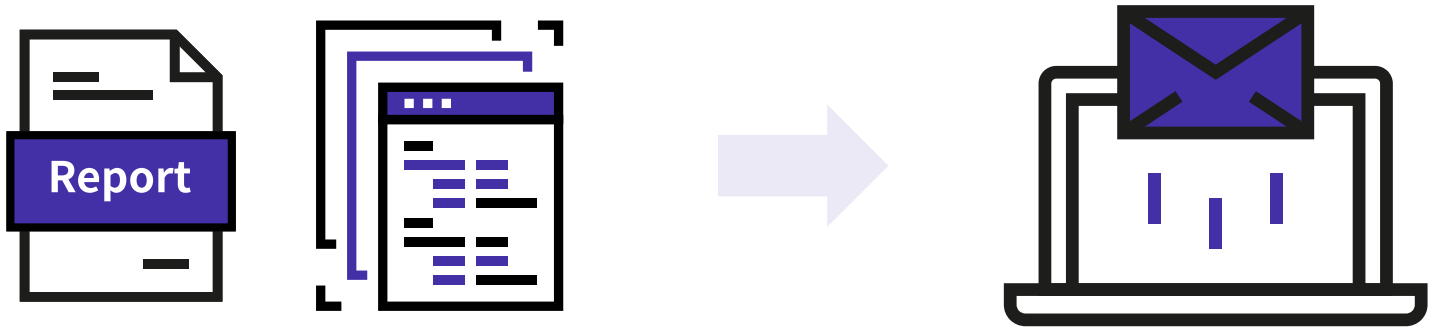
Genian NAC



대시보드 리포트

생성 주기 설정
(최소 30분)

리포트_이메일 발송

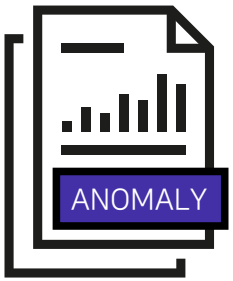


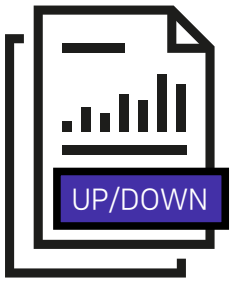
간편 리포트 상세 리포트 E-Mail 전송

Summary

Genian NAC

1. 로그





Option

2. 리포트

수집 주기 고정

수집 주기 변경 가능

Genians

문의 : 지니언스 네트워크보안기술부

ca-se-nac@genians.com