



관리자 매뉴얼



저작권정보

Copyright©2003 주식회사 앤앤에스피. All rights reserved.

앤앤에스피 로고, ‘(주)앤앤에스피’로고, ‘nNetDiode’로고는 한국에 있는 (주)앤앤에스피 회사의 상표 또는 등록상표입니다. 이 문서에 설명되어 있는 제품은 사용, 복사, 배포 및 디컴파일/리버스엔지니어링을 제한하는 라이선스 하에 배포됩니다.

이 문서 중 어떤 부분도 (주)앤앤에스피 Corporation 및 해당 라이선스 부여자의 사전 서면 없이는 어떤 방식으로든, 어떤 형태로든, 복제될 수 없습니다.

사용 설명서는 “있는 그대로” 제공되며, 상품성, 특정 목적의 적합성 또는 비침해성에 대한 묵시적 보증을 비롯하여 어떠한 명시적 또는 묵시적인 조건, 진술 및 보증도, 이러한 조건, 진술 및 보증의 배제가 법적으로 무효가 아닌 한 배제됩니다.

(주)앤앤에스피는 이 설명서의 제공, 성능 또는 사용과 관련되는 우발적 손해 또는 결과적 손해에 대한 책임을 지지 않습니다. 이 문서의 포함된 정보는 예고 없이 변경될 수 있습니다.

안내서 내용과 솔루션의 저작권은 컴퓨터 프로그램 보호법으로 보호 받고 있습니다.

nNetDiode V3.0 P10 S

nNetDiode V3.0 P10 R

nNetDiode V3.0 P15 S

nNetDiode V3.0 P15 R

nNetDiode V3.0 E10 S

nNetDiode V3.0 E10 R

nNetDiode V3.0 U10 S/R

상기 표기된 제품은 (주)앤앤에스피의 등록상표입니다.

이외의 회사명이나 제품명은 해당 회사 소유의 등록 상표입니다

(주)앤앤에스피

| | |
|-----|--------------------------------|
| 주 소 | : (06303) 서울특별시 강남구 논현로 100 2층 |
|-----|--------------------------------|

| | |
|----------|---|
| Homepage | : http://www.nnsp.co.kr |
|----------|---|

| | |
|----------|---------------|
| 고객서비스 센터 | : 02-576-4738 |
|----------|---------------|

| | |
|--------|-----------------|
| 기술 지원팀 | : 070-8895-5067 |
|--------|-----------------|

Revision History

| 버전 | 수정일 | 작성자 | 변경 내역 |
|-----|----------|-----|---------|
| 1.0 | 2021.8.9 | 박상현 | 최초 작성 |
| 1.5 | 2022.9.2 | 김지용 | 정책메뉴 수정 |

목 차

| | |
|--|----|
| 제1장 운영환경 | 11 |
| 1. 운영환경 | 12 |
| 1.1 운영 환경 | 12 |
| 1.1.1 기존 일방향 UDP 전송프로그램을 사용하는 경우 | 12 |
| 1.2 운영 시 유의 사항 | 13 |
| 1.2.1 보안 관리 | 13 |
| 1.2.2 절차적 환경 | 15 |
| 1.3 관리자 로그인 환경 | 16 |
| 1.3.1 관리자 UI 로그인 | 16 |
| 제3장 메뉴 구성 | 19 |
| 2. nNetDiode V3.0 메뉴 구성 | 20 |
| 2.1 nNetDiode V3.0 메뉴 구성도 | 20 |
| 2.2 nNetDiode V3.0 메뉴 설명 | 21 |
| 2.2.1 트래픽 통계 | 21 |
| 2.2.2 관리자 통계 | 21 |
| 2.2.3 보안정책 | 21 |
| 2.2.4 로그 정보 | 22 |
| 2.2.5 환경설정 | 23 |
| 제4장 메뉴별 기능 설명 | 25 |
| 3. nNetDiode V3.0 관리자 UI 메뉴별 설명 | 26 |
| 3.1 관리자 접속 및 계정관리 | 26 |
| 3.1.1 관리자 로그인 | 26 |
| 3.1.2 관리자 계정 생성 | 30 |
| 3.1.3 관리자 정보 수정 | 34 |
| 3.1.4 관리자 접속 설정 | 36 |
| 3.1.5 로그인 설정 | 39 |
| 3.2 시스템 모니터링 및 보안이벤트 분석 | 41 |
| 3.2.1 트래픽 통계 | 41 |
| 3.2.2 관리자 통계 | 42 |
| 3.3 보안정책 관리 | 43 |
| 3.3.1 보안정책 | 43 |
| 3.4 보안감사 관리 | 59 |
| 3.4.1 관리자 로그 | 59 |
| 3.4.2 보안 관리 로그 | 60 |

| | |
|-------------------------|-----------|
| 3.4.3 보안 감사 로그 | 60 |
| 3.4.4 접근 통제 로그 | 61 |
| 3.4.5 무결성 로그 | 62 |
| 3.4.6 오류 및 버퍼링 로그 | 62 |
| 3.5 환경 설정 | 63 |
| 3.5.1 시스템 | 63 |
| 3.5.2 로그 관리 | 67 |
| 3.5.3 메일 설정 | 67 |
| 3.5.4 장비소개 관리 | 69 |
| 제4장 부록 | 70 |
| 4. 부록 71 | |
| 4.1 용어설명 | 71 |

표 목차

| | |
|----------------------------------|----|
| [표 1] 관리자 로그인 방법 | 16 |
| [표 2] 관리자 로그인 필요 조건 | 16 |
| [표 3] nNetDiode V3.0 메뉴 구성 | 20 |
| [표 4] 관리자 정보 필수등록 사항 | 31 |
| [표 5] 관리자 로그 종류 | 59 |
| [표 6] 보안 관리 로그 종류 | 60 |

그림 목차

| | |
|--------------------------------------|-----------|
| [그림 1] Web UI 최초 접속 화면 | 17 |
| [그림 2] 관리자 Web UI 로그인 화면 | 17 |
| [그림 3] 관리자 Web UI 로그인 완료 | 18 |
| [그림 4] 관리자 로그인 화면 | 26 |
| [그림 5] 최초 로그인시 비밀번호 변경 화면 | 27 |
| [그림 6] 현재 비밀번호 불일치 오류 화면 | 27 |
| [그림 7] 동일 ID 입력 오류 화면 | 27 |
| [그림 8] 동일 비밀번호 입력 오류 화면 | 28 |
| [그림 9] 새 비밀번호 확인 오류 화면 | 28 |
| [그림 10] 관리자 계정 및 패스워드 입력 오류 화면 | 28 |
| [그림 11] 계정 잠김 알림 화면 | 29 |
| [그림 12] 접속 IP 오류 화면 | 29 |
| [그림 13] 관리자 등록 설정 메뉴 화면 | 30 |
| [그림 14] 관리자 등록 설정 화면 | 30 |
| [그림 15] 관리자 ID 등록 시 오류 화면 | 31 |
| [그림 16] 관리자 비밀번호 제한 글자수 오류 화면 | 31 |
| [그림 17] 관리자 비밀번호 조합 오류 화면 | 32 |
| [그림 18] 관리자 이름 미입력 시 오류 화면 | 32 |
| [그림 19] 관리자 이메일 미입력 시 오류 화면 | 32 |
| [그림 20] 관리자 계정 등록 현황 화면 | 33 |
| [그림 21] 관리자 정보 화면 | 34 |
| [그림 22] 관리자 정보 수정 화면 | 34 |
| [그림 23] 비밀번호 변경 화면 | 35 |
| [그림 24] 관리자 접속 IP 설정 화면 | 36 |
| [그림 25] 관리자 접속 IP 설정 화면 | 36 |
| [그림 26] 관리자 접속 IP 초과 사용 오류 화면 | 37 |
| [그림 27] 관리자 접속 IP 공백 입력 오류 화면 | 37 |
| [그림 28] 관리자 접속 IP 주소형식 오류 화면 | 37 |
| [그림 29] 관리자 접속장비 명 공백 입력 오류 화면 | 38 |
| [그림 30] 계정 잠김 설정 화면 | 39 |
| [그림 31] 로그인 실패 횟수 입력 오류 화면 | 39 |
| [그림 32] 계정 잠김 시간 입력 오류 화면 | 40 |
| [그림 33] 트래픽 통계 화면 | 41 |

| | |
|---|-----------|
| [그림 34] 관리자 통계 화면 | 42 |
| [그림 35] 관리자 접속 현황 검색 화면 | 42 |
| [그림 36] 보안정책 조회 화면 | 43 |
| [그림 37] Syslog 내부 전송 정책..... | 44 |
| [그림 38] Syslog 외부 전송 정책..... | 45 |
| [그림 38] FTP 내부 전송 정책..... | 46 |
| [그림 38] FTP 외부 전송 정책 | 47 |
| [그림 38] SFTP 내부 전송 정책 | 48 |
| [그림 38] SFTP 외부 전송 정책 | 49 |
| [그림 38] DB 내부 전송 정책..... | 50 |
| [그림 38] DB 외부 전송 정책..... | 51 |
| [그림 38] OPC 내부 전송 정책 | 52 |
| [그림 38] OPC 외부 전송 정책 | 53 |
| [그림 39] 보안 정책명 공백 입력시 오류 화면..... | 54 |
| [그림 40] 보안 정책 중복 등록 시 오류 화면 | 54 |
| [그림 41] 출발지 IP주소 공백 입력 시 오류 화면 | 54 |
| [그림 42] 출발지 IP주소 형식이 IPv4 형식이 아닐 경우 오류 화면 | 55 |
| [그림 43] 출발지 수신 포트 입력 값이 숫자가 아닐 경우 오류 화면 | 55 |
| [그림 44] 입력 값이 출발지 수신 포트 범위에 맞지않은 경우 오류 화면 | 55 |
| [그림 45] 일방향 전송 포트 번호가 포트 입력 값이 숫자가 아닌 경우 오류 화면 | 56 |
| [그림 46] 입력 값이 일방향 전송 포트 범위에 맞지않은 경우 오류 화면 | 57 |
| [그림 47] 도착지 IP주소 공백 입력 시 오류 화면 | 57 |
| [그림 48] 도착지 IP주소 형식이 IPv4 형식이 아닐 경우 오류 화면 | 57 |
| [그림 49] 도착지 수신 포트 입력 값이 숫자가 아닐 경우 오류 화면 | 58 |
| [그림 50] 입력 값이 도착지 포트 범위에 맞지않은 경우 오류 화면 | 58 |
| [그림 51] 관리자 로그 화면 | 60 |
| [그림 52] 보안 관리 로그 화면 | 60 |
| [그림 53] 이벤트 로그 화면 | 61 |
| [그림 54] 접근 통제 로그 화면 | 61 |
| [그림 55] 무결성 로그 화면 | 62 |
| [그림 56] 오류 및 버퍼링 로그 화면 | 62 |
| [그림 57] 내부 송신 시스템 설정 화면 | 63 |
| [그림 58] 외부 수신 시스템 설정 화면 | 64 |
| [그림 59] 프로그램 등록 메뉴 화면..... | 65 |
| [그림 60] 프로그램 정보 등록 화면..... | 65 |
| [그림 61] 무결성 점검 화면 | 66 |
| [그림 62] 로그 관리 설정 화면 | 67 |

| | |
|----------------------------|----|
| [그림 63] 메일 설정 화면 | 68 |
| [그림 64] 시스템 메일 상세 내용 | 68 |
| [그림 65] 장비소개 관리 화면..... | 69 |

제 1 장 운영환경

본 장에서는 매뉴얼의 개요, 문서구조 등의 일반사항을 간략히 설명합니다.

1. 운영환경

1.1 운영 환경

nNetDiode V3.0은 보호 받는 보안영역 네트워크(내부)와 非-보안영역 네트워크(외부)를 연결하는 네트워크 장비로 데이터를 일방향으로 전달하는 보안 기능을 수행합니다. 따라서 설치되는 기존 네트워크 환경에 대한 파악은 필수입니다.

가장 효율적이고 안정화된 네트워킹과 철저한 보안의 구현이라는 두 가지 목적을 효과적으로 달성 하기 위해서는 체계적인 네트워크 디자인과 구체적인 설치 계획이 요구됩니다.

다양한 네트워크 환경에서 보편적으로 적용할 수 있는 네트워크 구성 요소들을 설명하면서 네트워크 디자인과 변경 계획 수립 및 구현을 안내합니다.

1.1.1 기존 일방향 UDP 전송프로그램을 사용하는 경우

기존의 일방향 UDP 전송프로그램을 대체하여 nNetDiode V3.0을 사용할 경우 기존 일방향 UDP 전송프로그램은 그대로 사용하고 일방향 UDP 송신서버와 일방향 UDP 수신서버 사이에 nNetDiode V3.0을 설치하고 nNetDiode V3.0의 환경만 UDP 전송 환경으로 설정하면 됩니다.



기존 일방향 UDP 전송 프로그램을 사용하는 경우 일방향 UDP 송신서버와 일방향 UDP 수신서버 사이에 nNetDiode V3.0를 설치하여 사용하면 됩니다.
“제5장 nNetDiode V3.0 메뉴별 설명 > 5.1 UDP 설정” 항목을 참조합니다.

1.2 운영 시 유의 사항

1.2.1 보안 관리

■ 물리적 접근 제한

nNetDiode V3.0은 관리자 이외의 사람으로부터 보호받을 수 있는 장소에 설치되어야 합니다. 또한 내/외부의 네트워크 환경이 변화 될 때 마다, 변화된 환경을 nNetDiode V3.0에 반영하여야만 이전과 동일한 보안 기능을 제공 할 수 있습니다.

■ 관리자 식별 및 인증

관리자는 악의가 없고 nNetDiode V3.0 운용에 필요한 교육을 받았으며, 정해진 ID와 Password를 가지고 허용된 IP 주소에서만 nNetDiode V3.0에 접근이 가능해야 합니다.

■ 사용자 제공 서비스

nNetDiode V3.0은 nNetDiode V3.0가 보호하고 있는 네트워크내의 사용자에게 보안정책에 의해 허용된 서비스 만을 제공합니다. 보호하고자 하는 네트워크 사용자나 각종 서버의 구성을 nNetDiode V3.0가 보호하고 있는 네트워크에 포함되어 있는지 다시 한번 확인 하시기 바랍니다.

■ 관리자 보안관리 시 유의 사항

nNetDiode V3.0은 보안관리 기능을 제공합니다. 따라서 nNetDiode V3.0에 접속 시 인증을 위한 데이터가 외부로 유출되지 않도록 주의해야 하며, 관리자가 자리를 비울 시에는 반드시 관리콘솔 종료 상태를 확인 하시기 바랍니다.

기본적으로 nNetDiode V3.0의 경우 관리자가 WEB 접속 후 10분 동안 사용하지 않았을 경우, nNetDiode V3.0은 자체적으로 연결을 끊습니다. 따라서 연결이 끊겼을 경우 재 접속하여 사용하시기 바랍니다.

■ 지속적인 관리

nNetDiode V3.0은 지속적인 관리가 중요합니다. 관리자는 주기적으로 정책 및 감사기록을 확인하여 외부로부터의 불법적인 침입시도가 발생하지 않았는지 또한 시스템의 이상유무를 확인해야 합니다.

■ 동일한 보안 정책(Secure UDP)

nNetDiode V3.0에서 제공하는 전송 데이터의 기밀성 및 무결성 기능은, 그 특징상 동일한 보안 보안 정책을 설정해야만 전송 데이터의 기밀성 및 무결성을 정상적으로

제공합니다.



nNetDiode Tx와 nNetDiode Rx 간 전송 데이터의 기밀성 및 무결성을 보장하기 위해서는 HDD(Hard Disk Drive) 시리얼 번호 + 시간 값을 인코딩하여 생성한 Pre-Shared Key와 사전에 정의된 암호 알고리즘을 공유하고 있어야 합니다.

Pre-Shared Key에 문제가 발생한 경우, (주)앤앤에스피로 연락 주시기 바랍니다.



보안영역 전송통제서버 nNetDiode Tx와 비보안영역 전송통제서버 nNetDiode Rx 간 전송 데이터의 보호를 위해 기밀성 알고리즘으로는 'AES-256'을 사용하며 무결성 알고리즘으로는 'SHA256'을 사용합니다.

■ 정확한 시간 설정

nNetDiode V3.0의 운용시 발생한 보안 사건의 정확성 및 신뢰성을 위해 정확한 시간 설정이 이루어져야 합니다. nNetDiode V3.0의 운용 전 시스템에 설정된 시간을 다시 한번 확인 바랍니다.

■ 운영 체제에 대한 보강

nNetDiode V3.0은 Windows 운영체제인 Windows10 상에서 동작합니다. 만일 Windows10에 취약점이 발견 된 경우, (주)앤앤에스피에서 이에 대한 패치를 사전 연락 후 방문을 통해 수행합니다.



긴급한 패치가 필요하실 경우, (주)앤앤에스피로 연락 주시기 바랍니다.

1.2.2 절차적 환경

■ 올바른 설치

nNetDiode V3.0은 제품 설명서에 따라 올바르게 설치되어 있어야 합니다.

■ 올바른 설정

알맞은 정책과 설정으로 nNetDiode V3.0이 올바르게 동작할 수 있도록 합니다.

■ 적절한 대처

nNetDiode V3.0의 설치 과정 중에 발생하는 오류사항에 대하여 설치자로 하여금 적절한 조치를 신속히 취하도록 합니다.

1.3 관리자 로그인 환경

nNetDiode V3.0의 안정적인 운용을 위해, 관리자는 로그인 과정을 거쳐야만 합니다. 관리자의 로그인 방법은 아래와 같습니다.

| 로그인 방법 | 설명 |
|--------|--|
| Web UI | Web Browser를 통한 로그인을 나타냅니다. 관리자 로그인은 관리자 ID/PASSWD 방식으로 제공됩니다. |

[표 1] 관리자 로그인 방법

1.3.1 관리자 UI 로그인

시스템 설치 과정이 완료되면, 관리자는 관리자 UI를 통해 로그인 할 수 있습니다. 관리자 UI 로그인을 위해서는 다음의 조건이 충족되어야 합니다.

| 항목 | 내용 |
|----------------|---|
| Network | 보안영역 전송통제서버인 nNetDiode Tx가 연결 가능한 Network에 존재해야 합니다. |
| 관리자 IP address | Install 과정 중 등록한 최고 관리자 IP address나 최고 관리자에 의해 추가된 관리자 IP address만이 nNetDiode V3.0에 로그인 할 수 있습니다. Network으로 접속 가능하다 하더라도 IP address가 등록되지 않으면 해당 관리자 PC는 nNetDiode V3.0에 접속 할 수 없습니다. |
| 관리자 계정 | 관리자 IP address가 nNetDiode V3.0에 등록되어 있다 하더라도, 로그인 하고자 하는 관리자의 계정 정보가 nNetDiode V3.0에 등록되어 있지 않으면 로그인 할 수 없습니다. |

[표 2] 관리자 로그인 필요 조건

위 조건이 충족되면 다음의 순서에 의해 로그인 할 수 있습니다. 로그인 절차는 다음과 같습니다.

- ① 아래 그림과 같이 Internet Explorer를 실행하여, 아래와 같은 IP address를 입력합니다.

WebUI 접속 주소:
<https://200.20.10.2:8443>



[그림 1] Web UI 최초 접속 화면

이 화면은 관리콘솔 접근 시 nNetDiode V3.0과의 암호화 통신에 사용되는 SSL 암호 알고리즘에 사용되는 자체 발급한 인증서를 사용하기 때문에 나타나는 Chrome Browser의 경고 화면입니다.

- ② 관리자 로그인 진행을 위해 "이 웹사이트를 계속 탐색합니다(권장하지 않음)"을 선택합니다. 이후 다음과 같은 관리자 로그인 화면이 나타납니다.

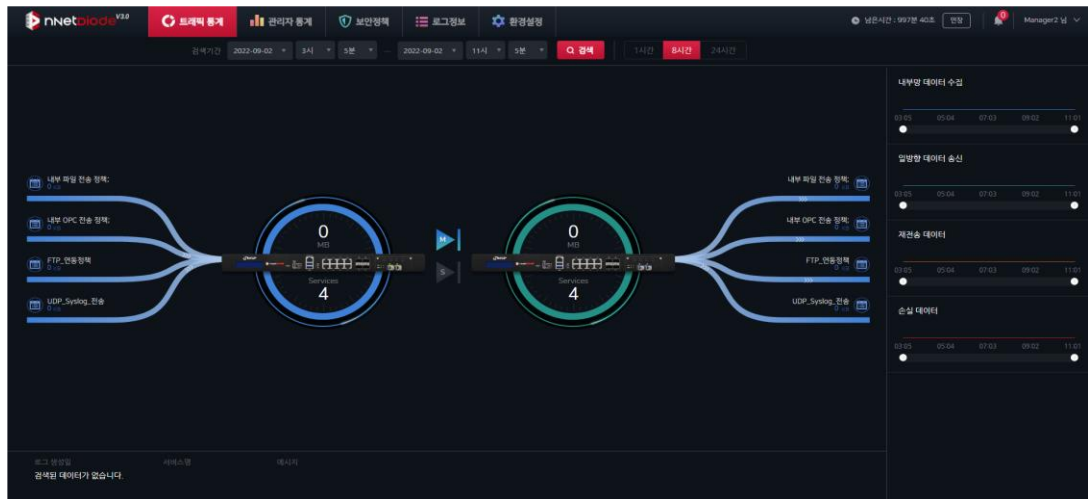


[그림 2] 관리자 Web UI 로그인 화면

관리자의 로그인 방식은 앞서 기술한 바와 같이, 관리자 ID/PASSWD 방식으로 제공됩니다.

1.3.1.1 비밀번호 로그인 방식

nNetDiode V3.0에서 기본적으로 제공되는 ID와 Install 과정 중 입력한 최고 관리자 비밀번호나 최고 관리자에 의해 추가된 관리자의 ID와 Password를 입력하여 Web UI에 로그인 합니다. 이후 다음과 같은 화면이 나타나면, 정상 로그인 된 것입니다.



[그림 3] 관리자 Web UI 로그인 완료

제 3 장 메뉴 구성

본 장에서는 nNetDiode V3.0의 관리자 UI 메뉴 구성에 대해 설명합니다.

2. nNetDiode V3.0 메뉴 구성

2.1 nNetDiode V3.0 메뉴 구성도

nNetDiode V3.0의 메뉴는 다음과 같이 구성되어 있습니다.

| 대분류 | 중분류 | 소분류 |
|--------|-------------|--------------|
| 트래픽 통계 | | |
| 관리자 통계 | | |
| 보안정책 | | |
| 로그 정보 | 관리자 로그 | |
| | 보안 관리 로그 | |
| | 보안 감사 로그 | |
| | 접근 통제 로그 | |
| | 무결성 로그 | |
| | 오류 및 버퍼링 로그 | |
| 환경설정 | 관리자 | 관리자 등록 |
| | | 관리자 접속 설정 |
| | | 로그인 설정 |
| | 시스템 | 내부 송신 시스템 설정 |
| | | 외부 수신 시스템 설정 |
| | | 프로그램 등록 |
| | | 자체 보호 |
| | 기타 | 로그 관리 |
| | | 메일 설정 |
| | | 장비 소개 관리 |

[표 3] nNetDiode V3.0 메뉴 구성

2.2 nNetDiode V3.0 메뉴 설명

2.2.1 트래픽 통계

nNetDiode V3.0은 일방향 전송 트래픽에 대한 기능을 제공합니다. 네트워크 트래픽 현황은 보안영역에서 보안영역 전송통제서버인 nNetDiode Tx로 전송한 트래픽을 표현한 내부망 데이터 수집, 보안영역 전송통제서버인 nNetDiode Tx에서 비보안영역 전송통제서버인 nNetDiode Rx로 일방향 전송한 트래픽을 표현한 일방향 데이터 송신에 대한 네트워크 트래픽 현황을 통계로 보여줍니다.

2.2.2 관리자 통계

nNetDiode V3.0은 관리자 접속 로그에 대한 통계 기능을 제공합니다. 관리자 접속 현황은 관리자의 접근 현황, 정책 변경 현황, 운영환경 변경 현황 등 관리자의 모든 행위 현황을 통계로 보여줍니다.

2.2.3 보안정책

보안정책은 보안영역 전송통제서버인 nNetDiode Tx와 비보안영역 전송통제서버인 nNetDiode Rx의 일방향 데이터 전송에 적용되는 전송 통제 정책을 설정합니다.

■ 전송 통제 정책 관리

보안영역 전송통제서버 nNetDiode Tx로 전송한 데이터를 비보안영역 전송통제서버 nNetDiode Rx로 일방향 전송하기 위한 서비스 포트 및 환경을 설정합니다.

전송 통제 정책은 정책명, 서비스 타입, 서비스, 내부 프로그램, 외부 프로그램 등과 출발지 IP, 출발지 수신 포트, 일방향 전송 포트, 도착지 IP, 도착지 포트 등으로 이루어진 경로들을 등록, 수정, 삭제할 수 있습니다.



일방향 전송 포트는 nNetDiode Tx에서 nNetDiode Rx로 데이터를 전송하는 Secure UDP 포트로 보안영역에서 nNetDiode Tx로 전송하는 프로토콜 포트와 무관합니다.

2.2.4 로그 정보

■ 관리자 로그

관리자 로그에서는 관리자 행위로 발생한 로그를 조회할 수 있습니다. 관리자 행위 로그로는 로그인 성공 및 실패 시 발생하는 로그, 관리자 계정 생성 및 수정 시 발생하는 로그, 로그아웃 시 발생하는 로그, 관리자 접속 및 제한 정책 수정 시 발생하는 로그 등이 있습니다.

■ 보안 관리 로그

보안 관리 로그에서는 관리자가 보안정책을 추가, 삭제, 변경한 행위로 발생한 로그를 조회할 수 있습니다. 보안 관리 로그로는 전송통제 보안정책의 추가, 삭제, 변경 시 발생하는 로그, 시스템 정보 변경 시 발생하는 로그, 메일 전송 정보 변경 시 발생하는 로그 등이 있습니다.

■ 보안 감사 로그

보안 감사 로그에서는 이벤트 로그를 조회할 수 있습니다. 이벤트 로그는 서비스 시작 및 중지 시에 대한 로그를 나타내며,

■ 접근 통제 로그

접근 통제 로그를 조회할 수 있습니다. 접근 통제 로그는 보안영역 서버 또는 非-보안영역 서버의 접근 허용 및 거부 시에 대한 로그를 나타냅니다.

■ 무결성 로그

무결성 로그를 조회할 수 있습니다. 무결성 로그는 서비스 프로그램에 대해 자체 무결성 보장하기 위한 검사를 수행 하였을 때 발생한 로그를 나타냅니다.

■ 오류 및 버퍼링 로그

오류 및 버퍼링 로그를 조회할 수 있습니다. 오류 및 버퍼링 로그는 nNetDiode V3.0에서 등록되어 수행하는 내부/외부 프로그램에서 오류 및 버퍼링이 있을 경우 발생하는 로그를 나타냅니다.

2.2.5 환경설정

2.2.5.1 관리자

■ 관리자 등록 설정

nNetDiode V3.0에서는 인가된 관리자에 대한 계정을 등록하는 기능을 제공합니다.

관리자 정보는 관리자 ID, 비밀번호, 이름, 부서, 직급, 유선전화, 휴대전화, 이메일 주소, 비고로 구성이 되며, 관리자 ID, 비밀번호, 이름, 이메일 주소는 필수 입력 사항입니다.

■ 관리자 접속 설정

nNetDiode V3.0에서는 인가된 관리자가 보안영역 전송통제서버인 nNetDiode Tx에 접속 할 수 있는 IP 를 설정합니다. IP는 최대 2까지만 등록이 가능합니다.

■ 로그인 설정

nNetDiode V3.0에서는 인가된 관리자가 로그인 인증 시 실패 횟수 및 실패 횟수를 초과했을 때 일정 시간 동안 접속을 제한하는 기능을 제공합니다.

2.2.5.2 시스템

■ 내부 송신 시스템 설정

내부 시스템의 수신 네트워크 정보 및 송신 네트워크 정보를 확인하고 시스템을 재 시작하는 기능을 제공합니다. 또한 보안영역 전송통제서버인 nNetDiode Tx의 세부 버전 정보를 확인할 수 있습니다.

■ 외부 수신 시스템 설정

외부 시스템의 수신 네트워크 정보 및 송신 네트워크 정보를 설정하고 시스템을 재 시작하는 기능을 제공합니다. 또한 비보안영역 전송통제서버인 nNetDiode Rx의 세부 버전 정보를 확인할 수 있습니다.

■ 프로그램 등록

보안정책에 의해 등록되어 실행하게 되는 보안영역에서 전송하는 데이터를 수집하여 nNetDiode Rx로 전달하는 기능을 수행하는 내부 프로그램과 nNetDiode Rx로 전달된 데이터를 비보안영역으로 배포하는 기능을 수행하는 외부프로그램을 등록, 수정 삭제 할 수 있습니다.

■ 자체 보호

서비스 프로그램에 대해 자체 무결성을 보장하기 위한 검사 수행 합니다. 무결성 검사는 관리자가 직접 무결성 검사를 실행 할 수 있으며, 일정 주기마다 시간을 설정하여 자동적으로 검사할 수 있습니다. 또한 서비스 프로그램의 업데이트 시 무결성 값을 업데이트 할 수 있습니다.

2.2.5.3 기타

■ 로그 관리

로그 관리에서는 로그 저장소 용량에 대한 임계 값을 설정합니다.

■ 메일 설정

메일 설정에서는 시스템의 디스크 용량 초과 및 시스템 내 서비스 프로그램이 손상되었을 경우 등 시스템 운영상에 문제가 발생 했을 시 관리자에게 경고 메일을 전송할 메일 서버 환경을 설정합니다.

■ 장비소개 관리

서비스 프로그램에 대해 자체 무결성을 보장하기 위한 검사 수행 합니다. 무결성 검사는 관리자가 직접 무결성 검사를 실행 할 수 있으며, 일정 주기마다 시간을 설정하여 자동적으로 검사할 수 있습니다. 또한 서비스 프로그램의 업데이트 시 무결성 값을 업데이트 할 수 있습니다.

제 4 장 메뉴별 기능 설명

본 장에서는 nNetDiode V3.0 관리자 UI 메뉴별 기능에 대해 설명합니다.

3. nNetDiode V3.0 관리자 UI 메뉴별 설명

3.1 관리자 접속 및 계정관리

3.1.1 관리자 로그인

관리자가 관리자 UI를 통하여 nNetDiode V3.0에 원격 접속하면 관리자 로그인 창이 뜨며 계정 및 비밀번호를 입력하고 로그인합니다.



초기 로그인할 경우 설치 시 입력한 관리자 계정과 비밀번호로 로그인합니다.



[그림 4] 관리자 로그인 화면



비밀번호 입력 시 보안을 위하여 비밀번호는 *****로 표시됩니다.

■ 최초 로그인 시 관리자 암호 변경

보안을 위해 최초 로그인 시에는 아래와 같이 아이디 및 비밀번호 변경 팝업이 나타나며, 이상 없이 변경해야만 접근이 가능합니다.



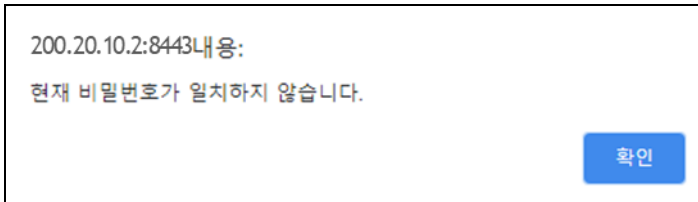
The image shows a web form titled "계정 및 비밀번호 변경" (Account and Password Change). It contains four input fields: "현재 비밀번호" (Current Password), "새 아이디" (New ID), "새 비밀번호" (New Password), and "새 비밀번호 확인" (Confirm New Password). At the bottom right, there are two buttons: "취소" (Cancel) and "변경" (Change).

[그림 5] 최초 로그인시 비밀번호 변경 화면

※ 초기 계정 및 비밀번호 변경 시 발생할 수 있는 오류 메시지들은 다음과 같습니다.

■ 현재 비밀번호 불일치 시

현재 등록된 관리자의 비밀번호가 일치하지 않을 때 발생하는 메시지입니다.

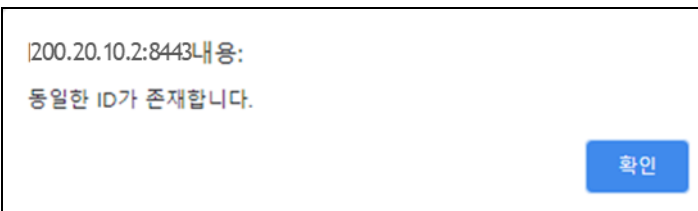


The image shows an error message box with the text: "200.20.10.2:8443내용: 현재 비밀번호가 일치하지 않습니다." (200.20.10.2:8443 Content: Current password does not match). There is a blue "확인" (Confirm) button at the bottom right.

[그림 6] 현재 비밀번호 불일치 오류 화면

■ 동일 아이디 입력 시

현재 등록된 관리자의 새 아이디와 동일한 아이디가 존재할 경우 발생하는 메시지입니다.

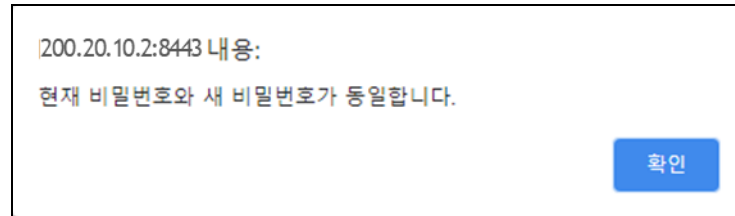


The image shows an error message box with the text: "200.20.10.2:8443내용: 동일한 ID가 존재합니다." (200.20.10.2:8443 Content: Duplicate ID exists). There is a blue "확인" (Confirm) button at the bottom right.

[그림 7] 동일 ID 입력 오류 화면

■ 동일 비밀번호 입력 시

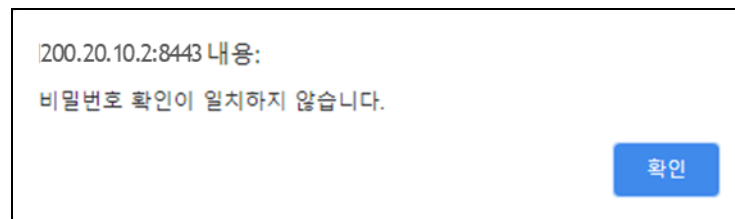
현재 등록된 관리자의 비밀번호와 새 비밀번호 값이 일치할 때 발생하는 메시지입니다.



[그림 8] 동일 비밀번호 입력 오류 화면

■ 비밀번호 확인 불일치 시

새 비밀번호 입력 시 새 비밀번호 확인 값과 다를 경우 발생하는 메시지입니다.

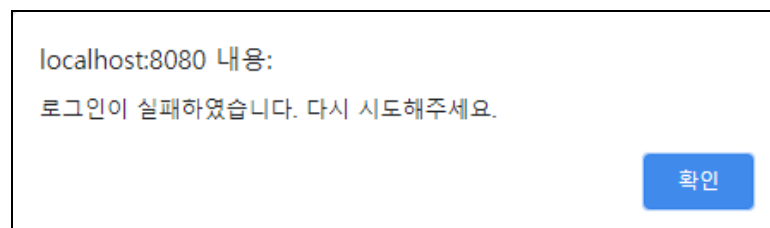


[그림 9] 새 비밀번호 확인 오류 화면

관리자 UI 로그인 시 발생할 수 있는 오류 메시지들은 다음과 같습니다.

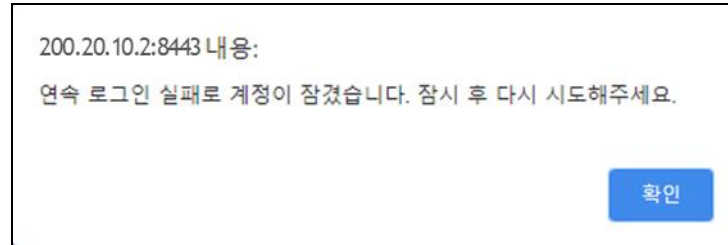
■ 로그인 실패 시

관리자 계정이나 비밀번호를 잘못 입력 할 경우 표시되는 메시지입니다.



[그림 10] 관리자 계정 및 패스워드 입력 오류 화면

관리자가 계정 및 비밀번호 입력을 설정된 횟수 이상 잘못 입력하면, 설정된 시간만큼 로그인에 제한됩니다. 연속 로그인 실패로 계정이 잠겼을 경우 표시되는 메시지는 아래와 같습니다



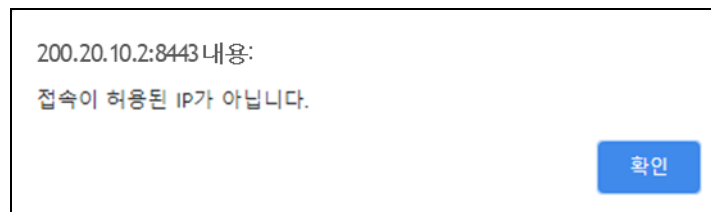
[그림 11] 계정 잠김 알림 화면



관리자가 계정 및 비밀번호 입력을 설정된 횟수(default = 5회)이상 잘못 입력하면, 설정된 시간(default = 10분)만큼 로그인에 제한됩니다.

■ 로그인 IP 제한

관리자 로그인 시 접속 허용 IP에 등록되지 않은 IP에서 접근 할 경우 아래와 같이 팝업을 띄우며 접근을 제한합니다.



[그림 12] 접속 IP 오류 화면



접속 IP 설정은 <환경설정> ▷ <관리자> ▷ <관리자 접속 설정>에서 추가 또는 변경할 수 있습니다.

3.1.2 관리자 계정 생성

<관리자 등록>에서는 계정을 최대 10개까지 등록할 수 있으며, 하나의 계정으로만 로그인 가능 합니다. 관리자 생성 순서는 다음과 같습니다.

- ① <환경설정> ▷ <관리자> ▷ <관리자 등록> 메뉴를 클릭하십시오.
- ③ 오른쪽 상단의 [관리자 등록] 버튼을 클릭하십시오.

| 관리자 등록 | | | | | | | | | | |
|--------|----------------|----------|--------------------|-----|----|-------------|---------------|---------------------|-----------|----|
| 관리자 등록 | | | | | | | | | | |
| 순번 | 관리자 ID | 이름 | 이메일 | 부서 | 직급 | 유선전화 | 휴대전화 | 등록일시 | 비고 | 삭제 |
| 1 | nnd3Manager | Manager | nnspp@nnspp.co.kr | 연구소 | 과장 | 02-123-1111 | 010-1234-1111 | 2022-07-01 01:33:57 | test test | |
| 2 | nnd2Manager | Manager2 | nnspp2@nnspp.co.kr | | | 02-123-2222 | | 2022-07-01 01:33:57 | test | |
| 3 | nnd3ManagerKH5 | Manager | nnspp@nnspp.co.kr | 연구소 | 과장 | 02-123-1111 | 010-1234-1111 | 2022-07-01 01:33:57 | test test | |
| 4 | nnspp | Manager | nnspp@nnspp.co.kr | | | | | 2022-07-01 01:33:57 | test | |

[그림 13] 관리자 등록 설정 메뉴 화면

- ④ 관리자 정보를 정확히 입력한 후 화면 하단의 [등록하기] 버튼을 클릭하십시오.

관리자 등록

필수입력

관리자 ID

비밀번호

이름

이메일 주소

직접선택

* 영문자, 숫자, 특수문자 3가지 조합

선택입력

부서

직급

유선전화

휴대전화

설명

취소하기

등록하기

[그림 14] 관리자 등록 설정 화면

관리자 등록 시 필수 입력 사항은 반드시 등록을 해야 하며, 필수 입력 사항은 [표 7]과 같습니다.

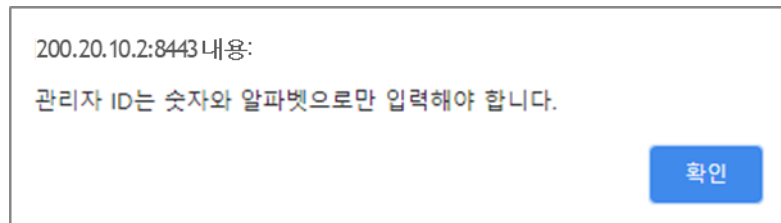
| 항목 | 기능설명 |
|--------|--|
| 관리자ID | nNetDiode 관리자 식별자를 입력합니다. |
| 비밀번호 | nNetDiode 관리자 비밀번호를 입력합니다. |
| 이름 | nNetDiode 관리자의 실제 이름을 입력합니다. |
| 이메일 주소 | nNetDiode 관리자의 이메일 주소를 입력합니다. |
| 등록 버튼 | 관리자 필수 사항 입력이 완료되면 등록 버튼을 누르면 등록이 완료됩니다. |

[표 4] 관리자 정보 필수등록 사항

※ 관리자 계정 생성 시 발생할 수 있는 오류 메시지들은 다음과 같습니다.

■ 관리자 ID 등록 시

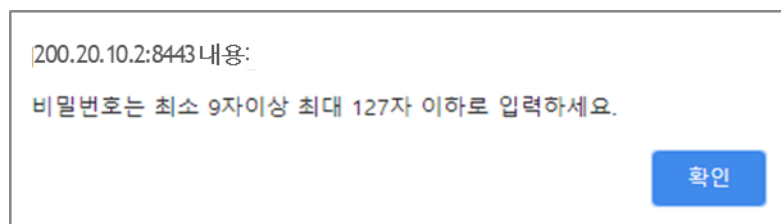
관리자 등록 시 ID는 숫자와 알파벳으로만 입력이 가능하며, 이외의 문자가 입력될 경우 아래와 같은 메시지가 출력됩니다.



[그림 15] 관리자 ID 등록 시 오류 화면

■ 관리자 비밀번호 등록 시 제약사항

관리자 등록 시 비밀번호는 최소 9자 이상 최대 127자 이하 및 영대소문자, 숫자, 특수문자(! @ # \$ % ^ & * ? _ ~) 3개의 조합으로 입력이 가능하며, 조합 조건이 맞지 않을 경우 아래와 같은 메시지가 출력됩니다.



[그림 16] 관리자 비밀번호 제한 글자수 오류 화면

200.20.10.2:8443 내용:

비밀번호는 영문, 숫자, 특수문자 3개 조합으로 입력하세요.

확인

[그림 17] 관리자 비밀번호 조합 오류 화면



비밀번호는 최소 9자 이상 최대 127자 이하이며 숫자, 특수문자(! @ # \$ % ^ & * ? _ ~), 대/소문자 중 3가지 이상 조합으로 구성되어야 합니다. 또한 비밀번호 입력을 설정된 횟수(default = 5회)이상 실패 시 설정된 시간(default = 10분) 동안 로그인에 금지됩니다. 설정 횟수와 시간은 <환경설정> > <관리자> > <로그인 설정> 에서 변경할 수 있습니다.

■ 관리자 이름 공백 입력 시

관리자 등록 시 이름은 해당 관리자의 성명을 의미하며, 문자열 제약이 없으나 아무것도 입력하지 않을 경우 아래와 같은 메시지를 출력합니다.

200.20.10.2:8443 내용:

이름을 입력하세요.

확인

[그림 18] 관리자 이름 미입력 시 오류 화면

■ 관리자 이메일 공백 입력 시

관리자 이메일 등록 시 문자열에 대한 제한이 없으나 아무것도 입력하지 않을 경우 아래와 같은 메시지가 출력됩니다.

200.20.10.2:8443 내용:

이메일 주소를 입력하세요.

확인

[그림 19] 관리자 이메일 미입력 시 오류 화면

관리자가 등록이 되면 아래 그림과 같이 관리자 목록에 추가 됩니다.

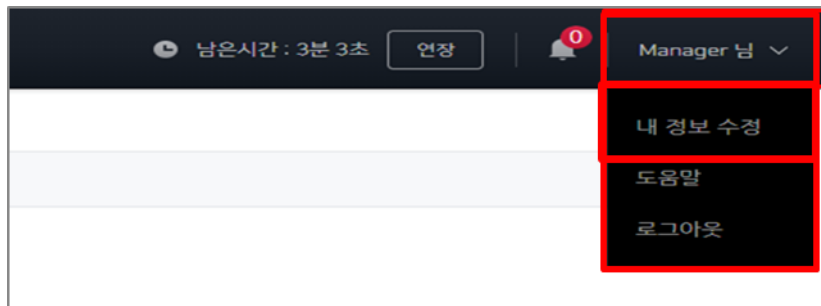
| 관리자 등록 관리자 접속 설정 로그인 설정 | | | | | | | | | | |
|-----------------------------|----------------|----------|----------------|-----|----|-------------|---------------|---------------------|-----------|----|
| 관리자 등록 | | | | | | | | | | |
| 순번 | 관리자 ID | 이름 | 이메일 | 부서 | 직급 | 유선전화 | 휴대전화 | 등록일시 | 비고 | 삭제 |
| 1 | nnd3Manager | Manager | nns@nns.co.kr | 연구소 | 과장 | 02-123-1111 | 010-1234-1111 | 2022-07-01 01:33:57 | test test | |
| 2 | nnd2Manager | Manager2 | nns2@nns.co.kr | | | 02-123-2222 | | 2022-07-01 01:33:57 | test | |
| 3 | nnd3ManagerKHS | Manager | nns@nns.co.kr | 연구소 | 과장 | 02-123-1111 | 010-1234-1111 | 2022-07-01 01:33:57 | test test | |
| 4 | nns | Manager | nns@nns.co.kr | | | | | 2022-07-01 01:33:57 | test | |

[그림 20] 관리자 계정 등록 현황 화면

3.1.3 관리자 정보 수정

관리자의 개인 정보를 수정할 경우에는 아래 절차를 수행합니다.

- ① 메인 화면의 우측 상단에 있는 [관리자 님] 버튼을 클릭하고, 아래 메뉴에서 <내 정보 수정> 메뉴를 클릭합니다.



[그림 21] 관리자 정보 화면

- ② 관리자 정보수정 화면에서는 현재 로그인 한 관리자의 정보를 보여주며, 정보 수정 후 우측 하단의 [수정] 버튼을 클릭하여 내용을 저장합니다.

내 정보 수정

필수입력

이름

Manager

비밀번호

비밀번호 변경

이메일 주소

nensp

@

nensp.co.kr

직접선택

선택입력

부서

연구소

직급

과장

유선전화

02-123-1111

휴대전화

010-1234-1111

설명

test
test

취소하기

수정하기

[그림 22] 관리자 정보 수정 화면

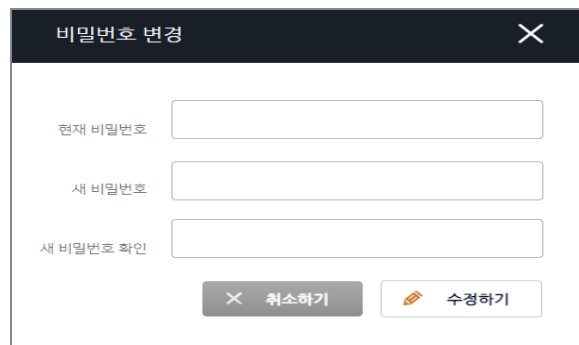
※ 관리자 계정 수정 시 발생할 수 있는 오류 메시지들은 다음과 같습니다.

■ 관리자 이름 수정 시

관리자 정보 수정 시 이름은 해당 관리자의 성명을 의미하며, 문자열에 대한 제한이 없으나 아무것도 입력하지 않을 경우 [그림 19]와 같은 메시지 팝업이 출력됩니다.

■ 관리자 비밀번호 수정 시

관리자 정보 수정 시 비밀번호를 변경하기 위해서는 [비밀번호 변경] 버튼을 눌러 아래와 같은 팝업창에서 변경을 수행합니다. 여기서, 비밀번호가 9자 이상 127자 이하 및 영대소문자, 숫자, 특수문자(! @ # \$ % ^ & * ? _ ~) 조합이 아닐 경우 [그림 17], [그림 18]과 같은 메시지가 출력됩니다.



비밀번호 변경

현재 비밀번호

새 비밀번호

새 비밀번호 확인

취소하기 수정하기

[그림 23] 비밀번호 변경 화면

■ 관리자 이메일 수정 시

관리자 이메일 수정 시 문자열에 대한 제한이 없으나 공백 또는 입력란에 입력하지 않을 경우 [그림 20]과 같은 메시지가 출력됩니다.

3.1.4 관리자 접속 설정

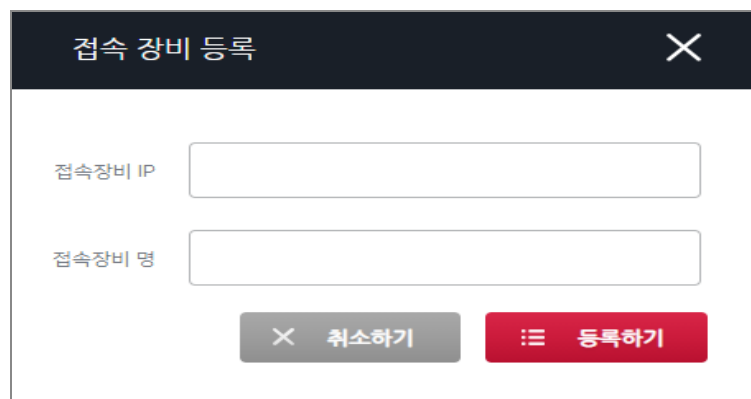
<관리자 접속 설정> 화면에서는 관리 프로그램에 접근 할 수 있는 허용 IP를 등록합니다. 관리자는 등록된 허용 IP에서만 접근이 가능하며, 최대 2개까지 허용 IP를 등록할 수 있습니다. 설정 방법은 아래와 같습니다.

- ① <환경설정> ▷ <관리자> ▷ <관리자 접속 설정> 메뉴를 클릭하십시오.
- ② 관리자 접속 IP의 수정 및 사용 여부를 변경 할 수 있으며, 등록 시 목록 상단의 [접속 장비 등록] 버튼을 클릭하여 접속 장비 등록 팝업을 띄우십시오.



[그림 24] 관리자 접속 IP 설정 화면

- ③ 접속 장비 등록 팝업에서 접속장비 IP 와 접속장비 명을 입력한 후 [등록하기] 버튼을 클릭하여 새로운 접속장비 IP를 등록하게 됩니다.

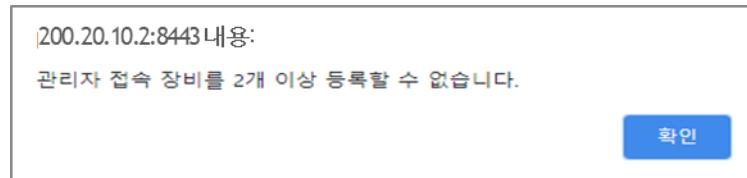


[그림 25] 관리자 접속 IP 설정 화면

※ 관리자 접속 설정 시 발생할 수 있는 오류 메시지들은 다음과 같습니다.

■ 관리자 접속 IP 초과 입력 시

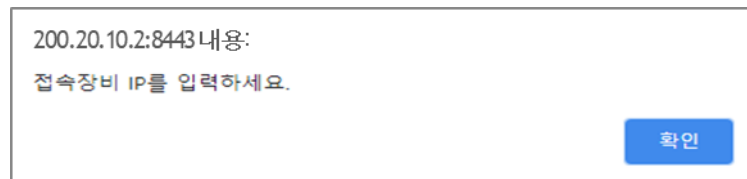
관리자 접속이 허용된 IP의 총 개수는 2개를 초과 할 수 없으며, 초과 시 아래와 같은 메시지가 출력됩니다.



[그림 26] 관리자 접속 IP 초과 사용 오류 화면

■ 관리자 접속 IP 공백 입력 시

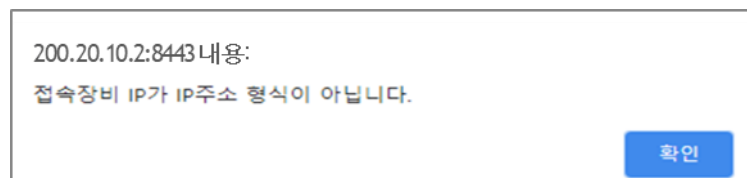
관리자 접속 IP를 등록할 때, 입력란이 공백이거나 미 입력하여 등록할 경우 다음과 같은 메시지 팝업이 출력됩니다.



[그림 27] 관리자 접속 IP 공백 입력 오류 화면

■ 관리자 접속 IP 등록 시 IPv4 형식이 아닌 경우

관리자 접속 IP를 등록할 때, IP가 IPv4 형식이 아니거나 문자열이 포함된 경우 아래와 같이 메시지 팝업이 출력됩니다.



[그림 28] 관리자 접속 IP 주소형식 오류 화면

■ 관리자 접속장비 명 공백 입력 시

관리자 접속장비 명을 등록할 때, 입력란이 공백이거나 미 입력하여 등록할 경우 다음과 같은 메시지 팝업이 출력됩니다.



[그림 29] 관리자 접속장비 명 공백 입력 오류 화면



관리자 접속 IP는 최대 2개까지 설정할 수 있습니다. 관리자는 동시에 한 개의 IP로 접근이 되며, 먼저 접근한 계정이 종료됩니다.

3.1.5 로그인 설정

로그인 설정은 관리자가 일정 횟수 이상 로그인을 실패 할 경우에 접근을 제한하는 정책을 설정하는 화면입니다. 계정 잠금 로그인 실패 횟수는 암호가 잘못 입력 되는 경우 제한 하기 위한 횟수를 나타내고, 계정 잠금 시간은 로그인 실패 횟수가 설정 값을 초과 했을 때 접근을 제한하는 시간입니다. 설정 방법은 아래와 같습니다.

- ① <환경설정> ▷ <관리자> ▷ <로그인 설정> 메뉴를 클릭하십시오.
- ② 화면의 계정 잠금 로그인 실패 횟수와 계정 잠금 시간을 입력한 후 우측 [수정] 버튼을 클릭하십시오.

[그림 30] 계정 잠금 설정 화면

※ 로그인 설정 시 발생할 수 있는 오류 메시지들은 다음과 같습니다.

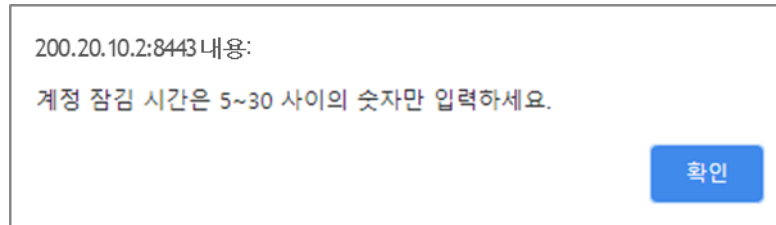
■ 계정 잠금 로그인 실패 횟수 수정 시

계정 잠금에 대한 로그인 실패 횟수 수정 시 2에서 5사이의 숫자를 입력해야 하며, 범위가 벗어났을 경우 아래와 같은 메시지 팝업이 출력됩니다.

[그림 31] 로그인 실패 횟수 입력 오류 화면

■ 계정 잠금 시간 수정 시

계정 잠금 시간 수정 시 5에서 30사이의 숫자를 입력해야 하며, 범위가 벗어났을 경우 아래와 같은 메시지가 출력됩니다.



[그림 32] 계정 잠금 시간 입력 오류화면



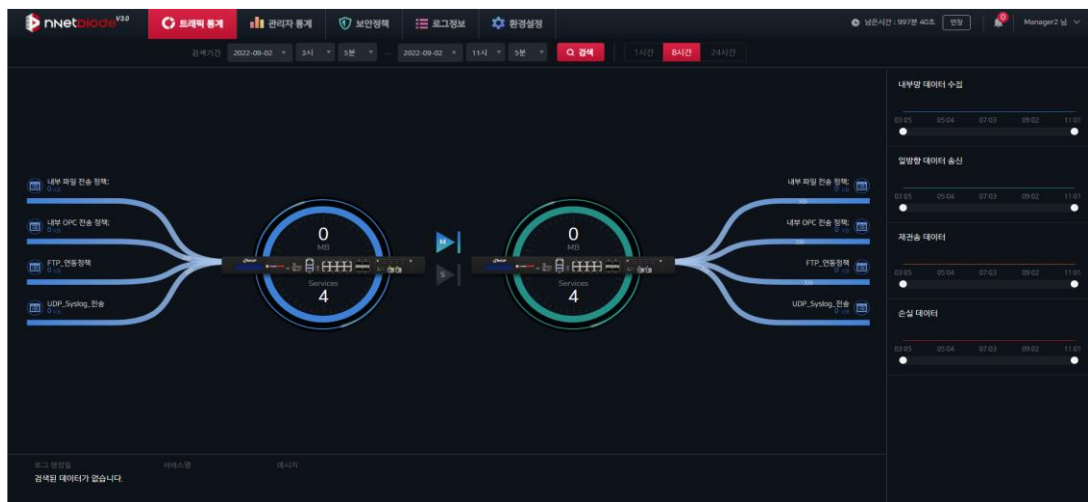
계정 잠금 로그인 실패 횟수의 디폴트 값은 5회이며, 계정 잠금 시간 디폴트 값은 10분입니다.

3.2 시스템 모니터링 및 보안이벤트 분석

3.2.1 트래픽 통계

네트워크 트래픽 현황에서는 보안영역과 보안영역 전송통제서버인 nNetDiode Tx 간, nNetDiode Tx와 비보안영역 전송통제서버인 nNetDiode Rx 간의 네트워크 트래픽 현황을 차트로 확인 할 수 있습니다.

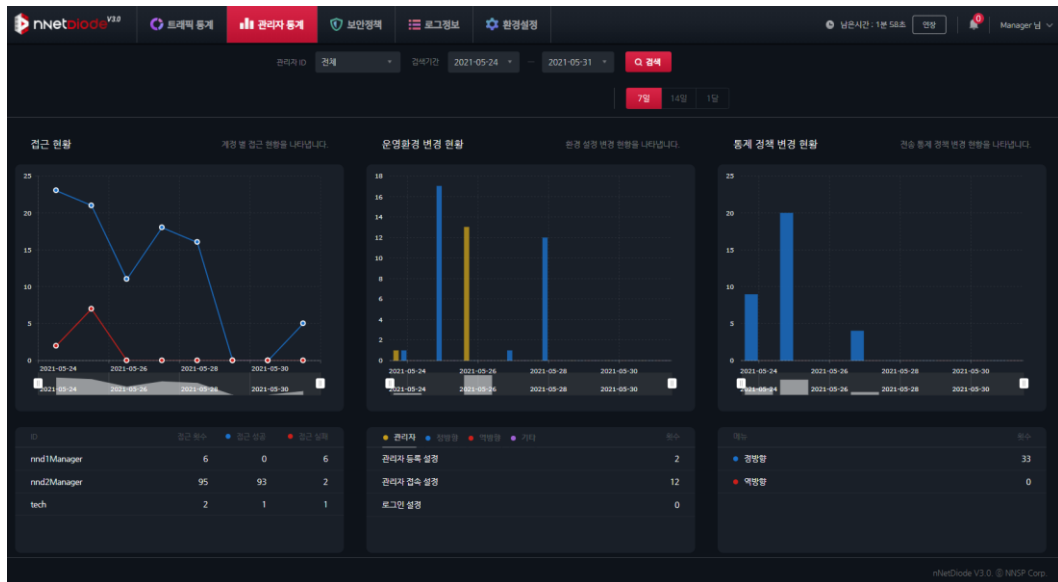
또한, 네트워크 절체 및 오류 등이 발생할 경우 전송하지 못한 데이터를 재전송 하는 현황을 확인할 수 있습니다. 일정 사이즈 이상(2GB) 데이터가 전송되지 않을 시 이후 데이터를 수신하지 않으며, 수신되지 않은 데이터는 데이터 전송 손실 차트에 표시됩니다.



[그림 33] 트래픽 통계 화면

3.2.2 관리자 통계

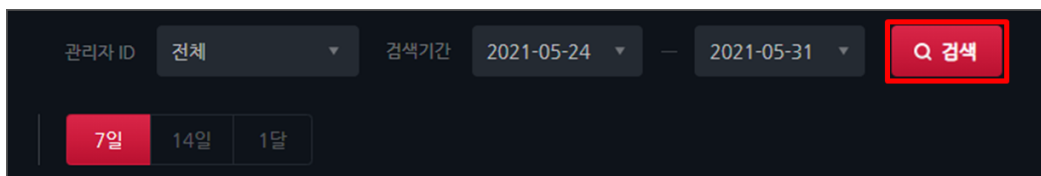
관리자 통계에서는 관리자의 접근, 정책 변경, 운영환경 변경 등 모든 행위 현황에 대한 통계를 보여줍니다.



[그림 34] 관리자 통계 화면

사용 방법은 다음과 같습니다.

- ③ <관리자 통계> 메뉴를 클릭하십시오.
- ④ 특정 관리자에 대한 정보를 보기 위해서는 상단 [관리자 ID] 셀렉트 박스를 클릭하여 관리자를 선택합니다.
- ④ 검색기간 입력란을 클릭하여 날짜를 설정한 후 우측의 [검색] 버튼을 클릭합니다.



[그림 35] 관리자 접속 현황 검색 화면

3.3 보안정책 관리

3.3.1 보안정책

데이터를 수신과 전송을 하기 위한 정책을 확인 및 등록, 수정, 삭제를 할 수 있습니다. 화면 접근 방법은 탭 메뉴인 <보안정책> 메뉴를 클릭하여 보안정책 화면으로 이동하여 접근합니다.

※ 사용하고 있지 않은 보안정책은 회색으로 흐릿하게 표시됩니다.

- ① <보안정책> 메뉴를 클릭하십시오.
- ② 보안 정책의 수정 및 삭제가 가능하며 정책 등록 시 화면의 좌측 상단에서 [정책 등록] 버튼을 클릭하십시오.

선택 삭제

정책 등록

| 정책번호 | 정책명 | 내부전송통계정책 | | | | | | | 외부전송통계정책 | | | | | | | 사용여부 | 수정 |
|--------------------------|-----|---------------|--------|--------|------------|------|-------------|------------|----------|--------|------------|------|---------|------------|-------------------------------------|------|----|
| | | 전원소 | 서비스 | IP | PORT | 계정 | 서버명 | 전원소 | 서비스 | IP | PORT | ID | 서버명 | | | | |
| <input type="checkbox"/> | 5 | 내부 파일 전송 정책 | FILE | sFTP | 1.1.1.1 | 8443 | nnd3manager | FtpTrans | FILE | sFTP | 1 | 8444 | | | <input checked="" type="checkbox"/> | | |
| <input type="checkbox"/> | 3 | 내부 OPC 전송 정책 | OPC | OPCDA | 1.1.1.3 | | manager | opc_Policy | OPC | OPCDA | 1.2.2.1 | 0 | Manager | opc_Policy | <input checked="" type="checkbox"/> | | |
| <input type="checkbox"/> | 2 | FTP_연동정책 | FILE | FTP | 10.10.1.10 | 1433 | 1313 | nNetNDR | FILE | FTP | 20.20.1.10 | 1433 | 1414 | nNetNDR | <input checked="" type="checkbox"/> | | |
| <input type="checkbox"/> | 1 | UDP_Syslog_전송 | STREAM | Syslog | 10.10.1.10 | 514 | | | STREAM | Syslog | 20.20.1.10 | 514 | | | <input checked="" type="checkbox"/> | | |

[그림 36] 보안정책 조회 화면

- ③ 등록하게 될 정책명을 입력하고, 서비스타입과 서비스타입에 따른 서비스명을 선택, 그리고 내부 프로그램명과 외부 프로그램명을 마지막으로 사용여부를 선택합니다.

3.3.1.1 Syslog 보안정책

The screenshot shows a configuration window titled "전송통제정책 정보 등록" (Transmission Control Policy Information Registration). At the top, there are fields for "정책번호" (Policy Number) set to 2, "정책명" (Policy Name) set to "SYSLOG 연동" (Syslog Interworking), and a "사용여부" (Usage) toggle switch that is turned on. Below this, there are two tabs: "step 1. 내부 전송 정책" (Step 1. Internal Transmission Policy) and "step 2. 외부 전송 정책" (Step 2. External Transmission Policy). The "step 1" tab is active. Under the "접속정보" (Connection Information) section, there are three fields: "컨텐츠" (Content) set to "STREAM", "서비스" (Service) set to "Syslog", "접속 IP" (Connection IP) set to "10.10.1.10", and "접속 PORT" (Connection Port) set to "514". At the bottom right, there are two buttons: "> 다음" (Next) and "X 취소하기" (Cancel).

[그림 37] Syslog 내부 전송 정책

- ① [정책번호]와 [정책명]을 지정합니다.
- ② Step1.내부 전송 정책 항목에서 접속정보에서 컨텐츠 [STREAM]을 선택하고 서비스 [Syslog]를 선택합니다.
- ③ 내부 Syslog 서버의 [접속IP]와 [접속PORT]를 입력합니다.

전송통계정책 정보 등록

정책번호 2

정책명 SYSLOG 연동 정책

사용여부 ☒

step 1. 내부 전송 정책

step 2. 외부 전송 정책

접속정보

컨텐츠 STREAM 서비스 Syslog

접속IP 20.20.1.20

접속PORT 514

< 뒤로

등록하기

× 취소하기

[그림 38] Syslog 외부 전송 정책

- Step2.외부 전송 정책 항목에서 접속정보에서 컨텐츠 [STREAM]을 선택하고 서비스 [Syslog]를 선택합니다.
- 외부 Syslog 서버의 [접속IP]와 [접속PORT]를 입력합니다.

3.3.1.2 FTP 보안정책

[그림 39] FTP 내부 전송 정책

- ① [정책번호]와 [정책명]을 지정합니다.
- ② Step1.내부 전송 정책 항목에서 접속정보에서 컨텐츠 [FILE]을 선택하고 서비스 [FTP]를 선택합니다.
- ③ 내부 FTP 서버의 [접속IP]와 [접속PORT]를 입력합니다.
- ④ FTP 서버의 [계정], [패스워드]를 입력합니다.
- ⑤ FTP 서버의 [서버명]을 입력합니다.

전송통제정책 정보 등록

정책번호 5

정책명 FTP 파일 전송 정책

사용여부 ☒

step 1. 내부 전송 정책

step 2. 외부 전송 정책

접속정보

컨텐츠 FILE 서비스 FTP

접속IP 20.20.1.10

접속PORT 21

계정 ftp

패스워드

서버명 FTPserver

< 뒤로

등록하기

× 취소하기

[그림 40] FTP 외부 전송 정책

- ① Step2.외부 전송 정책 항목에서 접속정보에서 컨텐츠 [FILE]을 선택하고 서비스 [FTP]를 선택합니다.
- ② 외부 FTP 서버의 [접속IP]와 [접속PORT]를 입력합니다.
- ③ FTP 서버의 [계정], [패스워드]를 입력합니다.
- ④ FTP 서버의 [서버명]을 입력합니다.

3.3.1.3 SFTP 보안정책

[그림 41] SFTP 내부 전송 정책

- ① [정책번호]와 [정책명]을 지정합니다.
- ② Step1.내부 전송 정책 항목에서 접속정보에서 컨텐츠 [FILE]을 선택하고 서비스 [SFTP]를 선택합니다.
- ③ 내부 SFTP 서버의 [접속IP]와 [접속PORT]를 입력합니다.
- ④ SFTP 서버의 [계정], [패스워드]를 입력합니다.
- ⑤ SFTP 서버의 [서버명]을 입력합니다.

전송통제정책 정보 등록

정책번호 5

정책명 SFTP 파일 전송 정책

사용여부 ☒

step 1. 내부 전송 정책

step 2. 외부 전송 정책

접속정보

컨텐츠 FILE 서비스 sFTP

접속 IP 20.20.1.10

접속 PORT 21

계정 ftp

패스워드

서버명 FTPserver

< 뒤로

등록하기

× 취소하기

[그림 42] SFTP 외부 전송 정책

- ① Step2.외부 전송 정책 항목에서 접속정보에서 컨텐츠 [FILE]을 선택하고 서비스 [SFTP]를 선택합니다.
- ② 외부 SFTP 서버의 [접속IP]와 [접속PORT]를 입력합니다.
- ③ SFTP 서버의 [계정], [패스워드]를 입력합니다.
- ④ SFTP 서버의 [서버명]을 입력합니다.

3.3.1.4 DB 보안정책

전송통제정책 정보 등록

정책번호 5

정책명

사용여부 ☒

step 1. 내부 전송 정책

step 2. 외부 전송 정책

접속정보

컨텐츠 DBMS

서비스 MSSQL

접속IP 10.10.1.10

접속PORT 1433

계정 sa

패스워드

서버명(DB ID) DBserver

> 다음

✕ 취소하기

[그림 43] DB 내부 전송 정책

- ① [정책번호]와 [정책명]을 지정합니다.
- ② Step1.내부 전송 정책 항목에서 접속정보에서 컨텐츠 [DBMS]을 선택하고 서비스 [MSSQL] 또는 [Oracle]를 선택합니다.
- ③ 내부 DB 서버의 [접속IP]와 [접속PORT]를 입력합니다.
- ④ DB 서버의 [계정], [패스워드]를 입력합니다.
- ⑤ DB 서버의 [서버명]을 입력합니다.

전송통제정책 정보 등록

정책번호 5

정책명

사용여부 ☒

step 1. 내부 전송 정책

step 2. 외부 전송 정책

접속정보

컨텐츠 DBMS

서비스 MSSQL

접속 IP 20.20.1.10

접속 PORT 1433

계정 sa

패스워드

서버명(DB ID) DBserver

< 뒤로

등록하기

× 취소하기

[그림 44] DB 외부 전송 정책

- ① [정책번호]와 [정책명]을 지정합니다.
- ② Step2.외부 전송 정책 항목에서 접속정보에서 컨텐츠 [DBMS]을 선택하고 서비스 [MSSQL] 또는 [Oracle]를 선택합니다.
- ③ 외부 DB 서버의 [접속IP]와 [접속PORT]를 입력합니다.
- ④ DB 서버의 [계정], [패스워드]를 입력합니다.
- ⑤ DB 서버의 [서버명]을 입력합니다.

3.3.1.5 OPC DA 보안정책

[그림 45] OPC 내부 전송 정책

- ① [정책번호]와 [정책명]을 지정합니다.
- ② Step1.내부 전송 정책 항목에서 접속정보에서 컨텐츠 [OPC]을 선택하고 서비스 [OPCDA]를 선택합니다.
- ③ 내부 OPC 서버의 [접속IP]와 [접속PORT]를 입력합니다.
- ④ OPC 서버의 [계정], [패스워드]를 입력합니다.
- ⑤ OPC 서버의 [ProgID]을 입력합니다.

전송통제정책 정보 등록

정책번호 8

정책명 OPC 연동 정책

사용여부 ☒

step 1. 내부 전송 정책

step 2. 외부 전송 정책

접속정보

컨텐츠 OPC 서비스 OPCDA

접속 IP 20.20.1.10

계정 opc

패스워드

서버명(Prog ID) OPC_ProgID

< 뒤로

등록하기

× 취소하기

[그림 46] OPC 외부 전송 정책

- ① Step2.외부 전송 정책 항목에서 접속정보에서 컨텐츠 [OPC]을 선택하고 서비스 [OPCDA]를 선택합니다.
- ② 외부 OPC 서버의 [접속IP]와 [접속PORT]를 입력합니다.
- ③ OPC 서버의 [계정], [패스워드]를 입력합니다.
- ④ OPC 서버의 [ProgID]을 입력합니다.

3.3.1.6 입력 시 오류 화면

■ 보안 정책명 공백 입력시

보안 정책 정보 등록 시 정책명은 정책명을 의미하며 문자열 제약이 없으나 아무것도 입력하지 않을 경우 아래와 같은 메시지를 호출합니다.

200.20.10.2:8443 내용:
정책명을 입력하세요.

확인

[그림 47] 보안 정책명 공백 입력시 오류 화면

■ 보안 정책명 중복 등록시

보안 정책 정책명 등록 시 동일한 정책이 있는 경우 아래와 같은 메시지가 출력됩니다.

200.20.10.2:8443 내용:
동일한 정책명이 존재합니다.

확인

[그림 48] 보안 정책 중복 등록 시 오류 화면

■ 출발지 IP주소 공백 입력 시

출발지 IP주소 입력 시 공백이거나 미입력한 상태에서 등록 할 경우 아래와 같은 메시지가 출력됩니다.

200.20.10.2:8443 내용:
출발지 IP를 입력하세요.

확인

[그림 49] 출발지 IP주소 공백 입력 시 오류 화면

■ 출발지 IP주소 등록시 IPv4 형식이 아닌 경우

출발지 IP주소를 등록할 때, IP가 IPv4 형식이 아니거나 문자열이 포함된 경우 아래와 같이 메시지 팝업이 출력됩니다. (예를 들어, "a12.b34.c45.d78" 입력시)

200.20.10.2:8443 내용:
출발지 IP가 IP 주소형식이 아닙니다.

확인

[그림 50] 출발지 IP주소 형식이 IPv4 형식이 아닐 경우 오류 화면

■ 출발지 수신 포트 번호가 숫자가 아닌 경우

출발지 수신 포트를 등록할 때, 입력 값이 숫자가 아닌 문자열이 포함된 경우 아래와 같이 메시지 팝업이 출력됩니다. (예를 들어, "a1000" 입력시)

200.20.10.2:8443 내용:
출발지 수신 포트 입력이 올바르지 않습니다.

확인

[그림 51] 출발지 수신 포트 입력 값이 숫자가 아닐 경우 오류 화면

■ 출발지 수신 포트 범위에 맞지않은 경우

출발지 수신 포트를 등록할 때, 포트 번호가 0에서 65535의 범위가 아닐 경우 아래와 같이 메시지 팝업이 출력됩니다. (예를 들어, "1000000" 입력시)

200.20.10.2:8443 내용:
출발지 수신 포트 범위는 0 - 65535 입니다.

확인

[그림 52] 입력 값이 출발지 수신 포트 범위에 맞지않은 경우 오류 화면

■ 일방향 전송 포트 번호가 숫자가 아닌 경우

일방향 전송 포트를 등록할 때, 입력 값이 숫자가 아닌 문자열이 포함된 경우 아래와 같이 메시지 팝업이 출력됩니다. (예를 들어, "a1000" 입력시)

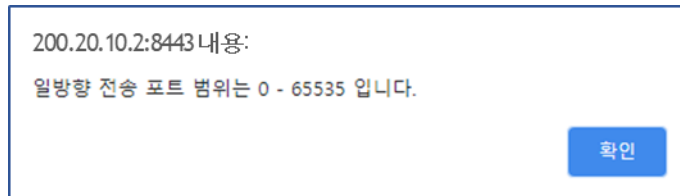
200.20.10.2:8443 내용:
일방향 전송 포트 입력이 올바르지 않습니다.

확인

[그림 53] 일방향 전송 포트 번호가 포트 입력 값이 숫자가 아닌 경우 오류 화면

■ 일방향 전송 포트 범위에 맞지않은 경우

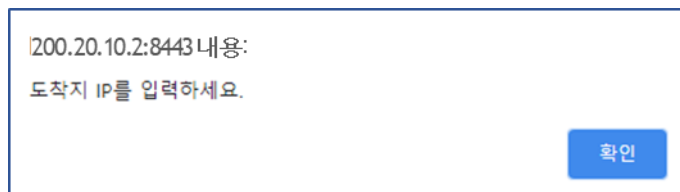
일방향 전송 포트를 등록할 때, 포트 번호가 0에서 65535의 범위가 아닐 경우 아래와 같이 메시지 팝업이 출력됩니다. (예를 들어, "1000000" 입력시)



[그림 54] 입력 값이 일방향 전송 포트 범위에 맞지않은 경우 오류 화면

■ 도착지 IP주소 공백 입력 시

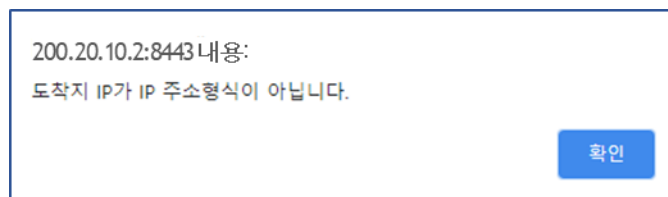
도착지 IP주소 입력 시 공백이거나 미 입력한 상태에서 등록 할 경우 아래와 같은 메시지가 출력됩니다.



[그림 55] 도착지 IP주소 공백 입력 시 오류 화면

■ 도착지 IP주소 등록시 IPv4 형식이 아닌 경우

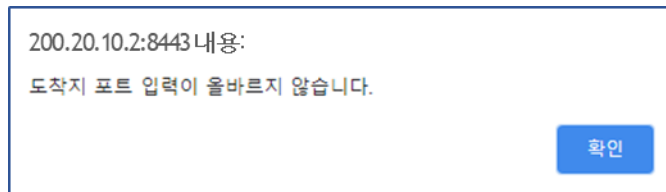
도착지 IP주소를 등록할 때, IP가 IPv4 형식이 아니거나 문자열이 포함된 경우 아래와 같이 메시지 팝업이 출력됩니다. (예를 들어, "a12.b34.c45.d78" 입력시)



[그림 56] 도착지 IP주소 형식이 IPv4 형식이 아닐 경우 오류 화면

■ 도착지 포트 번호가 숫자가 아닌 경우

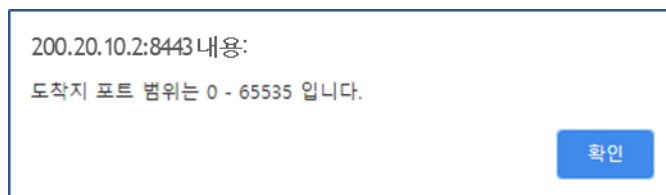
도착지 포트를 등록할 때, 입력 값이 숫자가 아닌 문자열이 포함된 경우 아래와 같이 메시지 팝업이 출력됩니다. (예를 들어, "a1000" 입력시)



[그림 57] 도착지 수신 포트 입력 값이 숫자가 아닐 경우 오류 화면

■ 도착지 포트 범위에 맞지않은 경우

도착지 포트를 등록할 때, 포트 번호가 0에서 65535의 범위가 아닐 경우 아래와 같이 메시지 팝업이 출력됩니다. (예를 들어, "1000000" 입력시)



[그림 58] 입력 값이 도착지 포트 범위에 맞지않은 경우 오류 화면

3.4 보안감사 관리

3.4.1 관리자 로그

관리자 로그는 관리 프로그램 운용 중에 발생하는 로그를 조회하는 화면으로써 조회할 수 있는 로그 항목은 아래와 같습니다.

| 로그 종류 |
|-----------------------------|
| 로그인 성공 및 실패 시 발생하는 로그 |
| 관리자 계정 생성 및 수정 시 발생하는 로그 |
| 로그아웃 시 발생하는 로그 |
| 관리자 접속 및 제한 정책 수정 시 발생하는 로그 |

[표 5] 관리자 로그 종류

관리자 로그는 <로그 정보> ▷ <보안 이벤트 로그> ▷ <관리자 로그> 메뉴에서 조회가 가능하며, 화면 우측의 [엑셀 다운로드] 버튼을 클릭하면 조회된 관리자 로그를 엑셀 파일로 저장할 수 있습니다. 관리자 로그 화면은 아래와 같습니다.

| 순번 | 관리자 ID | 로그 발생일 | 접속 IP | 작업 내용 | 작업 결과 | 위험도 | 세부 내용 |
|----|-------------|---------------------|---------------|-------|-------|-----|----------------|
| 21 | nnd2Manager | 2021-05-10 15:55:36 | 127.0.0.1 | 로그인 | 성공 | 정보 | |
| 20 | nnd2Manager | 2021-05-10 14:44:53 | 127.0.0.1 | 로그아웃 | 성공 | 정보 | |
| 19 | nnd2Manager | 2021-05-10 14:33:42 | 127.0.0.1 | 로그인 | 성공 | 정보 | |
| 18 | nnd2Manager | 2021-05-10 14:16:05 | 127.0.0.1 | 로그아웃 | 성공 | 정보 | |
| 17 | nnd2Manager | 2021-05-10 14:05:12 | 127.0.0.1 | 로그인 | 성공 | 정보 | |
| 16 | nnd2Manager | 2021-05-10 13:53:19 | 127.0.0.1 | 로그아웃 | 성공 | 정보 | |
| 15 | nnd2Manager | 2021-05-10 13:42:32 | 127.0.0.1 | 로그인 | 성공 | 정보 | |
| 14 | nnd2Manager | 2021-05-04 17:13:07 | 127.0.0.1 | 로그아웃 | 성공 | 정보 | |
| 13 | nnd2Manager | 2021-05-04 16:52:45 | 127.0.0.1 | 로그인 | 성공 | 정보 | |
| 12 | nnd2Manager | 2021-05-04 16:52:14 | 127.0.0.1 | 로그인 | 성공 | 정보 | |
| 11 | nnd2Manager | 2021-05-04 16:42:12 | 0:0:0:0:0:0:1 | 로그인 | 실패 | 경고 | 접속이 허용된 IP가 아님 |
| 10 | nnd2Manager | 2021-05-04 13:03:11 | 127.0.0.1 | 로그아웃 | 성공 | 정보 | |
| 9 | nnd2Manager | 2021-05-04 12:57:49 | 127.0.0.1 | 로그아웃 | 성공 | 정보 | |
| 8 | nnd2Manager | 2021-05-04 12:52:36 | 127.0.0.1 | 로그인 | 성공 | 정보 | |
| 7 | nnd2Manager | 2021-05-04 12:51:30 | 127.0.0.1 | 로그인 | 성공 | 정보 | |
| 6 | nnd2Manager | 2021-05-04 11:34:34 | 127.0.0.1 | 로그아웃 | 성공 | 정보 | |
| 5 | nnd2Manager | 2021-05-04 11:23:31 | 127.0.0.1 | 로그인 | 성공 | 정보 | |
| 4 | nnd2Manager | 2021-05-04 11:20:21 | 0:0:0:0:0:0:1 | 로그인 | 실패 | 경고 | 접속이 허용된 IP가 아님 |
| 3 | nnd2Manager | 2021-05-04 11:16:29 | 0:0:0:0:0:0:1 | 로그인 | 실패 | 경고 | 접속이 허용된 IP가 아님 |
| 2 | nnd2Manager | 2021-05-04 11:15:07 | 0:0:0:0:0:0:1 | 로그인 | 실패 | 경고 | 등록되지 않은 아이디 |
| 1 | nnd2Manager | 2021-05-04 11:14:55 | 0:0:0:0:0:0:1 | 로그인 | 실패 | 경고 | 등록되지 않은 아이디 |

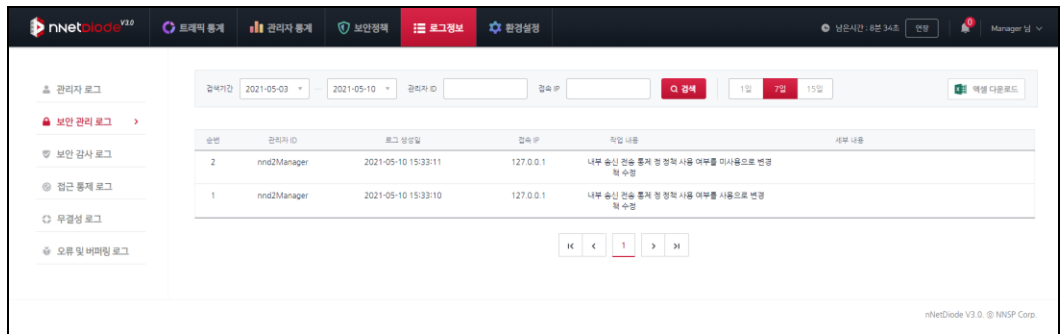
[그림 59] 관리자 로그 화면

3.4.2 보안 관리 로그

보안 관리 로그는 관리자가 변경한 정책에 대한 로그를 조회하는 화면으로써 서비스 프로그램의 시작, 보안 정책의 추가, 삭제, 변경에 로그를 조회 할 수 있습니다. 조회 할 수 있는 로그 항목은 아래와 같습니다.

| 로그 종류 |
|--|
| 보안 정책의 추가, 삭제, 변경 시 발생하는 로그 |
| nNetDiode V3.0 시스템의 정보 변경 시 발생하는 로그 |
| 관리자에 이벤트 전송하기 위한 메일 전송 정보 설정 시 발생하는 로그 |

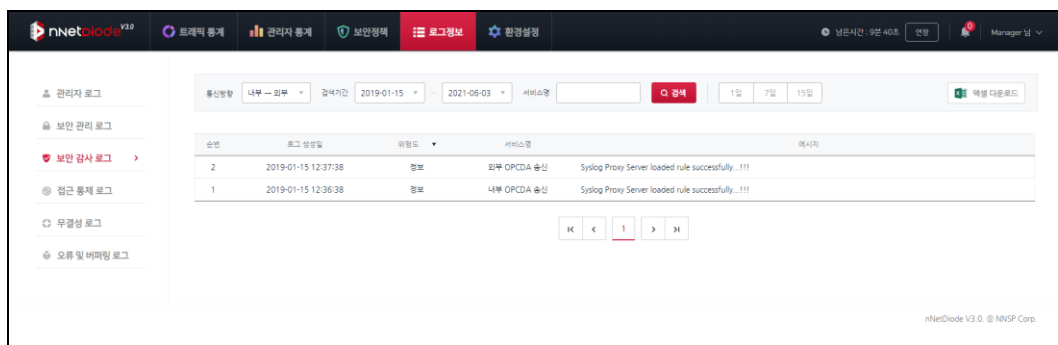
[표 6] 보안 관리 로그 종류



[그림 60] 보안 관리 로그 화면

3.4.3 보안 감사 로그

보안 감사 로그는 nNetDiode V3.0에서 일방향 데이터 전송 시 발생하는 서비스의 시작 및 중지 등의 이벤트 로그로 아래와 화면과 같이 조회 할 수 있습니다.



[그림 61] 이벤트 로그 화면

3.4.4 접근 통제 로그

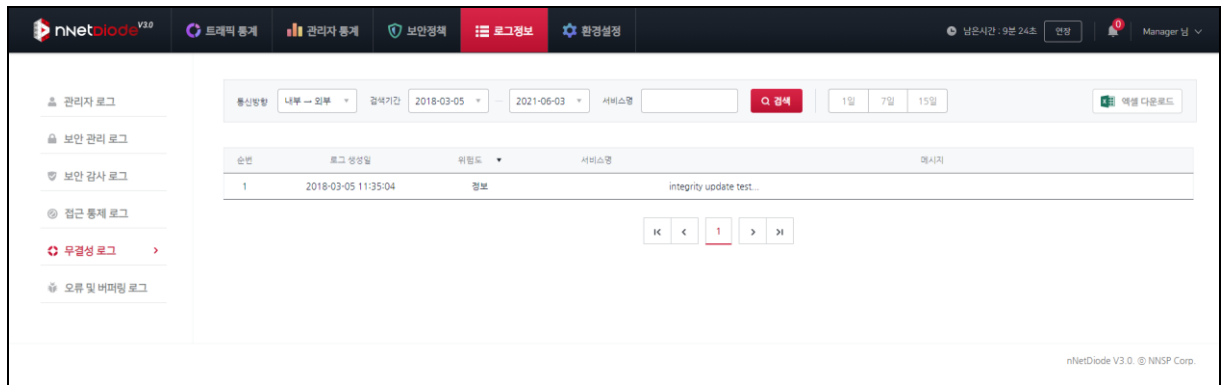
접근 통제 로그는 일방향 데이터 전송 시 발생하는 로그로 아래의 화면과 같이 조회할 수 있습니다.

| <div> <div> nNetDiode V3.0 트래픽 통계 관리자 통계 보안정책 로그정보 환경설정 </div> <div> 날짜: 2018-02-19 시간: 2021-06-03 로그: 이벤트 타입 전체 로그: 수신 구분 전체 검색 1일 7일 15일 액셀 다운로드 </div> </div> | | | | | | | | | |
|--|---------------------|-----|--------|--------|-----------------|----------|-------------|----------|--|
| 순번 | 로그 발생일 | 위험도 | 악세스 타입 | 송수신 구분 | 송발지 IP | 송발지 PORT | 도착지 IP | 도착지 PORT | |
| 3001 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 3000 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2999 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2998 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2997 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2996 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2995 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2994 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2993 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2992 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2991 | 2018-02-21 10:33:51 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2990 | 2018-02-20 12:53:18 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2989 | 2018-02-20 12:53:18 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2988 | 2018-02-20 12:53:18 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2987 | 2018-02-20 12:53:17 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2986 | 2018-02-20 12:53:17 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2985 | 2018-02-20 12:53:17 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2984 | 2018-02-20 12:53:17 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2983 | 2018-02-20 12:53:17 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2982 | 2018-02-20 12:53:17 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2981 | 2018-02-20 12:53:17 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2980 | 2018-02-20 12:53:17 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2979 | 2018-02-20 12:53:16 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2978 | 2018-02-20 12:53:16 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2977 | 2018-02-20 12:53:16 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2976 | 2018-02-20 12:53:16 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2975 | 2018-02-20 12:53:16 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2974 | 2018-02-20 12:53:16 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2973 | 2018-02-20 12:53:16 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |
| 2972 | 2018-02-20 12:53:16 | 정보 | Allow | 송신 | 200.200.200.149 | 7301 | 176.168.0.3 | 7301 | |

[그림 62] 접근 통제 로그 화면

3.4.5 무결성 로그

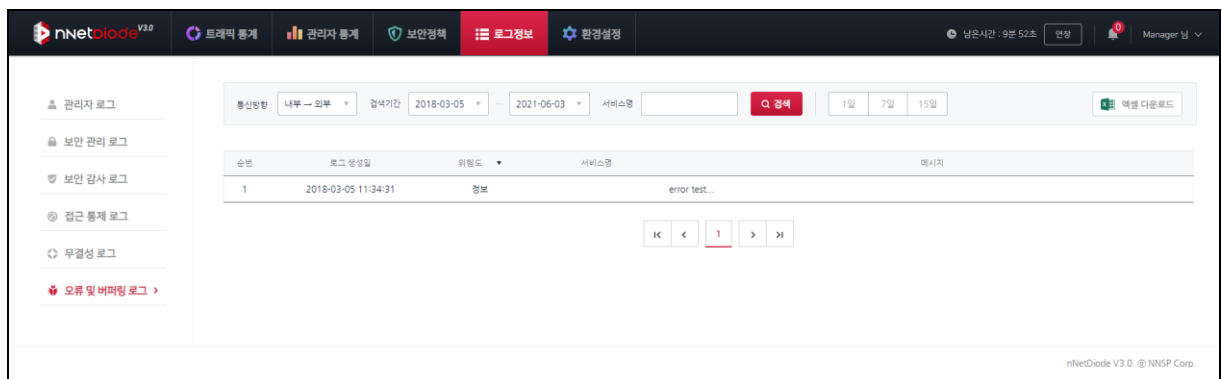
무결성 로그는 자체 보호 기능을 통하여 내부/외부 프로그램을 수동 또는 자동으로 무결성 검사를 수행하였을 때 발생하는 로그로 아래의 화면과 같이 조회 할 수 있습니다.



[그림 63] 무결성 로그 화면

3.4.6 오류 및 버퍼링 로그

오류 및 버퍼링 로그는 nNetDiode V3.0에 등록된 내부/외부 프로그램이 기능을 수행할 때 오류 및 버퍼링이 있을 경우 발생하는 로그로 아래의 화면과 같이 조회 할 수 있습니다.



[그림 64] 오류 및 버퍼링 로그 화면

3.5 환경 설정

3.5.1 시스템

3.5.1.1 내부 송신 시스템 설정

보안영역 전송통제서버인 nNetDiode Tx의 Master NIC정보와 Slave NIC정보 그리고 버전정보를 확인하고 시스템을 재시작 실행할 수 있습니다. 내부 송신 시스템 재시작 실행 방법은 다음과 같습니다.

- ① <환경설정> ▷ <시스템> ▷ <내부 송신 시스템> 메뉴를 클릭하십시오.
- ② 초기 네트워크 설정 이후 서비스 동작 중에 네트워크를 변경할 경우 하단의 [재시작 실행] 버튼을 클릭하십시오.

내부 송신 시스템 설정 | 외부 수신 시스템 설정 | 프로그램 등록 | 자체 보호

Master NIC

Intel(R) Ethernet Converged Network Adapter X710

Slave NIC

Intel(R) Ethernet Converged Network Adapter X710

버전정보 nNetDiode TX V3.0.1

⏻ 재시작 실행

* 시스템 네트워크 설정이 내/외부 모두 등록되어야 정상 동작 됩니다.

[그림 65] 내부 송신 시스템 설정 화면



서비스 재시작 시 완료 팝업이 나타날 때까지 대기해야 하며, 대기 시간은 약 3초에서 5초가 소요됩니다. 재시작 중 다른 페이지로 이동할 경우 에러가 발생될 수 있습니다.

3.5.1.2 외부 수신 시스템 설정

비보안영역 전송통제서버인 nNetDiode Rx의 네트워크 정보를 확인합니다.

- ① <환경설정> ▷ <시스템> ▷ <외부 수신 시스템> 메뉴를 클릭하십시오.
- ② 입력란에 네트워크 정보를 입력하고 [수정하기] 버튼을 클릭하십시오.
- ③ 초기 네트워크 설정 이후 서비스 동작 중에 네트워크를 변경할 경우 하단의 [재시작 실행] 버튼을 클릭하십시오.

내부 송신 시스템 설정
외부 수신 시스템 설정
프로그램 등록
자체 보호

Master NIC

Intel(R) Ethernet Converged Network Adapter X710

Slave NIC

Intel(R) Ethernet Converged Network Adapter X710

버전정보 nNetDiode RX V3.0.1

⏻ 재시작 실행

* 시스템 네트워크 설정이 내/외부 모두 등록되어야 정상 동작 됩니다.

* MAC 주소를 변경하면 내부 전송통제 서버가 재시작 됩니다.

[그림 66] 외부 수신 시스템 설정 화면

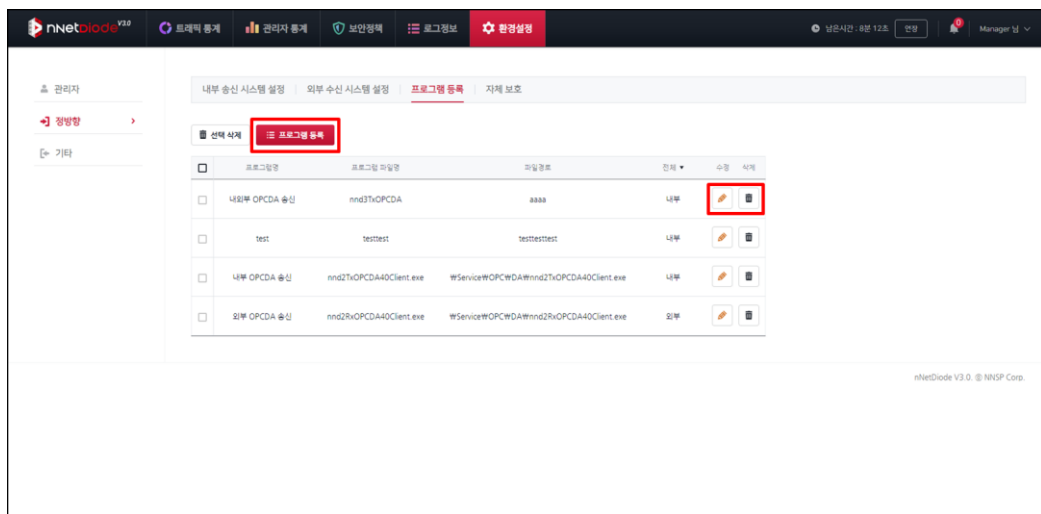


서비스 재시작 시 완료 팝업이 나타날 때까지 대기해야 하며, 대기 시간은 약 3초에서 5초가 소요됩니다. 재시작 중 다른 페이지로 이동할 경우 에러가 발생될 수 있습니다.

3.5.1.3 프로그램 등록

외부 프로그램과 내부 프로그램을 등록, 수정, 삭제할 수 있습니다.

- ① <환경설정> ▷ <시스템> ▷ <프로그램 등록> 메뉴를 클릭하십시오.
- ② 등록된 내/외부 프로그램 우측에 [수정], [삭제] 버튼을 클릭하여 수정, 삭제할 수 있습니다.
- ③ 새로운 내부 또는 외부 프로그램을 등록할 경우 목록 좌측 상단의 [프로그램 등록] 버튼을 클릭하십시오.



[그림 67] 프로그램 등록 메뉴 화면

- ④ 프로그램 정보를 정확히 입력한 후 화면 하단의 [등록하기] 버튼을 클릭하십시오.

프로그램 정보 등록
✕

프로그램명

프로그램 파일명

파일 경로

내/외부 구분

내부 ▼

✕ 취소하기

≡ 등록하기

[그림 68] 프로그램 정보 등록 화면

3.5.1.4 자체 보호

보안영역 전송통제서버인 nNetDiode Tx와 비보안영역 전송통제서버인 nNetDiode Rx에서 동작하고 있는 프로그램에 대해 무결성을 점검합니다.

- ① <환경설정> ▷ <시스템> ▷ <자체 보호> 메뉴를 클릭하십시오.
- ② 수동으로 프로그램 무결성 검사를 수행할 경우 하단의 [무결성 검사] 버튼을 클릭하십시오.
- ③ 프로그램 무결성 값을 업데이트 할 경우 하단의 [무결성값 업데이트] 버튼을 클릭하십시오.
- ④ 일정 시간마다 자동으로 무결성 검사를 수행하는 주기를 변경하고자 할 경우 좌측 하단의 무결성 점검 주기 시간을 원하는 시간 단위로 선택하고 [수정] 버튼을 클릭하십시오.

■ 무결성 검사

관리자가 보안영역 전송통제서버인 nNetDiode Tx와 비보안영역 전송통제서버인 nNetDiode Rx에 대한 무결성 검사를 실시합니다.

| 순번 | 프로그램명 | 프로그램 파일명 | 해시값 | 사이즈(byte) | 날짜 |
|----|--------------|-------------------------|-----|-----------|----|
| 1 | 내부 OPCDA 송신 | nnd2TxOPCDA40Client.exe | | | |
| 2 | test | testtest | | | |
| 3 | 외부부 OPCDA 송신 | nnd3TxOPCDA | | | |

[그림 69] 무결성 점검 화면



nNetDiode Rx는 nNetDiode Tx에서 무결성 검사 명령을 전송받아 무결성 검사를 수행하지만 검사 결과를 nNetDiode Tx로 전달 할 수 없어 nNetDiode Tx에서는 nNetDiode Rx의 검사 결과를 알 수 없습니다.

관리자는 nNetDiode Rx 내의 DBMS를 통해 무결성 검사 결과를 확인 할 수 있습니다.

3.5.2 로그 관리

로그 관리에서는 디스크가 몇 퍼센트(%) 이상 찼을 경우 관리자에게 알림을 할 것인지에 대한 디스크 임계값을 설정할 수 있습니다.

- ① <환경설정> ▷ <기타> ▷ <로그 관리> 메뉴를 클릭하십시오.
- ② 디스크 임계값 설정을 입력하고 하단의 [수정] 버튼을 클릭하십시오.

[그림 70] 로그 관리 설정 화면



디스크 임계값 설정에서 디폴트값은 90%이며 디스크 임계값에 도달하면 메일을 통해 관리자에게 이를 경고합니다.

3.5.3 메일 설정

관리 프로그램에서 관리자 알림 상황이 발생하여 메일 발송 시 사용할 메일 서버 정보를 설정합니다.

- ① <환경설정> ▷ <기타> ▷ <메일 설정> 메뉴를 클릭하십시오.
- ② 메일 서버의 HOST, PORT, ID, PW 및 보내는 메일 주소를 입력하고 하단의 [수정] 버튼을 클릭하십시오.

로그 관리 | **메일 설정** | 장비소개 관리

메일 서버 HOST

mail.test.co.kr

메일 서버 PORT

25

메일 서버 ID

Manager

메일 서버 PW

.....

보내는 메일 주소

manager@test.co.kr

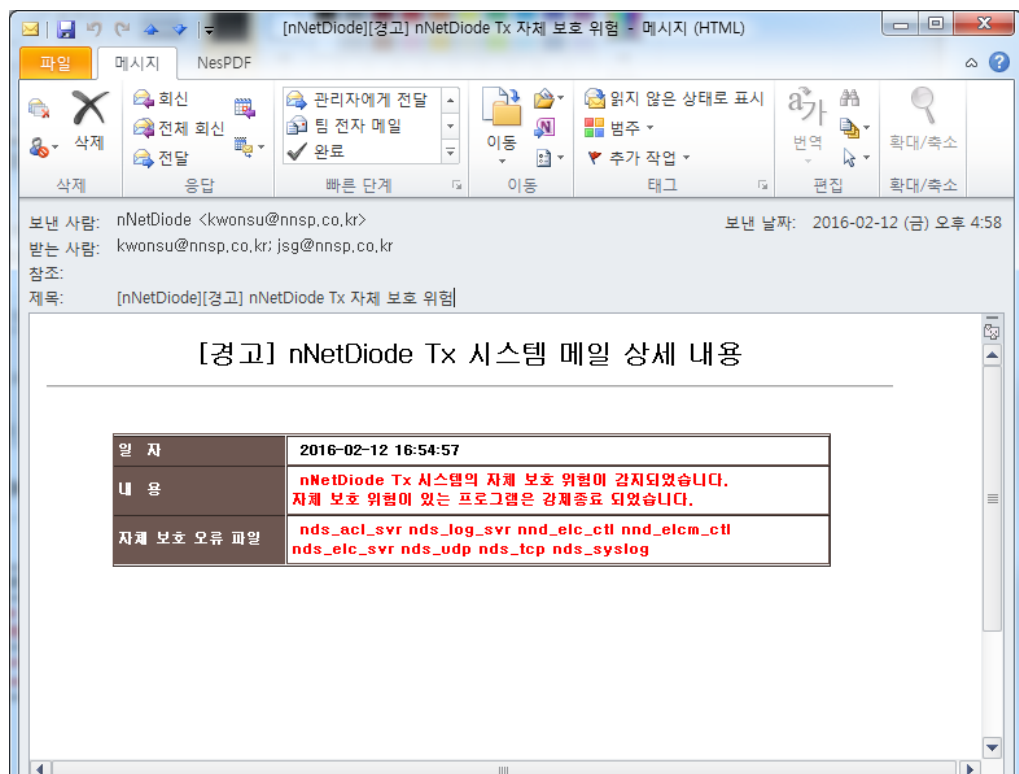
× 취소하기

수정하기

[그림 71] 메일 설정 화면

■ 경고 메일 발송

디스크의 용량 부족 및 서비스 프로그램의 무결성이 손상되었을 경우 관리자에게 경고 메일을 발송합니다.



[그림 72] 시스템 메일 상세 내용

3.5.4 장비소개 관리

설치한 nNetDiode 정보를 확인 및 관리 할 수 있습니다.

- ① <환경설정> ▷ <기타> ▷ <장비소개 관리> 메뉴를 클릭하십시오.
- ② 장비의 정보를 알맞게 입력하고 하단의 [수정하기] 버튼을 클릭하십시오.

The screenshot displays the '장비소개 관리' (Equipment Introduction Management) interface. At the top, there are navigation tabs: '로그 관리', '메일 설정', and '장비소개 관리' (which is selected). Below the tabs is a form with the following fields:

- 장비 이름**: nNetDiode V2.0
- 모델**: P1000S/R (with a dropdown arrow)
- 시리얼 넘버**: 1234-abcd-efgh-5
- OS**: Windows 10
- 기술지원**: 02 (dropdown), 111 (input), 111 (input)
- 설치날짜**: 2018-12-20 (with a dropdown arrow)
- 설명**: A large empty text area.

At the bottom of the form, there are two buttons: 'X 취소하기' (Cancel) and '수정하기' (Save/Update). The '수정하기' button is highlighted with a red rectangular box.

[그림 73] 장비소개 관리 화면

제 4 장 부록

본 장에서는 nNetDiode V3.0 시스템 운영 중 오류 시 대처방안에 대해 설명합니다.

4. 부록

4.1 용어설명

본 관리자 설명서에서 사용된 용어는 공통평가기준에 사용된 용어와 동일한 것은 공통평가기준을 따른다. 공통평가기준 외에 추가적으로 사용된 용어는 본 관리자 설명서 작성자에 의해 추가되었습니다.

보안영역(제어망)

외부와 물리적으로 분리되어 내부적으로 운영되는 제어 네트워크

비(非)-보안영역(외부망)

제어망 외부로 물리적으로 연결된 네트워크

전송통제서버(보안영역·비-보안영역)

일방향 망간 자료전송 제품이 설치되어 보안 정책에 따라 비 인가자(시스템) 접근통제 및 보안영역과 비-보안영역간 파일 및 스트림 전송에 대한 통제를 수행하는 시스템

MS-SQL Database

SQL 은 마이크로소프트(이하 MS)에서 개발한 프로그래밍 언어로 각종 자료를 저장하는 데이터베이스 서버를 관리하는데 쓰이는 언어를 뜻하며, MSSQL 서버는 SQL 에 기반해 MS 가 개발한 데이터베이스 서버

Syslog

시스템의 운영과 관련한 전반적인 로그로써, 하드웨어의 구동 및 서비스 동작과 에러 등 다양한 로그를 남김

Sybase Database

Sybase 는 관계형 데이터베이스 관리 시스템 전문 기업인 Sybase 가 개발하였으며, 마이크로소프트가 개발한 SQL 서버와 매우 유사한 구조를 가짐

OPC DA(Data Access)

OPC(OLE for Process Control)는 산업 자동화 표준으로써, 마이크로소프트(이하 MS)의 기본적인 OLE(ObjectLinking and Embedding)/COM 과 DCOM 기술을 기반으로 접근 허용된 Client 는 OPC Server 의 실시간 데이터를 얻거나 변경할 수 있는 기술

OPC HDA(Historical Data Access)

OPC DA 와 같이 COM 과 DCOM 기술을 기반으로하며, DA 와 같은 실시간 데이터를 OPC 서버에 저장 또는 축적하여 실시간 데이터 생성 이력 데이터를 얻거나 변경 할 수 있는 기술

AES(Advanced Encryption Standard)

고급 암호화 표준인 AES 는 1977 년 공표된 DES 암호화 기술을 대체하는 대칭 키 암호화 기술이며, 안전성(Security), 비용(Cost), 알고리즘 및 구현 특성(Algorithm and implementation characteristics)의 세 가지 조건을 만족