Genian NAC

감사로그 전송 가이드

V1.0

Updated : May. 2020

Genians

개정 이력

No	Date	Version	Updated Content	비고
1	2020. 05. 19	1.0	최초 버전 작성	

목차

1. 개요

Genian NAC 에서 감사로그란 시스템, 장비 등에서 발생하는 이벤트에 대한 로그를 뜻하며, 이벤트가 발생한 시간, 종류, 로그 ID 등이 표시됩니다. 또한 종류에 따라 ERROR, ANOMALY, WARN, INFO 4 가지 타입으로 구분됩니다.

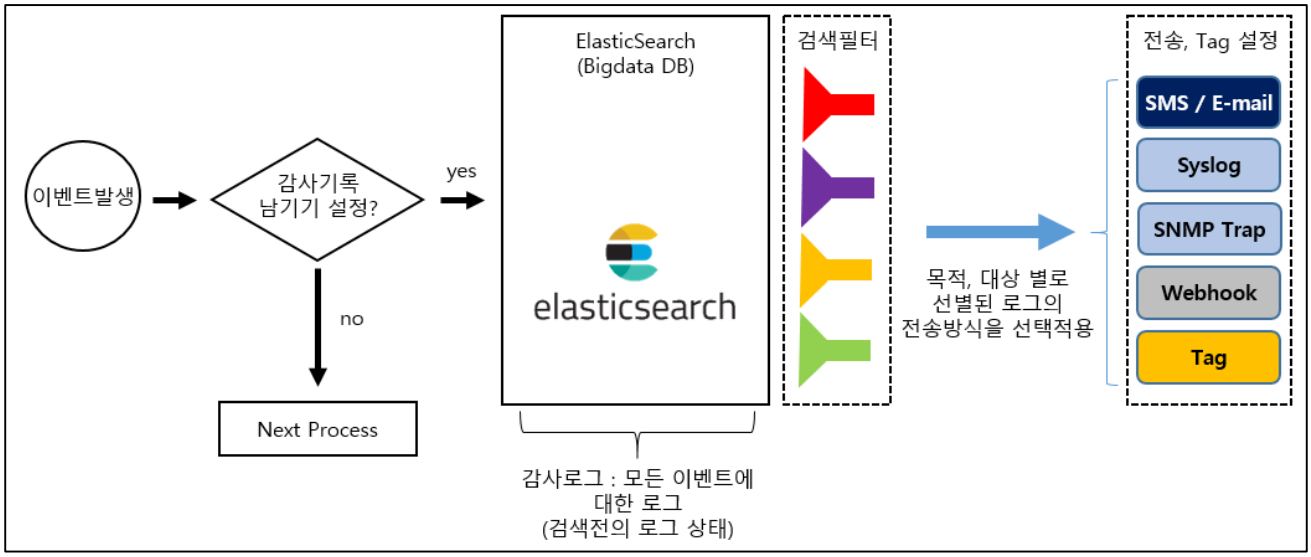
Genian NAC 는 대용량 감사로그 저장 및 검색을 위해 Elasticsearch 엔진을 사용하고 있습니다.

관리자는 Elasticsearch 를 이용하여, 전체는 물론, 다양하게 제공하는 검색조건을 이용하여 필요한 정보만을 열람, 별도 저장, 외부로 전송 할 수 있습니다.

Genian NAC 는 검색조건에 의해 NAC 에 존재하는 모든 데이터 중, 필요한 정보만 추출하는 검색필터를 생성하게 되며, 생성된 검색필터는 다양한 외부 기기와 연동을 위해, 각각의 처리 프로세스를 제공합니다.

Genian NAC 의 감사기록, 검색필터, 전송 설정의 흐름은 다음과 같이 동작합니다.

< 하나의 장비에서 각각의 이벤트에 따라 별도의 전송방식으로 설정이 됨에 주의 바랍니다.
예. 1)신규하드웨어 탐지 -> 1 번서버로 syslog 전송
2) 안티바이러스 미설치 단말 탐지 -> SMS 알림
3) 멀웨어 감염단말 탐지 -> 2 번서버로 syslog 전송 + Slack 알림 >



2. 사전 요구사항

Genian NAC에서 SYSLOG와 SNMP Trap 이벤트 전송 시 수신 받는 장비에서 포트를 활성화해야 합니다.

2.1 Networking 요구사항

Genian NAC의 이벤트를 수신 받는 장비에서 아래의 포트를 활성화 해야하고, 이벤트 전송에 사용되는 기본 포트는 다음과 같습니다.

- SYSLOG 포트 : 514(UDP), 6514(TCP)
- SNMP Trap 포트 : 162(UDP)
- Webhook 포트 : HTTP - 80(TCP) , HTTPS - 443(TCP) , Genian NAC V5.0 이상 - 8443(TCP)

3. 이벤트 전송 및 설정 방법

Genian NAC에서 이벤트를 전송하기 위해서는 검색필터를 활용하여야 하고, 이벤트 전송 방법에는 SYSLOG, SNMP Trap, Webhook 전송이 있습니다.

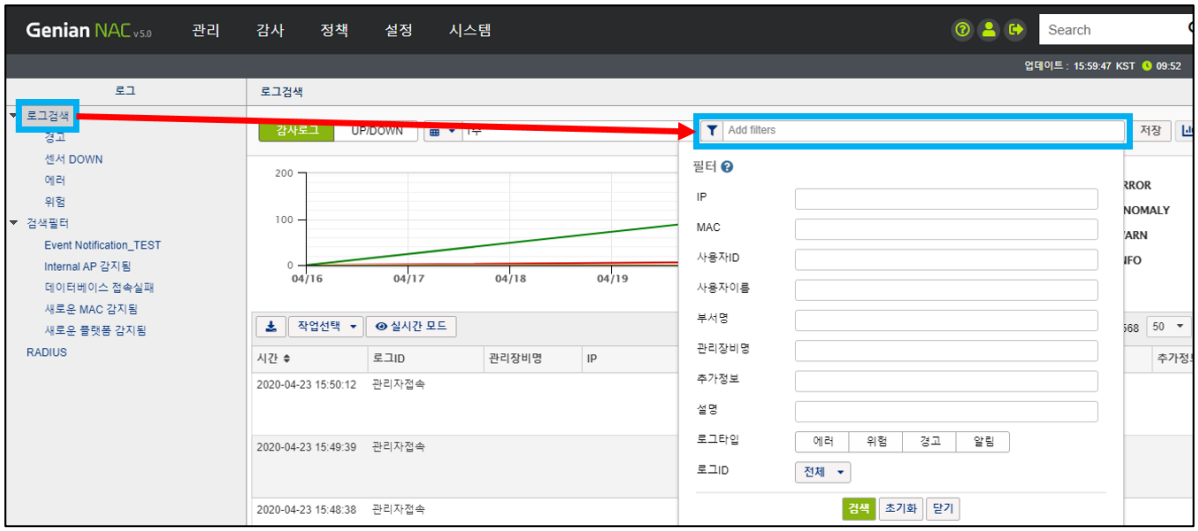
- 포트는 수신 받는 장비에서 정의한 포트로 변경 가능합니다.
- 이벤트 전송 시 메시지가 공백인 경우 아래와 같이 Defalut 매크로 값이 전송됩니다.
  {_DATETIME}{_LOGTYPE}{_LOGID}{_SENSORNAME}{_IP}{_MAC}{_FULLMSG}{_DETAILMSG}
- 메시지에 사용 가능한 매크로는 "5.1 이벤트 전송 시 로그 메시지 매크로 설정방법" 을 참고하시기 바랍니다.

3.1 검색필터 생성 방법

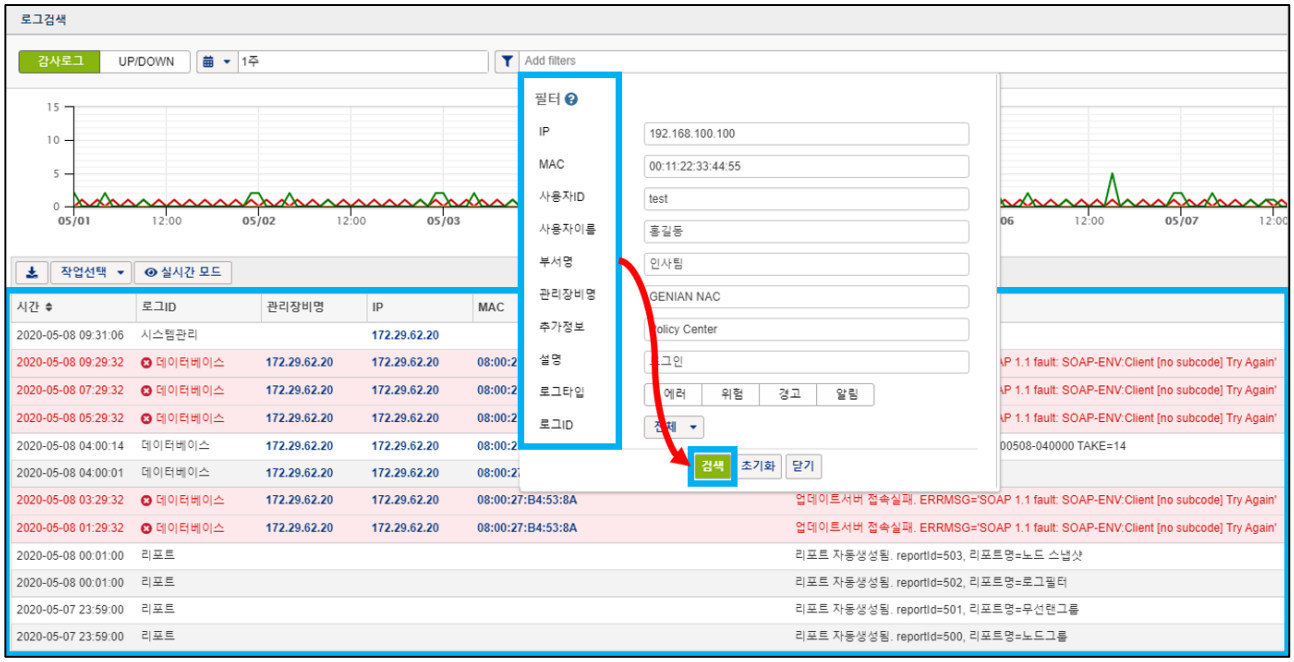
Genian NAC는 장비에서 발생하는 이벤트에 대해 선별적으로 관리하기 위해서 검색필터 기능을 제공합니다.

검색필터 생성 방법은 다음과 같습니다.

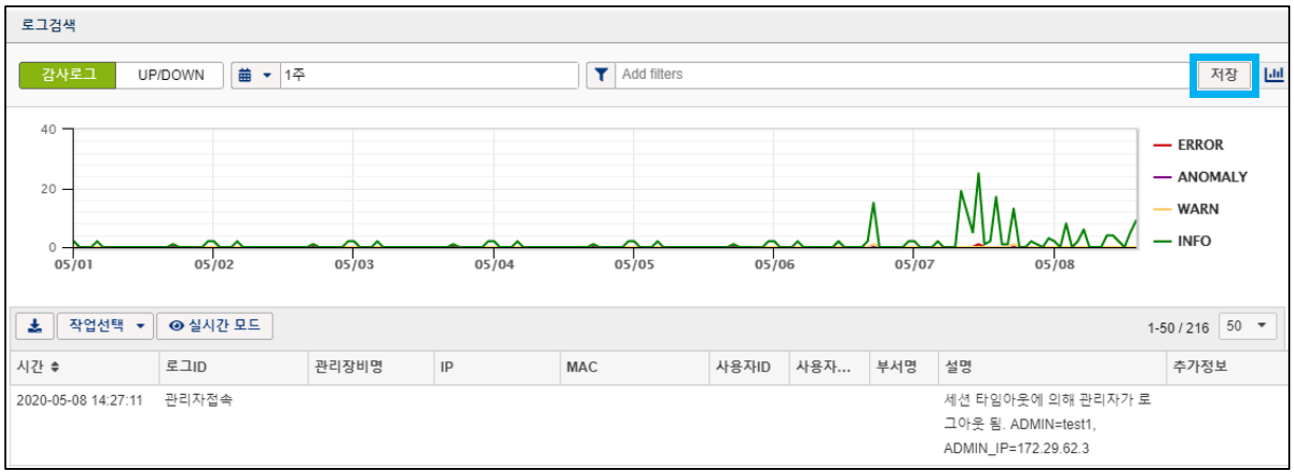
STEP 1: "감사 – 로그 – 로그검색" 메뉴로 이동 후 "Add filter" 아이콘 클릭



STEP 2: "필터" 대화상자에서 필요한 정보 선택 및 입력 후 "검색" 버튼을 클릭하여 로그 내용 확인.

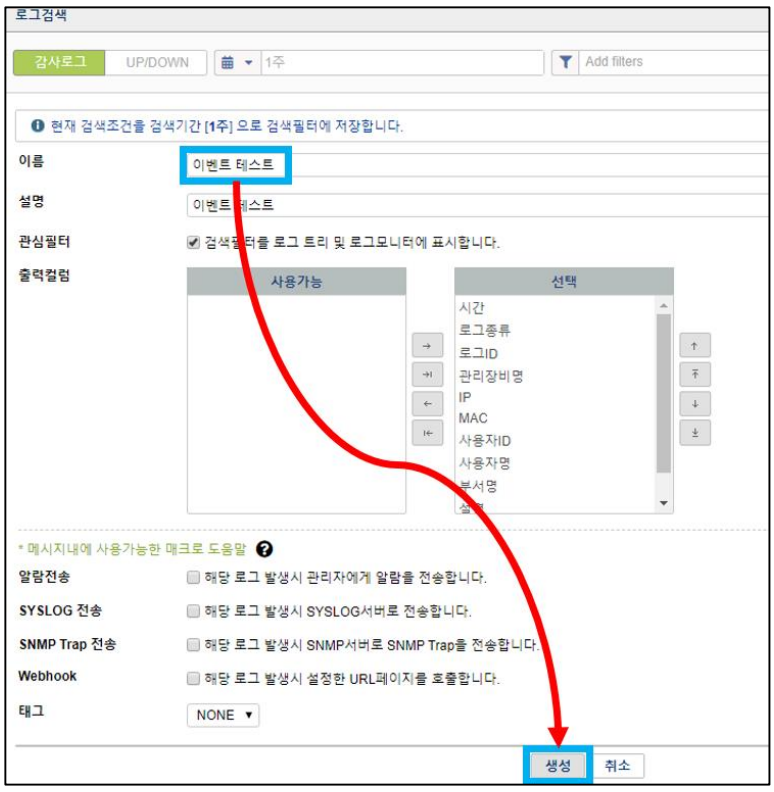


STEP 3: 로그 내용 확인 후 우측 상단에 "저장" 버튼 클릭.

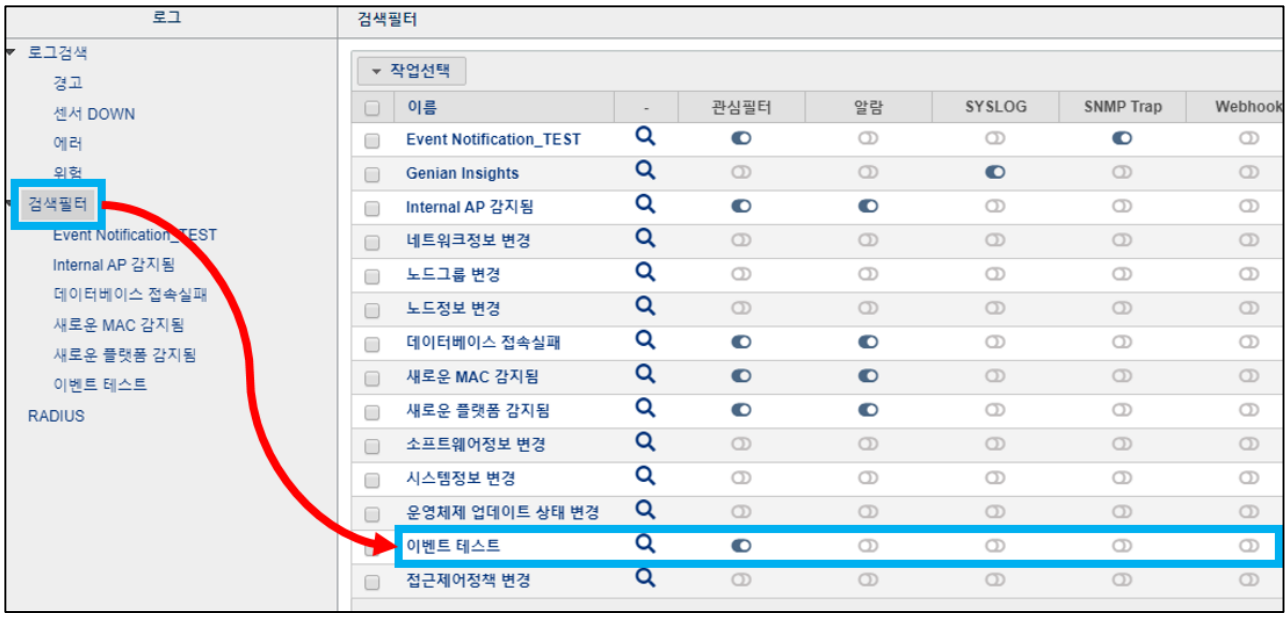


STEP 4: "이름", "설명(생략가능)" 항목 입력 후 "생성" 버튼 클릭

(※ SYSLOG, SNMP Trap, Webhook 전송방법은 3.2 SYSLOG 전송 설정 방법, 3.3 SNMP 전송 설정 방법, 3.4 Webhook 설정 방법 내용을 참고하시기 바랍니다.)



STEP 5: "감사 – 로그 – 검색필터" 메뉴에서 생성한 검색필터 확인.



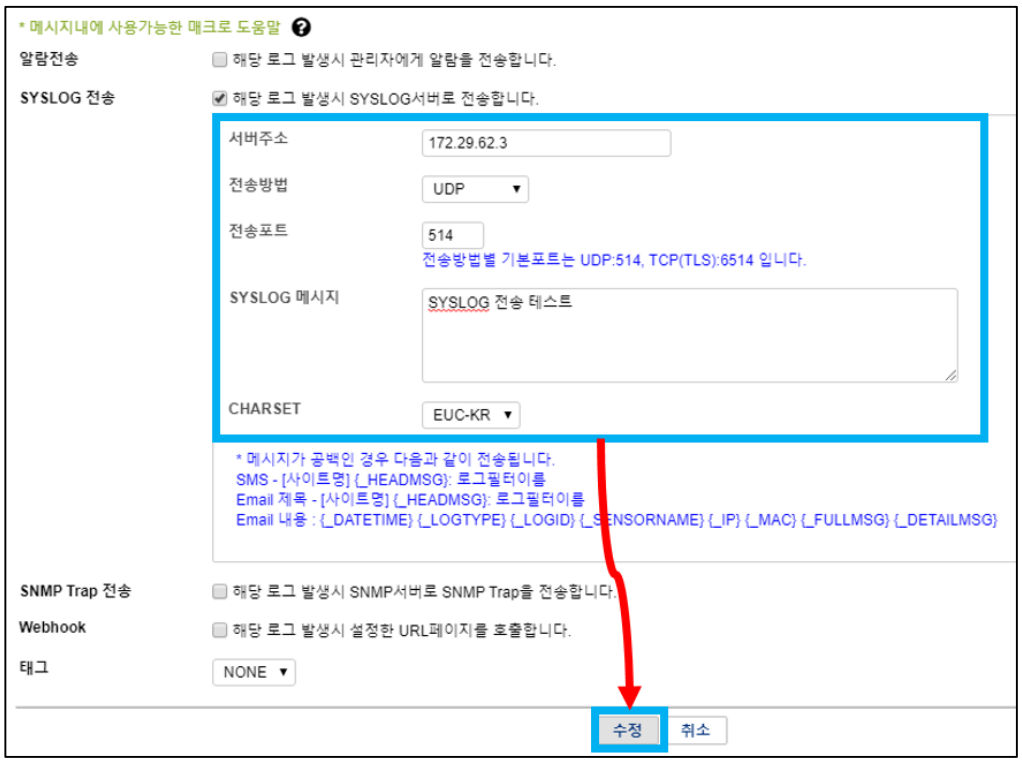
3.2 SYSLOG 전송 설정 방법

SYSLOG 전송은 주로 시스템 위주의 내용을 전달할 때 활용되고, 전송 설정 방법은 다음과 같습니다.

STEP 1: "감사로그 – 로그 – 검색필터" 메뉴에서 이벤트를 전송 할 필터 선택.

STEP 2: 하단에 "SYSLOG 전송" 체크박스 클릭.

STEP 3: 설정 값 입력 후 "수정" 버튼 클릭.



- 설정 방법
  - 서버주소: 이벤트를 수신 받을 서버 주소를 입력합니다.
  - 전송방법: UDP 혹은 TCP(TLS) 를 선택합니다.
  - 전송포트: UDP는 "514", TCP(TLS)는 "6514" 를 입력합니다.
  - SYSLOG 메시지: 사용 가능한 매크로 혹은 메시지를 입력합니다. (글로벌 로그 매크로 활용)
  - CHARSET: UTF-8 혹은 EUC-KR 을 선택합니다. (UTF-8 사용을 권장합니다.)

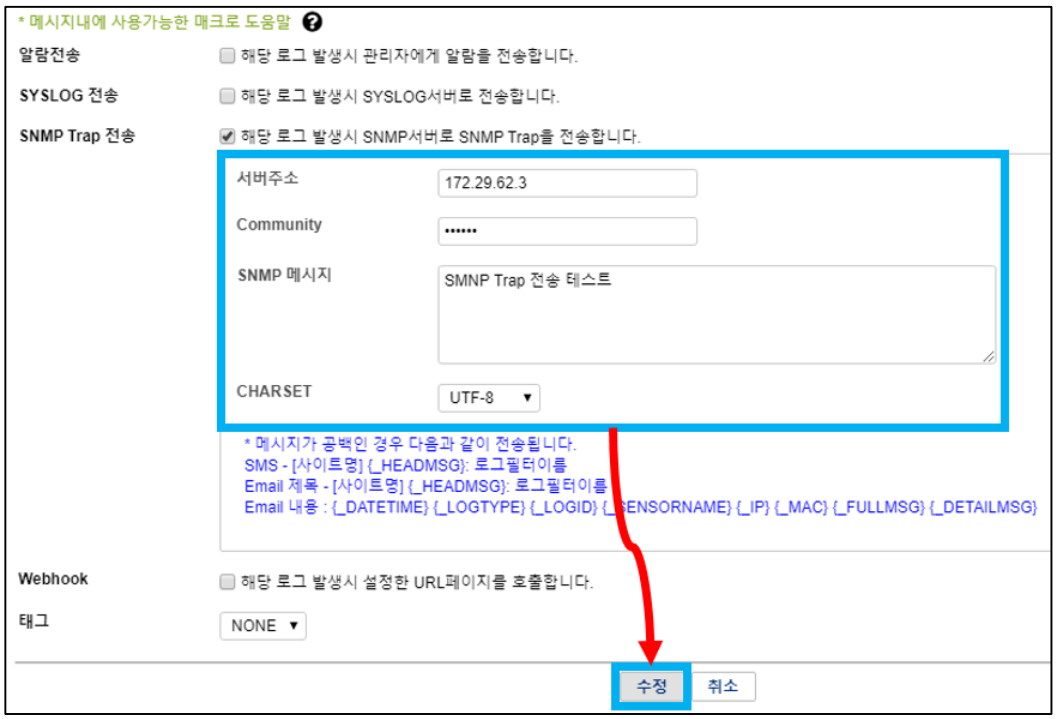
3.3 SNMP Trap 전송 설정 방법

SNMP Trap 전송은 주로 장비와 장비 간 이벤트 전송에 활용되고, 전송 설정 방법은 다음과 같습니다.

STEP 1: "감사로그 – 로그 – 검색필터" 메뉴에서 이벤트를 전송 할 필터 선택.

STEP 2: 하단에 "SNMP Trap 전송" 체크박스 클릭.

STEP 3: 설정 값 입력 후 "수정" 버튼 클릭.



- 설정 방법
  - 서버주소: 이벤트를 수신 받을 서버 주소를 입력합니다.
  - Community: SNMP 통신을 위해서 서버와 상호 합의된 값을 입력합니다. (ex. public)
  - SNMP 메시지: 사용 가능한 매크로 혹은 메시지를 입력합니다. (글로벌 로그 매크로 활용)
  - CHARSET: UTF-8 혹은 EUC-KR 을 선택합니다. (UTF-8 사용을 권장합니다.)

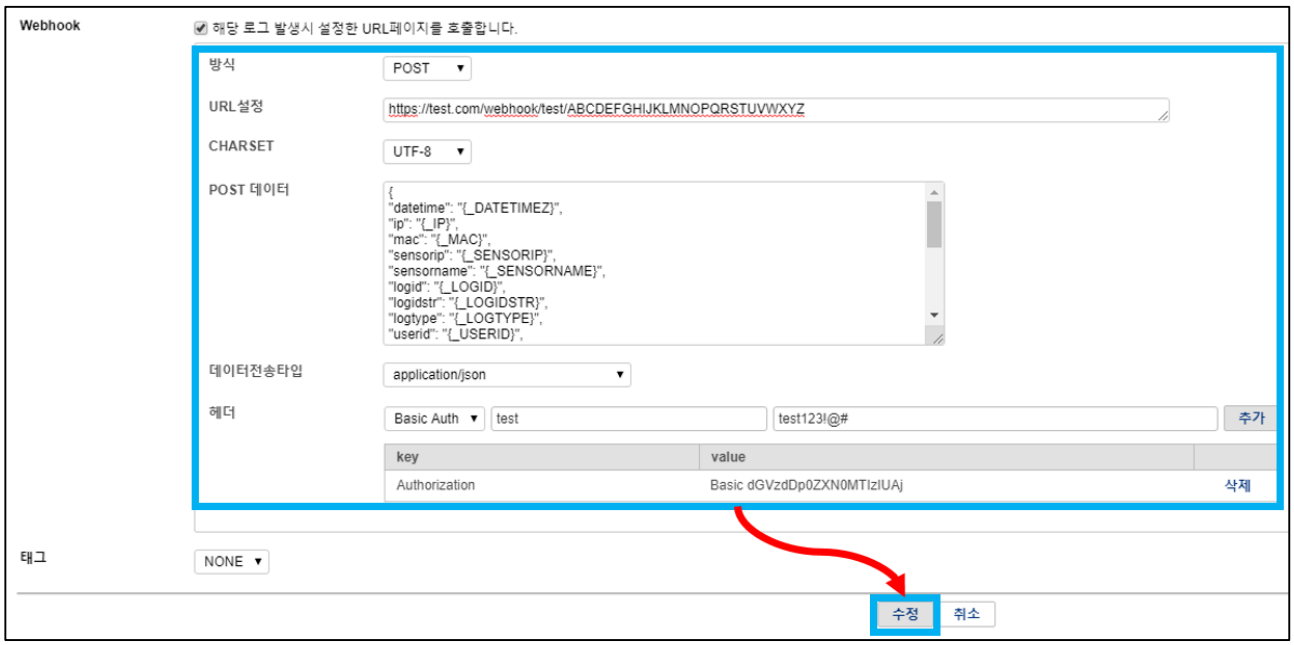
3.4 Webhook 설정 방법

Webhook 은 주로 Web 호출 및 타 장비와 API 사용 시 활용되고, 설정 방법은 다음과 같습니다.

STEP 1: "감사로그 – 로그 – 검색필터" 메뉴에서 이벤트를 전송 할 필터 선택.

STEP 2: 하단에 "Webhook" 체크박스 클릭.

STEP 3: 설정 값 입력 후 "수정" 버튼 클릭.



- 설정 방법
  - 방식: GET / POST / PUT / DELETE 중 원하는 방식을 선택합니다.
  - URL 설정: 전송할 URL 을 입력합니다.
    (위 이미지에 설정되어 있는 값은 예시이며, 실제 호출 할 URL을 입력해야 합니다.)
  - CHARSET: UTF-8 혹은 EUC-KR 을 선택합니다. (UTF-8 사용을 권장합니다.)
  - POST 데이터: 수신 받는 장비에서 보여줄 정보를 입력합니다. (글로벌 로그 매크로 활용)
  - 데이터 전송타입: 전송받는 서버에서 지정한 데이터 전송타입을 선택합니다.
  - 헤더: 사용자ID와 패스워드를 입력합니다.
    (호출할 URL에 ID와 패스워드를 설정하였을 시 입력합니다.)

4 감사로그 포맷

Genian NAC 의 감사로그 포맷 정보를 제공하여 검색필터 설정 및 타 장비와 연동 시 활용 가능합니다.

4.1 포맷 정의

컬럼정보	내용	상세내용
시간	로그 발생 시간	로그발생날짜 YYYY-MM-DD 로그발생시각 HH:MM:SS (ex. 2020-01-01 11:11:11)
종류	로그 생성 종류	ERROR: 에러로그, ANOMALY : 위험로그, WARN : 경고로그, INFO : 정보로그
로그 ID	로그 생성 분류 ID	로그 별 대분류
관리장비명	로그 발생 센터와 센서의 IP 혹은 장비명	로그가 발생된 센터와 센서의 IP 또는 노드를 관리하는 장비명
IP	로그 발생 노드 IP	로그가 발생된 노드의 IP
MAC	로그 발생 노드 MAC	로그가 발생된 노드의 MAC
사용자 ID	로그 발생 사용자 인증 ID	사용자 인증 시 사용자의 ID
사용자명	로그 발생 인증 사용자 명	사용자 인증 시 사용자 ID 내 사용자명
부서명	로그 발생 사용자 부서명	사용자 인증 시 사용자 ID 내 부서명
설명	로그 발생 시 상세 설명	텍스트 형태 및 각 로그종류마다 KEY=VALUE 형태의 데이터를 가짐
추가정보	로그 발생 시 추가 설명	관리자가 설정한 추가적인 정보

※ 로그 ID 컬럼의 상세한 내용은 4.2 이벤트 항목 별 로그 ID 정의를 참고하시길 바랍니다.

※ 추가정보 컬럼은 "설정 – 환경설정 – 감사기록 – 노드 감사기록 선택 – 추가정보 저장" 항목에서 선택하여 추가 가능합니다.

4.2 이벤트 항목 별 로그 ID 정의

로그 ID	이름	내용
100	노드관리	노드관리 시 발생되는 로그
101	GENIAN 장비	GENIAN 장비에서 발생되는 로그
102	동작상태변경	센서의 동작상태 변경 시 발생되는 로그
103	노드정보	노드의 상태 정보 변경 시 발생되는 로그
104	데이터베이스	백업 시 발생되는 로그
107	운영체제 업데이트 동기화	패치파일 업데이트 및 동기화 시 발생되는 로그
108	운영체제 업데이트 서비스	패치서비스 상태에 따른 이벤트 발생 로그
109	정책	정책 할당 및 변경에 대한 로그
110	그룹	그룹 할당 및 변경에 대한 로그
111	에이전트액션	에이전트 액션 수행 결과에 대한 로그
112	데이터무결성	중요 파일의 데이터 무결성 검사에 대한 수행 및 결과 로그
114	위험관리	위험관리 이벤트 발생 로그
116	인증	사용자 인증 수행 및 결과 로그
118	업데이트	패치 및 GENIAN 데이터 업데이트 로그
119	알람	SMS 전송 오류 로그
120	CLI	장비 CLI 접속 및 command 실행 히스토리 로그
121	데이터동기화	인사정보 동기화 이력 로그
122	네트워크제어	네트워크 접근제어 감사로그
123	무선랜 AP	무선랜 AP 감지 이벤트
124	DHCP	DHCP 할당 이력 로그
130	소프트웨어정보	해당 에이전트의 소프트웨어 정보 로그
131	시스템정보	시스템 정보 로그
132	네트워크정보	네트워크 정보 로그
133	무선센서정보	무선랜 AP 정보 로그
134	무선랜관리	무선랜 AP 관리 로그
140	SYSLOG	SYSLOG 전송 시 발생되는 로그
300	비정상노드	IP 충돌 위반 대상 이벤트 로그
401	IP 사용시작	IP 사용시작 및 노드 동작상태 관련 로그
402	AGENT 사용시작	에이전트 사용 및 동작상태 관련 로그
451	IP 사용종료	IP 사용종료 및 노드 동작상태 관련 로그
452	AGENT 사용종료	에이전트 종료 및 동작상태 관련 로그
501	RADIUS 접속	RADIUS 인증 성공 관련 로그
551	RADIUS 해제	RADIUS 세션 만료 관련 로그
900	관리자접속	관리자 UI 접속 로그
902	정책변경	정책 할당 및 상태 변경 이벤트 로그

904	설정변경	NAC 설정 변경 이벤트 로그
906	시스템관리	NAC 에이전트 및 설정 파일 변경 로그
908	사용자관리	인증사용자 계정 이력 로그
910	IP 사용관리	IP 관리정책 이벤트 로그
912	리포트	감사기록 엑셀 출력 및 리포트 출력 이벤트 로그
920	매체사용관리	매체 사용 신청서 생성/수정/삭제 시 발생하는 로그
930	라이선스사용관리	라이선스 권한 적용 및 사용 이벤트 로그
1000	바이러스치료성공	백신 연동 시 바이러스 치료 성공 로그
1001	바이러스치료실패	백신 연동 시 바이러스 치료 실패 로그
1002	바이러스치료완료	백신 연동 시 바이러스 치료 완료 로그
1003	읽기차단	매체제어 읽기 접근 차단 관련 로그
1004	쓰기차단	매체제어 쓰기 접근 차단 관련 로그
1005	읽기허용	매체제어 읽기 접근 허용 관련 로그
1006	쓰기허용	매체제어 쓰기 접근 허용 관련 로그
1007	에이전트	에이전트 상태 및 정책 이벤트 발생 로그
1009	에이전트인증코드	에이전트인증코드 정보 로그

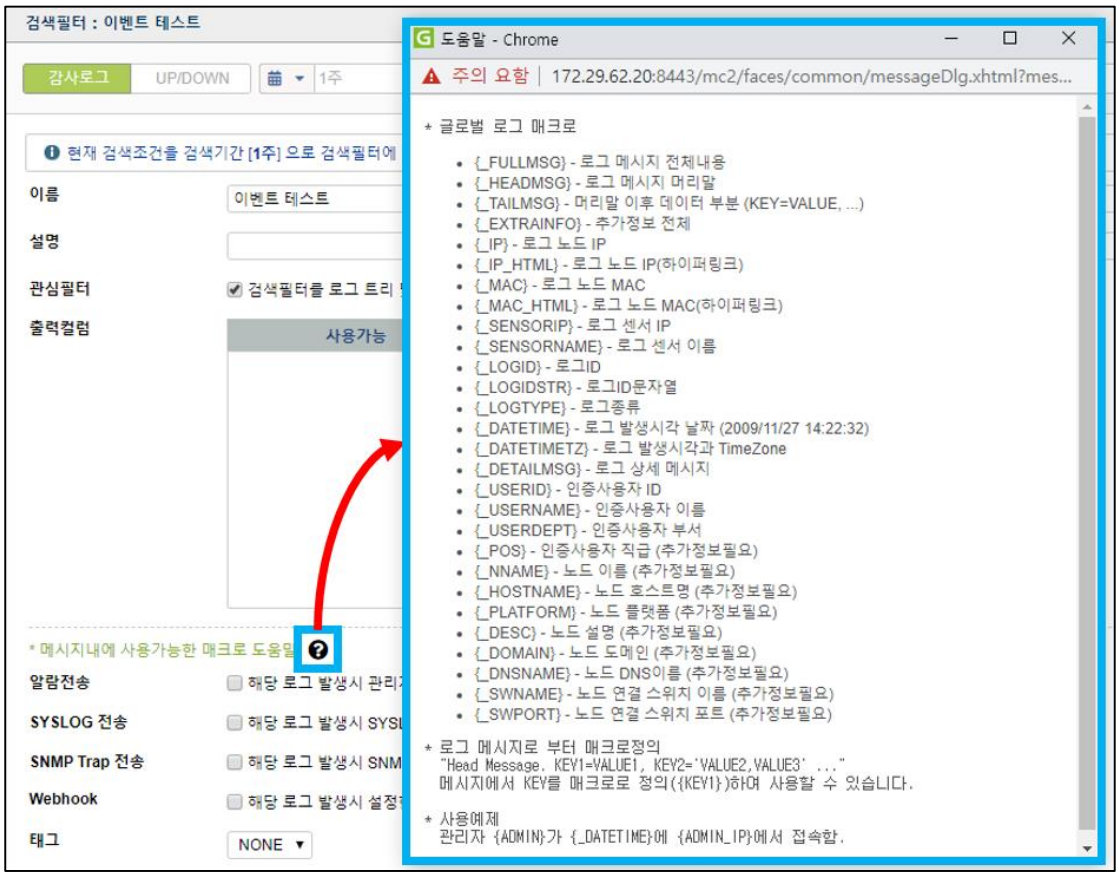
5. 매크로 설정 방법

Genian NAC는 사전에 정의되어 있는 매크로 변수를 활용하여 이벤트 전송 시 필요한 정보를 선택하여 전송할 수 있습니다. 또한 Http 매크로는 Webhook 사용자인증 연동 시 활용 가능합니다.

5.1 이벤트 전송 시 로그 메시지 매크로 설정 방법

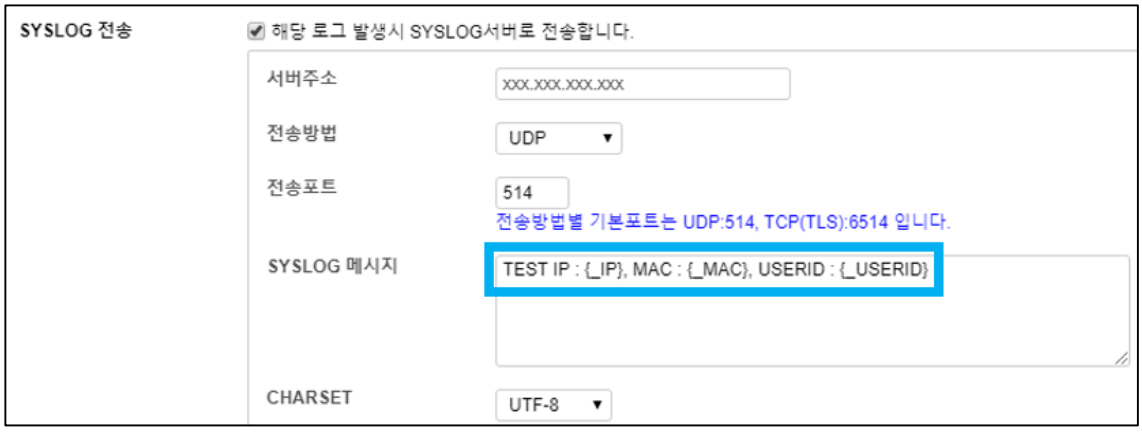
로그 메시지 매크로는 알람전송, SYSLOG 전송, SNMP Trap 전송, Webhook 에 동일하게 적용 가능합니다.

- 타 장비와 연동 시 주로 {_IP} – 로그노드 IP, {_MAC} – 로그노드 MAC, {_USERID} – 인증사용자ID 등을 활용합니다.
- 상세한 정보는 "감사 – 검색필터 – (필터 클릭)" 메뉴에서 "?" 아이콘을 클릭하여 확인 가능합니다.

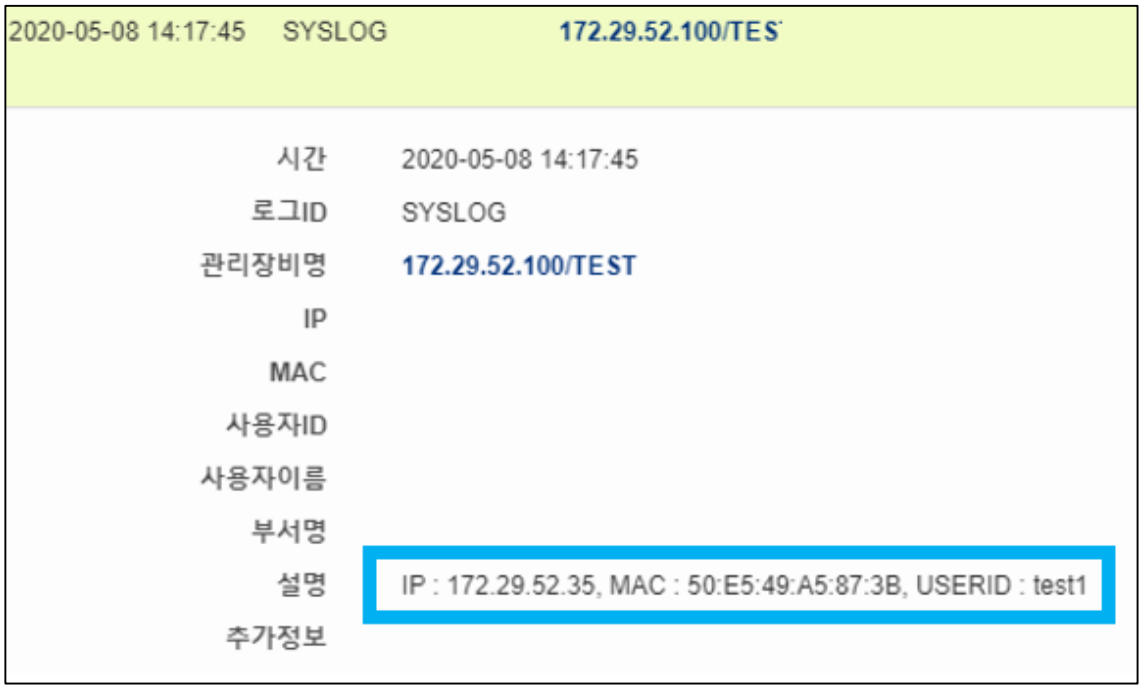


- 로그 메시지 매크로 사용 예제

STEP 1: 메시지 : *TEST IP : {_IP}, MAC : {_MAC}, USERID : {_USERID}* 입력.



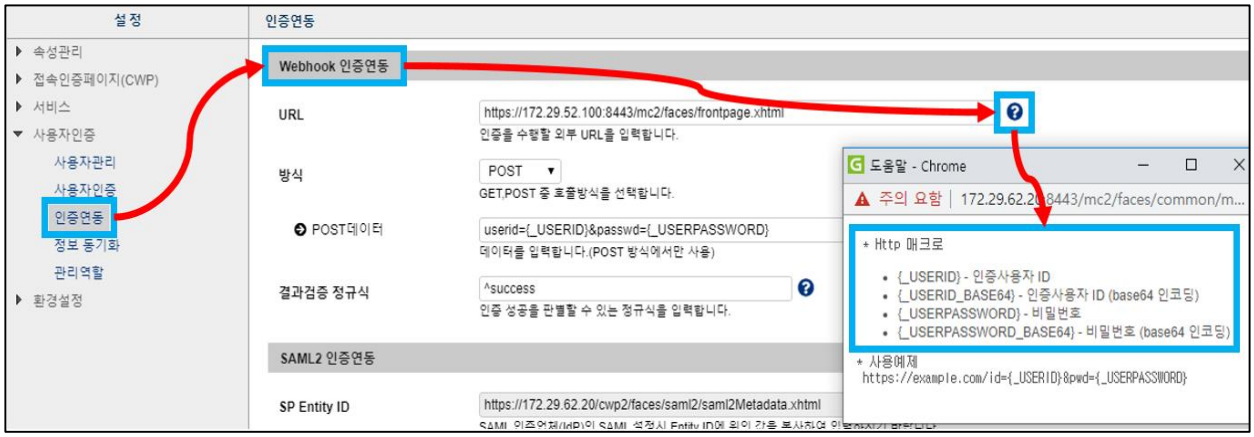
STEP 2: 로그를 발생시킨 후 아래와 같이 메시지 확인.



5.2 Webhook 사용자인증 연동 시 Http 매크로 설정 방법

Http 매크로는 Webhook 방식으로 사용자인증 연동 시 활용 가능합니다.

- 인증 연동 시 주로 {_USERID} - 인증사용자 ID, {_USERPASSWORD} - 비밀번호 등을 활용합니다.
- 상세한 정보는 "설정 – 사용자인증 – 인증연동 – Webhook 인증연동" 항목에서 "?" 아이콘을 클릭하여 확인 가능합니다.



- "POST 데이터" 입력란에는 Http 매크로를 활용할 수 있습니다.

  ※ POST 데이터란 URL 호출 시 전송할 데이터를 뜻하며, 방식이 POST 일 경우에 입력 가능합니다.

  ※ 입력 예제) *userid={_USERID}&userpw={_USERPASSWORD}*

- "결과검증 정규식" 입력란에는 URL 호출 후 응답코드를 통해 성공여부를 판별할 수 있는 값을 입력합니다.

  ※ 응답코드란 Webhook 을 통해 URL 호출 후 외부서버로부터의 성공 혹은 실패에 대한 코드나 문자를 뜻합니다.

  ※ 응답코드의 문자가 "Ok"일 경우 정규식에 "Ok" 입력 혹은 "Good" 으로 시작되는 문자열일 경우 "^Good" 입력합니다. 사용 예제는 아래의 표를 참고하시기 바랍니다.
  (응답코드의 문자열이 간단할 경우 정규식에 그대로 입력해도 무방하지만, 문자열이 긴 경우 시작되는 문자를 활용하여 성공여부를 판별할 수 있도록 앞에 '^' 특수문자를 입력하여 사용합니다.)

외부서버의 응답코드	결과검증 정규식 입력 예제
Ok	*Ok* (또는 *^Ok*)
Success	*Success* (또는 *^Success*)
Good Connect ~~~~	*^Good*

6. 참고

참고페이지 : [Docs] 로그 및 이벤트 관리 - https://docs.genians.com/release/ko/events.html

About the Documentation

본 문서는 Genian NAC의 내용 변경에 따라 주기적으로 업데이트 될 예정입니다.

본 문서에 대해 궁금한 사항이 있을 시 아래의 메일이나 Slack으로 연락바랍니다.

- 연구기획실 연구지원팀 / 김재현 / mkkim@genians.com
- 연구기획실 연구지원팀 / 김용학 / yhkim93@genians.com

추가 반영할 정보 및 포함될 내용에 대한 의견을 주시면 업데이트에 반영하겠습니다.

Notice

본 문서는 Genian NAC와 연동 시 참고 문서 목적으로 만들어졌습니다.

가급적 본 문서 그대로의 외부 유출 및 배포는 삼가해 주시고, 외부 공유가 필요한 경우 용도에 따라 가공 후 제공해 주시기 바랍니다.