Realize your vision

Samsung SDS
EMM

관리자 매뉴얼 (일반보안)

버전 2.0.2
최종수정일 2018. 2

SAMSUNG SDS

이 매뉴얼을 사용하기 전에 다음 사항을 읽어 주십시오.

펴낸 곳 삼성SDS(주)

주소 서울특별시 송파구 올림픽로 35길 125

대표 전화 +82 2 1644 0030

전자 메일 msupport.sds@samsung.com

홈페이지 www.samsungsds.com

서문

시작하기 전에

사용자의 단말 , 애플리케이션 , 콘텐츠 등의 완벽한 보안을 위해 Samsung SDS EMM (이하 EMM) 솔루션은 관리자 포털의 설정 및 사용 시나리오에 따라 법률상 수집 또는 처리가 제한되는 개인정보 (사용자 및 단말 정보) 를 수집할 수 있습니다 . 따라서 개인정보의 수집 및 처리 전 고객사의 법무정책 및 귀속 국가의 관련 법령을 반드시 확인하고 법률상 필요한 동의 절차를 밟아야 합니다 .

사용 대상

이 매뉴얼은 통합적인 보안 서비스를 제공하는 EMM 솔루션의 사용 방법을 담고 있습니다 . 또한 EMM 의 서비스 관리 , 단말 및 사용자 관리 , 정책 관리 , 인증서를 통한 보안 관리 , 환경 설정을 관리하는 운영자를 대상으로 합니다 . 운영자가 EMM 솔루션을 효과적으로 관리하기 위해서는 다음과 같은 지식과 경험이 필요합니다 .

- 시스템 운영 업무에 대한 일반 사항
- 데이터 관리에 대한 일반 사항
- 보안 업무에 대한 일반 사항
- 디바이스 제어 및 관리에 대한 일반 사항
- 웹 애플리케이션 사용에 대한 일반 사항

표기 규약

이 매뉴얼은 문서 내용의 이해를 돕기 위해 다음과 같은 표기 규약을 사용합니다 .

표기 규약	설명
볼드체활자	**볼드체활자**는 그래픽 유저 인터페이스 요소, 메뉴, 디렉터리 등을 표기할 때 사용합니다.
“ ”	“ “ 큰 따옴표는 다음과 같은 경우 사용합니다. • 그래픽 유저 인터페이스 중 페이지, 포털, 창 • 다른 책자, 백서 등을 참고하는 경우, 해당 출판물의 저자나 출판사를 언급하고 큰 따옴표 안에 책 제목을 표기
“상호 참고”	“상호 참고”는 문서 내 특정 토픽이나 다른 챕터 또는 다른 챕터의 토픽을 참고할 때 사용합니다. 상호 참고를 클릭하는 경우, 지정한 위치로 이동합니다.
고정폭 활자	고정폭 활자는 프로그래밍과 관련된 용어나 코드, 파일명을 표기할 때 사용합니다. • 영문 고정폭 서체: `Courier New` • 국문 고정폭 서체: 돋움
그림	그림은 본문의 이해를 돕기위해 그래픽, 일러스트레이션, 스크린 캡처 등을 설명할 때 사용합니다.
표	표는 본문에 많은 양의 정보를 쉽게 파악하여 나타낼 때 사용합니다.

부연 설명 및 지침

사용자에게 팁 , 조언 , 예외 사항 , 제한 사항 등을 알릴 때에는 Note 를 사용합니다 .

Note: EMM 사용을 위해 ELM License Key 값은 반드시 필수로 입력해야 합니다 .

개정 이력

솔루션 버전	매뉴얼 버전	매뉴얼 변경 일자	매뉴얼 변경 사항
1.0.0	1.0.0	2014.10	최초 발행
1.0.1	1.0.1	2014.12	1.0.1 매뉴얼 발행
1.1.0	1.1.0	2015.3	사용성 개선 및 보안 강화 반영
1.1.1	1.1.1	2015.6	1.1.1 매뉴얼 발행
1.1.2	1.1.2	2015.6	1.1.2 매뉴얼 발행
1.1.3	1.1.3	2015.7	1.1.3 매뉴얼 발행
1.2.0	1.2.0	2015.9	고보안과 일반보안 패키지 제품 - EMM 무력화 방지 기능 강화 - 내방객 MDM 및 관리 기능 추가 등
1.2.2	1.2.2	2015.10	- 리소스 변경 및 UI/UX 개선 - 프로파일의 설정 항목 추가
1.3.0	1.3.0a	2016.4	사용성 개선 - Android for work 지원
1.4.0	1.4.0a	2016.7	- Knox 최신 기능 지원 - Windows10 지원(모바일, 테블릿, PC) - Kiosk 기능 다양화, QR 코드 활용 단말 활성화 등 IT관리자 및 사용자 편의 기능 강화
1.4.1	1.4.1a	2016.8	삼성그룹향 관련 기능 개선
1.5.0	1.5.0a	2016.10	- 동기화 서비스 및 KME 서비스 추가 - 프로파일 구성요소 관리 추가
1.5.1	1.5.1a	2016.12	- Audit 대상 검색 추가 - 단말 상태 변경
1.6.0	1.6.0a	2016.3	Tizen Wearable 지원
1.6.1	1.6.1a	2017.5	- 대시보드 UI/UX 개선 - 외부 동기화 연계 추가 - 앱 접근 권한 설정 추가
2.0	2.0a	2017.10	- IMEI로 등록한 단말의 활성화 기능 추가 - AppWrapper 툴 제공
2.0.2	2.0.2a	2018.2	- iOS 인증서 등록 기능 추가 - 조직/그룹 변경 시 프로파일 배포 기능 추가 - 프로파일 적용 기능 추가

목차

1 개요

Samsung SDS EMM (Enterprise Mobility Management) 은 디바이스 제어부터 애플리케이션 , 데이터에 이르기까지 모든 레이어의 통합 보안 관리가 가능한 솔루션입니다 . 본 솔루션은 OS 에 관계없이 단일화된 하나의 관리자 포털에서 효율적인 모바일 관리 환경을 제공하며 , 사용자가 원하는 보안 정책과 사용 경험 기반의 User Interface 를 통해 업무에 대한 보안 관리 및 업무 생산성을 향상시킬 수 있습니다 .

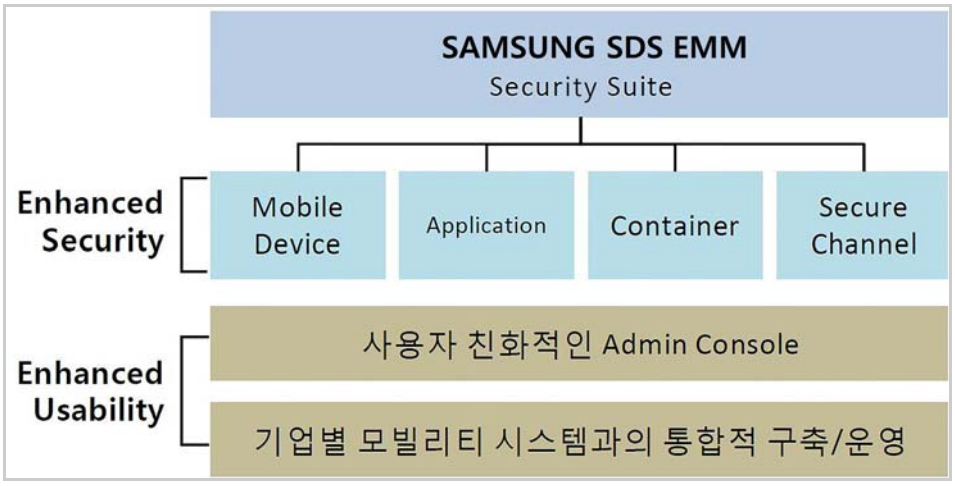


그림 1-1. Samsung SDS EMM의 구성 개념도

EMM 특징

강력한 보안 설계로 데이터를 완벽히 보호

EMM 은 설계 단계부터 최고 레벨의 보안 요구사항을 고려한 후 개발하여 발생 가능한 어떤 위협으로부터도 기업 데이터를 완벽히 보호합니다 .

- FIPS-140-2 인증 모듈을 적용하여 모든 데이터의 암복호화 가능
  (FIPS: US Federal Information Processing Standards)
- 인증서 기반에 애플리케이션 또는 통신 채널을 활용한 이중 인증을 구현

삼성전자 스마트폰의 기업용 모바일 보안 플랫폼인 삼성 Knox 지원

- EMM은 삼성전자 갤럭시 시리즈에 탑재된 기업용 모바일 보안 플랫폼 Knox 컨테이너를 가장 확실하게 지원합니다. 또한 모바일 OS (Android)만으로는 한계가 있는 단말 제어를 위해 제조사의 단말 관리 API를 제공받아 강화된 단말 제어를 수행하며 ,삼성전자 갤럭시 단말의 가장 최신 Knox API 기능까지 지원합니다.

- Knox Container Only Mode 지원
- Knox 컨테이너 내 최대 VPN 벤더사 지원
- Per-app VPN, CC Mode 지원
- 외장 메모리 허용 여부 지원

업계 최초 Standalone Tizen Wearable 지원

EMM 은 삼성전자 웨어러블 단말인 Tizen Wearable 을 지원합니다 . 관리자 포털에서 다수의 단말을 관리하고 , 업무용 모바일 애플리케이션의 설치를 편리하게 합니다 . 또한 단말의 기능을 제어하여 배터리 효율을 30% 까지 강화시킬 수 있습니다 .

- 스마트 폰과 페어링없이 Standalone 모드에서 원격으로 앱 배포 및 관리
- 단말 잠금 및 공장 초기화 등으로 단말 분실 시 데이터 보호
- 단말 정책 제어: Wi-Fi, 블루투스, NFC, GPS, 데이터

Samsung SDS Push로 안전하고 신뢰성 높은 양방향 Push 서비스 제공

Samsung SDS Push 는 멀티 플랫폼 (Android, iOS, Windows10) 을 지원하여 단말 적용 범위가 넓을 뿐만 아니라 사용자 , 단말의 증가에도 서비스를 유연하게 확장할 수 있습니다 . 또한 전송률 100%, 메시지 순서 보장 , 중복전송 방지 등 Public Push 의 한계를 넘어 신뢰성 높은 고품질의 양방향 Push 서비스를 제공합니다 . 통신 중 전달 되는 패킷은 물론 통신채널 보안을 통해 데이터까지 안전합니다 .

- 멀티 플랫폼(Android, iOS, Windows10) 및 멀티 애플리케이션 지원
- 안전하고 신뢰성 높은 고품질의 양방향 Push 서비스 제공
- 메시지 전송률 100% 보장, 메시지 순서 보장, 중복 전송 방지

Samsung SDS EMM Guardian 기능으로 단말 공장 초기화에도 안전

일반 EMM 은 단말의 공장 초기화 시 EMM 이 삭제되어 보안 정책이 적용되지 않습니다 . Samsung SDS EMM 의 Guardian 기능은 공장초기화로 인한 EMM 의 삭제를 감지하여 단말의 I/O 를 자동으로 제어하고 EMM 의 재설치를 유도하여 도난 , 분실에 따른 악의적인 데이터 유출을 막을 수 있습니다 .

- 단말 I/O 제어: 카메라, 외장메모리, USB 연결, 블루투스, 테더링, 화면 캡처

기업용 모바일 보안 웹브라우저(Secure Browser) 활용으로 기업 정보 유출 차단

단말의 기본 웹브라우저를 업무용으로 사용 시 텍스트 복제 , 스크린 캡쳐 등의 기능으로 기업 정보가 유출될 수 있습니다 . 또한 유해 사이트 접속 , 불법 파일 다운로드로 인한

바이러스 감염은 보안에 큰 위협이 됩니다 . EMM 의 Secure Browser 는 기업의 보안 정책을 적용하여 모바일 웹브라우저를 통한 정보 유출과 바이러스 감염 문제를 해결해 줍니다 .

- URL 블랙리스트 또는 화이트리스트 관리
- 파일 다운로드 허용 또는 차단
- 보안 정책 적용으로 텍스트 복제 및 스크린 캡쳐 등 금지

운영자를 위한 최적의 관리자 포털 제공

EMM 의 관리자 포털은 운영자 업무에 맞추어 직관적인 UI 와 기능간 연계로 운영자가 부담 없이 쉽고 간편하게 기업의 모바일 보안을 책임질 수 있도록 도와줍니다 . 운영자는 임직원 단말의 보안 상태를 한 눈에 모니터링하고 , 문제 파악에 필요한 정보를 빠르게 수집하여 보안 위반 발생 시 적절한 조치를 바로 취할 수 있어 기업의 보안을 안전하게 지킬 수 있습니다 .

- 운영자 중심의 시스템 설계로 관리자의 부담 최소화
- 보안 위반 발생 시 빠른 조취로 기업의 보안을 안전하게 유지

사전 정의한 이벤트 발생 시 보안 정책 즉각 적용

운영자는 사전에 이벤트 별로 정책을 정의할 수 있습니다 . 단말에서 이벤트 발생 시 규정된 정책 시나리오를 자동 적용함으로써 운영자가 직접 제어할 필요가 없으며 , 보다 안전한 모바일 보안 환경을 선제적으로 제공하는 동시에 운영의 효율성을 제고합니다 .

- 사전 정의 가능 이벤트: 시간, 앱, Wi-Fi SSID, SIM 카드 등

원격 지원 서비스로 신속하고 정확한 문제 해결

운영자는 원격 지원 서비스로 오류나 문의 사항 접수 시 원격으로 단말에 접속할 수 있습니다 . 이를 통해 고객의 복잡한 상황 설명이나 추가적인 조치 없이도 문제를 정확하게 파악하고 해결할 수 있으며 , 단말의 로그 분석으로 문제의 근본 원인을 파악하고 같은 문제의 발생을 사전에 예방할 수 있습니다 .

- 원격 지원서비스의 주요 기능: 화면 공유, 캡쳐, 파일 전송, 로그 수집

Kiosk Wizard를 통한 런처앱 제작

운영자는 Kiosk Wizard 로 기업용 단말에 원하는 배치 , 구성으로 특정 앱 , 위젯 , 안내 메시지만 노출되도록 설정할 수 있습니다 . 이를 통해 서비스 목적에 벗어난 사용 , 별도의 Kiosk 런처앱 구매나 개발없이 고객의 업무와 서비스에 맞도록 Kiosk 단말 구성이 가능합니다 .

- 관리자 포털에 등록된 애플리케이션과 위젯 (배경화면, 로고, 폴더, 메모, 시계, 달력, Text, 웹페이지 링크)으로 Kiosk 런처앱 구성

사용자 포털을 제공하여 사용자가 직접 단말을 관리

단말 분실 시 IT 운영자에게 연락할 필요 없이 사용자가 직접 EMM 사용자 포털을 통해 단말 잠금 실행 , 공장 초기화 실행 , 위치 조회를 할 수 있습니다 . 이를 통해 기업의 정보 유출을 방지합니다 . 동시에 운영자는 분실에 따른 업무 부담을 해소하고 공지 및 FAQ 제공을 통해 중복된 VoC 대응을 최소화합니다 .

- 사용자의 편의성을 제공하고 보안 위협에 신속 대처
- 운영자의 업무 효율성을 향상

EMM 기능

EMM 은 디바이스 관리 , 애플리케이션 관리 , 데이터 관리 및 통합 관리의 4 대 주요 보안 기능과 EMM AppStore 를 통해 사용자의 편의성을 제공하고 , 기업의 안정적인 Mobility 환경 구축을 지원합니다 .

디바이스 관리

EMM 은 무선 전송 기술을 이용하여 다양한 모바일 기기를 원격으로 제어하고 부서 , 개인 , 그리고 공간별 보안 정책의 차등 적용으로 기업 정보를 체계적으로 관리하고 보호합니다.

- 기업 정보 보안을 위해 카메라, 스크린 캡처 등의 차단 여부를 제어하는 모바일 설정 관리
- 단말 분실에 대응하여 원격 제어 및 데이터의 암호화 제공하는 모바일 보안 관리
- 화이트/블랙리스트를 기반으로 소프트웨어의 안전한 실행 제공하는 소프트웨어 설정 관리

애플리케이션 관리

EMM 은 업무용 모바일 애플리케이션을 효율적으로 공급하고 지원함으로써 급변하는 모바일 환경에서 업무 생산성 향상을 제공합니다 .

- 애플리케이션에 대한 사용자의 접근 및 권한 관리 기능 제공
- 업무 공간 접근을 위한 전용 폴더를 활용하여 애플리케이션 목록과 버전 확인
- 사용 현황 모니터링을 통해 향후 모바일 서비스 운영 정책 수립을 위한 데이터 제공

데이터 관리

EMM 은 동일한 단말 내 개인 데이터 영역와 업무 데이터 영역을 분리하여 기업 정보 접근 관리를 강화합니다 .

- 안전한 업무용 애플리케이션 사용을 위해 단말 내 전용 분리 공간 제공
- 애플리케이션 데이터를 암호화하여 저장
- 단말 분실 시 업무 데이터 영역만 선별 삭제 가능

통합 관리

EMM 은 관리자 포털에서 사용자의 단말에 정책을 전송하고 단말에 설치된 애플리케이션 또는 저장된 컨텐츠를 제어하는 등 편리한 통합 보안 관리 환경을 제공합니

- 조직 체계와의 연계를 통한 보안 정책 기능 제공
- 기업 모바일 애플리케이션의 배포와 관리 가능
- 단말 분실 등으로 인한 보안 유출 위험 발생 시 신속한 원격 제어 가능

EMM AppStore

EMM 은 사내 전용 인프라를 사용하여 업무용 애플리케이션을 안전하게 제공하고 적시에 배포합니다 . 이를 통해 급변하는 기업 환경 대응 및 효율적인 관리로 유지 비용을 절감합니다 .

- EMM AppStore를 통한 사내 애플리케이션의 효율적인 배포 및 관리
- Biz App Development를 통한 업무 생산성 및 협업 향상을 위한 애플리케이션 제공
- 업무별 적합한 다양한 애플리케이션을 제공하고 사용자가 원하는 애플리케이션 관련 기능을 추가할 수 있는 Biz App Eco-System 구축

운영 환경

EMM 서버 및 관리자 포털 운영을 위한 권장 사양은 다음과 같습니다 .

- EMM 서버
  - CPU: x64 Processor 2.0 GHz 이상
  - 메모리: 16GB 이상
  - 저장공간: 300GB 이상
  - OS: Microsoft Windows 2008 Enterprise Server(64bit) 이상
  - DBMS: Microsoft SQL Server 2008, 2016
    설치 하드웨어 외 소프트웨어의 세부 사양은 Microsoft 공식 홈페이지 참고
- EMM 관리자 포털
  - OS: Windows XP 이상
  - 웹 브라우저: Google Chrome 41 이상, Firefox 37 이상, Microsoft Internet Explorer 11 권장
  - 최적 해상도: 1,680 x 1,050(px)
- 단말 OS
  - Android: Android 4.4(Kitkat) ~ Android 8.0 (Oreo)의 삼성 및 타사 단말
  - iOS: iOS 8.0 이상
  - Windows: Windows10 1703 이상의 데스크탑 (Pro/Enterprise/Home)
  - Tizen Wearable: Tizen 2.3.2 이상

Note: 2.0.2 버전의 신규 사용자는 EMM Client와 Agent를 통합한 하나의 파일을 Android 단말에 설치하여 사용할 수 있습니다. 이전 버전에서 업그레이드를 한 사용자가 통합 Agent 파일을 사용하려면 단말에서 EMM을 비활성화한 후 재설치를 해야합니다.

시작하기

EMM 관리자 포털은 사용자의 단말 제어부터 애플리케이션 및 단말내 데이터까지 통합 보안 관리가 가능하며 , 단말의 보안 상태를 한 눈에 모니터링하여 문제 해결을 위한 정보를 수집할 수 있습니다 .

관리자 포털에 로그인하기

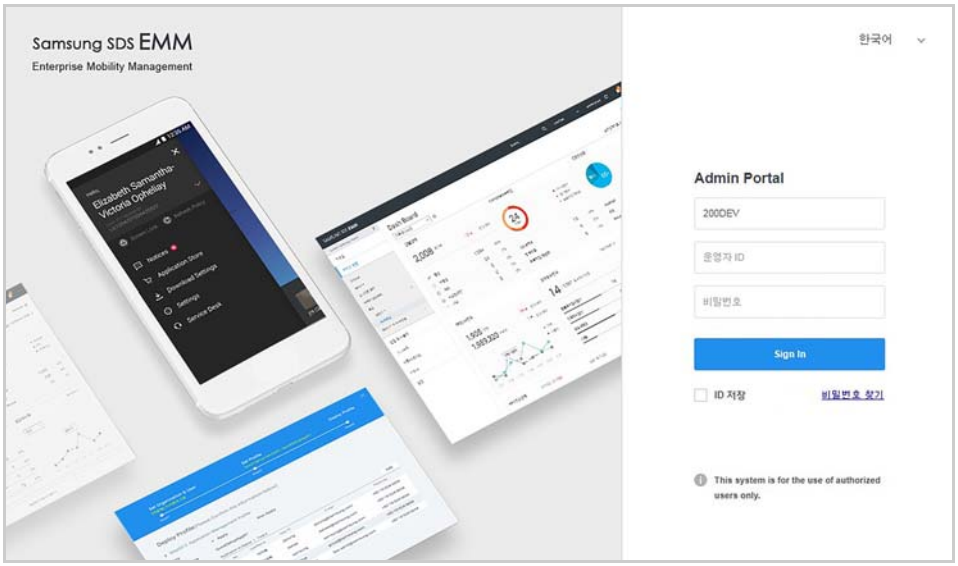
관리자 포털에 로그인하려면 회사명 , 운영자 ID, 비밀번호가 필요하며 EMM 운영 모드에 따라 로그인 방법이 다를 수 있습니다 .

- EMM이 Single-Tenant로 운영되는 경우, 회사명(Tenant ID) 입력란은 화면에 나타나지 않습니다.

- EMM이 Multi-Tenant로 운영되는 경우, TMS 운영자가 회사명(Tenant ID)을 관리하므로 TMS 운영자에게 문의하세요.
  Multi-Tenant 운영에 대한 자세한 내용은 “Samsung SDS TMS 매뉴얼”을 참고하세요.

관리자 포털에 로그인하려면 다음의 절차를 따르세요 .

관리자 포털은 영어 , 포르투갈어 , 스페인어 , 프랑스어 , 독일어 , 이탈리아 , 중국어 , 한국어를 지원합니다 .



1. EMM 관리자 포털의 로그인 페이지에 접속하세요.
2. 사용하려는 **언어**를 선택하고 **회사ID**, **운영자 ID**, **비밀번호**를 입력한 후, **Sign in**을 클릭하세요.
   - 해당 운영자 ID로 계속 로그인하려면 **ID 저장**을 클릭하세요.
   - 비밀번호를 찾으려면 **비밀번호 찾기**를 클릭하세요.
     - “비밀번호 찾기” 창에서 **운영자 ID@회사 ID**를 입력한 후, **확인**을 클릭하면 등록된 이메일 또는 전화번호로 임시 비밀번호가 발송됩니다.
   - 연속 5회 이상 비밀번호 입력 오류 시 해당 계정은 10분간 잠금 상태가 됩니다.
3. “OTP 인증” 창에서 SMS 또는 Email 주소로 전송받은 OTP 번호를 입력한 후, **확인**을 클릭하세요.
   - 관리자 포털에 2단계 인증이 TRUE로 설정되고, 사용자 등록 시 SMS 또는 Email 정보가 있어야만 OTP 전송이 가능합니다. 만약, 정보가 없는 경우 OTP가 전송되지 않습니다.

관리자 포털의 기본 UI

관리자 포털 상단의 기본 UI 는 다음과 같은 영역들로 구성되어 있습니다 .

번호	설명
1	EMM의 관리 영역입니다. 운영자의 비밀번호 변경, 세션 타임아웃 설정, 고대비 테마 설정 및 관리자 포털로부터 로그 아웃을 할 수 있습니다. • **비밀번호 변경**: 최소 8자에서 최대 30자까지 가능하며 하나 이상의 숫자, 특수문자, 그리고 영문자를 반드시 포함하여 구성합니다. • **세션 타임아웃 설정**: 운영자의 세션 타임아웃 시간을 설정합니다. 세션 타임아웃은 최대 60분까지 설정이 가능하며, 타임아웃 발생 5분전에 경고 팝업이 나타납니다. 세션 타임아웃은 **설정 > 서비스 > 환경 설정**의 **시스템 세션 타임아웃 시간(분)**에서 설정합니다. • **고대비 테마 적용**: 고대비 테마 적용을 통해 저시력 장애인의 경우라도 관리자 포털의 사용이 가능합니다. 
2	마크 영역입니다. EMM 관리자 포털 화면의 우측 ★을 클릭하면 해당 페이지가 즐겨찾기에 등록됩니다. 이 후 관리자 포털의 어느 화면에서든 ★을 클릭하여 즐겨찾기에 추가된 페이지로 쉽게 이동할 수 있습니다.
3	버튼과 검색 영역입니다. • 버튼 영역: 각 화면 우측 상단에 위치하며, 버튼에 따른 기능이 수행됩니다. • 검색 영역: 각 화면 좌측 상단에 위치하며 메뉴에 따라 검색 값을 입력한 후, 검색하는 텍스트 검색 기능과 조건 또는 검색 기준을 선택하여 검색하는 필터 검색 기능이 있습니다. 
4	칼럼 영역입니다. 칼럼명을 선택하여 칼럼을 정렬할 수 있습니다. 칼럼명 우측의 ∨을 클릭하면 **칼럼 목록**과 **Filters**가 보입니다. • 칼럼 목록: 칼럼명의 체크박스를 클릭하거나 해제하여 해당 칼럼을 보이게 하거나 숨길 수 있습니다. • Filters: 필터를 선택하여 해당 칼럼에 필터를 적용할 수 있습니다.
5	화면 확대 기능입니다. 팝업창 또는 각 메뉴 화면에서 ‹ 또는 ›을 클릭하여 왼쪽화면 영역을 좁히거나 넓힐 수 있습니다.

Note: 관리자 포털의 팝업 화면에서 입력 항목명 앞에 표시(*)는 필수 입력값이며, 나머지는 선택 사항입니다.

관리자 포털의 메인 메뉴

관리자 포털의 메인 메뉴는 다음과 같이 구성되어 있습니다 .

- 서비스 현황
  단말에 보내는 공지사항을 등록하고, EMM의 운영 현황을 모니터링 할 수 있는 대시보드를 관리합니다. 또한 서버나 단말의 중요한 정보를 모니터링 알림으로 제공하고, 단말 제어가 전송되지 않은 단말 정보를 미처리 단말 제어에서 확인합니다. 그외 서버, 단말, 커넥터 및 Audit 로그에 대한 정보와 EMM과 연계된 커넥터 사용에 대한 접속 통계 정보를 제공합니다.
- 단말 & 사용자
  사용자, 조직, 그룹 정보 및 사용자의 단말 정보를 통합적으로 관리합니다. 또한 단말과 그룹에 전송된 단말의 제어 이력과 전송된 이메일 또는 SMS 메시지 이력을 관리하고 AD/LDAP 연계를 통한 사용자, 그룹, 조직의 동기화 서비스를 제공합니다. 그외, E-FOTA 서비스를 통해 특정 펌웨어 버전으로 업데이트가 가능하도록 E-FOTA 그룹을 관리합니다.
- 프로파일
  사용자의 단말 관리 및 단말의 애플리케이션을 관리하기 위해 정책을 설정하고, 그룹 또는 조직의 단말에 적용하여 단말을 관리합니다. 또한 단말에 기간을 설정하여 사용자별 예외 정책을 설정합니다.
- 애플리케이션
  기업 내 배포를 위한 업무용 사내 애플리케이션과 Google PlayStore 및 Apple AppStore를 통해 배포되는 외부 애플리케이션을 관리합니다. 또한 Kiosk 런처 애플리케이션 및 단말에 설치되는 애플리케이션의 제어를 위해 제어 애플리케이션을 관리합니다. 그외, EMM의 SYSTEM 애플리케이션과 EMM에서 제공하는 애플리케이션을 관리합니다.
- 인증서
  외부인증기관을 통해 발급받은 Wifi, Generic VPN, VPN, Exchange, APNS, CA Cert, Mobile Mail 등의 네트워크 인증서와 사용자 인증서를 관리합니다. EMM은 CA (Certificate Authority)를 통해 발급된 모든 인증서를 관리하며, 프로파일 양식을 탬플릿화하여 인증서 관리가 가능합니다. EMM에서 등록가능한 CA 유형은 ADCS, Generic SCEP, NDES, CertAgent, EST입니다.
- 설정
  EMM 운영 시 필요한 모든 환경 설정과 메일, Audit, 인증, 프록시, Public Push, SMS, E-FOTA 등의 서버를 설정합니다. 또한 EMM 서비스를 위한 기준 정보, 라이선스 정보 및 메시지 템플릿 등을 관리합니다. 그외 관리자 포털의 운영자 및 EMM과 연계 가능한 연동 시스템 관리, EMM Open API 사용을 위해 API 사용자 설정, API 로그 및 API 사용 이력 관리, 그리고 Windows10의 CSP 설정과 PPKG 파일을 설정합니다.

모니터링 알림 팝업

운영자는 로그인 시 모니터링 알림 팝업을 통해 EMM 의 유효한 라이선스 정보를 확인합니다 . 또한 EMM 에서 설정한 정책의 적용 실패 , EMM 에서 발생된 변경 내용 , 단말의 변경 내용 , 보안 위반 사항 등을 확인합니다 . 그외 모니터링 알림 팝업에서 각 알림 항목을 클릭하거나 팝업 하단의 **전체 알림 확인**을 클릭하면 발생된 이벤트에 대한 내용 및 단말 정보 확인이 가능합니다 . 모니터링에 대한 자세한 내용은 54 페이지의 "3 모니터링 " 을 참고하세요 .

관리자 포털의 로고와 로그인 알림메시지 설정하기

관리자 포털의 로그인 전 웰컴 화면 하단에 나타나는 알림메시지와 로그인 후 , 보여지는 왼쪽 상단의 로고 이미지 변경이 가능합니다 .

로고 또는 로그인 알림메시지를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > Admin Console > 시스템 관리로** 이동하세요.
2. 화면 상단의 **로고 / 알림메시지**를 클릭하세요.

   - **로고**: 관리자 포털의 상단에 보여지는 로고를 등록합니다.
   - **로그인 알림메시지**: 관리자 포털에 로그인 전 화면 하단에 나타나는 알림메시지를 등록합니다.
3. “로고 / 알림메시지” 창에 로고와 로그인 알림메시지를 설정한 후, **저장**을 클릭하세요.

Wearable EMM 사용하기

삼성 전자 웨어러블 단말에서 Wearable EMM 의 사용이 가능합니다 . Wearable EMM 은 Tizen Wearable 플랫폼의 웨어러블 단말에서 운영되며 , 업무용 애플리케이션에 대한 관리 및 배포를 통해 웨어러블 제어가 가능합니다 .

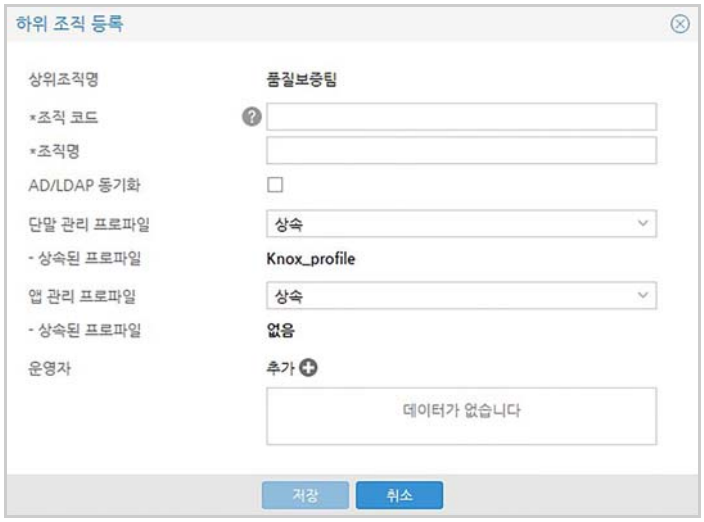
다음은 웨어러블 단말 사용을 위한 단계별 시나리오로 시나리오 예시 외에도 다양한 방법으로 Wearable EMM 을 사용할 수 있으며 , 기능에 대한 추가적인 자세한 내용은 각 챕터별 상세 설명을 참고하세요 .

조직 생성하기

관리자 포털에 조직을 생성하고 , 웨어러블 단말을 사용하는 사용자를 등록합니다 .

관리자 포털에 조직을 생성하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 왼쪽의 **조직**에서 조직을 추가하려는 상위 조직을 클릭하세요.
3. 조직 우측의 ⋯을 클릭한 후, **하위 조직 등록**을 클릭하세요.
4. 조직 코드, 조직명, AD/LDAP 동기화, 단말 관리 프로파일, 앱 관리 프로파일, 운영자 정보를 입력하세요.



5. **저장**을 클릭하세요.

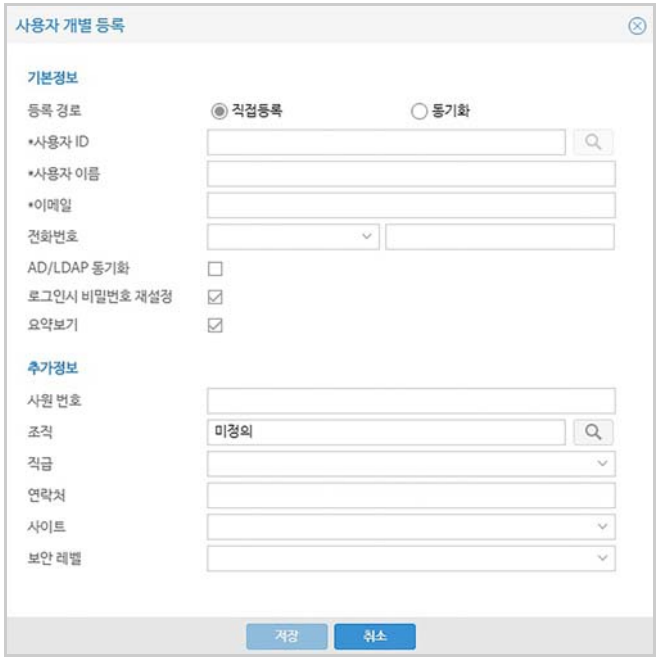
사용자 등록하기

조직을 생성한 후 , 사용자를 개별로 직접 등록합니다 . 사용자 등록에 대한 자세한 내용은 81 페이지 5 장의 " 사용자 계정 개별 등록하기 " 를 참고하세요 .

사용자를 개별로 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.

2. 조직을 선택한 후, 화면 상단의 ＋을 클릭한 다음 **개별 등록**을 선택하세요.
3. "사용자 개별 등록" 창에 사용자 정보를 입력하세요.



- **등록 경로**: **직접등록**을 선택하세요.
- 추가 정보에서 **조직** 우측의 🔍을 클릭한 후, 조직을 선택하면 사용자와 조직이 다시 매핑됩니다.

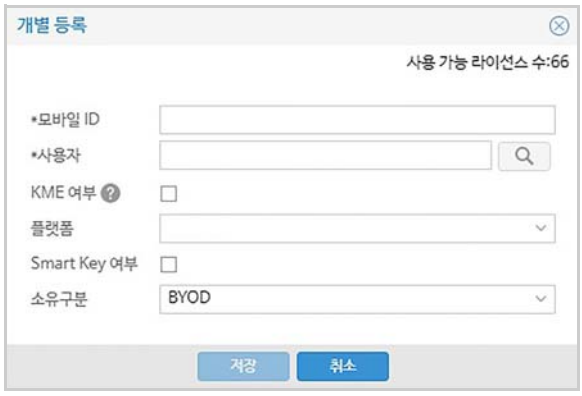
4. **저장**을 클릭하세요.

웨어러블 단말 등록하기

웨어러블 단말을 개별로 등록합니다 . 자세한 내용은 111 페이지 8 장의 " 개별 단말 등록하기 " 를 참고하세요 .

웨어러블 단말을 개별로 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. 화면 상단의 ＋을 클릭한 후, **개별 등록**을 선택하세요.



3. **모바일 ID**를 입력하고 **사용자** 입력란의 우측에서 🔍을 클릭한 후, "사용자 조회" 창에서 사용자를 선택하고 **확인**을 클릭하세요.

4. 웨어러블 단말을 등록하려면 **KME 여부**를 해제한 후, 플랫폼을 **Tizen Wearable**로 선택하세요.
   - **핸드폰 번호**를 입력하고 **소유구분** 을 선택하세요. **핸드폰 번호**를 반드시 입력해야만 단말 설치 정보에 대한 SMS 발송이 가능합니다.
5. **저장**을 클릭하세요.

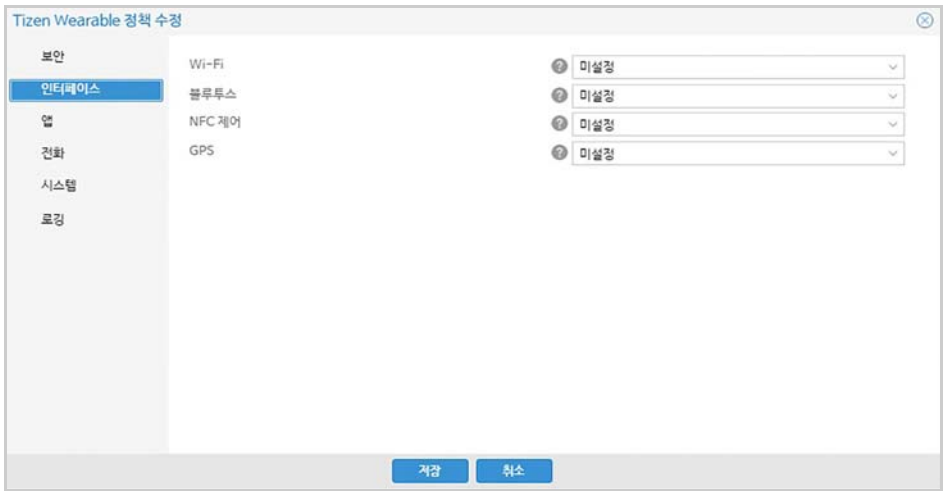
프로파일 생성하기

웨어러블 단말에 적용하려는 프로파일을 설정합니다 .

예시로 GPS 기능을 제어하는 프로파일을 신규로 생성하고 , 조직에 할당하여 사용자의 단말에 적용시키려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 화면 상단의 ＋을 클릭한 후, **신규등록**을 선택하세요.

3. “신규 등록” 창에 **프로파일명**과 **설명**을 입력하세요. (예: Control 1)
4. **다음**을 클릭한 후, 확인 메시지에서 **예**를 클릭하세요.
   - 한번 생성된 프로파일명은 수정이 불가능하며, 삭제만 가능합니다.
5. “단말 관리 프로파일” 창에서 좌측 메뉴 중 **Tizen Wearable > 정책**으로 이동하세요.
6. **Tizen Wearable 정책** 우측의 을 클릭하세요.
7. “Tizen Wearable 정책 수정” 창에서 좌측 메뉴 중 **인터페이스**를 클릭하세요.
8. **GPS**의 **금지**를 선택한 후, **저장**을 클릭하세요.
   - 설정한 GPS 금지 정책이 “단말 관리 프로파일” 창에 보여집니다.



9. **저장**을 클릭하세요.

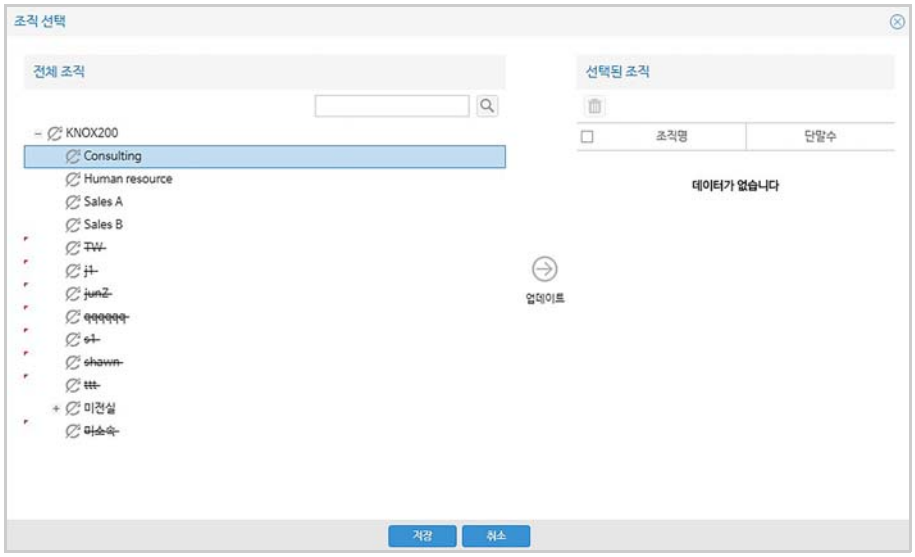
프로파일 할당하기

운영자는 사용자가 속해 있는 조직에 프로파일을 할당하여 단말에 정책을 적용합니다 .

프로파일 설정에 대한 자세한 내용은 134 페이지 10 장의 " 프로파일 " 을 참고하세요 .

조직에 프로파일을 할당하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 조직에 할당하려는 프로파일의 행을 선택한(예: **Control 1** 선택)후, Actions에서 을 클릭하세요. 또는 프로파일명을 클릭한 후, "단말 관리 프로파일" 창에서 **조직** 우측의 을 클릭하세요.



3. "조직 선택" 창에서 조직을 선택한 다음 **업데이트**를 클릭한 후, **저장**을 클릭하세요.
   - 하나의 조직에는 단 하나의 프로파일만 할당할 수 있으며, 이미 프로파일이 매핑된 조직은 전체 조직의 리스트에서 조직명에 취소선이 그어져 있습니다.
4. "프로파일 배포" 창에서 **예**를 클릭하면 조직의 단말에 프로파일이 즉시 배포됩니다.

웨어러블 단말에 설치 정보 전송하기

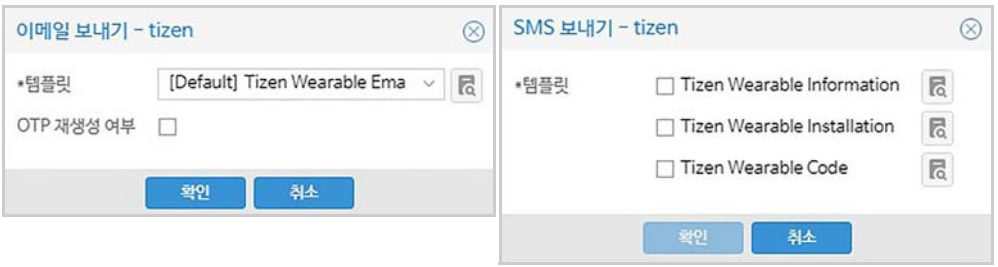
화면이 작은 웨어러블 단말의 특성을 고려하여 Wearable EMM 설치 및 활성화 시 사용자의 입력을 최소화 할 수 있는 방식을 제공합니다 .

웨어러블 단말에 개별 또는 대량으로 설치 정보를 전송하는 방법은 다음과 같습니다 .

- Wearable EMM 설치 정보인 다운로드 URL 주소를 SMS로 개별 단말에 전송
- KME (Bulk installation) 사이트에 대량의 단말 정보를 등록한후, 단말 설치 정보를 전송

운영자가 웨어러블 사용자에게 Wearable EMM 설치 정보를 SMS 또는이메일로 보내려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**으로 검색한 후, 단말을 선택하세요.
3. 설치 정보를 이메일로 보내려면 을, SMS로 보내려면 을 클릭하세요.
   - 여러 대의 단말에 보내려면 단말들을 선택한 후, 목록 상단의 또는 을 클릭하세요.



4. 이메일 또는 SMS의 **템플릿**을 선택하세요.
   - 템플릿 미리보기가 가능합니다.
   - 템플릿은 **설정 > 서비스 > 메시지 템플릿**에 등록되어 있습니다.
5. **확인**을 클릭하면, 해당 단말에 설치 정보가 전송됩니다.

웨어러블 단말 활성화하기

사용자는 웨어러블 단말에 Wearable EMM 을 설치한 후 , 해당 앱을 실행하여 로그인합니다 . Wearable EMM 에 로그인하면 웨어러블 단말이 활성화되고 설정된 정책이 즉시 적용됩니다 . 단말 활성화 방법과 자동 설치 애플리케이션 설치에 대한 자세한 내용은 “Samsung SDS EMM 사용자 매뉴얼 ” 의 Wearable EMM 사용하기를 참고하세요 .

사용자의 단말에 Wearable EMM 을 설치한 후 , 실행하려면 다음의 절차를 따르세요 .

1. 사용자의 웨어러블 단말에 전송된 **Tizen Wearable 설치 URL**을 클릭한 후, Wearable EMM을 설치하세요.
2. Wearable EMM을 실행하려면 아이콘을 탭하거나, Wearable EMM 위젯을 등록한 후, 위젯을 탭하세요.
3. 접속 URL 타입을 확인한 후, **다음**을 탭하세요.
   - **자동 입력**: EMM 관리자 포털에서 설치 정보를 발송하면 Tizen Wearable 단말에 수신된 SMS에서 정보를 추출하여 Wearable EMM 접속 URL 주소가 자동으로 입력됩니다.
     - 웨어러블 단말에서 **접속 URL**을 확인한 후, **다음**을 클릭하면 Wearable EMM에 로그인됩니다.
   - **수동 입력**: SMS 전송이 안되는 경우, 이메일 등 기타 경로로 전달된 서버 URL 주소를 직접 입력해야합니다.

- 접속 URL 타입을 선택한 후, '/'뒤의 상세 주소만 입력하거나 **Manual**로 선택한 후, 전체 URL 주소를 입력하세요.
  예)**접속 URL**이 https://goo.gl/7VgJuk인 경우, **접속 URL 타입**을 **goo.gl**으로 선택하고 아래 입력란에는 **7VgJuk**를 입력하세요.

4. 운영자로부터 전달받은 8자리 인증 코드를 입력하고 **LOGIN**을 탭하세요.
5. 최종 사용자 라이선스 동의서를 읽고 **예**를 탭하세요.
6. 라이선스 안내가 나타나면 맨 아래 끝까지 스크롤하여 **동의**를 선택한 후, **확인**을 탭하세요.
   - 라이선스 인증 절차 시 EMM은 자동으로 Samsung SDS Push 서비스를 등록하고, 정책 및 앱 프로파일 전송을 위해 단말과 항상 수신합니다.

사내 애플리케이션 등록하기

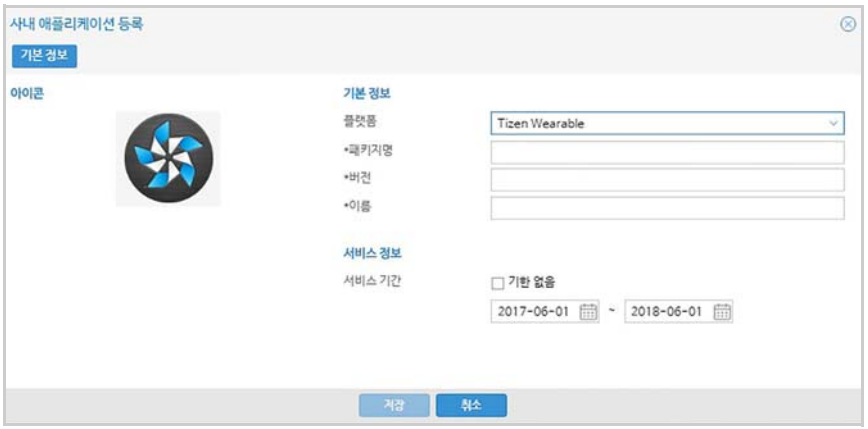
Wearable EMM 에 로그인 과정을 거쳐 웨어러블 단말이 활성화된 후 , 추가적으로 웨어러블 단말에 설치하려는 사내 애플리케이션 파일을 등록하여 배포할 수 있습니다 .

EMM 을 통해 웨어러블 단말에 Tizen Wearable 앱을 배포하려면 삼성 기어 앱 스토어에 가입한 후 , 앱을 등록해야 합니다 . 또한 모바일 단말과 페어링 없이 단독으로 사용하는 웨어러블 단말에 앱을 자동 설치하려면 Tizen 2.3.2.3 버전 이상이 설치된 웨어러블 환경에 앱에 대한 Stub API 권한이 있어야만 가능합니다 .

사내 애플리케이션을 등록하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > 사내 애플리케이션**으로 이동하세요.
2. 화면 상단의 ＋을 클릭하세요.

3. “사내 어플리케이션 등록” 창에 **기본 정보**를 입력하세요.



항목	설명
기본 정보	**플랫폼**: Tizen Wearable를 선택합니다. **패키지명**: 기어 앱 스토어에 등록된 패키지명과 버전을 입력합니다. • 웨어러블 단말의 앱은 기어 앱 스토어의 URL 주소를 클릭하여 설치하며, EMM 서버에 별도의 설치 파일 등록이 필요하지 않습니다. • 동일한 패키지(번들)를 갖는 애플리케이션은 여러 버전으로 등록이 가능합니다.
서비스 정보	**서비스 기간**: 애플리케이션 서비스 기간을 설정합니다. • 기한없음 또는 시작일과 종료일을 입력합니다.

4. **저장**을 클릭하세요.

애플리케이션 정책 설정하기

사내 애플리케이션으로 등록된 앱을 웨어러블 단말에 설치할 수 있습니다 . 애플리케이션 정책을 등록하면 웨어러블 단말에 로그인 시 자동으로 앱이 설치됩니다 .

애플리케이션을 추가하여 앱 정책을 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 앱 관리 프로파일**로 이동하세요.
2. 목록에서 애플리케이션을 추가하려는 프로파일명을 클릭하세요.
3. “앱 관리 프로파일” 창에서 **애플리케이션**을 클릭하세요.
4. “앱 관리 프로파일” 창에서 **애플리케이션** 우측의 ＋을 클릭하세요. “앱 목록” 창이 나타납니다.
5. Tizen 플랫폼의 애플리케이션을 선택한 후, **다음**을 클릭하세요.
6. “앱 정책 등록” 창의 정보를 입력한 후, **저장**을 클릭하세요.
   추가가 완료되면 해당 애플리케이션은 애플리케이션 목록에 보여집니다.
   - **구분**: 해당 애플리케이션의 구분을 **필수**로 설정하세요. 필수로 선택 시 웨어러블 단말에 필수 애플리케이션으로 설치됩니다.

웨어러블 단말 제어

운영자는 설정한 프로파일을 EMM 의 단말 제어를 통해 웨어러블 단말에 적용합니다 .

조직에 등록된 사용자의 단말을 프로파일로 제어하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. "사용자 & 조직" 화면의 **조직** 영역에서 프로파일이 할당된 조직을 선택하세요.

3. 단말제어를 보내려는 사용자를 선택한 후, 체크 박스를 클릭하세요.
   - 사용자는 다중 선택이 가능합니다.
4. 상단의 **단말제어**를 클릭한 후, **단말제어(Tizen Wearable)** 플랫폼을 선택하세요.
5. "단말 제어" 창에서 **Compliance**를 클릭한 후, **최신 단말 관리 프로파일/앱 정보 배포**를 클릭하세요.
6. 단말 제어 명령으로 프로파일을 전송하려면 **확인**을 클릭하세요.
   - 배포된 프로파일이 사용자의 웨어러블 단말에 전송되고 단말제어가 즉시 실행됩니다.

2 설정

EMM 관리자 포털의 효율적인 운영을 위해 시스템 환경을 설정하고 관리합니다 .

관리자 포털에서 설정 가능한 항목들은 다음과 같습니다 .

- 환경 설정: EMM의 각 환경 설정 항목들은 분류별로 구분되어있으며, 운영자에 의해 수정이 가능합니다. 환경 설정에서는 이메일 및 SMS 전송을 위한 서버 설정, 커넥터 서비스 운영 시 운영 시간 설정, Audit 로그 관리를 위한 외부 서버 설정, 프록시 서버 설정, Public Push 서버 설정, E-FOTA 서비스 설정 및 단말에서 EMM에 로그인 시 적용되는 인증 방식을 설정합니다. 또한, EMM 서비스를 위한 서버들의 정보 및 다운로드 URL 주소 등의 서비스 프로파일 정보와 프로파일 업데이트 주기를 설정합니다.
- 기준 정보: EMM의 운영을 위해 필요한 기준이 되는 정보들을 분류하여 관리합니다.
- 태블릿 모델 관리: EMM 사용을 위해 태블릿 모델을 등록하여 관리합니다.
- 서버 정보 및 서버 목록: 운영 중인 EMM 서버의 정보와 오픈 소스 정보를 관리하고, EMM 서버가 클러스터링 되어 있는 경우 여러곳에서 가동 중인 EMM 서버의 목록을 관리합니다.
- 라이선스 정보: EMM의 제품 패키지 라이선스를 관리합니다.
- 메시지 템플릿: SMS 또는 E-mail로 개인 정보 및 EMM 설치 정보를 발송하기 위해 메시지 템플릿을 등록하고 관리합니다.
- IMEI 관리: IMEI는 단말의 국제 고유 식별 번호로, IMEI를 등록한 단말만 활성화하기 위해 IMEI를 설정합니다.

환경 설정하기

운영자는 EMM 의 환경 설정 항목들을 관리합니다 . 분류별로 구분된 각 환경 설정 항목들은 운영자에 의해 임의로 추가할 수 없으며 , 환경 설정의 값만 수정이 가능합니다 .

다음은 환경 설정의 각 항목들에 대한 설명입니다 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.
2. 분류별 세부 사항을 확인하려면 **분류** 좌측의 ⊞을 클릭하세요.
   각 분류별 항목들에 대한 자세한 설명은 다음과 같습니다.

- **Admin**: 운영자의 로그인에 대한 제한 사항 및 OTP 인증 설정, 기본 국가코드 및 Copyright 정보 등에 대한 설정입니다.

분류	설명
2단계 인증	관리자 포털에 로그인 시 운영자 ID, 비밀번호 외 OTP 인증 여부를 설정합니다. OTP 인증을 위해서는 운영자의 SMS 또는 E-mail 정보가 반드시 필요합니다. 해당 정보가 없는 경우에는 OTP가 전송되지 않습니다. • TRUE • FALSE
기본 국가코드	EMM이 운영되는 지역의 국가코드를 설정합니다. 기본 국가코드는 운영자 및 사용자 등록 또는 외부 애플리케이션 등록 시 기본 값으로 사용됩니다.
로그인 연속 실패 허용 횟수	아이디 또는 비밀번호 입력 오류로 연속해서 로그인에 실패하는 경우, 실패를 허용하는 횟수를 설정합니다. 허용 횟수를 초과하여 입력하는 경우에는 사용자 계정 잠금 등이 실행됩니다. • 입력 범위: 최소 3회이상, 기본 값은 5회로 설정
운영자미사용계정 허용 일수 (일)	운영자가 계정 미사용 허용 일수에 설정한 기간 동안 로그인하지 않을 경우, 계정이 비활성화 되고 로그인이 불가능하게 됩니다. 다시 로그인하려면 수퍼 운영자에게 문의하세요. • 입력 범위: 10~100일, 기본 값은 30일로 설정
시스템 세션 타임 아웃 시간 (분)	관리자 포털의 세션 타임 아웃 시간을 설정합니다. • 입력 범위: 1~60분, 기본 값은 30분으로 설정
Copyright	관리자 포털의 좌측 하단에 나타나는 Copyright 정보를 설정합니다.
로그인 연속 실패 허용 횟수 초과시, 계정 잠금 설정	로그인 연속 실패 허용 횟수를 초과하여 로그인에 실패하는 경우, 다음 중 제약 사항을 선택하여 로그인을 제한할 수 있습니다. • 상위 운영자가 해제 시까지 비활성화 • 10분간 로그인 금지 • No Action
동시 로그인 제한	관리자 포털에 같은 계정으로 동시에 로그인하는 경우, 동시 로그인에 대한 허용 여부를 설정합니다. • 사용 • 미사용

- **Certificate**: 외부 인증서 저장 여부에 대한 설정입니다.

분류	설명
iOS 설정 인증서 서버 저장	iOS 단말인 경우 Wi-Fi, VPN, Exchange 사용을 위해 필요한 외부 인증서를 EMM 서버가 iOS 단말에 제공하며, 이를 위해 EMM 서버에 인증서를 저장할지 여부를 설정합니다. • TRUE: True로 설정하는 경우, iOS 용 외부 인증서를 최초 발급 시 EMM 서버에 인증서를 저장하여 프로파일을 적용할때 마다 저장된 인증서를 단말에 제공합니다. 또한, 사용자가 iOS 단말에서 Wi-Fi, VPN, Exchange 인증서를 삭제하려면 해당 항목이 True로 설정되어있어야 합니다. • FALSE: False로 설정하는 경우, 프로파일을 적용할때 마다 새로운 인증서를 발급받아 단말에 제공합니다.

- **Device**: 사용자 단말에 대한 설정입니다.

분류	설명
IMEI 등록 제한	IMEI는 모바일 단말마다 부여되는 단말의 고유 번호로 IMEI를 등록한 단말의 활성화 유무를 설정합니다. • TRUE: TRUE로 설정한 경우, **설정 > 서비스 > IMEI 관리**에서 IMEI를 등록한 단말만 활성화됩니다. • FALSE
단말 등록 서버 주소	단말 정보가 등록되는 EMM 서버의 주소를 설정합니다. URL 입력시 EMM 서버 주소의 끝에 '/'를 추가하여 입력합니다. 예: https://emm.sds.com:35443/
단말 자동 등록	사용자가 단말의 EMM에 로그인하는 경우, 사용자의 단말이 자동으로 EMM 서버에 등록될 수 있도록 설정합니다. 사용자 정보는 반드시 관리자 포털에 먼저 등록되어있어야 합니다. • 사용 • 미사용
사용자당최대활성 단말 수	사용자 당 활성화가 가능한 최대 단말 수를 설정합니다. • 미사용 • 입력 범위: 1~5개
단말 위치	단말의 위치 정보 확인을 위한 Map을 설정합니다. 기본 설정은 Google Map이며, 중국내 단말 위치 조회를 하려면 Baidu Map을 선택합니다. Map을 통한 단말의 위치 확인은 **단말 & 사용자 > 단말**의 **단말 상세** 화면에서 가능합니다. • Google Map • Baidu Map: 중국내 단말의 위치 조회시 사용

- **EMM Client**: 최초로 단말의 EMM에 로그인하는 경우, 보여지는 개인정보 취급정보 동의서(EULA)에 대한 설정입니다.

분류	설명
개인정보취급정보 제목	개인정보 취급정보 동의서(EULA)의 제목을 설정합니다.
개인정보취급정보 Url	개인정보 취급정보 동의서(EULA)의 내용이 작성된 Url 주소를 설정합니다.

- **Exception Policy Scheduler**: 사용자별 예외 정책 적용을 위한 스케줄 시간을 설정합니다.

분류	설명
예외정책적용/해제 스케줄 시각 (시)	사용자의 단말에서 사용자별 예외 정책 실행을 위해 **프로파일 > 사용자별 예외 정책**에서 기간을 설정하고, 예외 정책이 적용되는 시각을 설정합니다. • 입력 범위: 0~23시이며, 기본값은 자정 0시
예외정책적용/해제 스케줄 시각 (분)	사용자의 단말에서 사용자별 예외 정책 실행을 위해 **프로파일 > 사용자별 예외 정책**에서 기간을 설정하고, 예외 정책이 적용되는 시간의 분을 설정합니다. • 입력 범위: 0~59분이며, 기본값은 10분

- **Inventory Scheduler**: 플랫폼 별로 사용자의 단말 정보 수집에 대한 주기를 설정합니다.

분류	설명
Android 인벤토리 수집 주기 (시간)	Android 단말 정보 및 단말 위치 정보 수집 주기를 시간 단위로 설정합니다. (0으로 설정하면, 스케쥴러에 의한 단말 정보 수집이 수행되지 않음) • 입력 범위: 0, 4~24 시간
iOS 인벤토리 수집 주기 (시간)	iOS 단말의 단말 정보 수집 주기를 시간 단위로 설정합니다. (0으로 설정하면, 스케쥴러에 의한 단말 정보 수집이 수행되지 않음) • 입력 범위: 0, 4~24 시간
Windows 인벤토리 수집 주기 (MDM Agent Polling 주기, 시간)	Windows 단말의 단말 정보 수집 주기를 시간 단위로 설정합니다. (MDM Agent와의 동기화 주기를 따르며, 0으로 설정하면 스케쥴러에 의한 단말 정보 수집이 수행되지 않음) • 입력 범위: 0, 4~24 시간

- **MDM**: MDM의 기본 설정입니다.

분류	설명
APNs Topic	MDM용 APNs 인증서 소유자의 아이디로, **설정 > 서비스 > 환경설정 > APNs 설정**에서 인증서 업로드시 자동으로 입력됩니다. 만약, APNs Topic 값이 APNs 설정의 현재 Subject Name의 UID 값과 다를 경우, 현재의 UID 값으로 다음과 같이 입력하세요. 명령 프롬프트에서 다음과 같이 명령을 실행하여 "UID=" 뒤에 나오는 값을 APNs Topic에 설정합니다. `C:/> keytool -v -list -storetype pkcs12 -keystore {APNS 인증서 파일명}.p12 | find "UID"`
Attestation Api Key	Attestation API 호출을 위한 Key 값입니다.
Attestation 서버 주소	Attestation 서버의 주소입니다. Attestation 서버 접근 시 프록시 서버 사용 여부는 **설정 > 서비스 >환경설정**의 **네트워크**메뉴에서 설정합니다.
ELM License Key	Enterprise License Manager(ELM) 제품의 라이선스 Key 값입니다.
잠금화면에서 카메라 제어 사용 여부	단말의 화면잠금 상태에서 카메라 사용 여부를 설정합니다. • TRUE: TRUE로 선택한 경우, 화면의 잠김 상태에서도 카메라 사용이 가능합니다. • FALSE: FALSE로 선택한 경우, 화면의 잠김 상태에서는 카메라 사용이 불가능합니다.
Knox License Key 만료일	Knox 라이선스 만료일입니다.
Knox License Key	Knox 라이선스 Key 값입니다.
SCEP 서블릿 URL	Simple Certificate Enrollment Protocol(SCEP) 서비스를 지원하는 서블릿 URL의 주소입니다. 해당 값을 설정하지 않는 경우, EMM에 내장된 JSCEP 라이브러리가 사용됩니다.
MDM Service URL (http://host:port)	iOS에서 MDM 서비스를 사용하기 위해 설정되는 URL 주소로 주소의 형식은 http://host:port 입니다.

분류	설명
통신 데이터 서명 인증서 (iOS)	통신 데이터 서명 인증서는 iOS 단말인 경우, EMM 서버에서 단말로 데이터 전달이 안전하다는 것을 증명하기 위한 인증서입니다. 해당 인증서의 등록은 **인증서 > 외부 인증서**에서 인증서 용도를 iOS Sign Cert, 인증서 유형을 Server로 선택하여 등록하며, 등록된 인증서는 iOS 단말에 다운로드되어 사용됩니다.
KeepAlive 체크 주기 (시간)	KeepAlive 설정에 대한 자세한 내용은 26페이지의 " KeepAlive 설정하기"를 참고하세요.
Unenrollment 시 앱 삭제	Unenrollment 시 앱을 삭제할지 여부를 설정합니다. • 사용: 사용으로 선택한 경우, 운영자가 단말을 비활성화 상태로 변경 시 EMM은 Android 단말에 설치된 Managed App을 삭제한 다음 단말을 비활성화합니다. 또한 iOS 단말을 비활성화 상태로 변경하는 경우에는 삭제전에 삭제 예정인 앱 목록이 화면에 나타납니다. (Managed App은 Android 단말의 경우 사내앱을 , iOS는 EMM에 의해 설치된 모든 앱을 의미 함) • 미사용: 미사용으로 선택한 경우, 운영자가 단말을 비활성화 상태로 변경 시 단말만 비활성화 상태로 변경합니다.
단말 제어 방식	단말 제어 방식을 설정합니다. • Direct: Direct로 선택한 경우, 단말 제어 명령이 실패하더라도 **서비스 현황 > 미처리 단말 제어** 메뉴에 정보가 남지 않습니다. 단말 제어 명령이 실패한 정보를 확인하려면 **단말 & 사용자 > 단말**의 단말이력 컬럼 또는 **단말 & 사용자 > 단말제어이력**에서 확인합니다. • Queue: Queue로 선택한 경우, 단말 제어 명령이 실패하면 **서비스 현황 > 미처리 단말 제어** 메뉴에 실패 정보가 기록되며 ⚙을 클릭하여 실패한 단말 제어 명령에 대한 재 전송이 가능합니다.

• **Push**

분류	설명
Agent Ticket	EMM Agent Ticket 값으로, Push 설치 시 딜리버리로부터 발급받는 값입니다.
Agent Ticket Index	EMM Agent Ticket Index 정보로, Push 설치 시 딜리버리로부터 발급받는 값입니다.
Client Ticket	EMM Client Ticket 값으로, Push 설치 시 딜리버리로부터 발급받는 값입니다.
Client Ticket Index	EMM Client Ticket Index 정보로, Push 설치 시 딜리버리로부터 발급받는 값입니다.
Public Push	Public Push의 사용 여부를 설정합니다. MDM 분류 중 **단말 제어 방식**을 **Direct**로 설정했거나, Public Push 사용 여부 변경 전에 이미 EMM에 등록된 단말이 하나라도 있는 경우에는 Public Push의 사용 여부 변경이 불가능합니다. Public Push 설정에 대한 자세한 내용은 35페이지의 "Public Push 설정하기"를 참고하세요. • 사용 • 미사용

- **Service Desk**: 사용자의 단말에 보여지는 서비스데스크의 정보를 설정합니다.

분류	설명
서비스데스크 이메일 주소	서비스데스크 이메일 주소를 입력합니다.
서비스데스크 전화번호	서비스데스크 전화번호를 입력합니다.
서비스데스크 웹사이트	서비스데스크 웹사이트 주소를 입력합니다.

- **Service Broker**: 커넥터 서비스 사용 시 단말과 서버간의 데이터 무결성 확인 여부를 설정합니다.

분류	설명
개발자 모드	커넥터 서비스 사용 시 단말과 서버 간의 무결성 확인 여부를 선택합니다. • True: True로 선택한 경우, 무결성 확인을 하지 않습니다. • False: False로 선택한 경우, 무결성을 확인합니다.

- **Smart Key**: 자동차 제어를 위한 스마트키 사용 여부를 설정합니다.

분류	설명
스마트키 사용 여부	스마트키 사용 여부를 설정합니다. • True • False

- **Tizen Wearable**: Tizen Wearable 단말 사용을 위한 정보를 설정합니다.

분류	설명
Tizen Wearable ELM License Key	Tizen 지원을 위한 ELM 라이선스의 Key 값으로, Tizen Wearable에서 EMM을 사용하려면 해당 라이선스가 반드시 필요합니다.
Tizen Wearable Knox License Key 만료일	Tizen 지원을 위한 Knox 라이선스의 Key 만료일입니다.
Tizen Wearable Knox License Key	Tizen 지원을 위한 Knox 라이선스의 Key 값입니다.

분류	설명
EMM/TMS 서비스 URL	Tizen Wearable 단말에서 Wearable EMM에 로그인하려면 EMM 또는 TMS 서버의 주소 입력이 필요합니다. EMM 운영자는 https: //goo.gl 등의 단축 URL 생성 사이트에서 EMM/TMS 서버의 단축 URL을 Note 규칙에 맞게 등록할 수 있으며, 단축 URL 사용을 권장합니다.
	Note: https://goo.gl(권장)에 Tizen용 Wearable EMM 또는 TMS 서버의 단축 URL 등록 시 유의 사항은 다음과 같습니다. Single Tenant인 경우, • 예) https://[EMM host]:[EMM port]/**emm**/provision • 예) EULA URL : http(s)://[host]:[port]/**emm**/provision /**eula** Multi Tenant인 경우, • 예) https://[TMS host]:[TMS port]/**tms**/provision/ **[Tenant_ID]** • 예) EULA URL : http(s)://[host]:[port]/**tms**/provision/ [Tenant ID]/**eula**
인증 실패 횟수 (0의 경우, 무제한)	Tizen Wearable 단말에서 Wearable EMM에 로그인 시 사용자 인증을 위해 인증 코드 입력이 필요하며, 인증 코드 실패 횟수에 지정한 만큼 인증 코드 입력이 가능합니다.
인증 코드 발급 URL	인증 코드 발급을 위한 발급 사이트의 URL 주소를 입력합니다.
인증 코드 유효기간 (시간) (0의 경우, 무제한)	Tizen Wearable 단말에서 EMM에 로그인 시 사용자 인증을 위해 인증 코드 입력이 필요하며, 입력된 인증 코드는 인증 코드 유효기간에 설정한 시간 만큼만 유효합니다. 만약 설정한 유효시간을 초과한 경우에는 다시 인증 코드 발급이 필요합니다.

- **Windows 10**: WINDOWS 10에 관련된 정보를 설정합니다.

분류	설명
Onpremis 인증시 유효성 검사	MDM Agent의 활성화를 위해 Windows Provisioning Package (PPKG) 파일의 설정 값이 유효한지 검사 여부를 설정합니다. • True: True로 선택한 경우, Windows의 PPKG에 기입하는 UPN과 Secret 값의 일치 여부를 확인하여 Windows 10의 MDM Agent를 활성화합니다. 만약, 일치 하지 않는 경우에는 MDM Agent를 활성화하지 않습니다. • False: False로 선택한 경우, Windows의 PPKG에 기입하는 UPN과 Secret 값의 일치 여부를 확인하지 않습니다.
MDM Agent 동기화 기능 제공	MDM Agent와의 동기화 여부를 설정합니다. MDM Agent 동기화 설정을 통해 Windows의 정책 제어 및 설정 업데이트가 가능합니다. • True: True로 선택한 경우, 동기화를 설정합니다. • False: False로 선택한 경우, 동기화를 설정하지 않습니다.
MDM Provider Name	Windows가 설치된 기기의 설정 메뉴에서 확인되는 MDM의 제공자명을 입력합니다.

3. 설정이 완료되면 화면 좌측 상단  을 클릭하여 저장하세요.

Note:
- ELM License Key 값을 반드시 입력해야만 EMM 사용이 가능합니다.
- Knox 기능은 Knox 라이선스를 별도 구매해야만 사용이 가능하며, Knox 기능을 사용하지 않는 경우, Knox License Key 값을 빈 값으로 입력하세요.

KeepAlive 설정하기

EMM 서버와 단말의 연결 상태가 정상적인지 주기적으로 확인하기 위해 KeepAlive 체크 주기를 설정합니다 . 시간 설정은 6, 8, 12, 24 시간으로 설정이 가능하며 , 설정한 시간 간격으로 서버와 단말의 연결 상태를 확인합니다 .

KeepAlive 설정으로 단말을 분실하였거나 비 정상적인 연결 상태로 데이터 전송이 실패한 경우 , KeepAlive 에서 설정한 조취 방법에 따라 강력하게 단말을 보호할 수 있습니다 .

분류	설명
KeepAlive 기한 (일, 0의 경우 설정 안함)	EMM 서버와 단말간의 연결 상태를 확인하기 위해 KeepAlive 기한을 설정합니다. 최소 설정일은 3일에서 최대 365일까지 설정할 수 있으며, KeepAlive를 설정하지 않으려면 0으로 설정합니다. 만약, KeepAlive 기한을 10일로 입력 시 10일 동안 서버와 단말간의 연결 상태를 확인하고, 10일이 지난 후 **KeepAlive 기한 초과 후 조치**에서 설정한 대로 수행합니다. • 입력 범위: 최소 3~최대 365일
KeepAlive 기한 초과 후 조치 (Android Only)	KeepAlive 기한(일)으로 설정한 기간 동안 단말과 EMM 서버의 연결 상태를 확인하고, KeepAlive 기한 초과 후 서버와 단말간 연결이 되어있지 않으면 다음 중 하나를 수행하도록 선택합니다. • 미조치 • 단말 잠금 • Preloaded 이메일 앱 잠금 • 공장초기화(EMM Agent 2.0+): EMM Agent 2.0 이상에서만 공장초기화가 실행됨 • 공장초기화(SDCard포함): 공장초기화 시 SD 카드도 함께 삭제됨
KeepAlive 기한 초과 전 사전 공지 시간 (시간, Android Only)	KeepAlive 기한일 초과 전, KeepAlive 기한일을 알리는 사전 공지 시간을 설정합니다. • 입력 범위: 최소 1~최대 3시간
KeepAlive 주기 (시간, Android Only)	EMM 서버와 단말간의 연결 상태 확인을 위해 KeepAlive 업데이트 주기를 설정합니다. KeepAlive 주기를 4시간으로 설정한 경우, 단말은 4시간 마다 EMM 서버와의 연결을 시도합니다. • 입력 범위: 최소 4~최대 24시간

메일 서버 설정하기

사용자에게 EMM 의 등록 정보 및 설치 정보 , 서비스 안내 등을 메시지 템플릿으로 전송하려면 메일 서버의 설정이 필요합니다 . 또한 메일 서버 를 설정한 후 , 관리자 포털의 **단말 & 사용자 > 사용자 & 조직**에서 사용자 정보에 이메일이 등록되어있어야만 이메일 전송이 가능합니다 . 이메일 전송 시 메시지 템플릿은 관리자 포털의 **설정 > 서비스 > 메시지 템플릿**을 이용합니다 .

이메일 전송을 위해 메일 서버를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.

2. 화면 상단의 **메일 서버**를 클릭하세요.

- **발신 메일 주소**: 발신인의 이메일 주소를 입력합니다.
- **발신 이름**: 발신인의 이름을 입력합니다.
- **SMTP Host**: SMTP 호스트의 주소를 입력합니다.
- **암호화**: 발신되는 메일의 암호화 여부를 선택합니다.(안함 / SSL)
- **SMTP Port**: SMTP의 포트를 입력합니다.
  - **암호화**를 **안함**으로 선택한 경우, SMTP Port 번호의 기본값은 25입니다.
- **타임아웃(sec)**: 메일 서버의 타임아웃을 설정합니다.(5초~120초)
  - 기본값은 30초입니다.
- **인증**: 인증 여부를 선택합니다. 인증 필요를 선택시 다음 사항을 입력합니다.
  - **사용자 이름**: 인증에 필요한 사용자의 이름을 입력합니다.
  - **비밀번호**: 인증에 필요한 사용자의 비밀번호를 입력합니다.

3. 메일 서버가 정상적으로 운영되는지 확인하려면 **연결 테스트**를 클릭하세요.
4. **저장**을 클릭하세요.

커넥터 서비스 관리하기

커넥터 서비스와 연동되어 EMM 이 운영되는 경우 , 커넥터 서비스의 운영 시간을 설정할 수 있습니다 . 또한 비 운영시간 동안 안내하는 메시지를 단말에 보내거나 서비스에 대한 트랜잭션 로그 기록을 설정할 수 있습니다 .

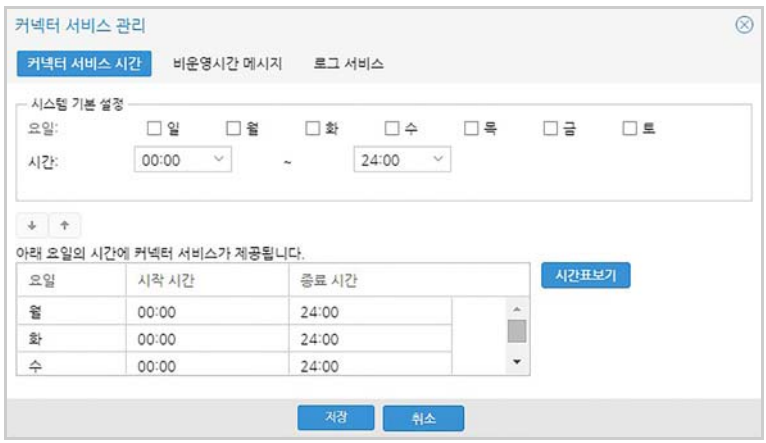
서비스 운영 시간은 서비스 그룹의 커넥터 서비스 시간에 설정된 운영 시간이 우선 적용되며 , 서비스 그룹의 커넥터 서비스에 운영 시간이 설정되지 않은 경우 , **설정 > 서비스 > 환경 설정**의 **관리**에서 설정한 서비스 운영 시간이 적용됩니다 .

커넥터 서비스 운영 시간을 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.
2. 화면 상단의 **관리**를 클릭하세요.

3. "커넥터 서비스 관리" 창의 **커넥터 서비스 시간** 탭을 클릭한 후, 서비스 운영 시간을 설정하고 **저장**을 클릭하세요.

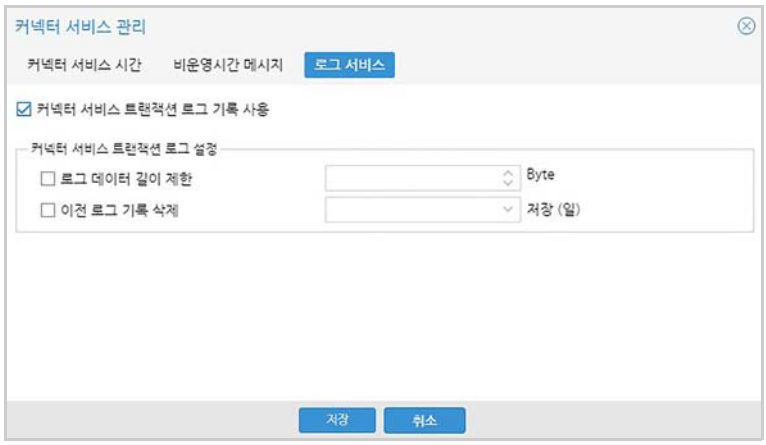
   • **커넥터 서비스 시간**: 서비스 운영 시간을 선택합니다.



항목	설명
시스템 기본 설정	서비스 운영 시간을 설정하면 선택한 날짜와 시간으로 서비스가 운영됩니다. 서비스 운영 시간은 다중 선택이 가능합니다. 예: 월 00:00~20:30, 화 00:00~24:00, 금 13:00~13:30 • 운영 일정을 추가하려면 원하는 요일과 시간을 선택한 후, ↓ 을 클릭합니다. • 운영 일정을 삭제하려면 삭제할 요일과 시간을 선택한 후, ↑ 을 클릭합니다.
시간표 보기	**시간표보기**를 클릭하면 설정된 운영 요일과 시간이 시간표 형식으로 나타납니다.

   • **비운영 시간 메시지**: 서비스 비 운영 기간을 안내하는 메시지를 입력합니다. 입력된 메시지는 서비스 비 운영 시 단말에 전송됩니다.

- **로그 서비스**: 커넥터 서비스에 대한 트랜잭션 로그 기록 여부를 설정합니다.



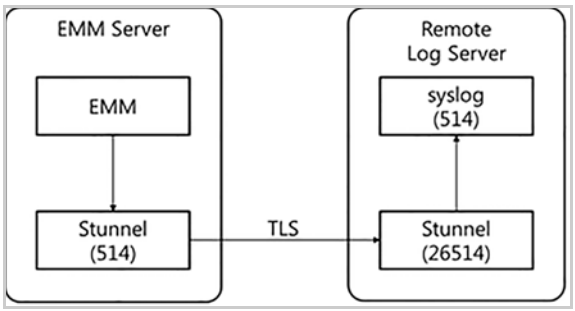
항목	설명
커넥터 서비스 트랜잭션 로그 기록 사용	**커넥터 서비스 트랜잭션 로그 기록 사용**의 확인란을 선택하면 커넥터 서비스의 트랜잭션 로그가 기록됩니다.
커넥터 서비스 트랜잭션 로그 설정	트랜잭션 로그 데이터의 길이와 기록 저장일을 설정합니다. • **로그 데이터 길이 제한**: 저장되는 트랜잭션 로그의 데이터 길이를 설정합니다. (Byte) • **이전 로그 기록 삭제 (일)**: **이전 로그 기록 삭제**의 확인란을 선택한 후, 저장일을 설정하면 저장일 이전의 로그 기록은 삭제됩니다. 저장일 설정은 최소 30일부터 최대 600일까지 설정이 가능합니다.

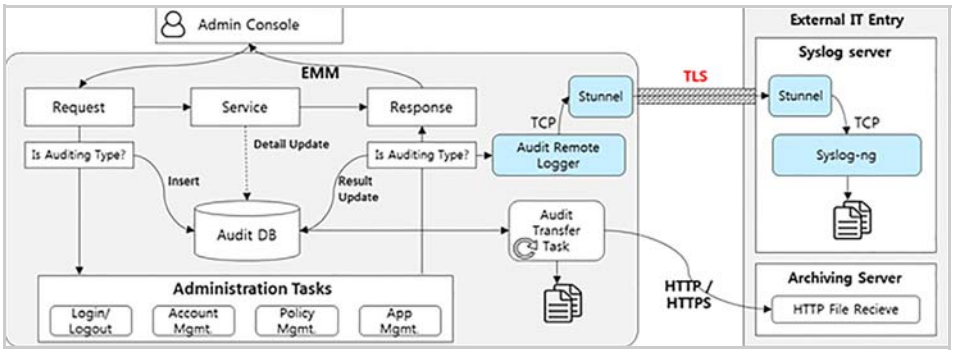
4. **저장**을 클릭하세요.

Audit 설정하기

EMM 은 관리자 포털 , 사용자 단말 , EMM 서버에 대한 정보를 Audit 로그에 기록하여 관리합니다 . Audit 로그는 EMM 서버의 데이터베이스와 원격 로그 서버에 저장이 가능하며 , Audit 로그를 원격 서버로 전송하기 위해 원격 로그 서버를 설정할 수 있습니다 . EMM 서버와 원격로그서버 간의 데이터 전송은 보안을 위해 TLS 보안 통신이 제공됩니다.

다음은 EMM 서버와 Audit 원격 로그 서버의 아키텍쳐입니다 .



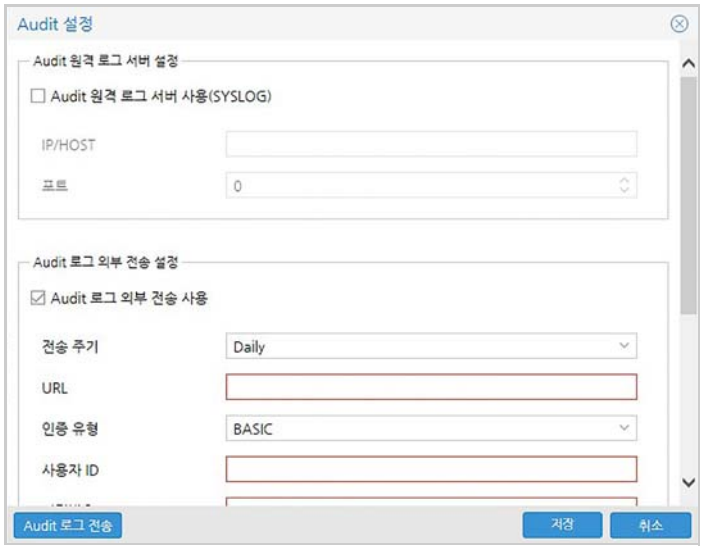


원격 로그 서버 설치 및 설정 , Stunnel 을 이용한 EMM 서버와 Audit 원격 로그 서버 간의 보안 통신을 위한 채널 설정에 대한 자세한 내용은 “Samsung SDS EMM 설치매뉴얼의 부록 C Audit Remote Logging” 을 참고하세요 .

EMM 서버와 원격 로그 서버 간의 설정이 완료되었다면 , 관리자 포털에서 원격 로그 서버의 정보를 입력할 수 있습니다 .

Audit 로그 및 원격 로그 서버를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.
2. 화면 상단의 **Audit 설정**을 클릭하세요.



- **Audit 원격 로그 서버 설정**: 원격 로그 서버로 Audit 로그를 전송하려면 **Audit 원격 로그 서버 사용(SYSLOG)**을 클릭합니다. IP/HOST 주소와 포트 정보를 입력한 후, **저장**을 클릭하면 Audit 로그가 원격 로그 서버에 전송 및 기록됩니다.
  - **IP/HOST**: Audit 원격 로그 서버의 IP 또는 호스트 주소입니다.
  - **포트**: Audit 원격 로그 서버의 포트 번호입니다.

- **Audit 로그 외부 전송 설정**: Audit 로그를 파일로 생성하여 외부 서버로 전송하려면 **Audit 로그 외부 전송 사용**을 클릭하고, 다음과 같이 정보를 입력합니다.

항목	설명
전송 주기	Daily, Weekly, Monthly, Annually 중 Audit 로그 전송 주기를 선택합니다.
URL	Audit 로그를 전송하려는 서버의 URL 주소를 입력합니다.
인증 유형	BASIC, NONE 중 인증 유형을 선택합니다. **BASIC**을 선택한 경우, 사용자 ID와 비밀번호를 입력합니다. • **사용자 ID**: 인증을 위한 사용자의 로그인 ID 입니다. • **비밀번호**: 인증을 위한 사용자의 비밀번호입니다.
언어	한글, 영어, 중국어 중 Audit 로그가 기록되는 언어를 선택합니다.
작업 서버	전송 작업을 실행하는 서버를 선택합니다.
전송 파일명	외부로 전송되는 Audit 로그의 파일명이 보여집니다.

- **Audit 로그 설정**
  - **Audit 로그 보존 한도**: Audit 로그 보존을 위해 한도를 건수로 설정합니다. 관리자 포털의 메인 화면 상단에 Audit 저장 한도가 90% 초과시 **Audit 저장 용량: 90%** 알림 메시지가 나타납니다.
    - 입력 범위: 1~10000건(백만~백억), 기본 값은 1백만 (단위: 백만)
  - **단말Audit DB로 가져오기**: True 또는 False 값을 설정합니다.
    - 기본 값은 True이며, 로그 서버(LTS)에 업로드된 단말의 Audit 로그가 DB에 저장됩니다.
    - False로 설정하면 로그 서버(LTS)에 업로드된 단말의 Audit 로그가 DB에 저장되지 않으므로 로그 처리를 위한 CPU 사용량을 줄일 수 있습니다. Audit 로그 처리에 대한 부하를 줄이려면 LTS를 EMM 서버와 분리하여 구성합니다. 자세한 내용은 “Samsung SDS EMM 설치 매뉴얼”을 참고하세요.

3. Audit 로그를 외부 서버로 전송하려면 하단의 **Audit 로그 전송**을 선택하고, 전송 요청 확인 메시지가 나타나면 **확인**을 클릭하세요.
4. Audit 설정을 저장하려면 **저장**을 클릭하세요.

사용자 인증 설정하기

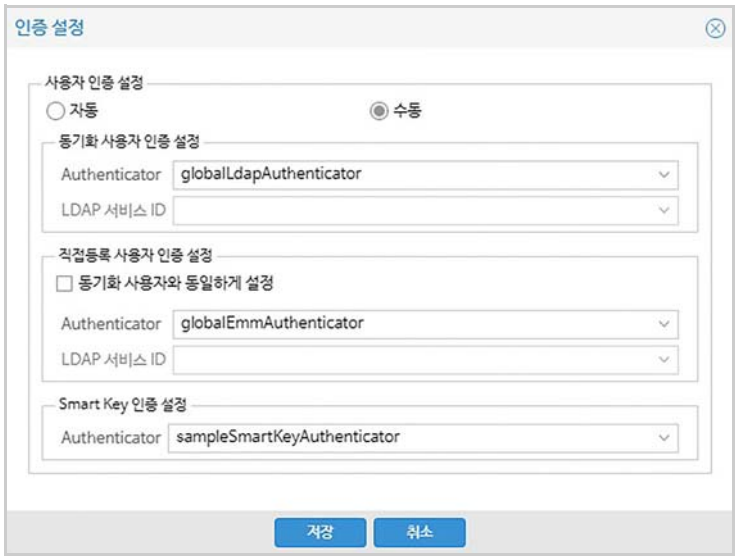
사용자가 단말의 EMM 에 로그인하려면 사용자 인증을 위한 절차가 반드시 필요합니다 .

사용자 인증은 다음과 같이 자동 또는 수동으로 설정할 수 있습니다 .

- 자동: EMM에서 제공하는 사용자 인증 방식으로 인증이 설정됩니다.
- 수동: 동기화 사용자 인증 설정 또는 직접 등록 사용자 인증 설정을 선택하여 설정할 수 있습니다. 동기화 사용자 인증 설정에 **globalLdapAuthenticator**로 설정하고, 직접 등록 사용자 인증 설정에 **globalEMMAuthenticator**로 설정하면 **자동** 설정과 동일하게 인증이 수행됩니다.

수동을 선택하고 사용자 인증을 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.
2. 화면 상단의 **인증 설정**을 클릭하세요.



- **사용자 인증 설정**: 사용자가 단말의 EMM에 로그인 시 사용자를 인증하는 방법을 설정합니다.

- **동기화 사용자 인증 설정**: AD/LDAP으로 동기화된 Directory 서비스를 통해 사용자 정보가 EMM 서버에 저장되며 해당 정보로 인증을 수행합니다.

항목	설명
Authenticator	• **globalEMMAuthenticator**: EMM 서버 내 저장된 사용자 ID와 비밀번호로 사용자를 인증합니다. • **globalLdapAuthenticator**: AD/LDAP 동기화로 저장된 사용자 ID와 비밀번호로 사용자를 인증합니다. • **globalLdapServiceAuthenticator**: EMM 서버 내 저장된 사용자 ID와 Directory 서비스를 통해 접속한 AD/LDAP의 사용자 비밀번호로 인증합니다.
LDAP 서비스 ID	**globalLdapServiceAuthenticator** 선택 시 인증을 위해 사용하려는 Directory 서비스 ID를 입력합니다.

- **직접등록 사용자 인증 설정**: 선택한 Authenticator에 따라 관리자 포털에서 운영자가 직접 등록한 사용자 정보로 인증하거나 Directory 서비스를 통해 인증하는 방식입니다.
  동기화 사용자와 동일하게 설정의 확인란을 선택하면 동기화 사용자 인증 설정 방식과 동일하게 인증하므로 하단의 선택항목들이 보이지 않으며, 선택 해제 시 다음 항목들의 입력이 가능합니다.

항목	설명
Authenticator	globalEMMAuthenticator, globalLdapAuthenticator, globalLdapServiceAuthenticator 또는 별도로 구현한 Authenticator를 선택합니다. • **globalEMMAuthenticator**: EMM 서버 내 저장된 사용자 ID와 비밀번호로 사용자를 인증합니다. • **globalLdapAuthenticator**: AD/LDAP 동기화로 저장된 사용자 ID와 비밀번호로 사용자를 인증합니다. • **globalLdapServiceAuthenticator**: EMM 서버 내 저장된 사용자 ID와 Directory 서비스를 통해 접속한 AD/LDAP의 사용자 비밀번호로 인증합니다.
LDAP 서비스 ID	**globalLdapServiceAuthenticator** 선택 시 인증을 위해 사용하려는 Directory 서비스 ID를 입력합니다.

- **Smart Key 인증 설정**: 스마트 키 인증 설정을 통해 자동차 제어가 가능한 사용자를 인증합니다.

항목	설명
Authenticator	sampleSmartKeyAuthenticator

3. **저장**을 클릭하세요.

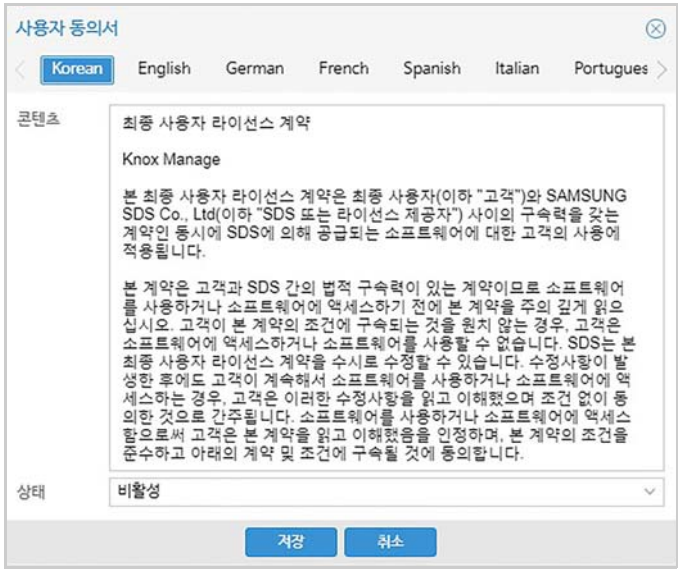
사용자 동의서 설정하기

사용자 동의서는 단말의 EMM 사용을 위한 동의서로 EMM 서버에서 단말로 다운로드 됩니다 . 사용자 동의서는 사용하는 언어에 따라 한국어 , 영어 , 독일어 , 프랑스어 , 스페인어 , 이탈리아어 , 포르투칼어 및 중국어를 선택하여 작성할 수 있습니다 .

사용자 동의서를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.

2. 화면 상단의 **사용자 동의서**를 클릭하세요.



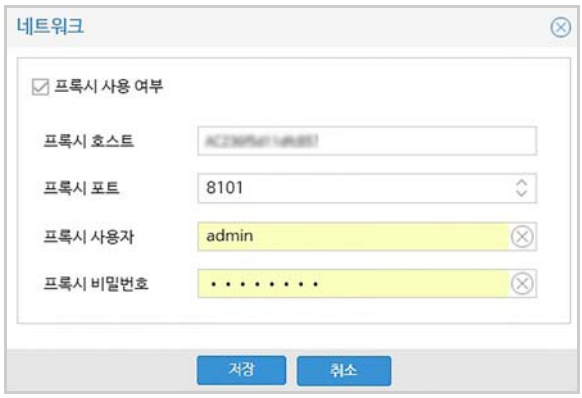
3. 작성하려는 언어 탭을 클릭한 후, **콘텐츠**에 사용자 동의서 내용을 입력하세요.
4. **상태**에서 활성화, 비활성화 중 사용자 동의서의 사용 여부를 선택하세요.
5. **저장**을 클릭하세요.

네트워크 설정하기

Android Attestation 서버의 접속이나 Android Public AppStore 에서 검색을 위해 필요에 따라 프록시 서버를 설정할 수 있습니다 .

프록시 서버를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.
2. 화면 상단의 **네트워크**를 클릭하세요.



- 프록시 서버를 사용하려면 **프록시 사용 여부**를 클릭합니다.
- **프록시 호스트**: 프록시 서버의 주소를 입력합니다.
- **프록시 포트**: 프록시 서버의 포트를 입력합니다.
- **프록시 사용자**: 프록시 서버 인증에 필요한 사용자를 입력합니다.

- **프록시 비밀번호**: 프록시 서버 인증에 필요한 사용자의 비밀번호를 입력합니다.

3. **저장**을 클릭하세요.

Public Push 설정하기

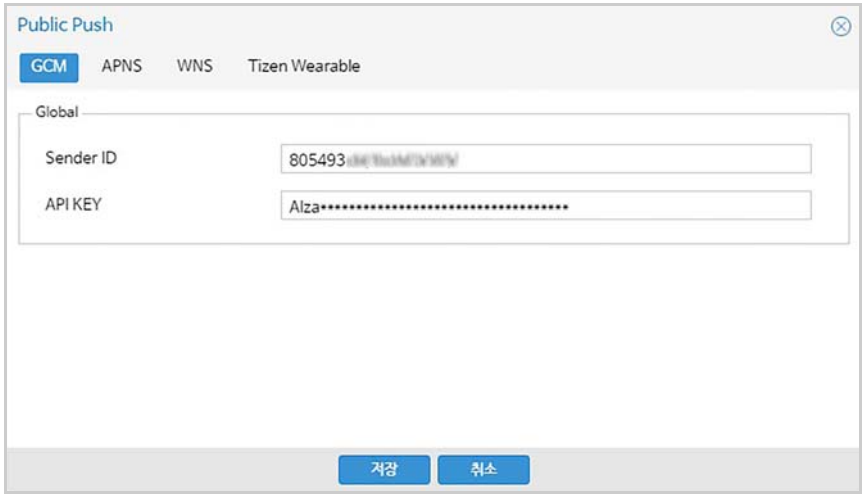
Google, Apple, Windows, Tizen Wearable 에서 제공하는 Public Push (GCM, APNs, WNS, Tizen Wearable) 서버를 설정하여 Push 알림 서비스를 이용할 수 있습니다 .

공통 Tenant 에서 설정 가능한 Public Push 정보는 다음과 같습니다 .

- GCM: Android 단말의 애플리케이션과 애플리케이션서버 사이의 메시지 전송을 담당하는 Google의 Cloud Push 서버로, Android 단말에 알림 메시지 전송을 위한 Push Notification Service를 제공합니다.
- APNs: iOS 단말에 알림 메시지 전송을 위한 Apple의 Push 서버로, Apple Push Notification Service를 제공합니다.
- WNS: Windows 10이 설치된 PC, 테블릿, 모바일 단말에 알림 메시지 전송을 위한 Push 서버로, Window Push Notification Services를 제공합니다.
- Tizen Wearable: Tizen Wearable 단말에 알림 메시지 전송을 위한 Tizen의 Push 서버로, Tizen Push Notification Services를 제공합니다.

Public Push 를 설정하려면 다음의 절차를 따르세요 .

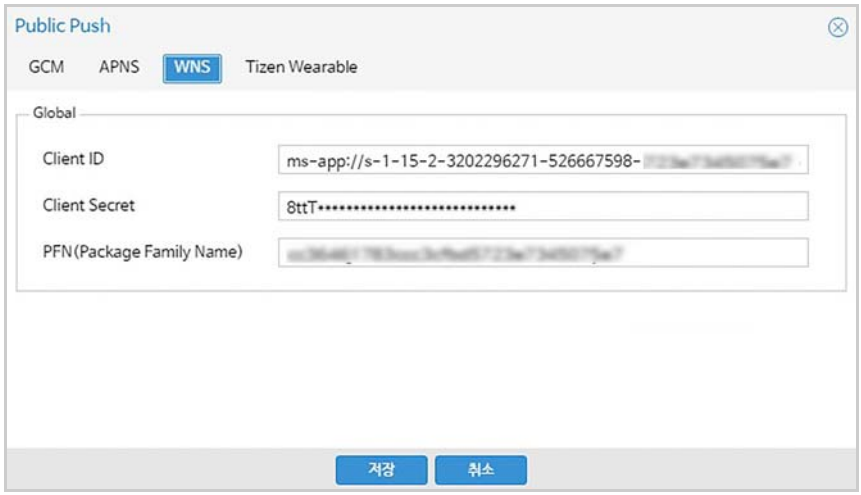
1. **설정 > 서비스 > 환경 설정**으로 이동하세요.
2. 화면 상단의 **Public Push**를 클릭하세요.
3. 다음은 GCM, APNs, WNS, Tizen Wearable의 Public Push 설정에 대한 설명으로 각 탭을 클릭한 후, 항목들을 입력합니다.
   - **GCM**: Sender ID와 APK KEY는 애플리케이션 서버에 저장된 정보이며 Client, Agent 구분없이 동일한 Sender ID를 사용합니다.



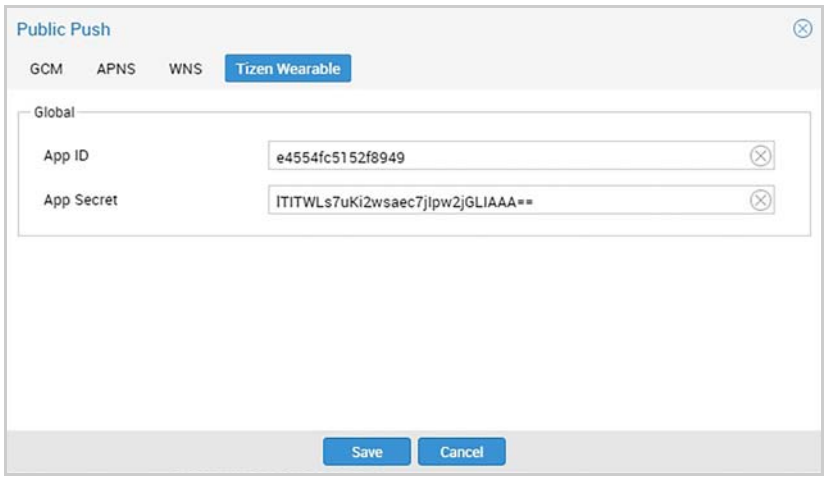
     - **Sender ID**: GCM 사용을 위해 등록 과정에서 발급받는 숫자열로, Push의 전송 ID입니다.

- **API KEY**: Google 서비스 사용을 위해 필요한 인증 키값입니다.

- **APNs**: APNs 서비스를 사용하기 위하여 인증서를 등록하려면 37페이지의 "APNs 설정하기"를 참고하세요. APNs 인증서가 이미 등록되어 있는 경우, 현재 등록된 인증서 정보와 만료일이 상단에 나타납니다.
- **WNS**: Push 알림 메시지 전송을 위해 인증 ID와 인증 암호가 필요합니다. 자세한 내용은 https://developer.microsoft.com 사이트의 **Windows 개발자 센터 > 대시보드**의 앱 관련 기능 메뉴를 확인한 후 Client ID, Client Secret, PFN 값을 확인합니다.



  - **Client ID**: 알림 메시지 전송 시 인증을 위한 인증 ID입니다.
  - **Client Secret**: 알림 메시지 전송 시 인증을 위한 비밀번호입니다.
  - **PFN**: Package Family Name을 입력합니다.
- **Tizen Wearable**: Tizen Push를 사용하려면 Tizen Agent가 **애플리케이션 > EMM 애플리케이션**에 “com.sds.Knox Manage.wearable” 패키지 명으로 등록되어있어야 합니다. 또한, Tizen Push 서비스를 통해 Tizen Wearable 단말에 알림 메시지를 전송하려면 Application ID와 Application Key가 필요합니다. Wearable Knox Manage 앱 전용으로 Tizen Push를 사용하려면 아래와 같이 App ID와 App Secret 값을 입력합니다.



  - **App ID**: Tizen Push 서비스 사용을 위한 Application ID입니다.
  - **APP Secret**: Tizen Push 서비스 사용을 위한 Application Key 값입니다.

4. **저장**을 클릭하세요.

APNs 설정하기

iOS 단말을 제어하려면 APNs 를 설정해야하며 , Apple 이 서명한 신뢰할 수 있는 인증서를 관리자 포털에 반드시 등록해야 합니다 .

EMM 에서는 두개의 APNs 인증서를 사용합니다 .

- App APNs 인증서: EMM 서버에서 EMM 애플리케이션으로 Push 메시지를 보내는 App APNs를 이용하기 위한 인증서로 Client에 설정합니다.
- MDM APNs 인증서: EMM 서버에서 iOS EMM 모듈로 Push 메시지를 보내는MDM APNs를 이용하기 위한 인증서로 Agent에 설정합니다.

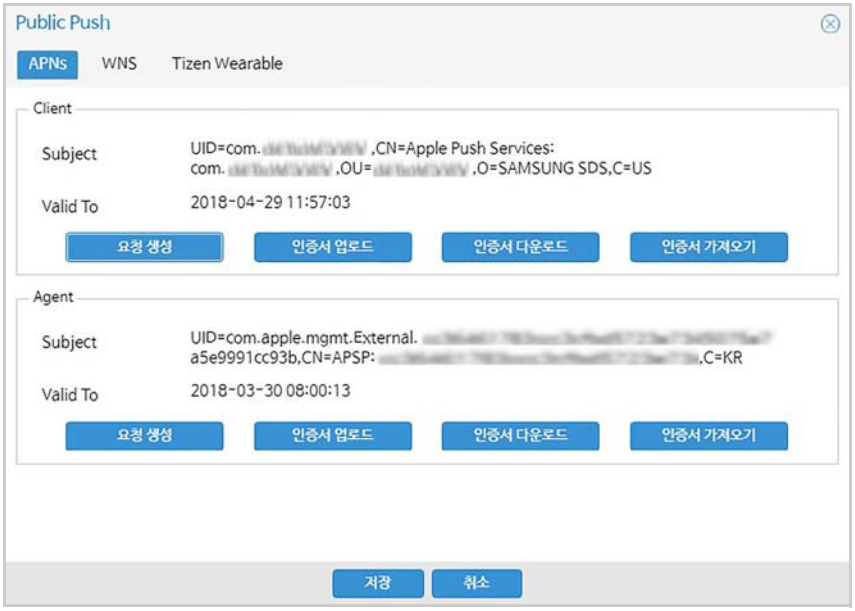
APNs 인증서는 관리자 포털에서 최초 등록한 후 , 1 년마다 갱신해야하며 APNs 인증서 갱신 방법은 등록 방법과 동일합니다 . 또한 , 인증서가 만료되면 관리자 포털에서 사용자의 iOS 단말로 단말 제어 명령을 전송할 수 없으며 , 사용자 단말에서는 인증서가 갱신되더라도 EMM 을 재 설치할 필요가 없습니다 . APNs 설정에서 등록한 APNs 인증서는 **인증서 > 외부 인증서**에서 확인이 가능하며 , 해당 메뉴에서 인증서 등록이나 갱신 및 삭제는 불가능합니다 .

APNs 설정하기 위해 준비해야할 사항은 다음과 같습니다 .

- https://appleid.apple.com
  : Apple 사이트에 로그인을 위해 Apple 계정을 생성하는 사이트로, 인증서 갱신 시 동일한 ID 사용을 위해 인증서 생성용 계정을 만드세요.
- https://developer.apple.com/programs/enterprise/
  : App용 APNs 인증서 발급 및 기업용 iOS 앱 빌드/배포를 위해 ADEP (Apple Developer Enterprise Program) 사이트 가입이 필요합니다.
  자세한 내용은 “Samsung SDS EMM 설치매뉴얼”을 참고하세요.

APNs 인증서에 대한 자세한 내용은 https://developer.apple.com/library/content/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/APNSOverview.html 를 참고하세요 .

APNs 인증서를 등록하려면 다음의 절차를 따르세요 .



1. “Public Push” 화면에서 APNs 인증서 발급 요청을 위해 서명 요청 파일인 CSR 파일(Certificate Signing Request)을 생성하려면 **요청 생성**을 클릭하세요.
   - 공개키와 개인키를 생성한 후, CSR을 생성하고 생성된 CSR에 벤더서명을 추가한 파일이 운영자의 PC로 다운로드됩니다.
   - Agent 인증서로 요청한 MDM용 APNs 인증서는 벤더 서명이 추가되지 않은 상태이므로 CSR 파일을 Samsung SDS EMM 기술지원 담당자에게 전달한 후, 벤더 서명을 추가한 CSR 파일을 전달받아야 합니다.
2. App용 인증서 발급하기: 1단계에서 생성된 CSR 파일을 업로드하여 인증서를 생성하세요. 자세한 내용은 “Samsung SDS EMM 설치매뉴얼”의 APNs 인증서 발급하기를 참고합니다.
3. MDM용 인증서 발급하기: 1단계에서 기술지원 담당자에게 전달받은 벤더 서명이 포함된 CSR 파일을 Apple Push 인증서 포털에 등록하세요.

   가. https://identity.apple.com/pushcert 사이트에 Apple ID로 로그인하세요.

   나. **Create a Certificate**를 클릭한 후, “Create a New Push Certificate” 화면에서 **파일 선택**을 클릭하여 가단계에서 받은 CSR 파일을 선택한 다음 **Upload**를 클릭하세요.

   다. “Confirmation” 화면에서 **Download**를 클릭하면 APNs 인증서(PEM) 파일이 발급됩니다. 브라우저 하단에서 해당 파일을 클릭하여 저장하세요.
4. PC에 저장한 APNs 인증서 파일을 EMM에 업로드하려면 **인증서 업로드**를 클릭하여 인증서 파일(PEM)을 선택한 후, **확인**을 클릭하세요. 등록된 인증서 정보와 만료일이 화면 상단에 나타납니다.
   - 다른 목적으로 APNs 인증서 파일(PKCS#12)를 사용하기위해 다운로드하려면 **인증서 다운로드**를 클릭하세요. 인증서의 비밀번호 설정을 위해 비밀번호를 입력한 후, **확인**을 클릭하세요.

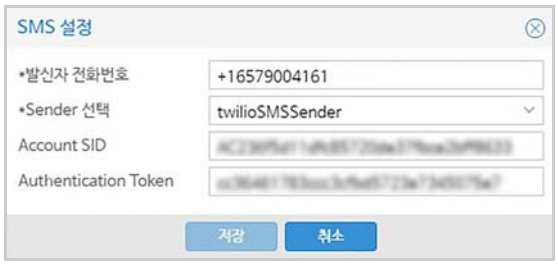
- 외부에서 생성한 CSR에 의해 발급된 APNs 인증서를 가져오려면 **인증서 가져오기**를 클릭하세요. 인증서 파일(PKCS#12)을 선택하고 비밀번호를 입력한 후, **확인**을 클릭하세요.

SMS 설정하기

사용자의 웨어러블 단말에 Wearable EMM 을 설치하거나 로그인하려면 SMS 설정이 필요합니다 . SMS 로 전송하려는 Tizen Wearable 의 설치 정보는 EMM 관리자 포털의 **설정 > 서비스 > 메시지 템플릿**에서 제공하며 , **단말 & 사용자 > 단말**에서 단말 등록 시 전화번호을 반드시 입력해야만 SMS 전송이 가능합니다 .

SMS 를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.
2. 화면 상단의 **SMS 설정**을 클릭하세요.
3. **발신자 전화번호**를 입력한 후, Sender를 선택하세요.



- **발신자 전화번호**: SMS을 보내려는 발신자의 전화번호를 입력합니다.
- **Sender 선택**: SMS 서비스를 제공하는 Sender를 선택합니다. **twilioSMSSender**를 선택한 경우, www.twilio.com 사이트에서 계정 등록을 통해 서비스가 가능하며, **sampleSMSSender**, **baseSMSSender**를 선택한 경우에는 SMS 서비스와 연동을 위한 별도의 개발이 필요합니다.
  - **sampleSMSSender**: 외부 사이트에서 직접 전송 모듈을 개발하여 SMS을 전송하는 방법입니다. 추가로 개발 작업이 필요하며, 개발에 대한 자세한 내용은 “EMM 개발자 매뉴얼”을 참고하세요.
  - **baseSMSSender**: EMM에서 제공하는 Open API를 통해 SMS Queue 테이블에 전송하려는 메시지를 저장하고, 외부 SMS 시스템에서 해당 데이터를 가져와 SMS을 전송하는 방법입니다. SMS Queue 테이블에 메시지를 저장하는 Open API에 대한 자세한 내용은 “EMM개발자 매뉴얼”을 참고하세요.
  - amazonSMSSender: SMS 전송을 위해 amazon 시스템을 사용하는 방법입니다. https://www.amazon .com 사이트에서 신규 가입을하면 해당 계정으로 Access Key와 Secret Key 값이 포함된 정보가 발송됩니다. amazon를 통해 SMS 서비스 사용에 대한 자세한 내용은 https://www.amazon.com 사이트를 참고하세요.
    - **Access Key**: amazon에서 받은 Access Key를 입력합니다.
    - **Secret Key**: amazon에서 받은Secret Key를 입력합니다.

- **twilioSMSSender**: SMS 전송을 위해 twilio 시스템을 사용하는 방법입니다. https://www.twilio.com 사이트에서 신규 가입을하면 해당 계정으로 Account SID와 Authentication Token 값이 포함된 정보가 발송됩니다. twilio를 통해 SMS 서비스 사용에 대한 자세한 내용은 https://www.twilio.com 사이트를 참고하세요.
  - **Account SID**: twilio에서 받은 Account SID를 입력합니다.
  - **Authentication Token**: twilio에서 받은 Authentication Token 값을 입력합니다.

4. **저장**을 클릭하세요.

E-FOTA 설정하기

Enterprise FOTA(E-FOTA) 서비스를 통해 사용자들의 단말에 설치된 펌웨어를 특정 펌웨어 버전으로 업데이트가 가능합니다 . 이를 위해 E-FOTA 라이선스 설정이 필요합니다 . 만약 E-FOTA 라이선스가 없는 경우 , 해당 메뉴는 관리자 포털에 나타나지 않습니다 .

E-FOTA 서비스를 위한 라이선스 및 연결 정보를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.
2. 화면 상단의 **E-FOTA 설정**을 클릭하세요.
   - **프로파일 > E-FOTA 그룹**에서 E-FOTA 그룹이 생성되어 있으면 연결 설정값을 수정할 수 없습니다.

분류	설명
라이선스	E-FOTA 서비스 사용을 위한 라이선스를 입력하세요.
서버 주소	E-FOTA 서버에서 API 호출을 위한 서버 주소를 입력하세요.
Token 주소	E-FOTA 서버의 API 호출을 위해 Token 발급이 필요하며, Token 요청을 위한 주소를 입력하세요.
MDM vendor ID	E-FOTA 사용을 위해 E-FOTA에서 Vender에게 발급하는 아이디를 입력하세요.

분류	설명
접속 ID	E-FOTA 서버에서 API 호출을 위한 접속 아이디를 입력하세요.
접속 비밀번호	E-FOTA 서버에서 API 호출을 위한 접속 비밀번호를 입력하세요.
고객 ID	E-FOTA 사용을 위한 고객 ID를 입력하세요.

3. E-FOTA 라이선스를 검증하려면 하단의 **라이선스 정보**를 클릭하세요.
4. **저장**을 클릭하세요.

프로파일 업데이트 주기 설정하기

EMM 서버는 주기적으로 단말 관리 프로파일의 정책을 단말에 전송합니다 . 다음과 같이 환경 설정에 프로파일 업데이트 주기를 설정하면 프로파일을 할당받은 전체 단말 플랫폼에 정해진 스케쥴에 따라 정책 업데이트가 실행됩니다 . 그외 , 프로파일별로 업데이트 주기를 설정하려면 215 페이지 12 장의 " 프로파일 업데이트 주기 설정하기 " 를 참고하세요 .

프로파일 업데이트 주기를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.
2. 화면 상단의 **프로파일 업데이트 주기 설정**을 클릭하세요.
3. "프로파일 업데이트 주기 설정" 창에서 **요일**, **시간대**, **시작시간**을 설정하세요.
   - **시작 시간**: HHMM의 4자리로 입력하며 0000-2359까지 입력 가능합니다.

4. **저장**을 클릭하세요.

기준정보 설정하기

기준 정보에서는 EMM 운영을 위해 기준이 되는 정보를 카테고리 별로 구분하여 관리합니다 . 기준 정보의 카테고리는 운영자에 의해 임의로 추가할 수 없으며 카테고리의 키 , 값 , 선택값 및 참조 코드 컬럼은 수정 여부 컬럼의 값에 따라 변경이 가능합니다 .

기준 정보에서 관리되는 정보는 다음과 같습니다 .

- 단말: 단말 모델, 상태, 소유 여부, 플랫폼, 펌웨어 및 통신사 정보

- 언어: 외부 애플리케이션 검색 시 플랫폼 별로 지원 가능한 언어, E-FOTA 그룹 등록 시 지원 가능한 언어
- 애플리케이션: 앱 상태, 앱의 자동 업데이트 여부, 필수 앱 여부 및 EMM 패키지 정보
- 프로파일: 프로파일에서 플랫폼 별 네트워크 설정 정보
- 사용자 정보: 사용자의 직급, 근무지 및 보안 레벨 정보
- 동기화 외부 연계: EMM과 외부 시스템(예: Square Mail)간의 연동 시 사용자 또는 조직 매핑을 위한 사용자 및 조직의 정보. EMM과 외부 시스템간의 연계에 대한 자세한 내용은 97페이지 6장의 “동기화 이력 조회하기"를 참고하세요.

기준정보를 추가하려면 다음의 절차를 따르세요 . 기준정보의 각 항목들은 필요에 따라 추가 , 수정 , 삭제가 가능합니다 .

1. **설정 > 서비스 > 기준 정보**로 이동하세요.
2. 화면 상단의 ＋을 클릭하세요.

3. “기준정보 추가” 창의 **기준정보** 탭을 클릭한 후, 키, 값, 분류,선택 값을 입력하세요.
   - 카테고리 선택: **분류** 항목에서 카테고리를 선택한 후, **선택값** 항목에서 미선택 또는 선택을 클릭합니다.
   - **분류**: 카테고리를 선택합니다.
   - **키**: 분류에서 선택한 카테고리의 키 값을 입력합니다.
     - **서비스 현황 > 대시보드 & 사용자 설정 > 보고서**에서 보고서 생성시 조회 조건 값으로 기준정보의 키 값이 사용됩니다.
   - **값**: 키에 대한 값을 입력합니다.
   - **선택값**: **선택**을 클릭시 해당 키 값이 기본값이 되고 카테고리의 맨 상단으로 이동합니다. (미선택, 선택)
4. “기준정보 추가” 창의 **참조정보** 탭을 클릭하세요.
   - **참조코드**: 참조 코드 정보가 있을 경우에만 입력합니다.
   - **참조정보** 탭에서 참조정보를 추가하려면 ＋을 클릭한 후, “참조 코드 추가” 창에 참조 코드를 입력합니다.
   - 참조 코드 값을 입력한 후, **저장**을 클릭합니다.
5. **저장**을 클릭하세요.

기준정보 확인하기

기준 정보에 설정된 키와 키 값은 관리자 포털에서 다음과 같이 활용되며 , 기준 정보를 확인하는 방법은 다음과 같습니다 .

기준정보 값	기준정보 확인 방법
Android OS Version Android Version iOS OS Version iOS Version Ownership Device Status Platform Windows OS Version Windows Device Type	**단말 & 사용자 > 단말**로 이동한 후, 단말 화면에서 단말의 상태, 플랫폼, OS버전, 소유(Ownership) 값을 확인합니다.
Android Firmware iOS Firmware Device Country Device Model Device Network	**단말 & 사용자 > 단말**로 이동한 후, **모바일 ID**를 클릭하여 "단말 상세" 창의 **기본 정보** 탭 **Details** 목록에서 단말 정보, 펌웨어, SIM 국가/네트워크 , 현재 국가/네트워크 값을 확인합니다.
Mandatory App	**단말 & 사용자 > 단말**로 이동한 후, **모바일 ID**를 클릭하여 "단말 상세" 창의 **앱** 탭에서 필수앱 여부(Mandatory App) 컬럼을 확인합니다.
AppClientLanguage AndroidMarketLang iOSMarketLanguage	Android와 iOS의 Market Language는 **애플리케이션 > 외부 애플리케이션**에서 외부 애플리케이션 등록 시 **검색 스토어** 항목에서 확인합니다.
Position Site Security Level	**단말 & 사용자 > 사용자 & 조직**으로 이동한 후, 사용자 개별등록 시, **직급**(Position), **사이트**(Site), **보안레벨**(Security Level) 값을 확인합니다.
Managed App EMM PackageName	**애플리케이션 > EMM 애플리케이션**으로 이동한 후, EMM 애플리케이션 등록 시 "EMM 애플리케이션 추가" 창의 **기타** 항목에서 자동 업데이트여부(Managed App)와 설치 파일 업로드 시 **패키지명**을 확인합니다.
EFOTA Language Code	**프로파일 > E-FOTA 그룹**으로 이동한 후, E-FOTA 그룹 등록 시 "E-FOTA 신규 등록"창에서 **언어코드** 값을 확인합니다.
Device Profile Configuration	**프로파일 > 단말 관리 프로파일**으로 이동한 후, "단말관리프로파일" 창의 각 플랫폼별 **설정** 메뉴에서 **카테고리** 항목을 확인합니다.
Tizen Push URL	웨어러블 단말에 Tizen Push Notification을 보내기 위한 지역별 RQM(Request Manager) 서버의 URL 주소입니다.
User Defined Organization Field User Defined User Field	EMM과 외부 시스템간의 연동 시 사용자 또는 조직 매핑을 위한 사용자 및 조직의 정보입니다. **단말 & 사용자 > AD/LDAP 동기화 > 동기화 외부 연계**로 이동하여 사용자 또는 조직 연계 탭을 클릭한 후, 매핑 방법 중 **Custom**에서 보여지는 사용자 또는 조직의 매핑 설정 값을 확인합니다. Custom 필드의 매핑 설정 값은 외부 시스템에 추가적으로 전달하려는 사용자 및 조직의 정보입니다.

태블릿 모델 관리하기

사용자가 태블릿 단말을 사용하는 경우 , 태블릿 단말에 맞는 EMM 및 애플리케이션 설치 , 업데이트 파일을 제공할 수 있도록 태블릿 모델을 등록하여 관리합니다 . 태플릿 모델은 필요에 따라 추가 , 수정 및 삭제가 가능합니다 .

태블릿 모델을 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 태블릿 모델 관리**로 이동하세요.
2. 화면 상단의 ＋을 클릭하세요.

- **플랫폼**: 플랫폼을 선택합니다.(Android / iOS)
- **모델 ID**: 테블릿의 모델 ID를 입력합니다.
- **모델명**: 태블릿의 모델명을 입력합니다.
- **상세 설명**: 태블릿의 상세 설명을 입력합니다.

3. **저장**을 클릭하세요.

서버 정보 및 서버 목록 관리하기

현재 운영 중인 EMM 서버의 기본 정보와 서버 목록을 관리합니다. EMM 서버가 클러스터링 되어있는 경우, EMM 서버가 여러 곳에서 기동될 수 있으며, 이때 각 서버에 대해 예약 작업과 모니터링을 위해 서버 목록을 관리합니다.

다음은 서버 정보 및 서버 목록을 관리하는 방법에 대한 설명입니다.

서버 정보 확인하기

EMM 서버의 정보를 확인하고 서버의 캐시를 비우거나 오픈 소스 정보를 확인하려면 다음의 절차를 따르세요.

1. **설정 > 서비스 > 서버 정보**로 이동하세요.
2. 서버 캐시를 비우거나 오픈 소스 정보 및 Restricted Rights를 확인하려면 **캐시비우기**, **오픈 소스 정보**, **Restricted Rights**를 클릭하세요.
3. 다음은 서버 정보에 대한 항목 설명입니다.

항목	설명
COMPUTERNAME	EMM 서버의 컴퓨터 이름
CRYPTOJ_VERSION	RSA CRYPTO-J 암호화 모듈의 버전
EMM Host	EMM 서버의 호스트 이름
EMM IP	EMM 서버의 IP 주소
EMM Version	EMM 버전과 빌드 넘버
FIPS Compliant	미국연방정보처리표준(FIPS) 준수 모드
JAVA_HOME	EMM 서버에 설치된 자바의 홈 경로
JMX PORT	EMM 서버에 설치된 JMX 포트
NUMBER_OF_PROCESSORS	EMM 서버의 CPU 수
OS	EMM 서버의 OS
PROCESSOR_ARCHITECTURE	EMM 서버의 CPU 프로세서의 종류
PROCESSOR_IDENTIFIER	EMM 서버의 CPU 설명
PROCESSOR_LEVEL	EMM 서버의 CPU 모델 번호
PROCESSOR_REVISION	EMM 서버의 CPU 수정 버전 번호
RMI PORT	EMM 서버의 RMI 포트
Tenant ID	EMM 서버의 Tenant ID

오픈 소스 및 Restricted Rights 정보

오픈 소스의 사용 , 제작 및 재 배포를 위해 오픈 소스 소프트웨어의 컴포넌트별 버전과 라이선스 정보 및 준수 사항 , 그리고 EMM 제품의 사용권 계약 조건 정보를 제공합니다 .

서버 목록 관리하기

클러스터링 되어있는 EMM 서버의 목록을 관리하려면 다음의 절차를 따르세요 .
서버 목록은 필요에 따라 추가 , 수정 및 삭제가 가능합니다 .

1. **설정 > 서비스 > 서버 목록**으로 이동하세요.
2. 화면 우측 상단 검색란에 **서버 IP**를 입력한 후, **Enter** 키를 누르거나 을 클릭하세요.
3. 다음은 서버 목록에 대한 설명입니다.

항목	설명
서버 IP	각 서버를 구분하기 위한 IP 주소
호스트 이름	서버의 호스트 이름
모니터링 포트	서버의 모니터링을 제공하는모니터링 포트
RMI 포트	서버의 RMI 서비스 포트
서비스 포트	서버의 서비스 포트
커넥터 서비스	서버의 커넥터 서비스 상태 (활성 / 비활성)
서버 구분	서버는 EMM 또는 Log Transfer Server(LTS)로 구분 • **EMM**: EMM 서버 • **LTS**: 로그 정보를 수집하는 서버
마지막 업데이트	서버의 마지막 업데이트일시

라이선스 관리하기

EMM 관리자 포털에서는 통합적으로 제품 라이선스를 관리합니다 . 라이선스 정보에는 회사명 , 라이선스 버전 , 유효 기간 , 보안 레벨 , 단독 제품 및 커넥터 정보 , 등록된 단말 수 , Knox Portal for mobile 사용 여부 등의 라이선스 정보를 포함하고 있으며 , 라이선스 유형에 따라 만료일 30 일 또는 90 일 전부터 라이선스 만료일에 대한 모니터링 알림이 관리자 포털에 표시됩니다 .
EMM 라이선스는 유효 기간 만료 시 EMM 사용에 제한 사항이 발생하며 , 라이선스 키를 업데이트하거나 라이선스 재 계약을 통해 Monthly 또는 Yearly 로 연장이 가능합니다 . 또한 EMM 관리자 포털의 메뉴 구성은 라이선스에 따라 보여지는 메뉴 및 정책들이 달라 질 수 있으며 , 라이선스에 대한 자세한 내용은 EMM 기술 운영팀에 문의하시기 바랍니다 .

단말 라이선스

EMM 라이선스 중 단말 라이선스는 EMM 서비스를 사용할 수 있는 최대 단말 수를 의미하며 , EMM 라이선스 별 단말 라이선스의 제한 사항은 다음과 같습니다 .

- 단말 라이선스는 최대 단말 한계 수량까지 등록할 수 있으며, 사용자 당 최대 5개까지 단말 등록이 가능합니다. 단, 구입한 최대 라이선스 수를 초과하여 등록할 수는 없습니다.

라이선스 확인하기

등록된 EMM 의 라이선 정보를 확인하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 라이선스 정보**로 이동하세요.
2. 라이선스에 관련된 정보를 확인하세요.

항목	설명
회사명	회사명이 표시됨
라이선스 버전	EMM 라이선스의 버전이 표시됨
보안 레벨	현재 운영중인 EMM의 버전이 표시됨(일반보안)
유효 기간	EMM 라이선스의 유효 일자가 표시됨
단독 제품	EMM 외 운영되는 제품이 표시됨 • PUSH
커넥터	라이선스에 유무에 따라 연계 가능한 커넥터가 표시됨 라이선스가 없는 커넥터는 관리자 포털 메뉴에 보여지지 않음 (예: DB, REST, FTP, SAP, MQ, WS)
단말 수	EMM에 등록 가능한 최대 단말 수가 표시됨 • 현재 등록된 단말 수가 표시됨
API Client 수	EMM 개발을 위한 API Client 수가 표시됨
mMail 수	라이선스에 등록된 모바일 메일의 사용자 수가 표시됨 • 현재 등록된 mMail 수가 표시됨
SecuCamera 수	라이선스에 등록된 SecuCamera의 수가 표시됨 • 현재 활성화된 SecuCamera의 수가 표시됨
방문자	방문자 메뉴 사용 여부가 표시됨 (사용, 미사용) • 사용: 방문자 관리를 위한 EMM 서버인 경우 방문자 관리에 대한 자세한 내용은 304페이지 18장의 "방문자 관리하기" 를 참고하세요. • 미사용: 방문자 관리를 위한 EMM 서버가 아닌 경우
Knox Portal for mobile	단말에서 Knox Portal 사용 여부가 표시됨 • 사용 • 미사용
삼성그룹향	삼성그룹향 사용 여부가 표시됨 • 사용 • 미사용

Note:
- EMM에서 방문자 메뉴, mMail, SecuCamera를 사용하려면 반드시 라이선스가 필요합니다. 라이선스 확인은 TMS 관리자 포털의 **관리 > Tenant**에서 해당 테넌트를 선택한 후, **라이선스**를 클릭하여 확인합니다. 자세한 내용은 "Samsung SDS TMS 관리 매뉴얼"의 라이선스를 참고하세요.
- EMM이 방문자 관리를 위한 서버로 사용되는 경우 로그인 시 사용되는 방문자 ID는 하나의 공통된 guest 아이디만 제공됩니다.

라이선스 등록하기

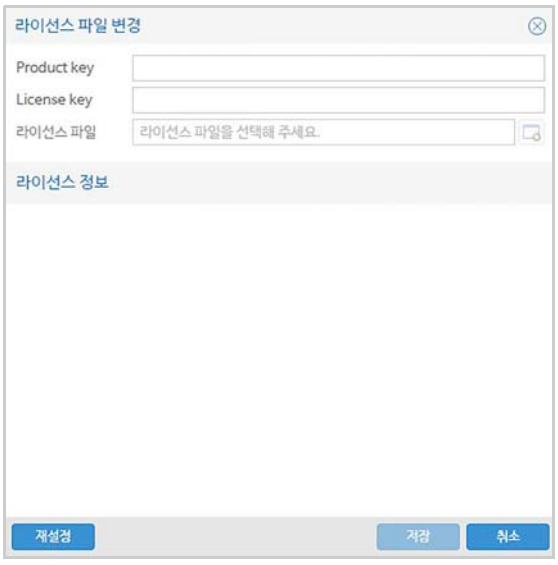
EMM 제품 라이선스가 등록되어있지 않은 경우 , EMM 은 데모 라이선스로 운영되며 EMM 사용에 제한이 있을 수 있습니다 . EMM 의 정상적인 운영을 위해서는 반드시 라이선스를 등록한 후 , 운영해야 합니다 .

EMM 운영 모드에 따른 라이선스 등록 방법은 다음과 같습니다 .

- Single-Tenant: EMM 관리자 포털에서 라이선스를 등록합니다.
- Multi-Tenant: TMS 관리자 포털의 라이선스 메뉴에서 라이선스를 등록합니다.

Single-Tenant 로 운영하는 경우 , 라이선스를 등록하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 라이선스 정보**로 이동하세요.
2. 화면 상단의 **라이선스 파일 변경**을 클릭하세요.



3. "라이선스 파일변경" 창에서 설치된 제품의 Product key, 발급 받은 License key 값을 입력하고 을 클릭한 후, 라이선스 파일을 선택하여 업로드하면 라이선스 정보가 하단에 나타납니다.
   - **Product key**: EMM 설치 시 생성되는 제품의 키 값입니다.
   - **License key**: EMM 라이선스의 키 값을 입력합니다.

4. 라이선스에 대한 정보를 확인한 후, **저장**을 클릭하세요.
   - **재설정** 클릭 시 발급받은 라이선스가 다시 설정됩니다.

> **Note:** Multi-Tenant 모드로 운영 시 라이선스 등록 및 관리는 TMS 서버에서 관리됩니다. 자세한 내용은 “Samsung SDS TMS 관리 매뉴얼”을 참고하세요.

서비스 프로파일 관리하기

서비스 프로파일은 단말이 활성화 될 때 , EMM 서버에서 단말로 다운로드되어 적용되는 서비스 정보로 서비스 프로파일에서 관리되는 정보는 EMM Server, EMM Client, Push Server, App Store, Audit Server, Log Server, MDM, mMail Server 의 정보입니다 . 서비스 프로파일의 각 항목별 설정에 대한 자세한 내용은 “Samsung SDS EMM 설치매뉴얼의 서비스 프로파일 설정하기 ” 를 참고하세요 .

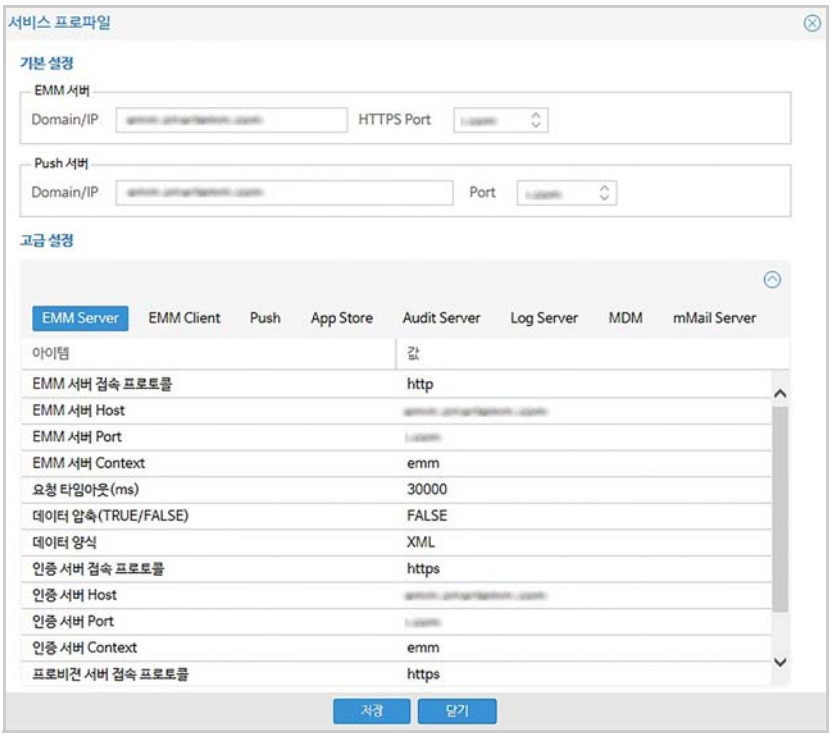
서비스 프로파일은 Single-Tenant 또는 Multi-Tenant 모드에 따라 다르며 , 각 모드에서 관리되는 서비스 프로파일의 다음과 같습니다 .

- **Single-Tenant 모드**: **설정 > 서비스 > 환경 설정**의 상단 우측에 **서비스 프로파일**이 활성화되며, 서비스 프로파일을 관리하려면 **서비스 프로파일**을 클릭합니다. 또한 서비스 프로파일의 서비스 정보는 아이템 ID별로 설정되고 운영자가 임의로 수정할 수 없습니다.
- **Multi-Tenant 모드**: TMS 관리자 포털의 **관리 > 서비스 프로파일**에서 서비스 프로파일을 관리합니다. 자세한 내용은 “Samsung SDS TMS 관리자 매뉴얼”을 참고하세요.

Single-Tenant 에서 서비스 프로파일을 관리하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 환경 설정**으로 이동하세요.

2. 화면 상단의 **서비스 프로파일**을 클릭하세요.



- **기본 설정**: 서비스 프로파일의 공통 설정 항목을 입력합니다. EMM, Push 서버의 정보를 입력하면 고급 설정의 해당 항목이 자동으로 동일하게 매핑됩니다.
  - 서버 라이선스가 없는 경우, 해당 서버는 설정 항목에 보이지 않습니다.
- **고급 설정**:
  - **EMM Server**: EMM 서버와 관련된 설정 정보를 입력합니다.
  - **EMM Client**: 단말에서 EMM 설치를 위한 다운로드 URL 주소를 입력합니다.
  - **Push**: Push 서버의 설정 정보를 입력합니다.
  - **AppStore**: AppStore 접속을 위한 URL 주소를 입력합니다.
  - **Audit Server**: Audit 서버의 설정 정보를 입력합니다. Audit 로그를 원격서버에 전송하여 관리하거나 파일로 생성한 후, 외부 서버로 전송하려면 29페이지의 "Audit 설정하기"를 참고하세요.
  - Log Server: Log 서버의 설정 정보를 입력합니다.
  - **MDM**: EMM 또는 Push Agent 다운로드 URL, iOS MDM 등록 URL, 공장 초기화 시 EMM Client 다운로드 URL 주소 등을 입력합니다.
  - **mMail Server**: 모바일 메일 서버의 설정 정보를 입력합니다.

3. 서버 환경에 맞춰 아이템에 해당하는 값을 수정한 후, **저장**을 클릭하세요.

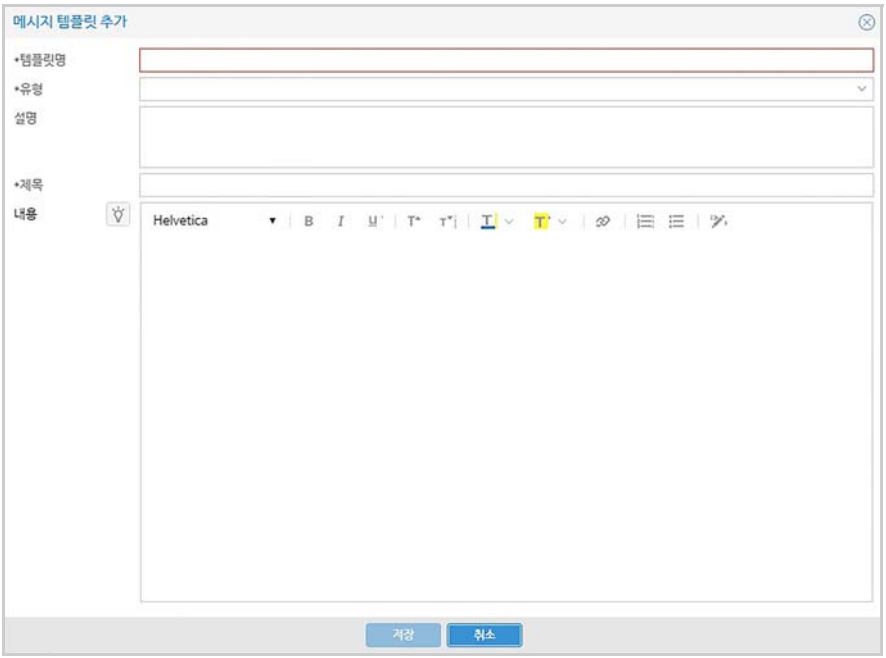
메시지 템플릿 관리하기

EMM 운영 중 사용자에게 SMS 또는 이메일을 발송하기 위해 메시지 템플릿을 등록하고 관리합니다 . 메시지 템플릿은 설치 및 운영자 인증을 위해 관리자 포털에서 기본으로 제공하는 유형이 있으며 , 해당 템플릿들은 수정 및 삭제 시 제한 사항이 있을 수 있습니다 .

그외 일반 또는 임시비밀번호 전송 유형의 템플릿은 관리자에 의해 등록 , 수정 , 복사 및 삭제가 가능합니다 .

메시지 템플릿을 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > 메시지 템플릿**으로 이동하세요.
   - QR 코드 전송, 임시 비밀번호 전송, Tizen Wearable 설치정보 전송 및 운영자 인증을 위한 템플릿은 관리자 포털에서 기본으로 제공합니다.
   - Tizen Wearable 설치정보 전송을 위한 SMS 템플릿은 다음과 같이 3개의 기본 템플릿으로 제공되며, 그 중 'Tizen Wearable Installation', 'Tizen Wearable Code' 템플릿은 Tizen 단말에서 정보를 파싱하기 위한 형식으로 임의로 수정이 불가능합니다.
2. 화면 상단의 ＋을 클릭하세요.



3. “메시지 템플릿 추가” 창에 다음 정보를 입력하세요.
   - **템플릿 명**: 메시지 템플릿명을 입력합니다.
   - **유형**: 메시지 템플릿 유형을 선택합니다.
     일반 유형의 템플릿은 내용 작성 시 을 클릭하여 다음과 같이 템플릿 유형에 맞는 참조 항목을 선택합니다. 선택된 유형에 따라 반드시 포함시켜야 하는 참조 항목의 항목 이름과 값은 다음과 같습니다.

템플릿 유형	참조 항목 이름	참조 항목 값
운영자 인증	• 운영자 OTP	• ${AdminOTPCode}
QR 코드 전송	• QR 코드	• ${QRCode}

템플릿 유형	참조 항목 이름	참조 항목 값
임시 비밀번호 전송	• 임시 비밀번호	• ${UserTempPassword}
Tizen Wearable 설치 정보	• Tizen EMM 설치 주소 • EMM/TMS 서비스 URL • 인증 코드 발급 URL • 인증 코드	• ${TizenClientAddress} • ${TizenShortenUrl} • ${TizenOTPUrl} • ${TizenOTPCode}

- **설명**: 메시지에 대한 간략한 설명을 입력합니다.
- **제목**: 메시지의 제목을 입력합니다.
- **내용**: 메시지의 내용을 입력합니다.
  - 을 클릭하면 "참조 항목" 창에서 메시지 발송시 실제 값으로 대체되어 발송되는 참조 항목 이름과 값이 나타납니다. 추가하려는 항목을 더블 클릭하여 템플릿에 추가하세요.

4. 메시지 템플릿의 작성이 완료되면 **저장**을 클릭하세요.
   - 등록한 메시지 템플릿은 메시지 템플릿 목록에서 확인합니다.

Note:
- "참조 항목" 창에서 Copyright, 서비스 데스크 이메일 및 전화번호, EMM/TMS 서비스 URL, 인증 코드 발급 URL 항목은 **설정 > 서비스 > 환경설정**에 해당 값들이 설정되어 있는 경우에만 템플릿에 자동으로 값이 입력됩니다.
- 템플릿에 이미지를 추가하려면 "이메일 템플릿 추가" 창에서 **소스 편집** 클릭하여 url 형식으로 이미지를 추가합니다.
- SMS 템플릿 중 Tizen Wearable Information 템플릿에 들어가는 내용이 80자를 초과하는 경우, 분할되어 전송됩니다.

IMEI 관리하기

IMEI 는 단말의 국제 고유 식별 번호로 , IMEI 를 등록한 단말만 활성화할 수 있도록 관리자 포털에 설정할 수 있습니다 . IMEI 등록은 개별 또는 CSV 파일로 일괄 등록할 수 있으며 , **설정 > 서비스 > 환경 설정**에서 **IMEI 등록 제한**을 **TRUE** 로 설정해야만 IMEI 등록이 가능합니다 .

IMEI 를 개별로 등록하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > IMEI 관리**로 이동하세요.
2. 화면 상단의 ＋을 클릭한 후, **개별 등록**을 선택하세요.

3. “개별 등록” 창에 **IMEI**를 입력하세요.
4. **저장**을 클릭하세요.

IMEI 파일 올리기

IMEI 를 파일로 일괄 등록하려면 다음의 절차를 따르세요 .

1. **설정 > 서비스 > IMEI 관리**로 이동하세요.
2. 화면 상단의 ＋을 클릭한 후, **일괄 등록**을 선택하세요.

3. **일괄 양식 등록 다운로드**를 클릭한 후, PC에 저장하세요.
4. CSV 파일에 IMEI 번호를 입력한 후, 저장하세요.
5. **Browse**를 클릭한 다음 작성한 파일을 선택한 후, 업로드하세요.
6. **확인**을 클릭하세요.

3 모니터링

운영자는 Audit, 보고서 , 대시보드를 통하여 EMM 운영 현황을 모니터링할 수 있습니다 . Audit 는 EMM 에 미리 정의된 Audit 이벤트의 처리 결과를 로그 정보로 제공합니다 . 지정한 Audit 이벤트에 대한 모니터링 알림을 설정하여 , 관리자 포털 로그인시 팝업 알림 또는 모니터링 알림 메뉴에 숫자 알림으로 Audit 이벤트 발생 정보를 받을 수 있습니다 . 사용자의 단말 상태나 단말 제어 이력이 단말에 로그로 저장됩니다 . 사용자가 단말에서 로그를 전송하거나 , 관리자 포털에서 단말 제어를 요청할 때 단말 로그는 EMM 으로 전송됩니다 . 단말로 전송된 로그는 파일로 다운로드하여 확인할수 있습니다 . 운영자는 단말 , 사용자 , 앱에 대한 정보와 단말 잠금 , 앱 위변조 , 최신 프로파일 등 EMM 운영 현황을 보고서를 통해 확인합니다 . 운영자는 EMM 에서 제공하는 보고서 쿼리를 기반으로 보고서를 만들고 , 만든 보고서를 기반으로 대시보드를 추가할 수 있는 기능을 제공함으로써 시스템 운영에 효율성을 높일 수 있습니다 .

Audit 이벤트

Audit 은 EMM 운영할때 관리자 포털 , 사용자 단말 , EMM 서버 , System 서버에서 발생하는 작업 (프로세스) 인 이벤트에 대한 회사 사용 정책과 보안 정책에 따라 기록된 로그를 분석하는 것입니다. 이는 EMM 시스템 사용 여부를 평가하고 장애 처리를 돕기 위해 사용됩니다 .

Audit 이벤트 유형

EMM 에서는 이벤트가 발생하는 관리자 포털 , EMM 서버 , 단말 , 시스템에 따라 이벤트 유형을 분류하고 , 이벤트가 발생하면 Audit 로그로 기록됩니다 . Audit 이벤트 유형에 따른 이벤트는 다음과 같습니다 .

- Console: 운영자의 로그인 정보, 계정 관리, 정책 관리, 애플리케이션 관리 및 연동 시스템 연결 정보등 관리자 포털에서 발생하는 이벤트입니다.
- Device: 단말의 Enrollment, 앱 패키지, 인증서 발급, 단말 제어 명령, 단말 관리 프로파일, EMM 로그인의 오류 및 변경 정보등 단말에서 발생하는 이벤트입니다. 단말에서 EMM 서버로 보내는 로그 파일 사이즈를 초과한 경우에는 EMM 서버로 Audit 로그를 전송후 새로운 파일에 Audit 로그가 기록됩니다.

- Server: EMM서버에서 단말로 또는 단말에서 EMM서버로 보내는 이벤트입니다. 단말에서 서버로 Audit 이벤트 요청 시에는 단말 사용자, Audit 이벤트의 로그를 수집하는 스케줄링 이벤트입니다.
- System: EMM 서버 로그 중에서 EMM 서버 기동 및 중지, 암호화등 시스템에 대한 이벤트입니다.

Audit 이벤트 레벨

EMM 운영할 때 발생하는 Audit 이벤트에 대하여 심각도 레벨을 표시합니다 . 심각도는 EMM 운영시 발생하는 오류 , 주의가 필요한 정보를 나타냅니다 . 운영자는 심각도 레벨로 이벤트 오류가 무엇이며 얼마나 치명적인지를 알수있고 , 이벤트 유형인 Console, Server, Device, System 에서 발생하는 이벤트의 심각도 레벨에 따른 조치를 취하거나 예의 주시할 수 있습니다 . 심각도 레벨은 다음과 같습니다 .

- Critical: 시스템 중단 등의 심각한 오류 발생에 대한 이벤트
- Error: 일반적인 오류 이벤트
- Warning: 오류는 아니지만 주의가 필요한 이벤트
- Notice: 알림이 필요한 이벤트
- Info: 관리자에게 필요한 일반적인 이벤트
- Debug: 개발자에게 필요한 상세하게 정의된 이벤트

Audit 로그 조회하기

시스템 운영 정보와 사용자 단말 로그 정보는 Audit 로그로 기록합니다 . Audit 로그의 대상은 EMM 서버 , 사용자 단말 , 관리자 포털 , 시스템이며 , 관리자 포털의 **서비스 현황 > 대시보드 & Audit 설정 > Audit 이벤트**에서 설정한 Audit 이벤트 발생 시 EMM 서버에 기록됩니다 . 모든 서버에서 Audit 로그는 각각의 서버 로그 파일에 기록됩니다 . Audit 이벤트 목록에 대한 자세한 내용은 314 페이지 18 장의 “Audit 이벤트 목록 " 를 참고하세요 . Push 서버에서 발생하는 Audit 정보에 대한 자세한 내용은 340 페이지의 " Push 의 Audit 로그 " 를 참고하세요 .

Audit 로그를 조회하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 로그 > Audit 로그**로 이동세요.
2. Audit 유형 목록과 화면 왼쪽 상단에서 을 클릭하여 조회하려는 날짜를 선택한 후 검색하거나, 검색란에 **사용자ID**, **모바일 ID** 또는 **이벤트**를 입력한 후 Enter Key 를 누르거나 을 클릭하세요.

- 검색된 결과 목록에 대해서 재검색이 가능

3. 목록에서 확인하려는 로그 항목을 클릭하세요. 목록 하단에 로그의 상세 내용이 표시됩니다.

항목	설명
로그 일시	Audit 로그가 발생한 일시입니다.
사용자 ID	이벤트를 발생시키는 주체입니다. • Console인 경우: admin 또는 사용자 ID • Server인 경우: 단말 사용자 또는 스케줄 작업인 경우에는 Batch user ID • Device인 경우 : 단말 사용자 ID • System인 경우: 스케줄 작업으로 SYSTEM으로 표시
모바일 ID	단말 제어에 관한 Audit 이벤트가 발생한 경우, 이벤트 작업 유형에 따른 모바일 ID 입니다. • Console인 경우: 단말 제어 Audit 로그 수집 할 모바일 ID • Server인 경우: 단말에서 EMM 서버로 이벤트 요청 시 모바일 ID이고, 단말에 대한 스케줄 작업인 경우 해당 모바일 ID 또는 Batch user • Device인 경우: 모바일 ID
접속 IP	관리자 포털을 접속한 IP 주소입니다.
이벤트 분류	이벤트 분류 목록은 314페이지 18장의 “Audit 이벤트 목록"를 참고하세요.
이벤트	발생된 이벤트 정보입니다.
결과	발생된 이벤트의 실행 결과 정보입니다.
조회	단말 제어에 관한 Audit 이벤트를 조회할 수 있는 링크를 표시합니다. 자세한 내용은 58페이지의 "단말 제어 Audit 조회하기"를 참고하세요. • 조회는 요청ID의 첫3자리만 표시되며 요청ID는 아래와 같은 조합으로 생성됩니다. - 1번째: 단말 플랫폼 (Android: A, iOS: I, Windows: W, Tizen: T) - 2번째: 애플리케이션(Android는 Agent: A, iOS는 (Agent: A, Client: C)) - 3번째: 프로세스 시작 지점 (Server: S, Device: D)

항목	설명
처리 정보	화면 하단의 처리정보에 대한 내용입니다. • 요청내역: Audit 이벤트를 요청한 상세 내역 정보입니다. • 결과 코드: 성공 또는 실패로 표시되며 이벤트의 결과를 조회합니다. • 결과 내역: Audidt 이벤트별 결과 내역 정보입니다. - 관리자 포털에서 정책을 변경하면 Profile 이벤트 분류의 이벤트 목록으로 기록됩니다. 예를 들어 Android 정책을 변경하는 경우 “General 정책 저장” 이벤트의 **요청 내역**에 저장되어야 할 전체 정책 목록이 조회됩니다. - “사용자당 단말 수 초과"는 단말 활성화 시, 사용자별 최대 활성화 단말수를 초과했을 때 발생합니다. 활성화 실패한 모바일 ID가 **결과 내역**에 조회됩니다. 사용자당 활성화 최대 단말수는 5대로 제한되어 있습니다. - "패키지 삭제 실패" 이벤트의 경우 삭제 실패된 packagename과 원인이 **결과 내역**에 조회됩니다
작업 Data	화면 하단의 작업 Data에 대한 정보입니다. 이벤트 유형, 이벤트 분류가 다음과 같은 경우 작업 Data 정보를 확인할수 있습니다. • 이벤트 유형이 Console인 경우: 단말에서 EMM 서버로 4000byte이상의 데이터를 보낼 시 • 이벤트유형이 Server인 경우: 이벤트 분류가 Device command이고, 이벤트가 Agent 단말 잠금 요청(단말->서버), Agent 단말 잠금 해제 요청(단말->서버), Agent 작업보고 요청(단말->서버) 또는 다중 단말 단말 제어 전송으로 처리일 경우 • 이벤드 유형이 Device인 경우: 이벤트 분류가 Device command이고, 이벤트가 단말 잠금/잠금해제 이력일 경우

주요 Audit 이벤트의 상세 설명은 다음과 같습니다.

- “암호화 모듈 자체 테스트”는 서버의 암호화 모듈(Crypto-J)의 암호화 무결성 체크에 대한 Audit 이벤트이며, **처리 정보** 탭에 처리 결과가 기록됩니다. 암호화 무결성 체크 대상은 다음과 같습니다.
  - JarVerify, SHA512, AES, TripleDES, KDFTLS10, HMACDRBG, ECDRBG, FIPS186Random, DSA, ECDSA, CTRDRBG

- "무결성 오류"는 EMM 서버를 기동하거나 파일이 변경되는 경우 발생하는 Audit 이벤트입니다. Signing하여 배포한 EMM 코드가 맞는지 무결성을 체크합니다. 만약 무결성 오류가 발생하는 경우 오류가 발생한 파일 경로와 오류 파일 목록이 **결과 내역**에 조회됩니다.

Note:

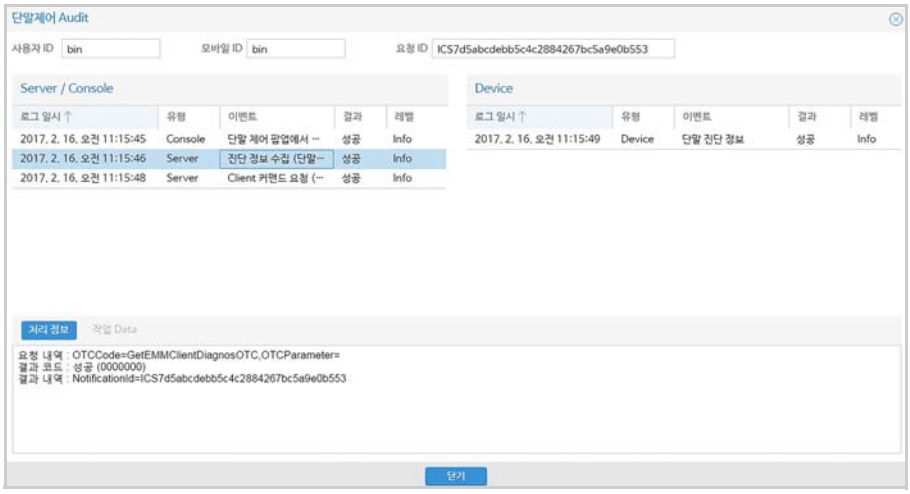
- **설정 > 서비스 > 환경설정** 메뉴의 **Audit 설정**에서 **Audit 로그 보존 한도**를 설정합니다. EMM 서버에 저장되는 Audit 로그의 저장 한도를 설정할 수 있습니다. **설정 > 서비스 > 환경설정** 메뉴에서 **Audit 설정** 버튼을 클릭한후, **Audit 로그 설정** 영역의 **Audit 로그 보존 한도**에서 설정하세요. **Audit 로그 보존 한도**로 설정한 건수의 90% 초과 시 관리자 포털에서 알림 메시지를 발생시킵니다.
- Audit 로그는 로그 보존 한도로 설정한 건수에 도달하더라도 계속 저장되기 때문에 운영 환경에 맞는 삭제 방법으로 Audit 로그를 삭제해야합니다. 고객사의 Audit 로그 관리 정책에 따라 관리합니다. 서비스 프로파일과 사용자 동의서 다운로드 로그는 Single-Tenant 모드의 경우 Audit 로그에서 조회 가능하고, Multi-Tenant 모드의 경우 TMS 관리자 포털에서 조회 가능합니다. 자세한 내용은 "Samsung SDS TMS 관리매뉴얼"을 참고하세요.
- **설정 > 서비스 > 환경설정** 메뉴의 **Audit 설정**에서 **단말 Audit DB로 가져오기**를 **TRUE**인 경우 단말에 대한 Audit 로그를 조회 할 수 있습니다. 자세한 내용은 29페이지 2장의 "Audit 설정하기"를 참고하세요.

단말 제어 Audit 조회하기

단말 제어 요청별로 요청 ID 가 생성되고 , 요청 ID 별로 단말 , 서버 및 관리자 포털에서 발생한 단말 제어 Audit 을 조회합니다 .

단말 제어 요청 ID 별로 Audit 을 조회하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 로그 > Audit 로그**로 이동하세요.
2. Audit 유형이나 화면 왼쪽 상단에서 을 클릭하여 조회하려는 날짜를 선택 후 검색하거나, 검색란에 **사용자 ID**, **모바일 ID** 또는 **이벤트**를 입력한 후 을 클릭하세요.
3. 목록에서 조회 항목의 값(요청ID 앞 3자리)을 클릭하세요.



4. “단말 제어 Audit”창에 사용자 ID, 모바일 ID, 요청 ID를 확인하세요.

항목	설명
사용자 ID	이벤트를 발생시키는 주체입니다. • Console인 경우: admin 또는 사용자 ID • Server인 경우: 단말 사용자 또는 스케줄 작업인 경우에는 Batch user ID • Device인 경우: 단말 사용자 ID • System인 경우: 스케줄 작업으로 SYSTEM으로 표시
모바일 ID	단말 제어에 관한 Audit 이벤트가 발생한 경우, 이벤트 작업 유형에 따른 모바일 ID 입니다. • Console/Server인 경우: 단말 제어 Audit 로그 수집 할 모바일 ID, 단말에서 EMM 서버로 이벤트 요청 시 모바일 ID이고, 단말에 대한 스케줄 작업인 경우 Batch user • Device인 경우: 모바일 ID
요청ID	• 단말 제어 요청별로 생성된 요청 ID 기준으로 단말, 서버 및 관리자 포털에서 발생한 Audit 이벤트의 단계별 상세 정보 제공 • 요청ID 생성 규칙 - 1번째: 단말 플랫폼 표시(Android: A, iOS: I) - 2번째: 애플리케이션 표시 (Android는 Agent: A, iOS는 (Agent:A, Client: C)) - 3번째: 프로세스 시작 지점 표시(Server: S, Device: D)

5. 요청ID 기준으로 발생한 단말 제어 Audit 이벤트와 **Console/Server** 영역과 **Device** 영역에서 로그 정보를 확인하세요.
   팝업 목록 하단에 로그 처리의 상세 정보가 나타납니다.

항목	설명
로그 일시	Audit 로그가 발생한 일시입니다.
유형	단말 제어에 관한 Audit 이벤트가 발생한 경우, 이벤트 작업 유형에 따른 모바일 ID 입니다. • Console/Server인 경우: 단말 제어 Audit 로그 수집 할 모바일 ID, 단말에서 EMM 서버로 이벤트 요청 시 모바일 ID이고, 단말에 대한 스케줄 작업인 경우 Batch user • Device인 경우: 모바일 ID
이벤트	발생된 단말 제어 Audit 이벤트 정보입니다.
결과	발생된 단말 제어 Audit 이벤트의 실행 결과 정보입니다.

Audit 로그 엑셀로 내보내기

Audit 로그의 상세 내역을 Excel 파일로 저장할 수 있습니다 . 내보내기한 Audit 로그 데이터는 EMM 서버에서 삭제되지 않습니다 .

Audit 로그를 Excel 파일로 내보내기하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 로그 > Audit 로그**로 이동하세요.
2. Excel 파일로 내보내려는 Audit 로그를 선택 후, 을 클릭하세요.
3. 좌측 하단의 Excel 파일을 클릭하세요.

- 항목: 로그 일시, 대상, 사용자 ID, 모바일 ID, 접속 IP, 이벤트 ID, 이벤트 분류, 이벤트결과, 레벨, 요청 내역, 결과 코드, 결과 내역, 작업 Data

Audit 대상 설정하기

Audit 이벤트를 이벤트 대상으로 설정하면 , 해당 Audit 이벤트 발생시 Audit 원격 로그 서버에 로그 정보가 기록됩니다 .

Audit 이벤트 대상으로 설정하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 대시보드 & Audit 설정 > Audit 이벤트**로 이동하세요.
2. Audit 이벤트 대상으로 설정하려면, **Audit 대상** 확인란을 선택하세요.
   - Audit 이벤트 대상으로 설정하지 않으려면, **Audit 대상** 선택을 해제합니다.
3. Audit 대상을 저장하려면 화면 좌측 상단을 클릭하세요.
   - 저장 확인 메시지가 나타나면 예를 클릭하세요.

Audit 이벤트 분류하기

Audit 이벤트는 대분류로 이벤트유형 , 중분류로 이벤트 분류로 나뉩니다 . 대분류는 이벤트가 발생하는 유형으로 관리자 포털 , 서버 , 단말 , 시스템이고 , 중분류는 이벤트 유형에 대한 기능으로 단말 제어 , 동기화 작업 , 앱관리 , EMM System 등 중분류로 나뉩니다 . 자세한 내용은 314 페이지 18 장의 “Audit 이벤트 목록 " 을 참고하세요 .

이벤트 분류	이벤트 유형			
	Console	Server	Device	System
AD/LDAP Sync	O	O		
Admin Login	O			
Administrators	O			
Alerts	O			
AppTunnel			O	
Applications	O	O		
Certificate Status			O	
Certificates	O			
Compliance		O	O	
Connectors	O			
Cryptographic Support				O
Dashboard	O			
Device Command	O	O	O	
Device			O	

이벤트 분류	이벤트 유형			
	Console	Server	Device	System
Devices	O			
E-FOTA	O	O		
Email	O	O		
EMM Agent			O	
EMM Client			O	
EMM System				O
Enrollment		O	O	
Groups	O			
Integrations	O			
Exception Profile per User		O		
InventoryScheduler		O		O
Kiosk Launcher			O	
License Management		O		
Logs	O	O	O	O
Notices	O			
Organization	O			
Profile			O	
Profiles	O	O	O	
Provision		O		
Push				O
SEG Profile	O	O		
Service Profiles	O	O		
Settings	O			
SmartKey		O		
SMS	O	O		
System Configuration	O			
Time Trigger		O		
TxHistory		O		
User			O	
User Login		O		
User Management	O			
Windows	O			

모니터링 알림

운영자는 모니터링 알림으로 EMM 서버 상태를 점검하고 , 정책 적용이 실패한 단말을 확인하고 , 악성 앱 설치되거나 정책을 위반한 단말을 확인할 수 있습니다 . 운영시 필요한 기본 알림은 미리 설정되어 있습니다 .

Audit 이벤트의 알림 분류는 다음과 같습니다 .

- **서버 상태 변경**: 시스템 오류에 대한 이벤트 발생한 경우
  - Server 인증서 만료, Server 인증서 폐기, 새로운 파일 생성, 기존 파일 삭제, 기존 파일 수정, 기존 파일 이름 재정의, 무결성 오류, 인증되지 않은 패키지에 대한 Audit 이벤트
- **정책 적용 실패**: 단말에 설정된 정책 중 실패한 경우, 단말에서 Push 사용을 위한 요청이나 이에 대한 응답인 경우
  - Agent 단말 정책 적용 실패, Agent 단말 제어 수행 실패, Client 단말 제어 수행 실패에 대한 Audit 이벤트, EMM서버와 단말 Push Agent간의 메시지 전송에 대한 Audit 이벤트
- **단말 상태 변경**: 단말 상태를 활성화 또는 비활성화로 변경할 경우
  - 단말 상태 갱신에 대한 Audit 이벤트
- **보안 위반**: 정책을 위반한 단말의 로그를 서버로 보내는 경우, 악성앱이 설치된 단말 로그를 서버로 보내는 경우
  - Agent 정책 위반 보고 요청 및 정책 위반 보고에 대한 알림 설정, Check Point MTP 악성앱 진단 정보로 단말에 악성앱 감지
- **기타**: 그외 이벤트 목록

모니터링 알림 조회하기

모니터링 알림으로 설정된 Audit 이벤트를 조회하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 모니터링 알림**으로 이동하세요.
2. 화면 좌측 상단의 을 클릭하여 조회하려는 날짜를 선택한 후 검색하거나, 우측 상단 검색란에 **모바일 ID**를 입력한 후 을 클릭하세요.

항목	설명
생성일	Audit 이벤트가 발생된 일시입니다.
알림 분류	발생된 이벤트의 알림 분류는 서버 상태 변경, 정책 적용 실패, 단말 상태 변경, 보안 위반, 기타로 나뉩니다.
Audit 이벤트	발생된 Audit 이벤트입니다.
모바일 ID	Audit 이벤트가 발생된 모바일 ID입니다.

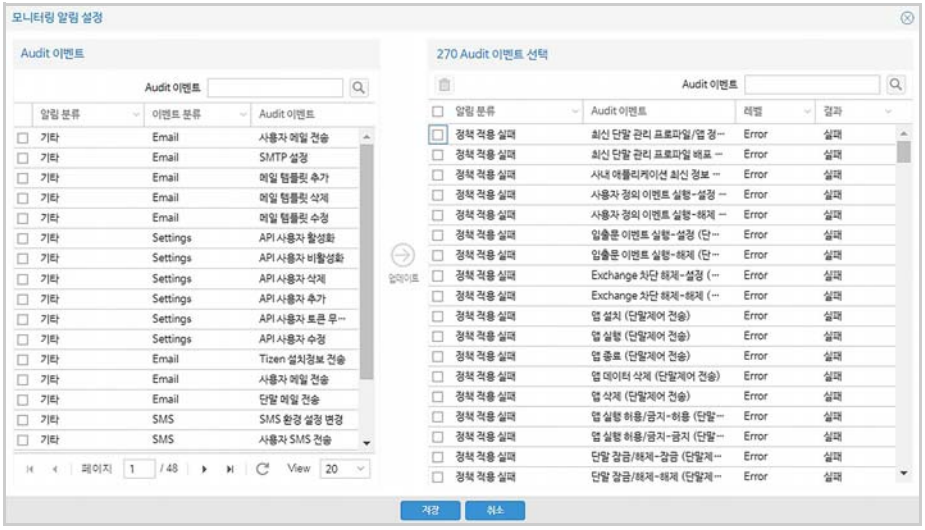
3. 목록에서 조회하려는 **Audit 이벤트**를 클릭하세요
   - **알림 상세** 영역에서는 Audit 로그 요약 및 상세 로그 내용이 표시됩니다.

- 정책 적용 실패 시에는 적용되지 않은 정책에 대한 정책명과 실패 사유를 확인할 수 있습니다.

모니터링 알림 설정하기

기본 설정외의 이벤트를 모니터링 알림으로 설정하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 모니터링 알림**으로 이동하세요.
2. 화면 왼쪽 상단 ⚙을 클릭하세요.
   “모니터링알림 설정” 창이 나타납니다.



3. Audit 이벤트 영역에서 이벤트를 입력하고, 🔍을 클릭하세요.
4. **Audit 이벤트** 영역에서 모니터링 알림으로 설정하려면 이벤트 항목을 선택한 후 ⊖을 클릭하세요.
   - **Audit 이벤트**영역: 모니터링 알림으로 설정할 수 있는 이벤트 항목

항목	설명
이벤트 분류	발생된 Audit 이벤트의 중분류 입니다. 자세한 내용은 60페이지의 "Audit 이벤트 분류하기"를 참고하세요.
Audit 이벤트	발생된 Audit 이벤트입니다.

   - **Audit 이벤트 선택**영역: 현재 모니터 알림 대상으로 설정된 이벤트의 수 및 항목
     - 모니터링 알림 대상으로 설정하려는 Audit 이벤트의 레벨과 결과는 변경 가능함

항목	설명
결과	발생된 Audit 이벤트 레벨에 따른 기본 실행 결과를 표시합니다. • 모두: 모니터링할 이벤트의 레벨이 성공 또는 실패일 경우 • 성공: 모니터링할 이벤트의 레벨이 성공일 경우 • 실패: 모니터링할 이벤트의 레벨이 실패일 경우

5. 모니터링 알림 대상으로 설정하려는 이벤트를 확인한 후 **저장**을 클릭하세요.

- 모니터링 알림 대상에서 제외하려면, **Audit 이벤트 선택**영역에서 이벤트를 선택하고, 상단의 을 클릭하세요. 기본으로 설정된 모니터링 알림 Audit 이벤트는 삭제할수 없습니다.

단말 로그 조회하기

운영자는 단말의 내부 동작 , 오류 , 상태를 확인하기 위해 관리자 포털로 전송된 단말 로그를 확인합니다 . 또한 Push 서비스를 사용하는 단말에 대해서는 Push Device Agent 로그를 확인합니다 . 단말 로그는 사용자가 EMM 에서 로그 보내기를 실행하는 경우 , EMM 서버로 전송됩니다 . 단말 로그에는 인벤토리 정보와 정책 및 단말 제어가 적용 시의 로그 메시지 등이 포함되어 있습니다. 로그 정책이 설정되어 있는 단말은 로그 정책에서 설정한 값을 우선으로 적용하여 로그를 수집합니다 . 로그 정책은 **프로파일 > 단말 관리 프로파일**에서 설정합니다 . 로그 정책 설정에 대한 자세한 내용은 368 페이지 18 장의 " 로깅 그룹 " 을 참고하세요 . 단말 로그의 기본 설정값은 EMM 설치시 다음과 같이 설정됩니다 .

- 로그 최대 수집 용량: 10MB
- 로그 최대 보관 기간: 7일
- 로그 기록 수준: DEBUG, 개발자에게 필요한 상세 정보 기록

단말 로그의 설정 값을 변경하는 방법은 Single-Tenant 모드와 Multi-Tenant 모드에 따라 다릅니다 .

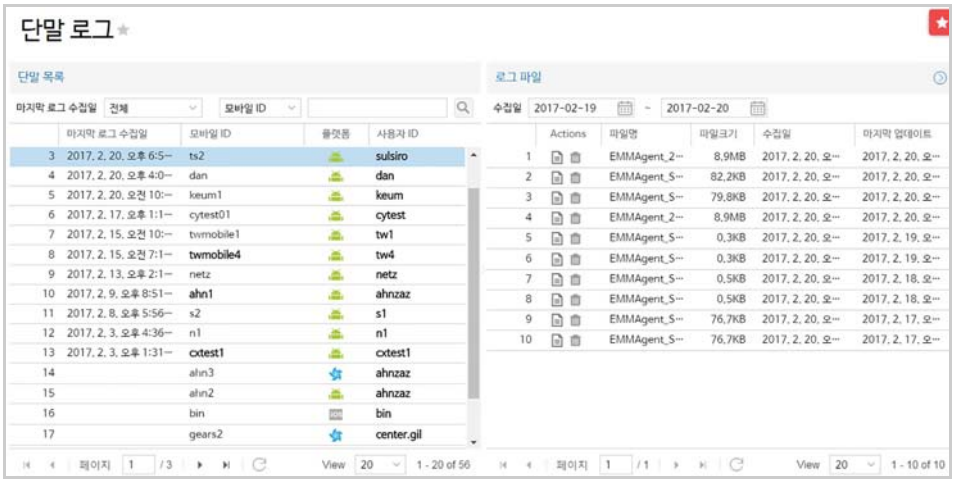
- Single-Tenant 모드: 설정 > 서비스 > 환경설정의 서비스 프로파일을 클릭하여 설정합니다.
- Multi-Tenant 모드: TMS 관리 콘솔의 관리 > 서비스 프로파일에서 설정합니다.

사용자 단말의 로그를 확인하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 로그 > 단말 로그**로 이동하세요.
2. 특정 단말 로그만 조회하려면, 우측 상단에서 검색 목록에서 **사용자 ID** 또는 **모바일 ID**를 선택하여 검색어를 입력한 뒤 **Enter** 키를 누르거나 을 클릭하세요.
   - **마지막 로그 수집일** 목록에서 전체, 7일 내, 14일 내, 30일 내 조건으로 단말 전체 로그를 필터링하여 조회할 수 있습니다.

항목	설명
마지막 로그 수집일	마지막으로 단말로그가 수집된 일시입니다.
모바일 ID	단말을 구분하기 위한 ID입니다.
플랫폼	단말의 OS 플랫폼입니다.
사용자 ID	단말의 사용자 ID입니다.

3. 목록에서 조회하려면 단말을 클릭하세요.
   우측의 **로그 파일** 영역에서 단말 로그에 대한 상세 내용이 표시됩니다.

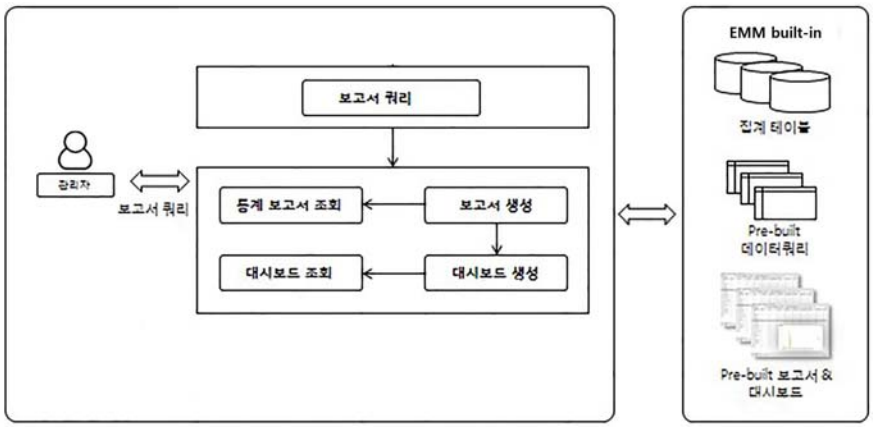


- 로그 파일 영역에서 을 클릭하여 조회 기간을 선택합니다.
- : 선택한 로그 파일을 텍스트 파일로 내보내기를 합니다.
- :선택한 로그 파일을 삭제합니다.

항목	설명
파일명	단말에서 생성된 로그 파일명입니다. 단말에서 로그를 발생하는 주체에 따라 파일명이 다릅니다. • EMMClient_yyyymmdd.log: EMM Client 로그 • EMMAgent_yyyymmdd.log: EMM Agent 로그 : Tizen Wearable은 EMMAgent 로그만 확인 • EMMClient_SecureStorageLog_{Level}_yyyymmdd.log :EMM Client 내부의 SecureStorage 로그 • EMMAgent_SecureStorageLog_{Level}_yyyymmdd.log :EMM Agent 내부의 SecureStorage 로그 • PUSH_DA_yyyy_mm_dd.txt: Push DA 로그 • PUSH_DA_DB_yyyy_mm_dd.txt:Push DA의 DB 상태로그
파일크기	단말 로그 파일의 크기입니다. • 파일 단위는 KB 이고 최소 크기는 0.1KB입니다. 파일의 크기가 1024KB가 넘으면 MB로 표시됩니다.
수집일	단말 로그를 수집한 일시입니다.
마지막 업데이트	단말 로그가 마지막으로 업데이트된 일시입니다.

보고서

운영자는 보고서를 통해 단말 또는 사용자 정보, 단말에 설치된 앱정보, 최신 프로파일 정책을 알수 있고, 이러한 EMM 운영 상황에 따라 필요한 조치를 취할 수 있습니다. EMM 에서 제공하는 보고서 쿼리를 이용하여 보고서를 만들고, 대시보드로 통계 정보를 확인할 수 있습니다.



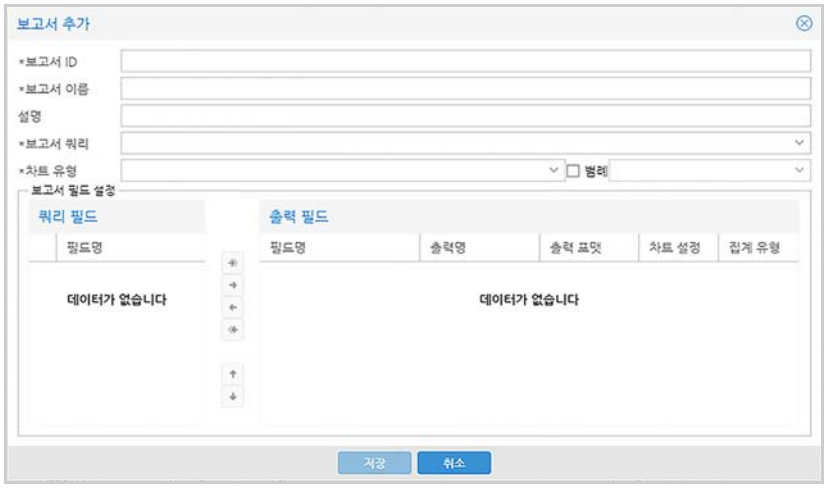
- **보고서 쿼리**: 통계 보고서를 생성하기 위한 SQL 쿼리를 간편하게 만들 수 있도록 제공한 것을 보고서 쿼리라 합니다.
  - 보고서 쿼리를 이용하여 새로운 보고서를 작성하며 자세한 내용은 70페이지의 "보고서 쿼리 목록"을 참고하세요.
- **보고서**: 보고서 쿼리를 이용하여 통계 보고서를 출력하기 위한 구성 요소입니다.
  - EMM에서 제공하는 보고서 목록에 대한 자세한 내용은 72페이지의 "보고서 목록"을 참고하세요.
- **대시 보드**: 여러 보고서를 한 화면에서 포틀릿 형태로 출력하기 위한 구성 요소입니다.
- **집계 테이블**: 보고서의 운영 및 집계 데이터가 저장 되어 있는 저장소입니다.

보고서 만들기

보고서 쿼리를 이용하여 새 보고서를 만들려면 다음의 절차를 따르세요.

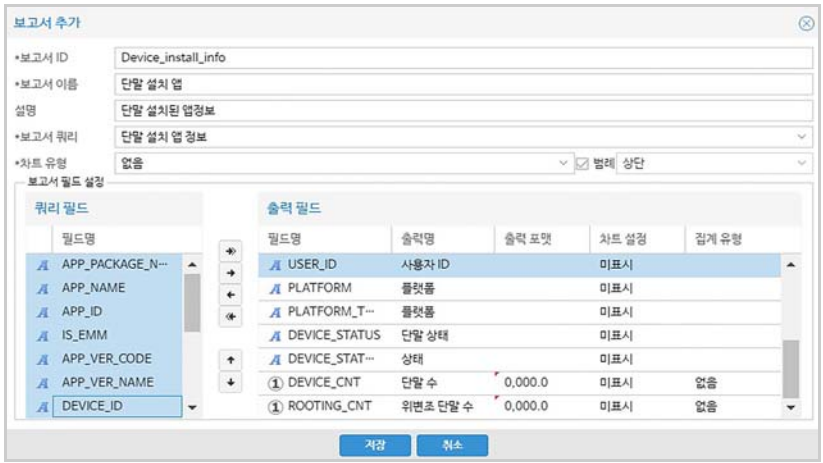
1. **서비스 현황 > 대시보드 & Audit 설정 > 보고서**로 이동하세요.

2. 보고서를 추가하려면 ➕을 클릭하세요.



3. “보고서 추가” 창에 보고서 정보를 입력하세요.

- **보고서 ID**: 보고서를 식별하기 위한 ID입니다.
- **보고서 이름**: 입력한 보고서 이름은 **서비스 현황 > 대시보드 & Audit 설정 > 대시보드 관리**에서 대시보드 추가 시, 보고서 리스트에서 확인됩니다.
- **설명**: 추가하려는 보고서에 대한 설명입니다.
- **보고서 쿼리**: EMM에서 제공하는 보고서 쿼리를 선택합니다. 보고서 쿼리에 대한 자세한 내용은 70페이지의 "보고서 쿼리 목록"을 참고하세요.
- **차트 유형**: 보고서 결과를 조회할 차트 유형을 선택합니다.
  - bar, stacked bar, column, stacked column, line, pie, donut.
- **보고서 필드 설정**: 보고서 쿼리를 선택하면, 해당 쿼리의 필드 목록이 **쿼리 필드** 영역에 나타납니다. 보고서 필드를 설정하려면 다음의 절차를 따르세요.



가. **쿼리 필드**영역에서 보고서에 표시할 필드명을 선택한 후, ➔을 클릭하여 우측 **출력 필드**로 추가하세요. 또는 ➔➔을 클릭하여 전체 필드를 추가하거나, Ctrl 키를 누르고 다중 선택하여 추가하세요.

나. **출력 필드**영역에서 기준 항목이 될 필드를 선택한 후, **차트설정** 목록에서 **카테고리**를 선택하세요.

- 출력 필드 중 반드시 하나의 카테고리가 선택되어야 합니다.

다. 카테고리로 설정한 필드를 기준으로 집계할 필드를 선택한 후, **차트설정** 목록에서 **Series**를 선택하세요. 숫자 타입의 필드만 Series로 지정할 수 있습니다.

라. 필요에 따라 보고서에 표시될 출력명, 출력 포맷, 집계 유형을 설정하세요.

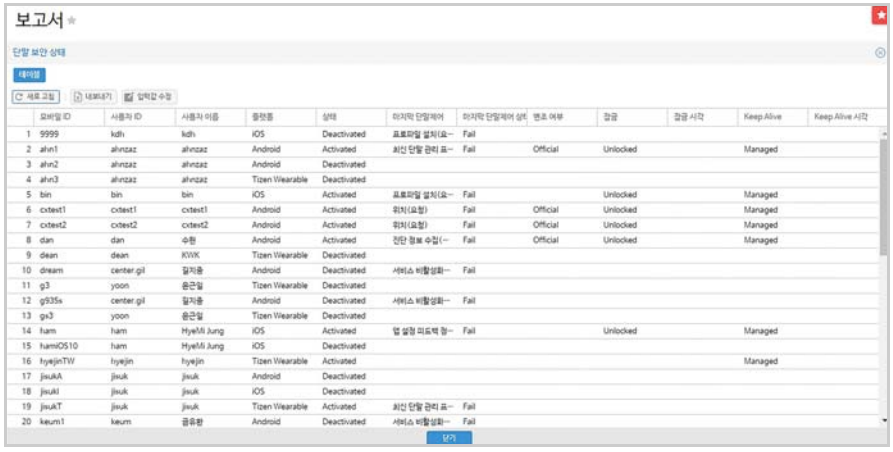
- **출력명**은 기본적으로 보고서 쿼리의 해당 필드 값이나 구분하기 쉬운 이름으로 입력하세요.
- **출력 필드**에 나타난 필드 중 데이터 타입이 숫자 또는 날짜인 경우, **출력 포맷**을 설정할 수 있습니다.
- **출력 필드**에 나타난 필드 중 데이터 타입이 숫자인 경우, **집계 유형**으로 합계, 평균, 최대값, 최소값 중 설정할 수 있습니다.

4. **저장**을 클릭하세요.

보고서 미리보기

보고서 작성 후 , 보고서를 미리보려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 대시보드 & Audit 설정 > 보고서**로 이동하세요.
2. 미리보려는 **보고서 ID**를 선택한 후, 을 클릭하세요.



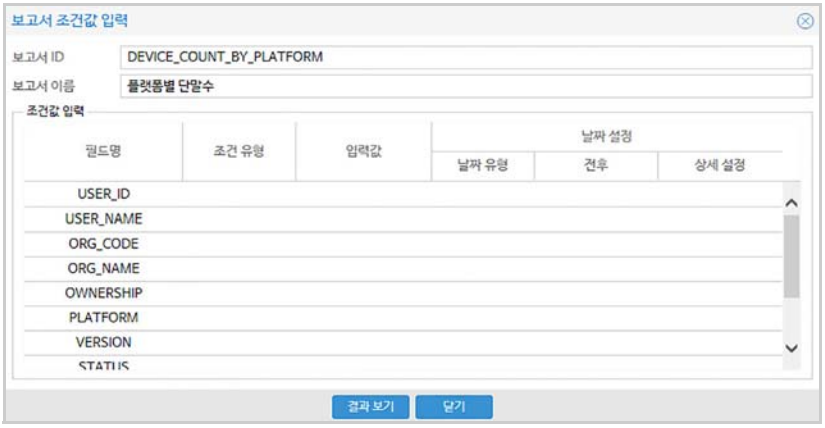
3. **테이블** 탭을 클릭하세요.
   보고서의 결과를 표 형식으로 조회합니다.
   - **내보내기**를 클릭하세요.보고서 결과를 Excel 파일로 저장합니다.
   - **입력값 수정**을 클릭하세요. 보고서 조건값을 입력할 수 있습니다. 자세한 내용은 68페이지의 "보고서 조건값 수정하기"를 참고하세요.
4. **차트**탭을 클릭하세요.
   보고서의 결과를 차트 형식으로 조회합니다.
   - 보고서 결과를 이미지로 저장하려면 **이미지 저장**을 클릭하세요.

보고서 조건값 수정하기

운영자는 다양한 조건에 맞는 보고서를 조회 할 수 있습니다 .

보고서 작성 시 조건값 변경 또는 수정하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 대시보드 & Audit 설정 > 보고서**로 이동하세요.
2. 운영자는 보고서의 날짜, 필드 조건에 따라 조회하거나 조건값을 수정하려면 **보고서 ID**를 선택 한 후, 을 클릭하세요.
3. **테이블** 탭에서 **입력값 수정**을 클릭 후, "보고서 조건값 입력" 창의 **조건값 입력** 영역에 조건을 입력하세요.



- 필드명의 데이터 타입이 문자와 숫자 유형인 경우, **입력값**에 상수만 입력할 수 있습니다.
- 필드명의 데이터 타입이 날짜 유형인 경우, **조건 유형**을 상수 또는 변수로 선택할 수 있습니다.
  - 상수: **조건 유형**을 상수로 선택하면 값을 직접 입력
  - 변수: **조건 유형**을 변수로 선택하면 **날짜 설정**의 날짜 유형, 전후, 상세 설정을 클릭하여 값을 입력
- **날짜 설정**: 조건 유형을 변수로 선택한 경우, 아래 사항 선택이 가능합니다.
  - **날짜 유형**: 날짜 유형으로 현재일, 현재월 선택 가능
  - **전후**: 날짜 유형에 대한 전후 계산 값, 현재월을 선택한 경우 현재월을 기준으로 전후를 계산함
  - **상세 설정**: 날짜 유형에서 현재일, 현재월 선택에 따라 시간 상세 설정이 다름
    - **날짜유형**에서 현재일 선택 시 시각 선택 (00:00~23:00)
    - **날짜유형**에서 현재월 선택 시 일자 선택 (1~말일)
      (예: 현재일이 2017-04-01 인 경우)

날짜 유형	전후	상세설정	계산결과	비고
현재월	-1	1	2017-03-01	전월 1일
현재월	-1	말일	2017-03-31	전월 말일
현재일	-1	00:00	2017-03-31 00:00	전일 00:00
현재일	0	23:00	2017-04-01 23:00	당일 23:00

4. 보고서 조건값 입력 후 **결과 보기**를 클릭한 후, 확인 메시지가 나타나면 **예**를 클릭하세요. 입력한 보고서 조건값은 저장됩니다.

보고서 쿼리 목록

EMM 에서 제공하는 보고서 쿼리 목록은 다음과 같습니다 . 보고서 쿼리에 필요한 입력 조건값 중 아래 항목에 표시값은 기준 정보의 키를 사용하며 , **설정 > 서비스 > 기준정보**에서 확인할 수 있습니다 . 자세한 내용은 41 페이지 2 장의 " 기준정보 설정하기 " 를 참고하세요 .

보고서 쿼리	보고서 설명	입력 조건 값
미처리 단말제어 수	처리 대기 중이거나 네트워크 오류등 미처리된 단말 제어 현황을 실행된 최근 일수,단말별 단말 제어 대기수를 조건으로 보고서를 만들수 있습니다.	• LAST_DAYS • QUEUE_COUNT
사용자별 예외 정책 현황	사용자별 예외 정책 적용에 대해 현재 적용여부(Y,N)를 조건으로 보고서를 만들수 있습니다 .	• PRESENT_VALID_YN (Y/N)
단말 설치 앱 정보	단말에 설치된 앱의 위변조 여부(Y,N)를 조건으로 앱정보 보고서를 만들 수 있습니다.	• IS_ROOTING (Y,N)
그룹별 사용자	그룹 ID, 그룹유형, 멤버 유형 코드에 조건을 걸어 그룹별 사용자에 대한 보고서를 만들 수 있습니다.	• GROUP_ID • GROUP_TYPE (M:Profile,N:General,S:Sync) • TARGET_TYPE (0:User Member, 1:Device Member)
커넥터 요청(집계)	시작 날짜, 만료 날짜, 사용자 ID, 커넥트 서비스 유형 코드, 커넥트 서비스 ID에 조건을 걸어 커넥터 서비스에 대한 보고서를 만들 수 있습니다.	• FROM_DATE • TO_DATE • USER_ID • SERVICE_TYPE (db : DATABASE, sap:SAP ERP, mq:MQ, directory:Directory) • SERVICE_ID
사용자 기본 정보	사용자 ID, 사용자 이름, 활성화 상태, 등록일에 조건을 걸어 사용자 기본 정보에 대한 보고서를 만들 수 있습니다.	• USER_ID • USER_NAME • ENABLED (0:Deactivated, 1:Activated) • REGISTERED_DAY
단말 프로파일 상태	단말 상태, 최신 프로파일 여부에 조건을 걸어 단말 프로파일 상태에 대한 보고서를 만들 수 있습니다.	• DEVICE_STATUS :기준정보의 Device Status 키 • IS_NOT_LATEST (Y/N)

보고서 쿼리	보고서 설명	입력 조건 값
단말 보안 상태	사용자 ID, 플래폼 코드, 단말 상태 코드, 변조 상태, 잠금 상태, Keep Alive 상태에 조건을 걸어 단말 보안 상태에 대한 보고서를 만들 수 있습니다.	• USER_ID • PLATFORM_CODE :기준정보 Platform 키 • DEVICE_STATUS_CODE :기준정보의 Device Status 키 • ROOTING_STATUS (Modified/ Official) • LOCK_STATUS (Locked/Unlocked) • UNMANAGED_STATUS (Managed/Unmanaged)
단말 상세 정보	사용자 ID,사용자이름,플래폼 코드, 단말 상태 코드, 변조 상태에 조건을 걸어 단말 상세 정보에 대한 보고서를 만들 수 있습니다.	• USER_ID • USER_NAME • ORG_NAME • PLATFORM_CODE : 기준정보 Platform 키 • DEVICE_STATUS :기준정보의 Device Status 키
앱 다운로드 (집계)	앱 다운로드 순위에 조건을 걸어 앱 정보에 대한 보고서를 만들 수 있습니다.	• FROM_DATE • TO_DATE
단말 기본 정보	언어, 앱 이름, 플랫폼, 앱 유형 코드, 활성화 여부 , 테스트 앱 여부, 키오스크 앱 여부, 단말 유형, 등록 일수에 조건을 걸어 앱 기본 정보에 대한 보고서를 만들 수 있습니다.	• USER_ID • USER_NAME • ORG_CODE • ORG_NAME • OWNERSHIP :기준정보 Ownership 키 • PLATFORM_CODE : 기준정보 Platform 키 • VERSION • STATUS • MANUFACTURER • MODEL • IS_ROOTING(Y,N)
그룹별 단말	그룹 ID, 그룹유형 코드, 멤버 유형 코드에 조건을 걸어 그룹별 단말 정보에 대한 보고서를 만들 수 있습니다.	• GROUP_ID • GROUP_TYPE (M:Profile,N:General,S:Sync) • TARGET_TYPE (0:User Member, 1:Device Member)
앱 다운로드 순위 (현재)	언어, 앱 다운로드 순위에 조건을 걸어 앱 정보에 대한 보고서를 만들 수 있습니다.	• LANG • RANK

보고서 쿼리	보고서 설명	입력 조건 값
앱 다운로드 순위 (집계)	언어, 앱 다운로드 순위에 조건을 걸어 앱 정보에 대한 보고서를 만들 수 있습니다.	• RANK
앱 기본 정보	언어, 앱 이름, 플랫폼, 앱 유형 코드, 활성화 여부 , 테스트 앱 여부, 키오스크 앱 여부, 단말 유형, 등록 일수에 조건을 걸어 앱 기본 정보에 대한 보고서를 만들 수 있습니다.	• LANG(ko, en, zh) • APP_NAME • APP_PLATFROM : 기준정보 Platform 키 • APP_TYPE (IA : Internal App,PA: Public App) • IS_ACTIVATED • IS_TEST (Y,N) • IS_KIOSK (Y,N) • DEVICE_TYPE (A: all device ,P: Phone-only, T:Tablet-only) • ENROLL_DAYS

보고서 목록

EMM 에서 제공하는 보고서 목록은 다음과 같습니다 .

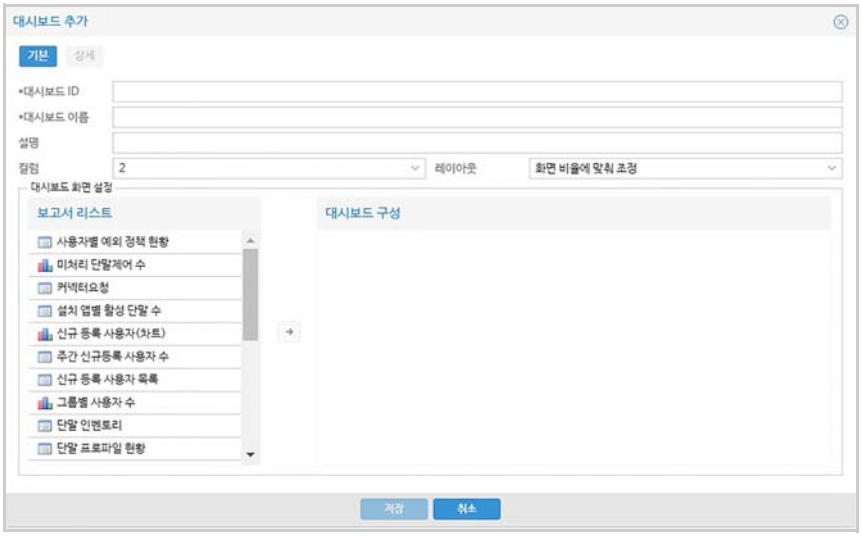
보고서 이름	비고	설명
신규 등록 사용자 목록		최근 7일간 신규 등록된 사용자ID,사용자 이름, 조직, 회사 직급등의 정보
주간 신규등록 사용자수		최근 7일간 신규 등록된 사용자ID,사용자 이름, 조직 및 상태 정보
신규 등록 사용자(차트)		최근 7일간 신규 등록된 사용자 집계에 대한 날짜별 차트 정보
사용자별 예외 정책 현황		사용자별 예외 정책 현황
그룹별 사용자 수		그룹ID, 그룹유형 멤버유형에 따라 집계된 사용자 수 정보
단말 보안 상태		모바일ID에 따라 단말상태, 변조 여부, KeepAlive사용여부 정보 및 마지막 단말 제어 정책명 조회
단말 SIM/ROAMING 현황		모바일ID에 따라 단말 상세정보와 단말 SIM 상태 및 로밍 사용 여부 조회
단말 프로파일 현황		모바일ID에 따라 할당된 MDM 최종 프로파일정보,할당된 EMM 앱관리 최종 프로파일 정보 및 각 프로파일의 최근 변경일자 정보
단말 인벤토리		조직,플랫폼,제조사,모델에 따라 집계된 단말 수 정보
단말 설치 앱		사용자에 따라 단말에 설치된 앱, 변조된 앱, 정상 설치된 앱에 대해 집계된 단말 수 정보
버전별 단말수		단말 플랫폼 및 버전에 따라 집계된 단말 수 정보
단말 상태별 단말수	집계	단말 상태에 따라 집계된 단말 수 정보

보고서 이름	비고	설명
플랫폼별 단말수	집계	단말 플랫폼에 따라 집계된 단말 수 정보
제조사별 단말수		제조사별 집계된 단말 수 정보
설치앱별 활성 단말 수	집계	앱, 플랫폼에 따라 설치된 앱별 단말수
그룹별 단말수	집계	그룹ID, 그룹유형, 멤버유형에 따라 집계된 단말 수 정보
커넥터 요청		일정 기간동안 커넥터 서비스 요청 결과
미처리 단말제어 수	집계	단말로 전송 대기 중인 미처리 단말제어 수를 단말별로 누적하여 미처리 수가 많은 순서로 보여줌
신규 등록 앱		최근 7일간 신규 등록된 앱 정보
앱 다운로드 순위(현재)		
앱 다운로드 순위(집계)		
앱 다운로드 Top 3(현재)		
앱 다운로드 Top 3(집계)		

보고서를 이용한 대시보드 만들기

운영자는 제공된 보고서나 **서비스 현황 > 대시보드 & Audit 설정 > 보고서**에서 작성된 보고서를 이용하여 대시보드를 구성할 수 있습니다 . 운영자는 제공된 보고서를 이용하여 대시보드를 만들 수 있고 , 수퍼 운영자만 새로 만든 보고서를 이용할수 있습니다 .

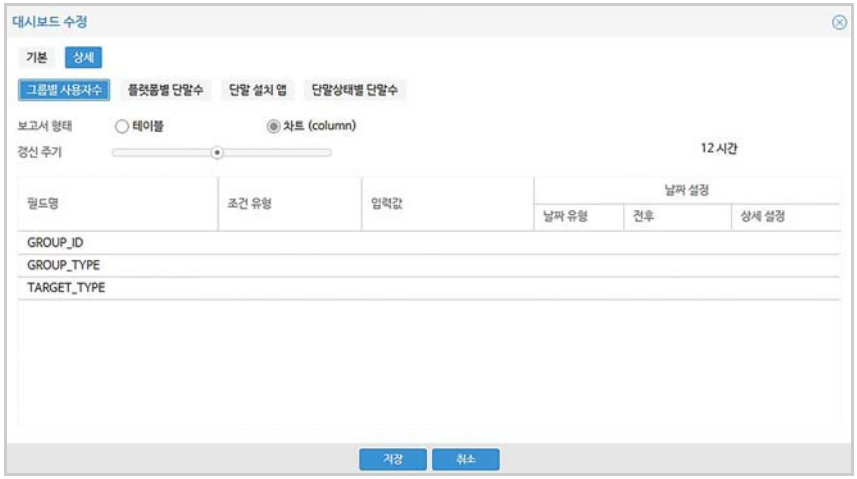
1. **서비스 현황 > 대시보드 & Audit 설정 > 대시보드 관리**로 이동하세요.
2. 대시보드를 추가하려면 ➕을 클릭하세요.



3. **"대시보드 추가"** 창의 **기본** 탭에 대시보드 정보를 입력하세요.
   - **대시보드 ID**: 대시보드를 식별하기 위한 ID를 입력합니다.

- **대시보드 이름**: **서비스 현황 > 대시보드** 또는 **서비스 현황 > 대시보드 & Audit 설정 > 대시보드 관리**에서 표시될 대시보드 이름을 **설명**과 함께 입력합니다.
- **컬럼**: 대시보드에 가로로 추가할 보고서 포틀릿의 최대 값으로 1~3 중 선택합니다.
- **레이아웃**: 보고서 포틀릿의 높이입니다.
  - 화면 비율에 맞춰 조정: 현재 브라우저 크기에 맞게 조회되어 스크롤바가 생기지 않음
  - 고정된 높이 유지: 현재 브라우저 크기에 맞게 포틀릿 높이가 조정되며 스크롤바가 생성됨

4. **대시보드 화면 설정**영역에서 대시보드에 포함시키려는 보고서를 선택한 후, **Ctrl** 키를 누르고 보고서를 다중 선택한 후 → 을 클릭하세요.
   대시보드 영역의 보고서 포틀릿은 끌어다 놓기로 위치를 조정할 수 있습니다.
   - **보고서 리스트**: 대시보드에 추가할 수 있는 보고서 목록입니다.
   - **대시보드 구성**: 대시보드에 추가된 보고서 포틀릿이 표시됩니다.
5. **상세** 탭을 클릭하여 선택한 보고서들의 상세 정보를 입력하세요.
   - **기본** 탭의 **대시보드 화면 설정**영역에 보고서가 1개 이상 추가된 경우, **상세** 탭이 활성화됩니다.
   - **상세** 탭에서 등록된 각 보고서를 탭 형식으로 조회할 수 있으며, 각 보고서의 형태나 갱신 주기를 설정할 수 있습니다. 입력된 보고서별, 사용자별 조건 값을 확인할 수 있습니다.



6. **저장**을 클릭하세요.

Note:
- 운영자는 대시보드를 삭제, 수정, 복사, 미리보기 할 수 있습니다.
- EMM에서 제공하는 기본 대시보드는 삭제가 불가능하고, 해당 대시보드의 삭제할 경우 삭제 불가 확인 메시지가 나타납니다.

대시보드 메인으로 설정하기

운영자가 보고서를 이용하여 만든 대시보드 중 선택하여 메인으로 설정할 수 있습니다 .

설정된 대시보드를 해제하면 기본 대시보드가 메인 대시보드로 나타납니다 .

대시보드를 메인으로 설정하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 대시보드 & Audit 설정 > 대시보드 관리**로 이동하세요.
2. 우측 상단 검색란에 **대시보드 ID** 또는 **대시보드 이름**을 입력한 후 **Enter** 키를 누르거나 을 클릭하세요.
3. 선택한 대시보드를 메인으로 설정하려면 대시보드 이름의 좌측에 위치한 을 클릭하세요.
4. **서비스 현황 > 대시보드**로 이동 시 설정한 대시보드가 메인으로 나타납니다.

4 조직

관리자 포털에서 계층적으로 구성된 조직 및 해당 조직에 소속된 사용자와 단말을 확인할 수 있습니다 . 조직에는 운영자를 한 명 이상 지정할 수 있습니다 . 조직 운영자로 지정된 운영자가 관리 화면에 로그인하면 관련 기능만 보여집니다 . 또한 조직 정보를 활용하여 그룹을 구성할 수도 있습니다 . 운영자는 **설정 > Admin Console > 운영자**에서 관리합니다 . EMM 의 조직은 단말 정책 및 설정을 적용하거나 애플리케이션 권한을 관리하는 단위입니다 . 조직 등록은 AD/LDAP 동기화 서비스를 이용하여 일괄로 하거나 운영자가 직접 조직을 계층화하여 구성할 수 있습니다 .

단말 & 사용자 > 사용자 & 조직의 조직도에서 조직을 클릭한 후 에서 최신 프로파일 배포 , 조직 정보 조회 , 수정 , 삭제를 선택할 수 있습니다 . **단말 & 사용자 > 단말 / 사용자 & 조직**의 목록에서는 컬럼의 항목 위치를 이동하거나 컬럼 정렬 순서를 변경하면 최종 상태로 자동 저장되고 , 을 클릭하면 초기 상태로 되돌릴 수 있습니다 .

그룹 또는 조직 정보 변경 시 팝업창에서 소속된 모든 사용자의 단말에 프로파일을 배포할 수 있습니다 . 사용자 계정의 조직을 변경하는 경우에도 해당 사용자 단말에 바로 프로파일을 배포할 수 있습니다 .

하위 조직이 있는 상위 조직을 삭제하는 경우 , 하위 조직은 삭제 후의 상위조직으로 이동됩니다 . 조직 등록 시 단말에 적용할 단말관리 프로파일 , 앱 관리 프로파일 및 운영자를 설정할 수 있습니다 .

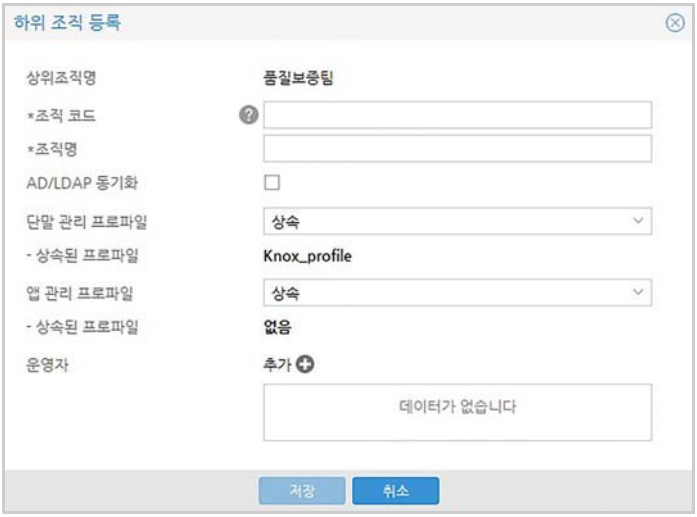
조직 등록하기

조직 계층도의 원하는 위치에 새로운 조직을 추가할 수 있습니다 .

조직을 추가하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직도에서 추가될 조직 계층의 상위 조직을 클릭하세요.

3. 조직 우측의 ⋯을 클릭한 후 **하위 조직 등록**을 클릭하세요.



4. 필수 항목 및 추가 정보를 입력하세요.
   - **조직 코드**: 조직 코드 체계에 따른 신규 코드를 입력하세요.
   - **조직명**: 조직 체계에 따른 신규 조직명을 입력하세요.
   - **AD/LDAP 동기화**: AD/LDAP 동기화 여부를 체크하세요.
   - **단말 관리 프로파일**: 조직에 적용할 단말 관리 프로파일을 선택하세요.
     - **상속된 프로파일**: 상속으로 선택한 단말관리 프로파일의 상속된 프로파일이 자동으로 보여집니다. 해당 프로파일이 없는 경우는 없음으로 표시됩니다.
   - **앱 관리 프로파일**: 조직에 적용할 앱 관리 프로파일을 목록에서 선택하세요.
     - **상속된 프로파일**: 상속으로 선택한 앱관리 프로파일의 상속된 프로파일이 자동으로 보여집니다. 해당 프로파일이 없는 경우는 없음으로 표시됩니다.
   - **운영자**: 추가를 클릭한 뒤 "운영자 선택" 창에서 조직 관리 운영자를 선택한 후 **확인**을 클릭하세요.
5. **저장**을 클릭하세요.

조직원 이동하기

사용자를 다른 조직으로 이동 시 팝업 창에서 사용자 단말에 최종 프로파일을 배포할 수 있습니다 .

조직도 화면에서 구성원을 원하는 조직에 끌어다 놓거나 , 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직도에서 이동할 사용자가 속한 조직을 클릭하세요.

3. 이동할 구성원을 선택한 후 ➠을 클릭하세요.

4. "조직 선택" 창에서 이동하려는 조직을 선택한 후 **확인**을 클릭하세요.
5. "프로파일 배포" 창에서 **확인**을 클릭하세요.
   - 이동된 사용자의 단말에 프로파일이 배포됩니다.

조직원 삭제하기

삭제된 사용자는 조직도 상의 미소속으로 이동됩니다 .

조직내의 사용자를 삭제하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직도에서 삭제할 사용자가 속한 조직을 클릭하세요.
3. 삭제할 사용자의 🗑을 클릭하세요.
   여러 사용자를 삭제하려면 상단의 🗑을 클릭하세요.
4. 삭제 확인 팝업 메시지가 나타나면 **예**를 클릭하세요.

조직에 프로파일 배포하기

조직도 상에서 원하는 조직에 최신 프로파일을 배포할 수 있습니다 .

조직에 프로파일을 배포하려면 다음의 절차를 따르세요 .

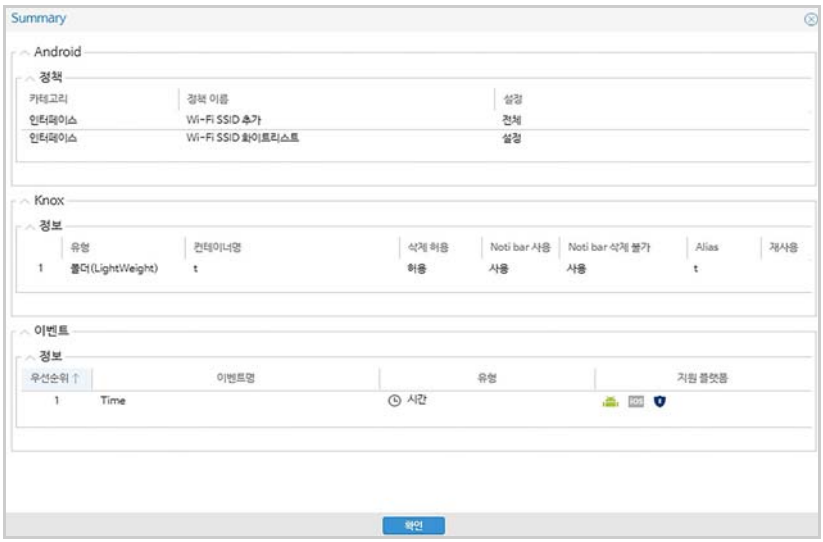
1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직 우측의 ⋯을 클릭한 후 **최신 프로파일 배포**를 선택하세요.

- 조직의 모든 사용자의 단말에 최신 프로파일이 적용됩니다.

3. 완료 팝업창에서 **확인**을 클릭하세요.

조직에 적용된 프로파일 보기

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직 우측의 ⋯을 클릭한 후 **보기**를 선택하세요.
3. "조직 조회" 창에서 **단말 관리 프로파일** 또는 **앱 관리 프로파일**을 클릭하세요.
   - 단말 관리 프로파일



   - 앱 관리 프로파일

     - 조직에 적용된 앱관리 프로파일을 최종 상태로 할당하려면 **프로파일 할당**을 클릭하세요,

5 사용자 및 운영자 계정

EMM 사용자에는 운영자의 등록 방법에 따라 직접등록 사용자와 동기화 사용자가 있습니다 . 사용자 개별 등록은 운영자가 사용자 정보를 직접 등록하거나 동기화 서비스를 통해 개별 사용자 정보를 가져옵니다 . 다수의 사용자 등록은 파일 업로드 또는 동기화 서비스를 이용합니다 .

사용자의 단말 정보 및 단말 상태를 관리하고 , 단말 제어 명령을 전송하여 단말 기능을 제어합니다 . EMM 라이선스 한도 내에서 단말에 mMail 과 SecuCamera 사용 권한을 부여할 수 있습니다 . 부여 방법은 TMS (Tenant Management System) 에서 라이선스 정보의 mMail 기능 사용 여부와 사용자 수를 등록합니다 . EMM 에 등록된 사용자 메일 주소로 단말 활성화에 필요한 QR 코드 및 초기화 비밀번호 등을 발송할 수 있습니다 .

운영자는 EMM 사용자를 개별 또는 일괄로 등록할 수 있습니다 .

- 개별 등록: 직접 등록, 동기화 서비스를 통한 등록
- 일괄 등록: 파일 업로드 등록, 동기화 서비스를 통한 등록

AD/LDAP 동기화 사용자의 경우 , 대상 시스템 정보를 가져와 자동으로 등록합니다 .

사용자 계정 정보

EMM 에서는 사용자 계정과 관련하여 다음의 항목들을 관리합니다 .

- 등록 경로: 사용자 등록 방법으로 직접 등록과 동기화 등록이 있음
- 사용자 ID, 이름: 사용자의 단말 EMM 로그인 ID, 사용자 성명
- AD/LDAP 동기화: 동기화 서비스를 통한 사용자 여부
- 로그인시 비밀번호 재설정: 사용자 로그인 시 초기 비밀번호를 사용하는 경우, 패스워드를 재설정할 지 여부
- mMail: mMail 기능 사용 여부
- SecuCamera: 보안 카메라 기능 사용 여부로서, 라이선스에 SecuCamera 사용자 수가 먼저 등록되어 있어야 기능을 부여할 수 있음
- 사원번호: 조직 내 사원 번호가 있는 경우만 해당
- 조직: EMM의 조직도 상의 조직 정보
- 직급: EMM 사용 조직 내의 직급
- 이메일, 연락처: 조직 내에서 주로 사용하는 메일 주소와 전화번호
- 사이트: 사용자가 EMM을 적용받는 장소

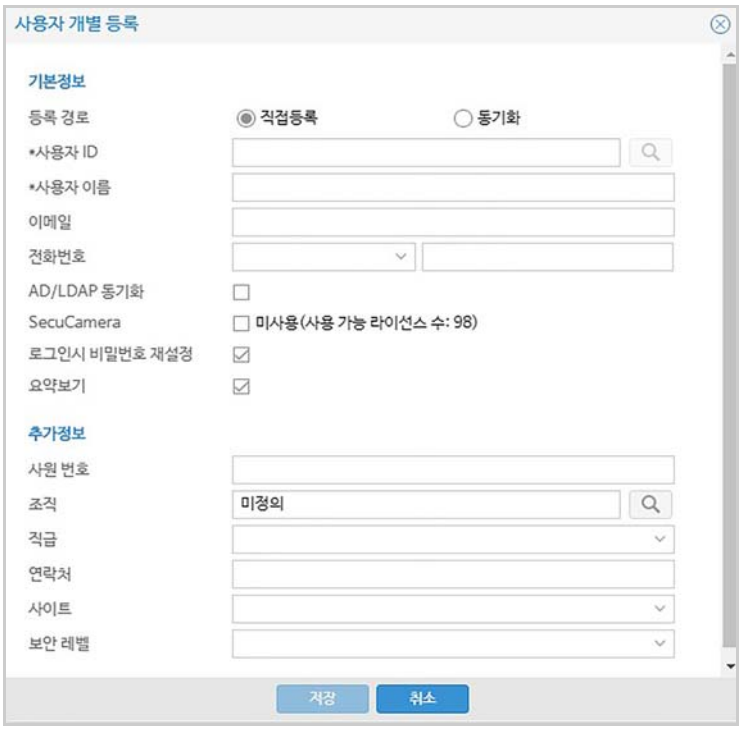
- 보안 레벨: 사용자의 보안 등급으로서 Level1 ~ Level5까지 있음
- UPN: Windows 도메인에 로그인 시 사용되는 사용자 로그인 이름인 user principal name. 사용자 로그인 이름 + UPN 접미사 형태로 입력하며, 접미사 형태는 "@domain_name"입니다.
  예: 사용자 이름이 EMMuser1인 경우, EMMuser1@mydomain.com
- DN: LDAP 개체의 고유 이름으로 동기화 사용자 설정 시 자동 입력됨
- 태그: 그룹, 조직 등으로 분류되지 못하는 기타 속성을 운영자가 텍스트로 입력
- 서비스 역할: EMM 커넥터 서비스 사용을 위한 역할 설정. **설정 > 커넥터 > 역할 관리**에서 등록한 역할 중에서 선택함
- 기타 정보: 이름, 중간이름, 표시이름, 부서, 관리자 이름, 이메일 사용자 이름, 연락처 정보

사용자 계정 개별 등록하기

사용자 개별 등록 시 사용자 비밀번호는 임시 비밀번호로 자동 부여됩니다 . 사용자 계정 등록 후 비밀번호를 변경할 수 있습니다 . 비밀번호 변경과 관련한 자세한 내용은 87 페이지의 " 사용자 비밀번호 변경하기 " 를 참고하세요 .

사용자 계정을 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. ➕을 클릭한 후 **개별 등록**을 클릭하세요.



3. “사용자 개별 등록” 창에서 사용자 정보를 등록하세요.

- **로그인시 비밀번호 재설정**: 사용자 계정의 초기 비밀번호는 ID와 동일하게 부여됩니다. **로그인시 비밀번호 재설정**을 체크하면 사용자가 단말에서 EMM 로그인 시 비밀번호 변경창에서 새로운 비밀번호로 변경합니다.

4. **저장**을 클릭하세요.
5. 사용자의 단말을 등록하려면 확인 팝업창에서 **예**를 클릭하세요.
6. "등록 단말"창에서 ＋을 클릭하세요.
7. "개별 등록"창에 단말 정보를 입력한 후 **저장**을 클릭하세요.
8. "등록 단말"창에서 **확인**을 클릭하세요.

사용자 계정 정보 수정하기

사용자 계정 정보를 변경하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직도에서 사용자가 속한 조직을 클릭하세요. 또는 검색 항목을 입력한 후 을 클릭하세요.
3. 수정하려는 사용자의 을 클릭하세요.
4. "사용자 수정" 창에서 정보를 변경한 후 **저장**을 클릭하세요.
   - **조직**이 변경된 경우 "프로파일 배포" 팝업창이 나타나며, 사용자 단말에 새로운 조직의 프로파일을 배포하려면 **예**를 클릭하세요.

사용자 계정 파일 올리기

사용자 계정 정보를 엑셀 파일로 작성하여 일괄로 등록할 수 있습니다 . 이미 등록된 사용자는 업데이트 됩니다 .

EMM 이 제송하는 엑셀 파일의 양식은 다음과 같습니다 .

- User ID, Password: 단말 EMM “사용자 단말 로그인” 창의 사용자 ID, 비밀번호로 사용됩니다.
  - 비밀번호를 입력하지 않는 경우, 초기 비밀번호는 ID와 동일하게 부여되며, **로그인시 비밀번호 재설정** 항목은 on으로 설정됩니다. 비밀번호를 입력한 경우에는 재설정하지 않습니다.
- AD/LDAP sync: AD/LDAP을 통하여 동기화 할 경우 0, 하지 않을 경우 1을 입력하세요.
- Org Code: 해당 코드로 사용자를 조직과 매핑합니다.
- User name, Emp No, Email, Contact, Position Code: 사용자 이름, 사원번호, 이메일 주소, 직급코드
- Site Code: EMM을 사용하는 장소
- Security Level Code: 사용자의 보안 등급
- Country Code: ISO 3166-1 alpha-2 체계의 국가코드
- Mobile Phone: SMS 메시지를 전송하기 위한 - 생략된 전화번호

사용자 계정을 엑셀 파일로 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. ➕을 클릭하여 옵션 활성화 후 **일괄 등록**을 클릭하세요.
3. “사용자 일괄 등록” 창에서 **일괄 양식 다운로드**를 클릭하세요.
4. 다운로드한 엑셀 파일 템플릿 파일에 정보를 입력한 후 저장하세요
5. **Browse**를 클릭한 다음 엑셀 파일을 선택한 후 업로드하세요.
6. **확인**을 클릭하세요.

동기화 사용자 개별 등록하기

단말 & 사용자 > AD/LDAP 동기화 > 동기화 서비스에 등록된 동기화 서비스를 통해 LDAP 시스템에서 개별 사용자 계정 정보를 등록할 수 있습니다 . 등록 방법은 동기화 서비스를 선택하고 필터와 키워드를 이용해 사용자를 검색하여 등록합니다 .

동기화 개별 사용자를 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.

2. ➕을 클릭한 후, **개별 등록**을 클릭하세요.
3. "사용자 개별 등록" 창의 **등록 경로**에서 **동기화**를 선택하세요.

4. "동기화 사용자 등록" 창에서 **동기화 서비스**, **필터**, **키워드 검색**을 입력하세요.
   - **동기화 서비스**: 사용자 검색을 원하는 동기화 서비스를 선택하세요.
     - **단말&사용자 > AD/LDAP 동기화 > 동기화 서비스**에 등록된 동기화 서비스 목록이 보여집니다.
   - **필터:** 동기화 서비스 선택 시 해당 필터가 입력됩니다.
   - **키워드 검색**: 해당 필터 내에서 사용자를 검색하기 위한 키워드를 입력한 후 🔍을 클릭하세요.
5. **확인**을 클릭하세요.
6. 팝업 메시지 창에서 **예**를 클릭하세요.

동기화 사용자 일괄 등록하기

동기화 서비스를 통해 LDAP 시스템에서 가져온 사용자를 일괄 등록할 수 있습니다 . 이미 등록되어 있는 동기화 서비스를 선택하고 필터와 키워드로 해당 사용자를 검색하여 등록합니다 . 동기화 서비스는 **단말 & 사용자 > AD/LDAP 동기화 > 동기화 서비스** 에서 등록합니다 .

동기화 사용자를 일괄 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. ➕을 클릭한 후, **동기화 일괄 등록**을 클릭하세요.

3. "동기화 일괄 등록" 창에서 동기화 서비스, 필터, 키워드 검색을 입력하세요.
4. LDAP 사용자 중 등록할 사용자를 선택한 후 **업데이트**를 클릭하세요.
5. **선택된 사용자** 목록에서 선택한 후 **확인**을 클릭하세요.
   - 선택한 LDAP사용자를 취소하려면 을 클릭하세요..
6. 확인 메시지 팝업에서 **예**를 클릭하세요.

사용자 계정 관리하기

운영자는 사용자의 단말 정보 , 비밀번호 , 권한 등의 정보를 관리합니다 . 사용자의 상태를 활성화 또는 비활성화 할 수 있습니다. 단말 플랫폼별로 단말 제어 명령을 전송하여 단말 기능을 제어합니다 .

EMM 라이선스에 설정된 사용자 수에 따라 다음의 기능을 사용자 계정에 부여할 수 있습니다 .

- mMail 사용: 사용자는 활성화된 단말에서 mMail을 통해 메일 송수신을 할 수 있습니다.
- SecuCamera 사용: 사용자는 EMM 적용 중에도 카메라 사용이 가능하며, 사진 파일은 보안을 위해 서버로 전송됩니다.

운영자는 단말 사용자에게 일괄 또는 개별적으로 메일을 발송할 수 있습니다 . 메일 템플릿을 등록한 뒤 메일 발송 시 선택합니다 . 메일 발송은 사용자 정보에 등록되어 있는 메일 주소로만 가능합니다 .

사용자 계정 활성화/비활성화하기

사용자 라이선스 수 만큼의 사용자 계정을 활성화할 수 있습니다 . 사용자 계정 추가 시 기본 상태는 활성화 상태입니다 . 만약 잔여 라이선스가 없다면 비활성화 상태로 추가됩니다 .

사용자 계정을 활성화 또는 비활성화하려면 다음의 절차를 따르세요 .

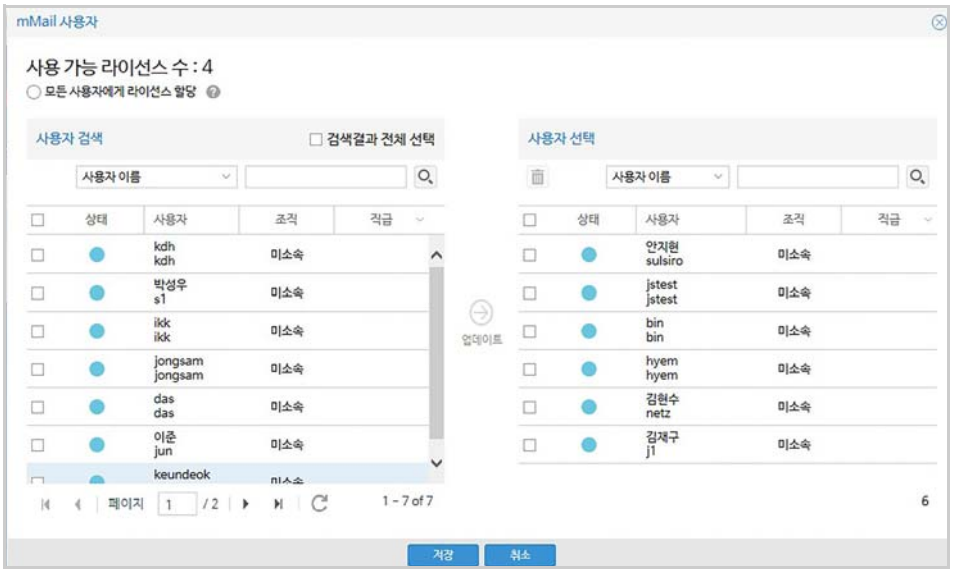
1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. **조직도**나 **키워드** 검색 기능을 이용하여 사용자를 검색하세요.
3. 사용자 목록에서 활성화또는 비활성화할 사용자를 선택하세요.
4. 비활성화 상태의 단말을 활성화하려면 을 클릭하세요.
   활성화 상태의 단말을 비활성화하려면 을 클릭하세요.
5. 상태 변경 확인 팝업 메시지가 나타나면 **확인**을 클릭하세요.

사용자에 mMail 기능 부여하기

활성화 상태의 사용자에게 mMail 사용 권한을 설정 또는 해제할 수 있습니다. 라이선스 정보에 mMail 사용자 수가 남아 있는 경우에 부여할 수 있습니다 .

사용자의 mMail 사용 기능을 관리하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 상단의 을 클릭하세요.



   - **모든 사용자에게 라이선스 할당**: 클릭 시, 해당 조직의 활성 상태인 사용자 수가 보여집니다. 라이선스 수가 부족하면 알림 메시지가 뜨고 더 이상 할당할 수 없습니다.
3. 사용자 검색 및 선택 후 **업데이트**를 클릭하세요.
   mMail 사용 기능을 취소하려면 사용자를 선택한 후 을 클릭하세요.
4. **저장**을 클릭하세요.

사용자 계정에 SecuCamera 기능 부여하기

활성화 상태의 사용자에게 SecuCamera 사용 기능을 설정 또는 해제할 수 있습니다 . 라이선스 정보에 SecuCamera 사용자 수가 남아있는 경우에 기능을 부여할 수 있습니다 .

사용자가 SecuCamera 를 사용할 수 있도록 하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 상단의 을 클릭하세요.
3. 사용자를 선택한 후, **업데이트**를 클릭하세요.
   SecuCamera 사용 기능을 취소하려면 사용자를 선택한 후, 을 클릭하세요.
4. **저장**을 클릭하세요.

사용자 비밀번호 변경하기

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직도나 키워드 검색 기능을 이용하여 사용자를 검색하세요.
3. 변경하려는 사용자의 🔑을 클릭한 후, **비밀번호 변경**을 클릭하세요.
4. "비밀번호 변경" 창에서 **새로운 비밀번호**, **비밀번호 확인**을 입력한 후 **확인**을 클릭하세요.

사용자 비밀번호 초기화하기

사용자 비밀번호를 초기화하면 사용자의 메일 주소로 임시 비밀번호가 전송됩니다 . 비밀번호 초기화 메일에 사용되는 템플릿은 **설정 > 서비스 > 메시지 템플릿**에서 확인 가능합니다 .

사용자 비밀번호를 초기화하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직도나 키워드 검색 기능을 이용하여 사용자를 검색하세요.
3. 변경하려는 사용자의 🔑을 클릭한 후, **비밀번호 초기화**를 클릭하세요.

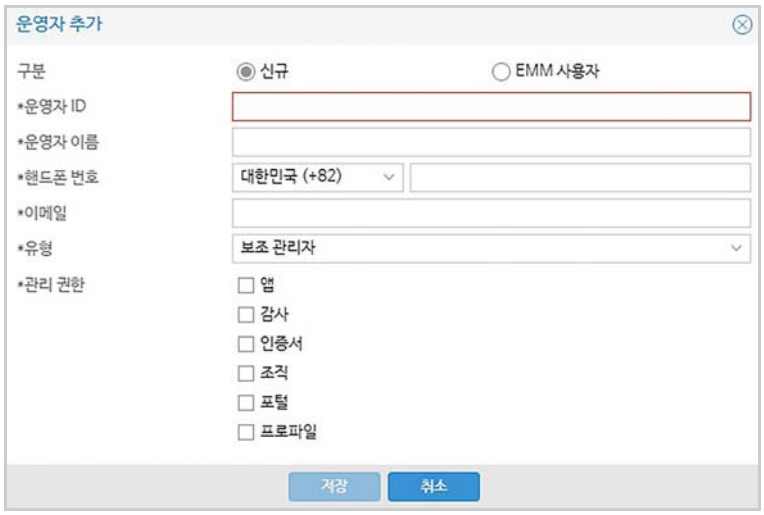
4. 템플릿을 선택한 후, 상세 정보를 보려면 🔍을 클릭하세요.
5. **확인**을 클릭하세요.

운영자 계정 등록하기

EMM 의 운영자는 수퍼 운영자 , 보조 운영자 , 읽기 전용 운영자 , 그리고 방문자 운영자로 구분합니다 . 수퍼 운영자는 보조 운영자를 추가 , 수정 , 삭제 , 활성화 및 비활성화 시킬 수 있습니다 . 또한 운영자가 관리하는 조직을 설정하고 수행 역할에 따라 앱 , 인증서 , 조직 , 포털 , 프로파일 , 방문자 권한을 지정할 수 있습니다 . 보조 운영자는 수퍼 운영자가 할당한 권한에 대해서만 EMM 관리와 조직 관리가 가능합니다 . 읽기 전용 운영자는 모든 메뉴에 대해 조회만 가능합니다 . 방문자 관리 운영자는 방문자의 등록된 단말 , 프로파일 정책을 조회만 할 수 있으며 , 방문자 단말 제어 , 프로파일 적용 및 변경 등은 수퍼 운영자가 실행해야 합니다 .

운영자 계정을 등록하려면 다음의 절차를 따르세요 .

1. **설정** > **Admin Console** > **운영자**로 이동하세요.
2. 운영자를 추가하려면 ⊞을 클릭하세요.



3. "운영자 추가" 창에 운영자 정보, 운영자 유형 및 관리 권한을 입력하세요.
   - **방문자**: 방문자로 등록된 단말 정보와 프로파일에 대해 조회만 가능한 권한입니다.
4. **저장**을 클릭하세요.

보조 운영자의 비밀번호 변경하기

운영자의 초기 비밀번호는 수퍼 운영자가 설정합니다 . EMM 관리자 포털에 처음 로그인시 초기 비밀번호를 문의하세요 . 로그인 후에는 비밀번호 변경이 가능하며 , 비밀번호는 8~30 자로서 숫자와 특수 문자가 하나 이상 반드시 포함되어야 합니다 .

수퍼 운영자의 비밀번호 변경하기

수퍼 운영자는 본인과 보조 운영자의 비밀번호를 변경할 수 있습니다 .

수퍼 및 보조 운영자의 비밀번호를 변경하려면 다음의 절차를 따르세요 .

1. **설정** > **Admin Console** > **운영자**로 이동하세요.
2. 비밀번호를 변경하려는 **운영자**를 선택한 후, 🔑을 클릭하세요.
3. "비밀번호 변경" 창에 **새로운 비밀번호**를 입력하세요.
4. **저장**을 클릭하세요.

보조 운영자의 관리 조직 설정하기

보조 운영자는 조직 관리 권한이 있는 경우 , 관리하고자 하는 조직을 설정할 수 있습니다 . 수퍼 운영자는 모든 조직을 관리할 수 있습니다. 보조 운영자는 전체 조직 중 설정한 조직 및 그 하위 조직에 대한 관리가 가능하며 관리 조직을 변경할 수도 있습니다 .

보조 운영자가 관리하려는 조직을 설정하거나 삭제하려면 다음의 절차를 따르세요 .

1. **설정 > Admin Console > 운영자**로 이동하세요.
2. **운영자**를 선택한 후, 조직 선택을 위해 을 클릭하세요.
3. "조직 선택" 창에서 좌측의 검색란에 **조직명**을 입력한 후, **Enter** 키를 누르거나 을 클릭하세요.
4. **전체 조직** 영역에서 관리하려는 조직을 선택한 후, 을 클릭하세요.
   - 선택한 조직이 선택된 조직 영역으로 이동됩니다.
   - 조직을 삭제하려면 선택된 조직 영역의 조직명을 선택한 후, 을 클릭하세요.
5. **저장**을 클릭하세요.

운영자 계정을 활성화 또는 비활성화하기

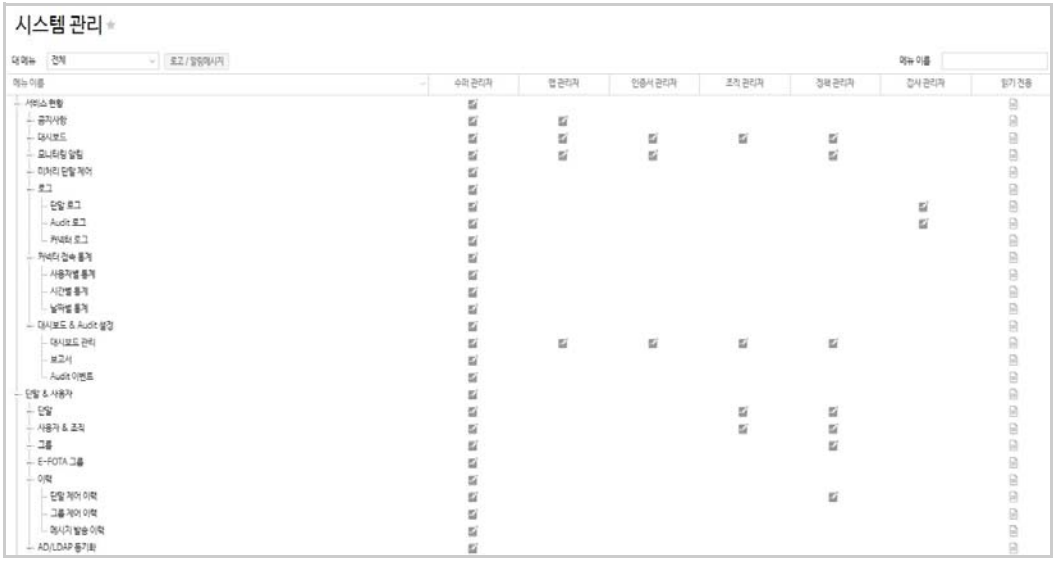
운영자가 일정 기간 동안 관리자 포털에 로그인 하지 않으면 운영자의 상태는 비활성화 상태로 변경됩니다 . 수퍼 운영자는 비활성화 된 운영자의 계정을 활성화시킬 수 있습니다 . 비활성화 된 운영자는 관리자 포털에 로그인이 불가능하며 , 로그인 시 " 계정이 잠겨있습니다 ." 라는 메시지가 표시됩니다 .

운영자 계정을 활성화 또는 비활성화하려면 다음의 절차를 따르세요 .

1. **설정 > Admin Console > 운영자**로 이동하세요.
2. 운영자를 활성화하려면 **운영자**를 선택한 후, 을 클릭하세요.
   운영자를 비활성화하려면 **운영자**를 선택한 후, 을 클릭하세요.
3. 상태 변경 확인 메시기자 나타나면 **예**를 클릭하세요.

운영자 권한에 따른 콘솔 메뉴 확인하기

수퍼 운영자는 관리자 포털의 모든 메뉴를, 일반 운영자는 수퍼 운영자가 부여한 권한에 따른 메뉴를 관리할 수 있습니다. 읽기 전용 운영자는 모든 메뉴에 대해 읽기 권한만 있으므로 등록, 수정, 삭제 등의 관리는 불가능합니다.



운영자 권한에 따라 사용 가능한 관리자 포털 메뉴를 확인하려면 다음의 절차를 따르세요.

1. **설정 > Admin Console > 시스템 관리**로 이동하세요.
2. 시스템 관리에서 **대 메뉴**를 선택하세요.
3. 화면 우측 상단 "메뉴 이름" 창에 **메뉴 이름**을 입력한 후, **Enter** 키를 누르거나 을 클릭하세요.

6 AD/LDAP 동기화

EMM 의 동기화 서비스에서는 회사 내 AD/LADP 시스템과의 연계를 통해 사용자 , 그룹 및 조직 정보를 EMM 에 등록하고 , 특정 주기로 기간계 시스템의 갱신된 정보를 자동 동기화시키는 기능을 제공합니다 .

AD/ LDAP 동기화는 디렉토리 커넥터 서비스에 기반하여 관련 정보를 인증 및 검색합니다 . 또한 운영자는 동기화 주기를 설정하거나 동기화 시 제외할 대상을 등록할 수 있으며 , 동기화 서비스를 활성화 또는 비활성화하여 실행을 제어할 수 있습니다 . 활성화된 동기화 서비스는 설정된 반복 주기에 따라 자동 실행되며 , 설정 주기 이외에 즉시 실행도 가능합니다 .

동기화 서비스 설정 정보

기본 정보

항목	설명
동기화 서비스 ID	서비스 등록 시 부여
자동 동기화 설정	자동 활성화 여부 • 표준 시간대: 동기화 서비스가 동작할 표준 시간대 • 예약 작업 유형: 동기화 예약 작업의 반복 주기 • 일정 설정: 시작일과 시작 시간 설정
서비스 대상	사용자, 그룹, 조직 정보
Directory 유형	MS Active Directory 또는 Others
IP/HOST	Directory 서버의 IP 또는 HOST 주소
포트	Directory 서버의 포트
암호화 방식	Directory 서버 연결 시 암호화 방식으로서 없음, SSL, TLS 중 선택

항목	설명
인증 방식	Directory 서버 연결 시 사용할 인증 방식을 없음, Simple, DIGEST-MD5, CRAM-MD5, GSSAPI 중 선택
인증 상세	**인증 방식**으로 DIGEST-MD5(SASL) 또는 CRAM-MD5(SASL)을 선택한 경우: • **SASL Realm**: 공백이 아닌 Realm 값 입력 • **보호 품질**: 아래의 데이터 보호 품질 중 선택 - **인증만**: 인증시에만 데이터를 보호 - **무결성 보호 인증**: 인증뿐 아니라 송수신 데이터에 대해서도 무결성을 보장 - **무결성 및 프라이버시 보호 인증**: 인증뿐 아니라 주고 받는 데이터를 암호화하여 무결성을 보장 • **보호 강도**: 데이터 보호 강도를 선택 - **높음**: 높음 선택시 128 비트 암호화 사용 - **중간**: 중간 선택시 56 비트 암호화 사용 - **낮음**: 낮음 선택시 40 비트 암호화 사용 - **쌍방향 인증 사용**: 쌍방향 인증 사용을 클릭 시, 서버와 클라이언트에서 주고 받는 데이터에 키를 삽입하여 데이터 유효성 확인 **인증 방식**으로 **GSSAPI(Kerberos)**을 선택한 경우: • **Kerberos 자격 증명 구성**: Kerberos 티켓에 대한 획득 방법 선택 - **Cache 티켓 사용**: EMM내 발급받은 티켓이 있을 경우 선택 - **신규 발급**: 기본 설정의 사용자 ID, 사용자 암호를 사용하여 신규 티켓 발급 • **Kerberos 구성**: Kerberos 서버 구성 방법을 선택 - **내부 시스템 정보 사용**: Java Property 정보에 정의된 Kerberos 서버 정보 사용 - **직접 입력**: Kerberos 서버 정보 직접 입력 - **Realm**: Kerberos 서버의 Realm을 입력 - **KDC(Kerberos Key Distribution Center) Host**: KDC Host 또는 IP 주소 입력 - **KDC(Kerberos Key Distribution Center) 포트**: KDC 포트 입력

사용자 정보

항목	설명
Base DN	사용자 동기화 경우 Directory 서버의 탐색 시작 위치를 설정하세요. Base DN 설정 관련 자세한 사항은 287페이지 16장의 “Base DN 설정하기"를 참고하세요.
필터	데이터 필터에 사용될 LDAP Syntax 문자열로서, Object Class와 변수명을 설정하세요. 자세한 내용은 289페이지 16장의 “출력 필드 설정하기"를 참고하세요.
자동 동기화	설정된 예약 작업 시간에 동기화 서비스 자동 진행여부 선택
삭제 사용자 처리	동기화 시 통합 시스템에서 삭제된 사용자를 EMM으로 가져올지 여부를 선택
사용자 정보 맵핑	매핑할 사용자 정보를 설정하세요. • **입력값 사용**을 선택하는 경우, 기간계 시스템과의 매핑값은 초기화 되고 운영자가 입력한 값으로 매핑됩니다. • **UPN**: Windows 도메인에 로그인 시 사용되는, 사용자 로그인 이름(User Principal Name)입니다. 입력 형태는 사용자 로그인 이름 + UPN 접미사이며, UPN 접미사 형태는 "@domain_name"입니다. 예: 사용자 이름이 EMMuser1 인 경우, EMMuser1@mydomain.com • **DN(고유 이름)**: LDAP Entity 고유 이름 • **객체 식별자**: 동기화 사용자 식별 ID • **보안레벨**: 사용자의 보안 등급을 선택
Custom 필드 맵핑	동기화 외부 연계 서비스에서 사용할 사용자 정보 팹핑값을 속성을 지정하여 등록합니다. 연계 서비스에서 사용자 정보를 Custom 방법으로 등록 시 사용됩니다. **맵핑 대상**과 **맵핑 속성**을 입력한 후 ⊕을 클릭하세요.

그룹 정보

항목	설명
Base DN	사용자 동기화 경우, Directory 서버의 탐색 시작 위치를 설정하세요. Base DN 설정 관련 자세한 사항은 287페이지 16장의 “Base DN 설정하기"를 참고하세요.
필터	그룹 필터에 사용될 LDAP Syntax 문자열로서, Object Class와 변수명을 설정하세요. 자세한 내용은 289페이지 16장의 “출력 필드 설정하기"를 참고하세요.
자동 동기화	설정된 예약 작업 시간에 동기화 서비스를 자동으로 진행할 지 여부를 선택
구성원 자동 동기화	동기화 대상 그룹의 구성원을 EMM 사용자로 자동 동기화
삭제 그룹 처리	동기화 시 기간계 시스템에 삭제된 그룹을 EMM에 가져올 지 여부를 선택
그룹 정보 맵핑	매핑할 그룹 정보를 설정하세요. • **입력값 사용**을 선택하는 경우, 기간계 시스템과의 매핑값은 초기화 되고 운영자가 입력한 값으로 매핑됩니다. • **DN(고유 이름)**: LDAP Entity 고유 이름 • **객체 식별자**: LDAP entity의 ID

조직 정보

항목	설명
Base DN	사용자 동기화 경우, Directory 서버의 탐색 시작 위치를 설정하세요. Base DN 설정 관련 자세한 사항은 287페이지 16장의 “Base DN 설정하기"를 참고하세요.
필터	그룹 필터에 사용될 LDAP Syntax 문자열로서, Object Class와 변수명을 설정하세요. 자세한 내용은 8장의 289페이지 16장의 “출력 필드 설정하기"를 참고하세요.
자동 동기화	설정된 예약 작업 시간에 동기화 서비스를 자동으로 진행할지 여부를 선택
삭제 조직 처리	동기화 시 통합 시스템에 삭제된 조직을 EMM에 가져올지 여부를 선택
조직 정보 맵핑	**입력값 사용**을 선택하는 경우, 기간계 시스템과의 매핑값은 초기화되고 운영자가 입력한 값으로 매핑됩니다.
Custom 필드 맵핑	동기화 외부 연계 서비스에서 사용할 조직 정보 팹핑값을 속성을 지정하여 등록합니다. 연계 서비스에서 조직 정보를 Custom 방법으로 등록 시 사용됩니다. **맵핑 대상**과 **맵핑 속성**을 입력한 후 ⊕을 클릭하세요.

동기화 서비스 등록하기

Directory 서비스를 이용하여 사용자 , 조직 , 그룹 정보를 가져오기 위한 동기화 서비스 를 등록합니다 . 등록한 후에는 바로 실행이 가능합니다 .

동기화 서비스를 추가하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > AD/LDAP 동기화 > 동기화 서비스**로 이동하세요.
2. 화면 상단의 ➕을 클릭하세요.
3. “동기화 서비스 추가” 창에서 **기본 설정** 탭을 입력하세요.
   - 기본 설정 정보의 자세한 내용은 91페이지의 "기본 정보"를 참고하세요.
4. 동기화 대상에 따라 활성화된 **사용자**, **그룹**, 또는 **조직** 탭을 선택한 후, 입력하세요.
   - 입력 항목에 대한 자세한 내용은 91페이지의 "동기화 서비스 설정 정보"를 참고하세요.
5. 입력 내용으로 동기화 기능 검증을 위해, **테스트**를 클릭하세요.
6. **저장**을 클릭하세요.
7. 확인 팝업 메시지 창에 **예**를 클릭하세요.

동기화 서비스 활성화/비활성화하기

동기화 서비스를 활성화하거나 비활성화하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > AD/LDAP 동기화 > 동기화 서비스**로 이동하세요.
2. 비활성화 상태의 서비스를 활성화하려면, 해당 동기화 서비스의 ⚫을 클릭하세요.
   활성화 상태의 서비스를 비활성화하려면, 해당 동기화 서비스의 🔵을 클릭하세요.
3. 확인 메시지가 나타나면 **예**를 클릭하세요.

동기화 서비스 실행하기

동기화 서비스를 원하는 시점에 즉시 실행할 수 있습니다 . 실행 처리 직전 동기화 예상 개수를 팝업 창에서 확인할 수 있습니다 .

동기화 서비스를 즉시 실행하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > AD/LDAP 동기화 > 동기화 서비스**로 이동하세요.
2. 즉시 실행할 동기화 서비스의 ▶을 클릭하세요.
3. "동기화 즉시 실행" 창에서 동기화 유형에 맞게 **자동(추천), 동기화 대상 사용자/조직/그룹 추가** 중에 선택하세요.
   - **자동(추천)**: 해당 아이템의 모든 사용자 또는 조직을 동기화
   - **동기화 대상 사용자/조직/그룹 추가**: 특정 사용자/조직/그룹만 선택하여 동기화

     가. 동기화 대상 **사용자/조직/그룹 추가**를 선택한 후, **다음**을 클릭하세요.

     나. 추가 방법으로 **설정 내 모든 사용자/그룹/조직**, **직접 선택(추천)** 중 선택하세요.
     직접 선택의 경우 "사용자/조직/그룹 선택" 창이 활성화됩니다.

     다. 해당 사용자/조직을 선택한 후, **확인**을 클릭하세요.

     라. **확인**을 클릭하세요.
   - **수동 설정**: 조직 대상 유형이 사용자/조직/그룹인 경우에 대하여 다음 항목을 선택하세요.

     가. **수동 설정**을 선택한 후, **다음**을 클릭하세요.

     나. 동기화 대상 검색 방법으로 **전체 검색**, **변경 내역만 검색**을 선택하세요.

     다. 동기화 검색 대상으로 추가, 수정, 삭제를 선택하세요.

     라. **확인**을 클릭하세요.

동기화 예외 대상 복원 및 삭제하기

동기화 서비스 실행 시 예외 처리된 사용자 , 조직 , 그룹을 동기화 예외 대상 목록에서 확인합니다 .

다음의 경우에는 사용자 , 조직 , 그룹이 동기화 예외 대상으로 포함됩니다 .

- EMM에서 삭제된 경우
- 연동 시스템에서 삭제된 경우
- 동기화 그룹에서 삭제된 경우
- 중복, 거부, 부적합
- 동기화 시점에 이미 동일한 ID가 EMM에 존재하는 경우
- 조직/사용자 정보에 동기화 예외 대상으로 설정된 경우
- 연동시스템의 정보가 EMM 구조에 적합하지 않은 경우

동기화 예외 대상을 복원하거나 삭제한 후 , 다시 동기화를 시도할 수 있습니다 . 예외 대상에서 삭제하게 되면 해당 사용자 / 그룹 / 조직은 다음 동기화 실행 시 다시 대상에 포함됩니다. 동기화 예외 대상을 다시 복원시키면 해당 동기화 서비스가 한 번 실행됩니다.

예외 대상이 된 동기화 사용자 / 그룹 / 조직을 복원하거나 삭제하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > AD/LDAP 동기화 > 동기화 예외 대상**으로 이동하세요.
2. **대상 ID**, **연동 시스템 ID**, **서비스 ID**를 이용하여 검색하세요.
   - **대상 유형**: 사용자, 그룹, 조직
   - **예외 유형**
     - **삭제됨(EMM)**: EMM에서 삭제된 사용자, 그룹 및 조직
     - **삭제됨(연동시스템)**: 연동시스템에서 삭제된 사용자,그룹 및 조직을 삭제하거나, 복원 시 다음 동기화 서비스 실행 결과에 따라 다시 동기화 예외 대상 목록에 포함될 수 있음.
     - **중복됨**: 동기화 시점에 동일한 ID의 사용자, 그룹 및 조직이 존재하여 예외 대상으로 등록됨
     - **거부됨**: 동기화 대상 제외로 설정된 사용자, 그룹 및 조직
     - **부적합**: 동기화 데이터 중에 EMM 구조에 적합하지 않게 등록된 사용자 및 조직
   - 검색조건 입력
     - **대상 ID**: 예외대상이 되는 ID (사용자 ID 혹은 조직 코드)
     - **연동시스템 ID**: 연동시스템에서의 사용자 고유 이름
     - **서비스 ID**: 동기화 서비스 ID
3. 대상선택 후, 또는 을 클릭하세요.

- 삭제: 예외 대상에서 삭제하면서 다음 동기화 예약 실행 시 동기화 대상이 됨
- 복원: 예외 대상에서 삭제하면서 바로 동기화 실행하여 목록에 추가됨

Note: 대상 복원 시 장비 정보, 역할에 대한 정보는 복원되지 않습니다.

동기화 이력 조회하기

1. **단말 & 사용자 > AD/LDAP 동기화 > 동기화 이력**으로 이동하세요.
2. 동기화 서비스의 유형, 등록 일자, 동기화 ID를 입력한 후 을 클릭하세요.
3. 동기화 이력 상세 정보를 조회하려면 을 클릭하세요.

외부 시스템과 동기화 서비스 연계하기

EMM 의 AD/LDAP 을 통한 사용자 및 조직 동기화 기능과 인증 기능을 외부 시스템에 제공하는 기능입니다 . 외부 시스템과 연결한 후 , EMM 의 사용자 / 조직 정보를 외부 시스템의 정보화 매핑하여 제공합니다 . 또한 외부 시스템에서 로그인 시 EMM 이 제공하는 인증 정보를 이용하게 됩니다 .

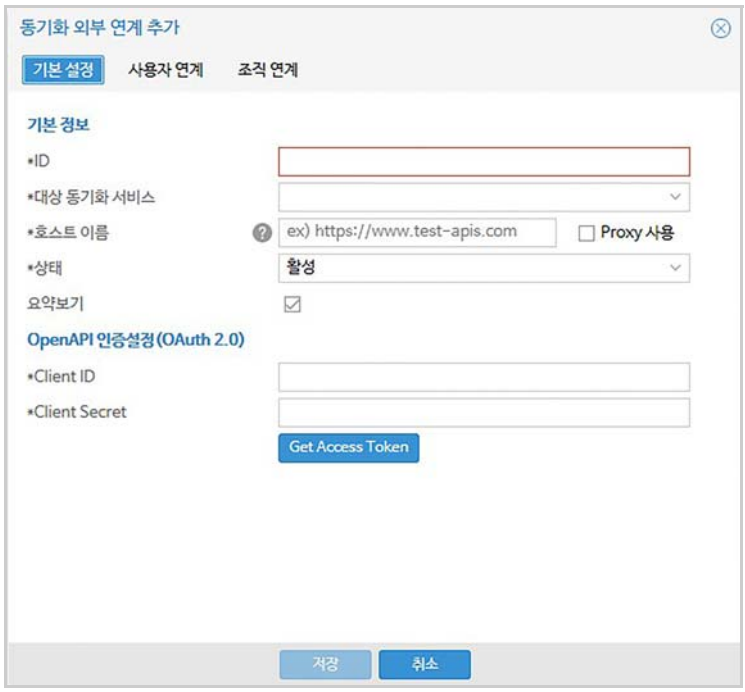
동기화 외부 연계 서비스 등록하기

동기화 사용자 및 조직 정보를 외부 연계 시스템에 제공하기 위한 서비스를 등록합니다 . 외부 시스템 연결을 위한 기본 설정 정보를 입력한 후 사용자 및 조직 정보를 외부 시스템의 정보와 매핑합니다 . 서비스 설정 후 추가되거나 변경되는 사용자 / 조직 정보는 자동으로 갱신되어 연계 시스템에 전달됩니다 .

동기화 외부 연계 서비스를 추가하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > AD/LDAP 동기화 > 동기화 외부 연계**로 이동하세요.

2. 화면 상단의 ＋을 클릭하세요.



3. "동기화 외부 연계 추가" 창에서 **기본 설정** 탭을 입력하세요.

항목	설명
ID	동기화 외부 연계 서비스 ID를 부여
대상 동기화 서비스	외부 시스템에 제공할 EMM 동기화 서비스 ID
호스트 이름	연계할 외부 시스템의 호스트 이름
상태	동기화 외부 연계 서비스의 상태로서 활성 또는 비활성

Open API 인증 설정 (OAuth 2.0)	• 외부 서비스를 위한 범용적인 인증 표준 프로토콜인 OAuth를 위한 항목 입력
	  • Client ID, Client Secret: 외부 서비스에서 미리 발급받아 놓은 Client ID와 Client Secret
	  • **Grant Type**:
	  - **Client credentials**: Client secret을 안전하게 보관할수 있는 애플리케이션일 때 ID와 secret으로 인증하는 방식
	  - **Resource owner password**: **사용자 ID**, **비밀번호** 필수 입력
	  • **SCOPE**: 발급 받을 Access Token의 접근 범위를 입력
	  • **Access Token URL**: 인증 토큰을 발급받기 위한 주소 입력
	• 인증 토큰 발급: 입력 정보를 바탕으로 인증 토큰을 발급받기 위해 **Get Access Token** 클릭.
	Get Access Token 성공 시 **저장** 버튼 활성화됨.
	  • 인증 토큰 발급 후에는 **비밀번호** 변경 시에도 기존 인증 토큰은 유효함

4. 연계하고자 하는 대상에 따라 **사용자 연계** 또는 **조직 연계** 탭을 선택한 후 정보를 입력하세요.

   • **API 설정**: 외부 시스템에 사용자/조직을 추가, 수정, 삭제하기 위한 API가 위치한 URL 주소를 입력하세요.

- **매핑 방법**: EMM 사용자/조직 정보의 속성값을 외부 연계 시스템의 속성값과 매핑합니다.
  - Custom: 외부 시스템에 전달할 EMM의 사용자/조직 정보를 운영자가 입력한 설정값을 토대로 변환하여 연계 시스템으로 보냅니다.
  - Auto: EMM의 사용자/조직 정보를 그대로 연계 시스템으로 보냅니다.
- 매핑 설정: Custom 방식의 경우, EMM의 사용자/조직 정보와 연계 시스템의 정보를 연결해 줍니다.

5. **저장**을 클릭하세요.
6. 확인 팝업 메시지 창에서 **예**를 클릭하세요.

7 그룹

그룹은 단말에 정책 및 설정을 적용하거나 애플리케이션 권한을 관리하기 위한 단위입니다 . 그룹을 구성하는 정보에 따라 다음의 그룹을 등록하고 관리합니다 .

- 일반 그룹: 사용자 또는 단말 정보로 구성된 그룹이며, 프로파일을 할당할 수 없습니다.
- AD/LDAP 동기화 그룹: AD/LDAP에서 그룹 정보를 동기화 서비스를 통해 가져온 그룹
- 프로파일 그룹: 프로파일 적용을 위한 그룹으로, 사용자 프로파일 또는 단말 프로파일로 구성된 그룹의 사용자 프로파일과 단말 프로파일을 혼용하여 구성할 수 없습니다.
  - 사용자가 프로파일 그룹에 포함되어 있더라도 사용자가 보유한 단말을 단말 프로파일 그룹에 추가할 수 있습니다.
  - 프로파일 정책 적용은 단말 프로파일, 사용자 프로파일, 조직 순서로 적용됩니다.
  - 프로파일 그룹을 생성 또는 삭제하는 경우와 프로파일 그룹의 사용자를 추가 또는 삭제하는 경우, 팝업 창에서 해당 사용자의 단말에 변경된 프로파일을 바로 배포할 수 있습니다.

그룹 등록 시 정보를 공개할 운영자의 범위를 다음과 같이 설정합니다 .

- 공개: 모든 운영자에게 공개
- 비공개: 그룹을 등록한 보조 운영자와 수퍼 운영자에게만 공개

그룹에 정책 할당 , 단말 제어 전송은 해당 그룹을 추가한 보조 운영자와 수퍼 운영자만 가능합니다 .

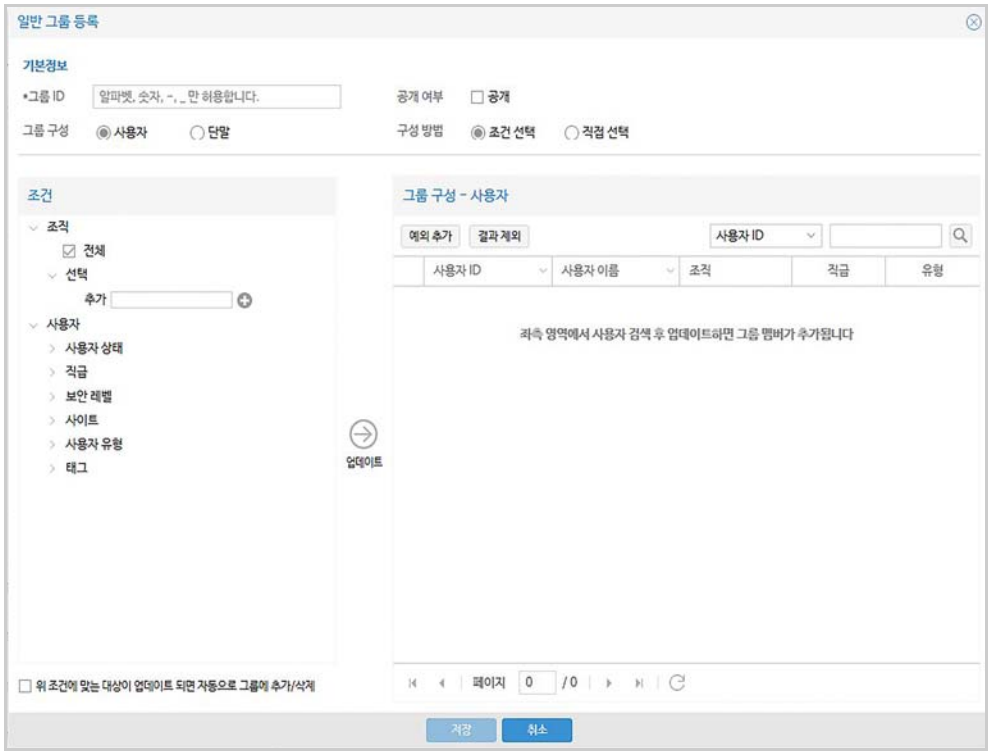
태그 그룹

사용자 계정 항목 중 태그 정보를 이용하여 그룹 생성이 가능합니다 . 태그는 운영자가 사용자를 분류하기 위해 텍스트로 정의하는 항목입니다 . 사용자 계정의 태그를 유형별로 입력 한 후, 일반 그룹 등록 시 검색하여 동일 태그를 가진 사용자를 하나의 그룹으로 구성할 수 있습니다 .

일반 그룹 등록하기

사용자와 단말로 구성되는 일반 유형의 그룹을 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 그룹**으로 이동하세요.
2. ➕을 클릭한 후 “일반 그룹 등록” 을 클릭하세요.



3. **그룹 구성**에서 용도에 맞게 **사용자**, **단말** 중에 하나를 선택하세요.
4. 그룹의 공개여부를 확인하세요.
   - 공개 선택: 그룹을 추가한 운영자를 포함한 모든 운영자에게 공개
   - 공개 해제: 그룹을 추가한 보조 운영자와 수퍼 운영자에게 공개
5. **구성 방법**을 **조건 선택**, **직접 선택** 중에 선택하세요.
   - 구성 방법 중 **조건 선택**에서는 좌측의 조건을 선택한 후, **업데이트**를 클릭하세요.
   - 구성 방법 중 **직접 선택**에서는 좌측에서 사용자나 단말을 직접 선택한 후, **업데이트**를 클릭하세요.
6. **저장**을 클릭하세요.

일반그룹에 예외적으로 추가할 대상 지정하기

일반 그룹 구성 시 , 조건과 상관없이 추가하고자 하는 대상이 있는 경우 **예외 추가**로 등록해 놓습니다 . **예외 추가**에 등록된 대상은 그룹 등록 , 수정 시 항상 포함됩니다 .

1. **단말 & 사용자 > 그룹**으로 이동하세요.
2. 사용자를 추가할 일반 그룹의 ✏️을 클릭하세요.

3. "일반 그룹 수정" 창의 정보 수정 후 **업데이트**를 클릭하세요.
4. 그룹 구성 목록 상단의 **예외 추가**를 클릭하세요.
5. "예외 추가" 창에서 ➕을 클릭하세요.
6. 검색 조건을 설정한 다음키워드를 입력한 후 🔍을 클릭하세요.
7. 검색 목록에서 선택한 후 **업데이트**를 클릭하세요.
8. 화면 하단의 **확인**을 클릭하세요.
9. 확인 메시지가 나타나면 **예**를 클릭하세요.

일반그룹에 제외 대상 지정하기

일반 그룹 구성 시 , 조건과 상관없이 제외하고자 하는 대상을 **결과 제외**로 등록해 놓습니다 . **결과 제외**에 등록된 대상은 그룹 등록 , 수정 시 항상 제외됩니다 .

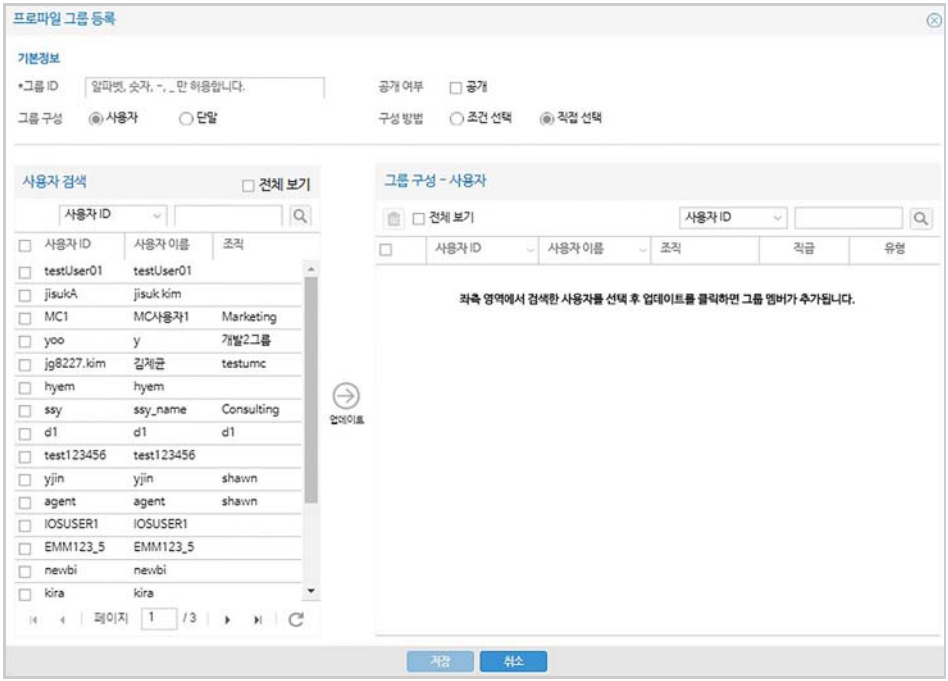
1. **단말 & 사용자 > 그룹**으로 이동하세요.
2. 사용자를 추가할 일반 그룹의 ✏을 클릭하세요.
3. "일반 그룹 수정" 창의 정보 수정 후 **업데이트**를 클릭하세요.
4. 그룹 구성 목록 상단의 **결과 제외**를 클릭하세요.
5. "곌과 제외" 창에서 ➕을 클릭하세요.
6. 검색 조건을 설정한 다음키워드를 입력한 후 🔍을 클릭하세요.
7. 검색 목록에서 선택한 후 **업데이트**를 클릭하세요.
8. 화면 하단의 **확인**을 클릭하세요.
9. 확인 메시지가 나타나면 **예**를 클릭하세요.

프로파일 그룹 등록하기

프로파일 유형의 그룹을 추가하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 그룹**으로 이동하세요.

2. ➕을 클릭한 후 **프로파일 그룹 등록**을 클릭하세요.



3. "프로파일 그룹등록" 창에 **그룹 ID**를 입력한 후, **그룹 구성**을 **사용자**, **단말** 중 선택하세요.
4. 그룹의 **공개 여부**를 확인하세요.
   - **공개** 선택: 그룹을 추가한 운영자를 포함한 모든 운영자에게 공개
   - **공개** 해제: 그룹을 추가한 보조 운영자와 수퍼 운영자에게 공개
5. **구성 방법**에서 **조건 선택**, **직접 선택** 중에 선택한 후, 그룹 정보를 구성하세요.
   - 구성 방법 중 **조건 선택**에서는 좌측의 조건을 선택한 후, **업데이트**를 클릭하세요.
   - 구성 방법 중 **직접 선택**에서는 좌측 검색 영역에서 사용자나 단말을 직접 선택한 후, **업데이트**를 클릭하세요.
6. "프로파일 할당" 창에서 단말관리 프로파일과 앱관리 프로파일을 선택한 후 **저장**을 클릭하세요."프로파일 배포"창에서 **예**를 클릭하세요.
   - 프로파일을 그룹의 모든 단말에 프로파일이 배포됩니다.

동기화 그룹 등록하기

EMM 의 AD/LDAP 동기화 서비스를 통해 사내 통합 시스템의 그룹 정보를 EMM 의 동기화 그룹으로 등록합니다 . 동기화 서비스를 지정한 후 검색을 통해 개별 그룹을 등록하거나 일괄로 등록할 수 있습니다 .

동기화 유형의 그룹을 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 그룹**으로 이동하세요.

2. ➕을 클릭한 후 **AD/LDAP 동기화 그룹 등록**을 클릭하세요.

3. "**AD/LDAP** 동기화 그룹 등록" 창에서 동기화 그룹을 검색하세요.
   - **동기화 서비스**: 설정된 동기화 서비스 목록에서 선택하세요.
   - **Base DN, 필터**: 선택된 동기화 서비스의 값이 자동으로 입력됩니다.
   - **키워드 검색**: 검색 키워드 입력한후 🔍을 클릭하세요.
     전체 검색 시 *을 입력하세요.
4. 검색 결과의 동기화 그룹 목록에서 대상을 선택한 후 **다음**을 클릭하세요.
   이미 등록된 동기화 그룹을 선택한 경우 알림 메시지 창이 나타납니다.

5. "**AD/LDAP**동기화 그룹 등록" 창의 정보를 입력하세요.
   - 그룹 ID: 부여할 EMM 내의 그룹 ID
   - 구성원 자동 동기화: 해당 그룹의 구성원도 함께 동기화 할지 여부를 선택
   - 그룹 공개 여부: 선택 여부에 따라 그룹 공개 항목에 Y 또는 N으로 표시됨
   - 그룹 구성원: 동기화 그룹의 구성원을 동일하게 **전체**로 하거나 **선택**하세요.

- 전체: 동기화 서비스 대상 그룹의 전체 구성원과 동일
- 선택: “동기화 그룹 등록” 창에서 원하는 구성원을 검색하여 추가하세요.

6. **저장**을 클릭하세요.

프로파일 그룹에 프로파일 할당하기

프로파일 그룹별로 단말 관리 프로파일과 앱관리 프로파일을 할당 할 수 있습니다 .

1. **단말 & 사용자 > 그룹**으로 이동하세요.
2. 목록에서 **구분** Filters를 **프로파일**로 선택하세요.
3. 프로파일 그룹을 선택한 후 해당 그룹의 을 클릭하세요.

4. “프로파일 할당” 창에서 **단말 관리 프로파일** 또는 **앱 관리 프로파일**을 입력하세요.
5. **저장**을 클릭하세요.

8 단말 등록

EMM 을 이용할 단말을 등록합니다 . EMM 에서 운영하는 단말 플랫폼으로는 Android, iOS, Windows, Tizen Wearable 이 있습니다 . Tizen Wearable 은 삼성 전자의 wearable 기기에서 운영되는 Knox 기반의 플랫폼입니다 . 단말 등록은 개별 또는 일괄로 가능합니다 . 삼성 전자 단말의 경우 , Knox 포털 내 Knox Mobile Enrolment (KME) 기능을 이용하여 대량의 단말을 등록하고 활성화할 수 있습니다 .

단말 활성화 절차

단말에서 EMM 을 사용하기 위해서는 다음과 같이 단말을 등록하고 활성화시킵니다 .

1. **단말 & 사용자 > 사용자 & 조직**에서 사용자를 등록하세요.
2. **단말 & 사용자 > 단말**에서 단말을 등록하세요.
3. 사용자에게 설치 파일 링크가 담긴 문자를 전송하세요.
4. 선택 사항: Tizen Wearable 단말에 대한 EMM 설치 정보를 사용자에게 보내세요.
   - Wearable 단말에 설치 정보 내보내기에 대한 자세한 내용은 113페이지의 "Wearable 단말에 설치정보 보내기"를 참고하세요.
5. 사용자는 단말 플랫폼에 따라 다음의 시스템 애플리케이션을 Public store에서 다운로드 받아 설치하세요.
   - Android 플랫폼의 경우: EMM Client, EMM Agent, Push Agent를 설치하세요.
   - iOS, Windows 플랫폼의 경우: EMM Client를 설치하세요.
   - Tizen Wearable 플랫폼의 경우: Wearable EMM을 설치하세요.
6. 사용자는 단말의 EMM에 로그인하세요.
   - 사용자의 EMM 로그인에 대한 자세한 내용은 “Samsung SDS EMM 사용자 매뉴얼”의 3.1 EMM 로그인하기를 참고하세요.

플랫폼별 단말 정보

Android, iOS, Windows, Tizen wearable 플랫폼에서 영역별로 관리되는 단말 정보는 다음과 같습니다 .

영역	단말 정보	Android	iOS	Windows	Wearable
기본	• 단말상태 • 모바일 ID • 모델이름 • 플랫폼 • 소유구분 • Knox 컨테이너 정보 • 마지막으로 단말 정보를 가져온 일시 • 단말 소유자 정보	O	O	O	O
Security	• 적용 중인 단말 관리 프로파일 정보 • 적용 중인 EMM 앱관리 프로파일 정보 • KeepAlive 여부 • 외장 SD 카드 암호화 여부 • Enterprise FOTA	O	O	O	O
	• OS위변조 여부 • 앱 위변조 여부 • CC 모드 사용 여부 • 단말 메모리 암호화 여부 • 지문 인증 • 홍채 인증	O	-	-	-
	• 하드웨어 암호화 수준 • 단말잠금 비밀번호 설정 • iCloud백업 • iTunes/AppStore 로그인 • 감독모드 여부 • 활성화방지 여부	-	O	-	-
	• 인증코드 • OTP Valid 여부 • OTP 유효기간	-	-	-	O

영역	단말 정보	Android	iOS	Windows	Wearable
Details	• 단말 잠금 여부 : **+More** 클릭 시 사유 제공 • 위치 정보 • Wi-Fi, Bluetooth • 메모리 정보 • 전화번호 • MAC 주소 • 펌웨어 • IMEI / MEID • 시리얼번호 • 제조사 • SIM 상태 • SIM 국가/ 네트워크 • 로밍여부 • 현재 국가/네트워크 • 기타 정보	O	O	O	O
	IMSI	O	-	-	-
	• 음성로밍 여부 • 데이터로밍 여부 • 위치 서비스 사용 여부 • 방해 금지 모드 여부	-	O	-	-
	• 단말 구분 • 단말 OS • 단말이름 • OS 빌드	-	-	O	-
SDK	• SDK종류 • 버전 • 라이선스 발급일자/만기일자	O	-	-	-

단말 상태

EMM 사용 단말의 상태는 다음과 같이 구분됩니다. 비활성, 활성화 금지 상태의 단말에는 단말 제어 명령을 전송할 수 없습니다. 단말 삭제는 비활성, 활성화 금지 상태에서만 가능합니다.

- ✔ Provisioning: 정상적으로 단말이 등록된 후, EMM이 활성화되기 전의 상태입니다.
- ◯활성: EMM이 활성화되어 사용 중인 상태입니다.
- ⃠활성화금지: 비활성 상태의 단말이 활성화될 수 없도록 운영자가 차단해 놓은 상태입니다.
- ⛔시스템차단: 단말이 상태보고기한 (KeepAlive)을 초과하거나 공장 초기화되어 시스템에서 단말의 EMM 활성화를 차단한 상태입니다.
- ◌비활성: EMM을 통한 단말 제어가 불가능한 상태입니다.

- 관리자차단: 사용자가 단말을 분실하거나 교체 하면서 활성화 상태로 남아 있는 단말을 운영자가 관리자 포털에서 차단해 놓은 상태입니다.

KME용 단말 등록하기

삼성 전자 단말의 경우 , 여러 대의 단말 등록 및 활성화를 위한 Knox mobile enrolment (KME) 기능을 이용할 수 있습니다 . KME 는 삼성 전자에서 제공하는 포털을 이용하여 대량의 단말을 편하게 등록하고 활성화 시키는 기능입니다 .

운영자는 Knox 홈페이지의 KME 포털에 EMM 기본 정보와 KME 대상 단말 목록을 등록합니다 . 등록된 KME 용 단말의 경우 , 사용자가 Wi-Fi 최초 연결 시 단말 활성화가 자동으로 진행됩니다 . KME 대상 단말을 일반적인 방법으로 활성화할 수는 없습니다 . KME 활용 방법에 대한 자세한 내용은 470 페이지 18 장의 “Knox Mobile Enrollment" 를 참고하세요 .

KME 절차

KME 방식으로 단말을 등록하는 방법은 다음과 같습니다 .

1. KME 포털 아이디와 비밀번호를 삼성전자에 승인 요청하여 부여 받으세요.
   - Knox 홈페이지의 KME 포털, https://www.samsungknox.com/en/products/knox-mobile-enrollment에 로그인하세요.
2. 단말을 등록하기 위한 MDM 서버 URI를 입력하세요.
3. KME 포털에 필요한 MDM 프로파일을 다음과 같이 생성하세요.

   가. 프로파일명을 입력하세요.
   - 예: KME for SDS EMM

   나. 단말에 설치할 EMM Client, EMM Agent, Push를 다운로드 받을 URL을 등록하세요.
   - 등록 순서는 1. EMM Agent, 2. EMM Client, 3. Push 입니다.
   - 입력한 위치에 실제 APK 파일이 있는지 체크한 후, 없는 경우 다음 단계가 진행되지 않습니다.

   다. Knox EULA 및 Knox license를 등록하세요.
4. KME 대상 단말 정보를 다음의 두 가지 방법으로 등록하세요.
   - CSV 파일 업로드: EMM 관리자 포털에서 생성한 CSV 파일을 KME 포털에 등록하세요.
     - CSV 파일 정보: 필수 항목은 IMEI 또는 Serial number, UserID, Password 이고 선택 항목은 MobileID 또는 기타 정보입니다.
     - EMM 관리자 포털에서의 CSV 파일 생성 방법에 대한 내용은 110페이지의 "KME 포털에 등록할 단말 파일 만들기"를 참고하세요.

- KME 앱을 이용한 스캐닝: KME 운영자는 전용 단말을 이용하여 Google Play Store에서 KME앱을 다운로드 받으세요.
  - KME 앱을 실행한 다음 SCAN DEVICES를 클릭한 후 단말의 IEMI 또는 Serial number를 스캐닝하세요. 스캐닝한 정보를 KME 포털에서 확인하세요.

5. 4단계에서 등록한 단말에 3단계에서 생성한 프로파일을 할당하세요.
   - 사용자가 KME 단말을 개봉하거나 공장 초기화하는 경우, Wi-Fi 연결 시 자동 활성화가 진행됩니다.
6. 단말이 활성화되었는지 관리자 포털의 **단말 & 사용자 > 단말**에서 확인하세요.

KME 포털에 등록할 단말 파일 만들기

KME 포털에 등록할 KME 용 단말 파일을 CSV 형태로 만듭니다 . 파일 양식은 다음과 같습니다 .

- **KME ID**: 단말의 고유번호로서 IMEI 또는 Serial number
- **사용자 ID**: EMM 단말 사용자 ID
- **사용자 비밀번호**: 임시 비밀번호로서 사용자 ID
- **Mobile ID**: EMM 단말 ID

KME 포털용 단말 파일을 만드려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. 화면 상단의 을 클릭한 후, **내보내기(KME)**를 선택하세요.
3. 좌측 하단에 생성된 CSV 파일을 클릭하세요.

KME 단말 EMM에 등록하기

KME 로 등록할 단말을 EMM 에 업로드합니다 . EMM 이 제공하는 엑셀 파일 양식을 다운로드하여 작성한 후 등록합니다 . 등록 파일은 파일 접근 제한 (DRM) 을 해제한 파일이어야 합니다 . 파일 양식은 다음과 같습니다 .

- **Mobile ID**: EMM 단말 ID
- **User ID**: EMM 단말 사용자 ID
- **KME ID**: 단말 고유번호인 IMEI 또는 Serial number
- **KME여부**: Y 또는 N

KME 용 단말 파일을 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.

2. ➕을 클릭한 후, **일괄 등록 (KME)**을 선택하세요.

3. **일괄 등록 (KME) 양식 다운로드**를 클릭한 후 PC에서 작성하세요.
4. **Browse**를 클릭한 후 CSV 형태의 KME 단말 파일을 선택하세요.
5. **확인**을 클릭하세요.

개별 단말 등록하기

사용자가 EMM 을 사용하려면 , 운영자가 먼저 해당 단말을 관리자 포털에 등록해야 합니다 . 개별 등록 또는 엑셀 템플릿으로 일괄 등록할 수 있습니다 . 라이선스의 단말 개수 초과 시는 등록할 수 없습니다 . 이미 등록된 단말을 다시 등록하려면 기존 단말을 삭제한 후 등록합니다 . 단말 삭제는 비활성 , 활성화 금지 상태인 단말만 삭제할 수 있습니다 .

- 한 사용자가 여러 단말을 동일한 모바일ID로 사용할 수는 없습니다.
- 여러 사용자가 각자의 단말을 같은 모바일ID로 등록할 수 있습니다.

단말 등록 정보는 다음과 같습니다 .

- **모바일 ID**: 단말 식별 ID로서 전화번호, MAC 주소, 닉네임 중 선택하세요. KME용 단말인 경우에는 KME ID
- **KME 여부**: KME용 단말의 경우 클릭한 후 단말 고유번호인 IMEI 또는 Serial number를 입력하세요.
- **플랫폼**: 단말 플랫폼을 Android, iOS, Windows, Tizen Wearable 중 선택하세요.
  - Wearable 단말의 경우 설치 SMS 메시지 전송에 필요한 전화 번호를 입력하세요.
- **소유 구분**: 소유 구분에 따라 선택하세요.

- BYOD: 임직원 소유의 단말
- COPE: 회사 소유의 개인 단말

단말 정보를 개별적으로 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. ➕을 클릭한 후, **개별 등록**을 선택하세요.
3. "개별 등록" 창에서 단말 정보를 입력한 후 **확인**을 클릭하세요.
4. 사용자 항목에 있는 🔍을 클릭하세요.
5. “사용자 조회” 창에서 **사용자 이름**, **사용자 ID** 또는 **조직**을 선택한 후 🔍을 클릭하세요.
6. 추가하려는 사용자를 선택하고 **확인**을 클릭하세요.
7. **확인**을 클릭하세요.

단말 일괄 등록하기

여러 대의 단말 정보를 엑셀 파일로 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. ➕을 클릭**한 후, 일괄 등록**을 선택하세요.
3. **일괄 양식 등록 다운로드**를 클릭하여 엑셀 파일을 PC에 저장하세요.
4. 다운로드한 엑셀 파일의 템플릿에 단말의 Mobile ID, User ID, Type, Platform과 Tizen Wearable 단말의 경우 전화번호를 입력한 후 저장하세요.
5. **Browse**를 클릭한 다음 작성한 파일을 선택한 후 업로드하세요.
6. **확인**을 클릭하세요.

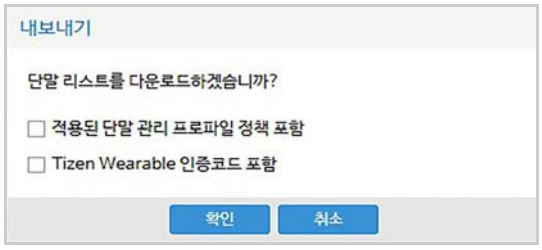
단말 목록 내보내기

단말 정보를 엑셀 파일로 저장할 수 있습니다 . Android 와 iOS 단말에 적용된 단말 관리 프로파일 정책포함 여부와 Tizen 인증코드 표함 여부를 선택할 수 있습니다 . 엑셀 파일에 단말관리 프로파일 정책은 Android 단말의 경우 JSON 형식으로 iOS 단말의 경우에는 XML 코드 형식으로 저장됩니다 . 코드에 대한 자세한 내용은 417 페이지 18 장의 “ 단말 적용 프로파일 코드 " 를 참고하세요 .

단말 정보를 엑셀 파일로 저장하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.

2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**으로 검색한 후 단말을 선택하세요.
3. 화면 상단의 을 클릭한 후 **내보내기**를 클릭하세요.



4. 단말 관리 프로파일 정책 포함 여부와 Tizen 인증코드 포함 여부를 클릭하세요.
5. 엑셀 파일을 작성한 후 저장하세요.

Wearable 단말에 설치정보 보내기

Wearable 단말의 경우 설치 정보를 SMS 또는 Email 로 단말에 전송합니다 . Wearable 단말에 전송되는 설치 정보는 다음과 같습니다 .

- EMM 설치를 위한 설치 URL
- EMM 활성화를 위한 EMM/TMS 서비스 URL
- 단말 정보로서 사용자 ID, Mobile ID, Tenant ID
- 사용자 인증코드 및 인증코드 생성 URL

설치 정보 전송 시 템플릿을 사용합니다 . SMS 로 전송 시에는 Tizen Wearable Information, Tizen Wearable Installation, Tizen Wearable Code 템플릿을 선택하여 발송합니다 . 해당 템플릿은 **설정 > 서비스 > 메시지 템플릿**에 등록되어 있습니다 . 메시지 템플릿에 대한 자세한 내용은 50 페이지 2 장의 " 메시지 템플릿 관리하기 " 를 참고하세요 .

Tizen Wearable 사용자 인증 코드는 단말 등록시 생성되며 , 이메일 또는 SMS 전송 시 재생성 여부를 선택할 수 있습니다 . 또한 사용자가 인증코드 생성 URL 에 접속하여 발급받을 수 있습니다 . 이에 대한 자세한 내용은 "Samsung SDS EMM 사용자 매뉴얼 " 을 참고하세요 .

Tizen Wearable 단말 설치 관련 환경 설정 정보는 **설정 > 서비스 > 환경 설정**의 Tizen Wearable 분류에서 등록합니다 . 사용자는 인증 코드를 개별 또는 여러 대의 단말에 보낼 수 있습니다 . 여러 단말을 선택하여 전송한 경우 전송 가능 단말에만 보내지고 전송 실패한 단말은 audit 기록에 남습니다 .

Wearable 단말에 EMM 설치 메시지를 보내려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직** 또는 **단말 & 사용자 > 단말**로 이동하세요.
2. 검색 조건을 입력한 후 을 클릭하세요.
3. 메시지를 보낼 사용자나 단말의 또는 을 클릭하세요.

4. 이메일 템플릿을 **Tizen Wearable 설치정보**로 선택하세요.
5. **확인**을 클릭하세요.

QR 코드 전송하기

EMM 은 사용자의 단말 활성화에 필요한 정보를 QR 코드로 생성하여 제공합니다 . QR 코드는 EMM 의 Tenant ID, 사용자 ID, 단말 ID, EMM 도메인 정보로 구성됩니다 .

운영자는 사용자에게 이메일로 QR 코드를 전송합니다 . 단말 사용자가 수신 이메일의 QR 코드를 단말의 EMM 초기 화면에 입력하여 로그인하면 단말은 활성화됩니다 . 메일 발송 전에 QR 코드 전송 템플릿을 EMM 관리자 포털의 **설정 > 서비스 > 메시지 템플릿**에 등록합니다 .

사용자의 메일 주소로 QR 코드를 전송하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직도에서 조직을 선택하거나 키워드를 입력한 후 을 클릭하세요.
3. 전송하려는 사용자나 단말의 을 클릭하세요.
4. “이메일 보내기-사용자명”창에서 **템플릿**을 입력하세요.
5. 선택한 템플릿의 상세 정보 조회 시 을 클릭하세요.
6. “메시지 템플릿 조회”장에서 **확인**을 클릭하세요.
7. “이메일 보내기-사용자명”에서 **확인**을 클릭하세요.
8. 발송 확인 메시지 창에서 **예**를 클릭하세요.

9 단말 관리

운영자는 활성화 상태의 단말에 애플리케이션을 설치하고 관련 설정 정보를 조회할 수 있습니다 . 사용자 단말에 설치된 애플리케이션을 업데이트하거나 삭제한 후 재설치할 수 있습니다 .

EMM 은 기본 대시보드를 제공하며 , 운영자가 EMM 에서 제공되는 보고서 쿼리를 기반으로 통계 보고서를 만들고 이를 이용해 대시보드를 구성할 수도 있습니다 . 대시보드를 통해 활성화 중인 단말 수 , 컴플라이언스 위반 건수 , 조직별 사용자 현황 , 단말 제어 이력 , 러아선스 성태 등을 확인할 수 있습니다 .

단말 관리를 위해 사용자 , 조직 , 그룹별로 활성화 단말에 단말 제어 명령을 보냅니다 . 단말 제어 중에서 많이 사용하는 주요 단말 제어 명령은 플랫폼별로 다음과 같으며 , 단말 제어 시 Frequently Used 영역에 분리되어 있어 빠르게 선택 가능합니다 .

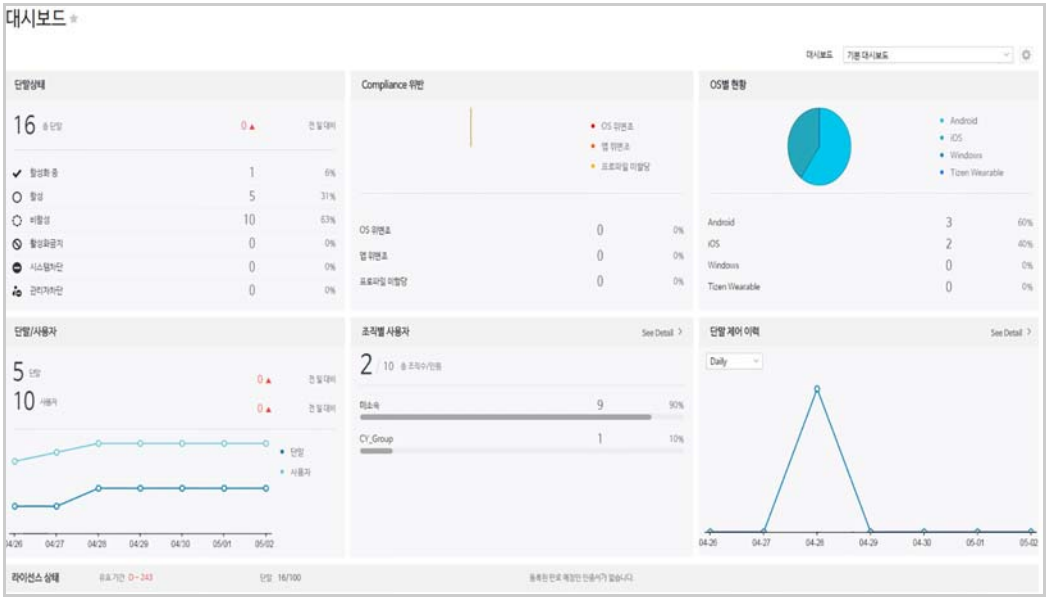
영역	단말 제어	Android	Knox container	iOS	Windows	Wearable
Compliance	최신 단말 관리 프로파일/앱 정보 배포	O	O	O	-	O
단말 관리	단말 잠금/해제	O	-	O	O	O
	단말 잠금 비밀번호 초기화	O	-	O	-	-
	공장 초기화 + SD Card 초기화	O	-	O	O	O
EMM	메시지 전송	O	O	O	-	-
단말 확인	단말/앱 정보 수집	O	-	-	-	-
	위치	O	-	O	O	O
컨테이너 관리	컨테이너 잠금/해제	-	O	-	-	-
	컨테이너 잠금 비밀번호 초기화	-	O	-	-	-
	컨테이너 삭제	-	O	-	-	-

단말 제어 이력과 미처리 단말 제어 내역을 확인할 수 있습니다 . 단말 상태 확인 후 상태 변경도 가능합니다 . 단말 진단 정보 로그를 수집한 후 로그 파일의 조회 및 다운로드가 가능합니다 .

EMM 은 check point MTP (mobile treat prevention) 기능과 연계하여 악성앱을 차단하는 기능을 제공합니다 . 운영자는 check point MTP 콘솔에서 MTP Agent 가 탐색한 악성앱을 EMM 모니터링 알림에서 확인할 수 있습니다 .

대시보드 보기

EMM 은 단말과 사용자 현황을 보여주는 기본 대시보드와 EMM 대시보드를 제공합니다 . EMM 관리자 포털 로그인 시 첫 화면에는 기본 대시보드가 나타납니다 .



기본 대시보드의 단말 상태 , Compliance 위반 , OS 별 현황 영역의 단말 숫자를 클릭하면 **단말 & 사용자 > 단말** 메뉴로 이동하게 되고 , 운영자는 OS 위변조 , 앱 위변조 , 프로파일 미할당 등에 대한 적절한 조치를 취할 수 있습니다 .

기본 대시보드는 영역별 다음의 내용으로 구성됩니다 .

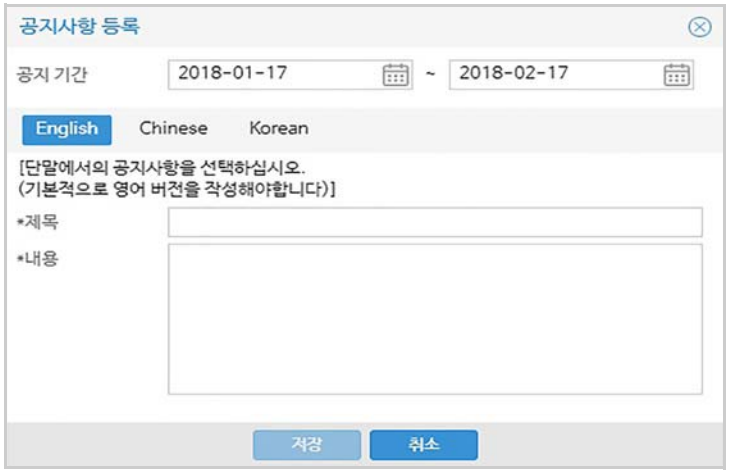
- **단말 상태**: 단말 상태별 단말 수와 전일 대비 증감 현황을 보여줍니다.
  단말 상태에 대한 자세한 내용은 108페이지 8장의 “단말 상태"를 참고하세요.
- **Compliance 위반**: 활성화된 단말 중 OS 위변조, 앱 위변조, 프로파일 미할당된 단말 수를 보여줍니다. 해당 숫자를 클릭하면 **단말 & 사용자 > 단말**로 이동하게 되고, 필요한 단말 제어 명령을 전송할 수 있습니다.
- **OS별 현황**: Android, iOS, Windows, Tizen Wearable 단말 중 활성화 단말 수를 보여줍니다.
- **단말/사용자**: 일자별 활성 상태의 단말 및 사용자 수 현황을 보여줍니다.
- **조직별 사용자**: 조직별 활성 상태의 사용자 수를 사용자가 많은 상위 조직순으로 보여줍니다.
- **단말 제어 이력**: Daily, Weekly별 단말 제어의 증가, 감소 현황을 보여줍니다.
- **라이선스 상태**: 라이선스 유효일 및 라이선스 상의 전체 단말 수와 활성화된 단말 수를 보여줍니다. 만료일이 일주일 미만으로 남은 EMM 단말 인증서의 만료일을 안내합니다.

대시보드를 조회하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 대시보드**로 이동하세요.
2. 우측 상단 **대시보드** 목록에서 **대시보드 이름**을 선택하세요.
3. 보고서로 구성된 대시 보드를 새로 고침하려면 각 보고서의 을 클릭하세요.
4. 보고서로 구성된 대시보드를 수정하려면, 상단 을 클릭하세요.
   - 대시보드 **유형**이 **기본 대시보드**이거나 **서비스 현황 > 대시보드 & Audit 설정 > 대시보드 관리**에서 메인 대시보드로 설정된 대시보드의 경우에는 이 비활성화됩니다.

단말 공지사항 등록하기

운영자는 사용자 단말에 공지하려는 내용을 공지 기간과 함께 등록할 수 있습니다 . 같은 기간에 공지 사항은 한 개만 가능합니다 . 공지사항 언어는 영어 , 중국어 , 한국어를 지원합니다 . 등록된 공지사항은 단말 로그인 시 단말 설정 언어로 보여집니다 . 영문은 필수 입력 항목이며 중문 , 국문이외의 언어를 사용하는 단말의 경우에는 영문으로 보여집니다 . 공지사항 확인은 **서비스 현황 > 공지사항**에서 가능합니다 .



사용자의 단말에 공지될 내용을 등록하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 공지사항**으로 이동하세요.
2. 공지사항을 추가하려면 을 클릭하세요.
3. 공지사항 정보를 입력 후, **저장**을 클릭하세요.
   - **공지 기간**: 게시 시작일은 오늘부터 한 달 이내에서 선택하세요.
   - **내용**: 문장 마지막에 공백을 입력하면 안됩니다.

단말 목록 보기

단말 & 사용자 > 단말에서 단말의 상태 , 모바일 ID, 플랫폼 등의 기본 정보 외에 단말 위변조 여부 , 단말 제어 이력 및 단말 진단 등을 조회할 수 있습니다 .

단말에 적용된 프로파일과 단말 Knox 컨테이너의 생성 여부를 볼 수 있습니다 . 단말 제어 이력을 일자별로 조회할 수 있습니다 . 마지막으로 전송된 단말 제어 명령을 볼 수 있고 KME 용 단말의 경우 KME 여부가 Y 로 표시됩니다 . 단말의 악성 앱 정보는 Malware 항목에 표시되며 상세 정보를 조회할 수 있습니다 . “Malware 정보 ” 창에 악성 앱의 패키지명 , 삭제 여부가 보여지며 , 미처리 악성앱을 삭제할 수 있습니다 . 단말 조회 시 각 항목별로 원하는 내용을 필터링할 수 있습니다 . 항목 필터링 시 상단에 이 나타납니다 . 검색 필터를 초기화하려면 상단의 을 클릭합니다 . 컬럼의 항목을 마우스로 끌어서 위치를 이동하면 변경된 상태로 저장되고 , 초기 위치로 되돌리려면 을 클릭합니다 .

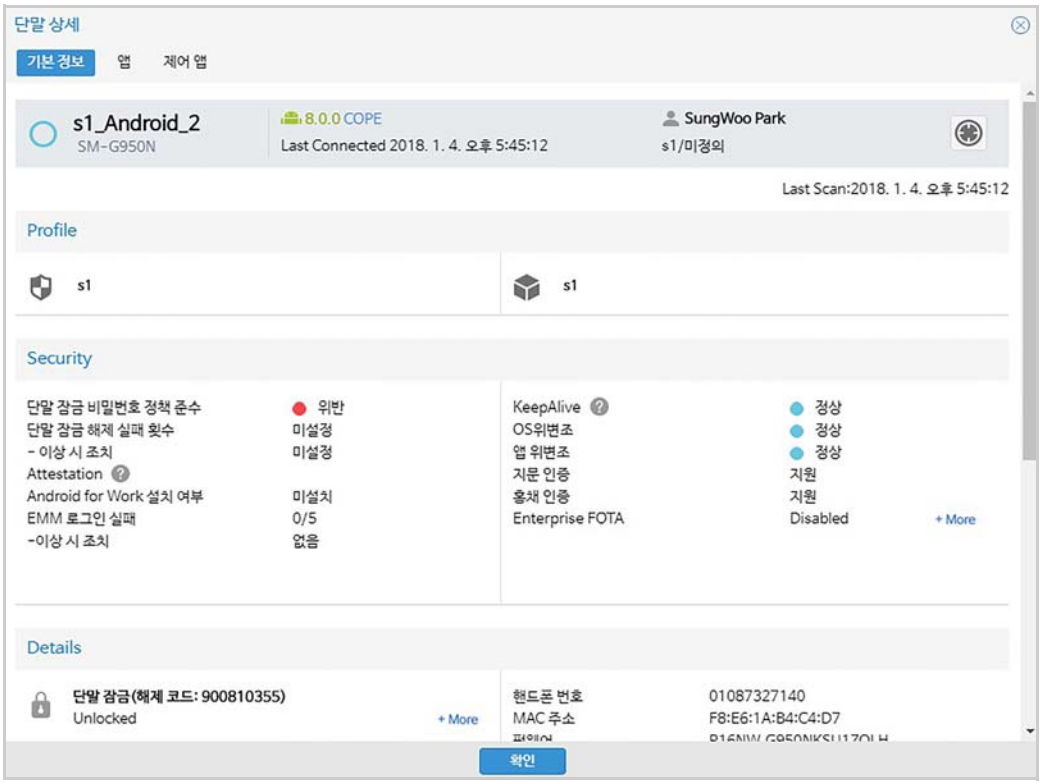
마지막 단말제어는 단말제어 전송이 완료된 경우 파란색 , 진행 중인 경우 검정색으로 표시됩니다 . 단말 상태에 대한 자세한 내용은 108 페이지 8 장의 “ 단말 상태 " 를 참고하세요 .

단말 상세 정보 보기

활성화 또는 활성화금지 상태인 단말의 기본 정보, 단말에 설치된 앱 정보와 제어 앱 정보를 **단말 & 사용자 > 단말**의 단말 상세 창에서 확인합니다.

기본 정보

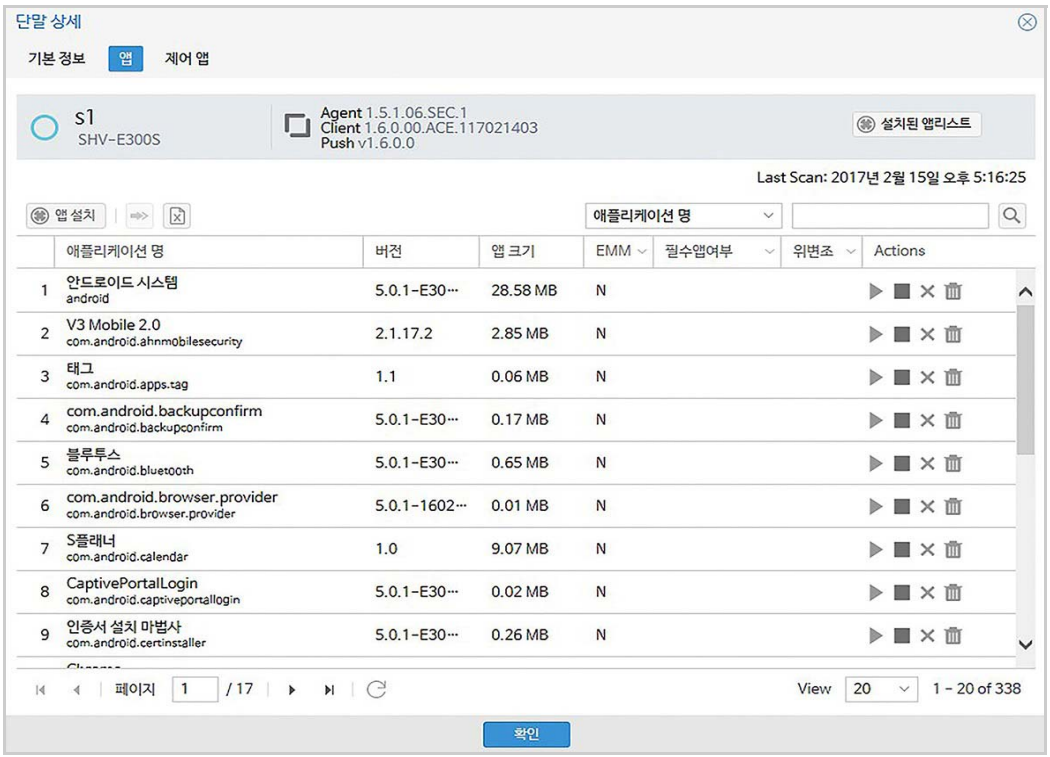
보안 관련 정보, 단말에 적용된 프로파일, 네트워크, 단말 위치 정보 및 SDK 설치 정보 등이 표시됩니다. 단말 플랫폼별 기본 정보는 107 페이지의 " 플랫폼별 단말 정보 " 와 동일합니다.



- **단말 제어:** ⚙을 클릭한 후 원하는 단말 제어 명령을 전송하세요.
  단말 제어 전송에 대한 자세한 내용은 128페이지의 "단말 제어하기"을 참고하세요.
- **Profile**: 프로파일명 클릭 시, 단말에 적용된 단말관리 프로파일과 앱관리 프로파일의 상세 정보가 보여집니다.
- **KeepAlive**: 주기적으로 단말과 서버의 연결 상태 정보를 제공합니다. 단말을 분실했거나 데이터 연결에 실패한 경우, KeepAlive는 강력하게 단말을 보호합니다. 설정한 시간을 초과하는 경우, 단말은 잠금 상태가 되거나 초기화됩니다.
  - 단말과 서버가 연결되어 있을 경우 파란색 동그라미, 아닌 경우 빨간색 동그라미로 보여집니다. 회색 동그라미는 **설정 > 서비스 > 환경설정**에서 KeepAlive가 설정되지 않은 경우(0)입니다.
  - KeepAlive 설정 관련 자세한 내용은 26페이지 2장의 “KeepAlive 설정하기"를 참고하세요.

앱 정보

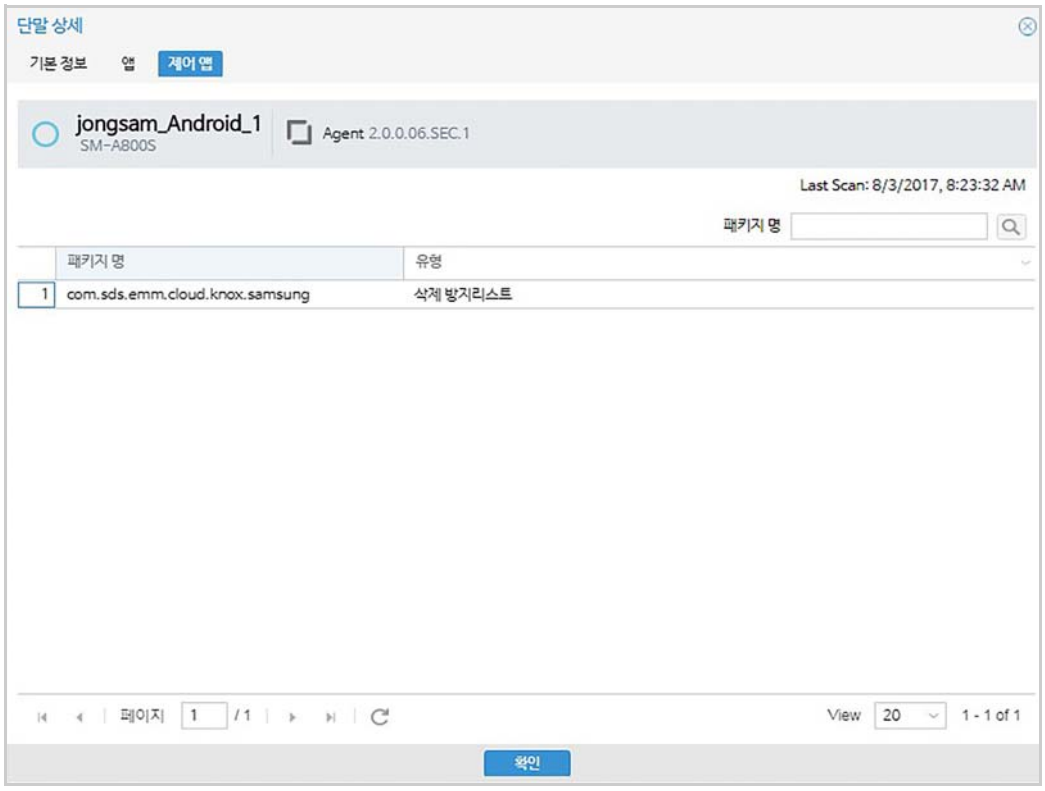
단말의 EMM 버전 정보와 애플리케이션 정보를 조회할 수 있으며 엑셀 파일로 저장할 수 있습니다 .



- 필수앱 여부 확인
- 앱 위변조 여부 확인
- 앱 실행/중지/데이터제거/삭제 명령 전송
- 단말에 사내 앱 설치 및 삭제 후 설치
- iOS의 경우는 설정 정보 조회, 피드백 조회 가능
  - : 설정 정보, : 피드백 조회
- Knox 컨테이너 및 Android for Work이 설치된 단말의 경우, 단말 ID 옆의 ▼를 클릭한 후 컨테이너를 선택합니다.
  - Android for Work 단말에는 앱 설치/실행/삭제 등 앱관련 단말제어 명령을 전송할 수 없습니다.
  - EMM 항목의 Y는 EMM 애플리케이션을 의미합니다.

제어앱 정보

단말에 설치된 화이트 / 블랙 리스트 애플리케이션 정보를 조회할 수 있습니다 .



- 단말 EMM 애플리케이션의 버전
- 애플리케이션 패키지명
- 화이트/블랙 리스트 유형
- 해당 애플리케이션이 설정된 이벤트 (iOS)

단말 프로파일 상세 보기

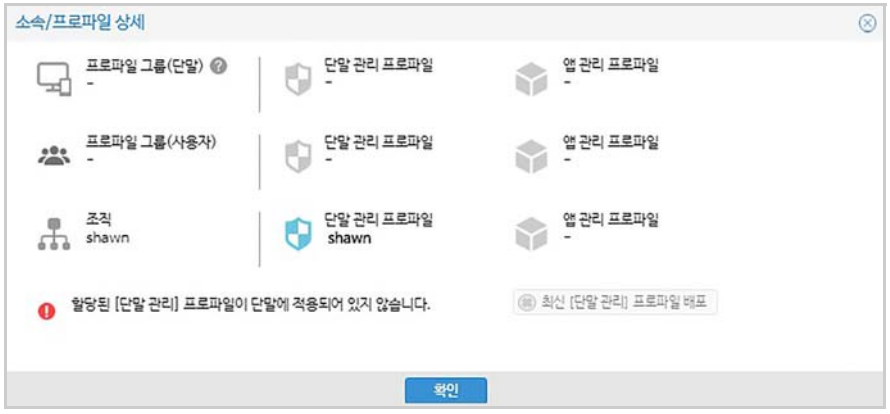
단말이 속한 그룹 및 조직 정보와 적용된 프로파일의 상세 정보를 조회할 수 있습니다 . 적용된 프로파일은 단말 목록에 프로파일 할당 , 미할당 , 부분할당으로 구분하여 표시되며 , 프로파일명 클릭 시 상세 정보로 이동합니다 .

단말 프로파일은 프로파일 그룹 (단말) > 프로파일 그룹 (사용자) > 조직의 순서로 우선 순위가 높은 정책만 적용됩니다 . 단말 프로파일 상세 정보에서 확인 후 , 활성 단말에 미적용 프로파일이 있는 경우 최신 단말관리 프로파일 배포 단말 제어를 전송할 수 있습니다 .

단말에 적용된 프로파일의 상세 정보를 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.

3. 해당 단말의 **소속/프로파일** 항목을 클릭하세요.



4. 프로파일 상세 정보를 보려면 프로파일명을 클릭하세요.
5. 활성 단말에 미적용 프로파일이 있는 경우, **최신/단말관리 프로파일 배포**를 클릭하세요.
6. **확인**을 클릭하세요.

단말 애플리케이션 관리하기

단말 제어 명령을 전송하여 단말에 설치된 앱 리스트를 확인할 수 있습니다 . 운영자는 단말에 설치된 비활성화 상태의 애플리케이션을 활성화 상태로 변경할 수 있으며 , 단말에서 더 이상 사용하지 않는 애플리케이션과 관련 테이터를 삭제할 수 있습니다 .

Note: 사용자가 Knox 컨테이너의 EMM과 Push Agent를 삭제한 경우 재설치는 불가능합니다. Knox 컨테이너를 삭제한 후 다시 생성해야 합니다.

단말에 애플리케이션 설치하기

사용자 단말에 설치된 애플리케이션을 업데이트하거나 삭제한 후 재설치할 수 있습니다 . iOS 단말의 경우 , 업데이트는 안되며 삭제 후 설치만 가능합니다 . 애플리케이션 설치를 위한 단말 제어 명령을 전송합니다 . EMM 서버에 새로운 버전의 애플리케이션이 있는 경우 단말은 자동으로 업데이트합니다 .

단말에 애플리케이션을 설치하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.
3. 단말의 **모바일 ID** 항목을 클릭하세요.
4. "단말 상세" 창에서 **앱** 탭을 클릭하세요.

5. **사내/Kiosk 앱 설치**를 클릭하세요.
   iOS 단말의 경우 **앱 설치**를 클릭하세요.
6. 설치 유형을 **설치 및 업데이트**와 **삭제 후 설치** 중에서 선택하세요.
7. 설치하려는 애플리케이션을 선택하세요.
8. **확인**을 클릭하세요.
9. 확인 팝업 메시지가 나타나면 **예**를 클릭하세요.

단말 애플리케이션 삭제하기

단말에 설치된 애플리케이션을 삭제할 수 있습니다 . 애플리케이션 뿐만 아니라 관련된 데이터도 삭제할 수 있습니다 . 단 , iOS 단말의 경우 데이터는 삭제할 수 없습니다 . EMM 애플리케이션 삭제에 대한 자세한 내용은 234 페이지의 " EMM 애플리케이션 삭제하기 " 를 참고하세요 . 사용자 단말의 Knox 영역에서 EMM 과 Push Agent 가 삭제되면 사용자는 재설치할 수 없습니다 . 재설치하려면 Knox 를 삭제하고 다시 설치해야 합니다 . EMM 애플리케이션 삭제에 대한 자세한 내용은 235 페이지의 " EMM 애플리케이션 삭제 및 위변조 방지하기 " 를 참고하세요 .

단말의 애플리케이션을 삭제하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.
3. 단말의 **모바일 ID** 항목을 클릭하세요.
4. "단말 상세" 창에서 **앱** 탭을 클릭하세요.
5. 애플리케이션 데이터를 삭제하려면 을 클릭하세요.
   애플리케이션을 삭제하려면 을 클릭하세요.
6. 삭제 확인 팝업 메시지가 나타나면 **예**를 클릭하세요.

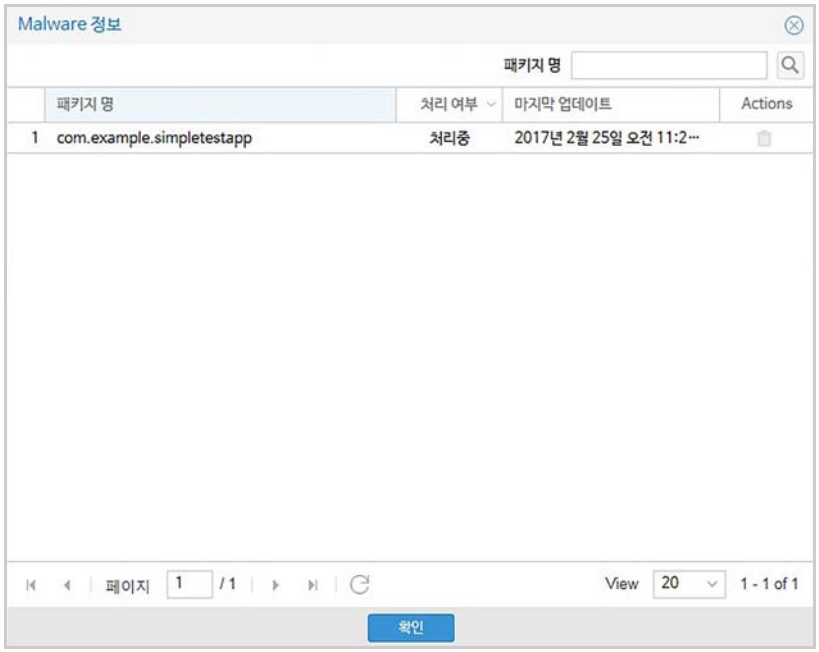
악성앱 (Malware) 삭제하기

악성앱 정보는 단말 목록에서 확인 가능하며 삭제 할 수 있습니다 . 삭제 방지된 악성 앱은 삭제할 수 없습니다 .

단말의 악성앱을 삭제하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.

3. 단말의 **Malware** 항목을 클릭하세요.



4. "Malware 정보" 창에서 앱을 선택한 후 을 클릭하세요.
5. 확인 팝업 메시지가 나타나면 **예**를 클릭하세요.

단말 애플리케이션 실행/종료하기

단말 제어 명령을 전송하여 단말에 설치된 애플리케이션을 실행 또는 종료시킵니다 .

Android 와 Wearable 단말만 가능합니다 .

단말의 애플리케이션을 실행 또는 종료하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.
3. 단말의 **모바일 ID** 항목을 클릭하세요.
4. "단말 상세" 창에서 **앱** 탭을 클릭하세요.
5. 애플리케이션을 실행하려면 을 클릭하세요.
   중지하려면 을 클릭하세요.
6. 확인 팝업 메시지가 나타나면 **예**를 클릭하세요.

단말에 설치된 앱목록 가져오기

단말에 설치된 앱 목록을 갱신하기 위해 단말 제어 명령을 전송하려면 , 다음의 절차를 따르세요 .

1. **단말 &사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.

3. 단말의 **모바일 ID** 항목을 클릭하세요.
4. "단말 상세" 창에서 **앱** 탭을 클릭하세요.
5. **설치된 앱리스트**를 클릭하세요.
6. "단말제어 - 설치된 앱 리스트" 창이 나타나면 **확인**을 클릭하세요.
7. 성공 안내 팝업 메시지가 나타나면 **확인**을 클릭하세요.

iOS 단말의 애플리케이션 피드백 삭제하기

단말 제어 명령을 전송하여 iOS 단말의 애플리케이션 관련 피드백을 삭제하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.
3. 단말의 **모바일 ID** 항목을 클릭하세요.
4. "단말 상세" 창에서 **앱** 탭을 클릭하세요.
5. **설치된 앱리스트**를 클릭하세요.
6. "단말제어 - 설치된 앱 리스트" 창에서 **관리되는 앱 피드백 삭제**를 클릭하세요.
7. 성공 메시지가 나타나면 **확인**을 클릭하세요.

단말 상태 변경하기

단말 상태 변경 시 관련 단말 제어 명령이 전송됩니다. 단말의 현재 상태에 따라 다음과 같이 변경 가능합니다 .

- : 단말 제어 전송 또는 오프라인 인증의 방법으로 단말의 상태를 비활성화합니다.
  - **관리자차단** 선택 시, 활성화 상태의 단말을 단말 통신 없이 관리자차단 상태로 변경할 수 있습니다.
- : **단말 제어**와 **상태만 변경** 중 선택하여 단말 상태를 비활성화로 변경합니다.
  - 단말 제어: 단말에 비활성화 단말 제어 명령을 전송합니다.
  - 상태만 변경: 단말 통신 없이 서버의 단말 상태만 비활성화로 변경합니다.
- : 단말의 활성화 금지 상태를 비활성로 변경합니다.
- : 단말의 상태를 활성화 금지로 변경합니다.
- : 단말의 상태를 비활성으로 변경합니다.
- : 단말 제어 또는 상태만 변경 중 선택하여 단말 상태를 비활성화로 변경합니다.
  - 단말 제어: 단말에 비활성화 단말 제어 명령을 전송합니다.
  - 상태만 변경: 단말 통신 없이 서버의 단말 상태만 비활성화로 변경합니다.

단말과 서버의 단말 상태가 불일치하는 경우 , 관리자 차단 상태로 변경하게 되면 단말 통신 없이 단말 상태가 비활성화 또는 활성화 금지 상태로 변경됩니다 . 단말과 서버의 단말 상태가 불일치한 단말이 서버에 통신을 요청한 경우 , 해당 단말의 EMM Agent 는 비활성화되며 audit 기록은 남지 않습니다 .
단말 비활성화 시에 Android 단말에 설치된 사내 앱과 iOS9 이상 단말의 EMM 관련 모든 앱이 자동 삭제되도록 설정할 수 있습니다 . 자동으로 삭제되도록 하려면 **설정 > 서비스 > 환경 설정**의 **Unenrollment 시 앱 삭제**를 **사용**으로 설정합니다 .

단말 상태를 변경하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. 변경하고자 하는 단말의 **상태** 항목을 클릭하세요.
3. 상태 변경 확인 팝업 메시지가 나오면 **예**를 클릭하세요.

오프라인 비활성화하기

EMM 과 통신이 불가능한 상황에서 사용자가 단말 내 EMM 을 직접 비활성화하여 삭제할 수 있습니다 . 비활성화 인증 코드는 전화 등 유선상의 방법으로 사용자에게 전달하여 사용자가 직접 해당 코드를 입력하여 비활성화를 수행합니다 . 활성화 상태의 Android 단말만 가능합니다 . 사용자가 오프라인 비활성화 인증 코드를 입력하는 방법에 대한 자세한 내용은 “Samsung SDS EMM 사용자 매뉴얼 ” 을 참고하세요 .

사용자가 단말 비활성화를 하기 위한 인증 코드 안내는 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. 비활성화하고자 하는 단말의 **상태 아이콘**을 클릭하세요.
3. “상태 변경” 창에서 **오프라인 인증**을 클릭하세요.
4. 단말 사용자에게 전화를 통해 **오프라인 비활성화 인증 코드**를 안내하세요.
5. 사용자는 단말에 **오프라인 비활성화 인증 코드**를 입력하세요.
6. 사용자가 단말에 인증코드를 입력한 후, **확인**을 클릭하세요.
   - 단말 비활성화 제어 명령이 단말로 전송됩니다.

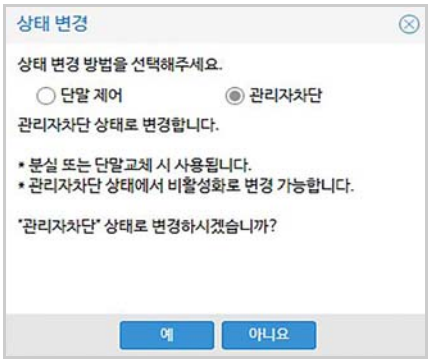
관리자차단 상태로 변경하기

사용자가 단말을 분실하거나 단말을 교체한 이후에도 서버의 단말 상태가 활성화 상태로 남아있을 수 있습니다 . 이 경우 운영자는 관리자차단 상태로 변경하여 단말의 보안을 유지합니다 . 관리자차단 상태로 변경하면 단말과의 통신없이 서버의 단말 상태만 변

경됩니다 . 관리자차단 상태의 단말을 비활성화시킬 수 있습니다 .

단말 상태를 관리자차단 상태로 변경하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. 활성 상태 단말의 **상태** 항목의 아이콘을 클릭하세요.



3. “상태 변경” 창에서 **관리자차단**을 클릭하세요.
4. **예**를 클릭하세요.

단말상태 변경이력 확인하기

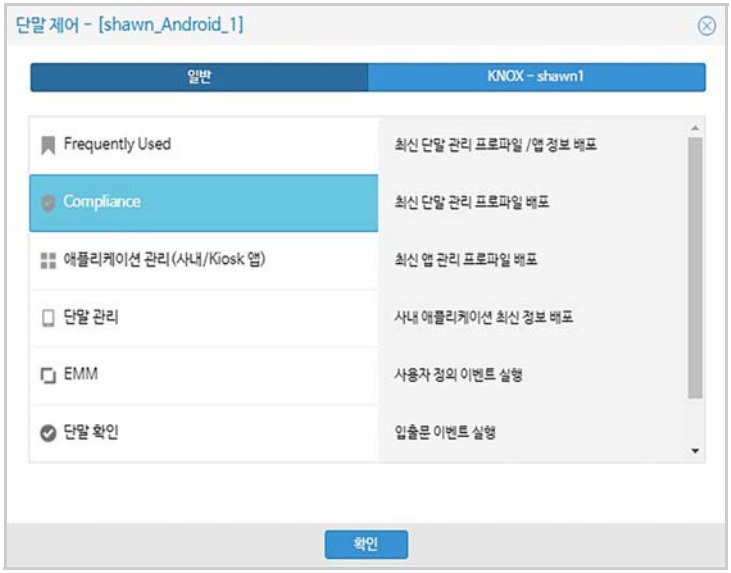
단말의 EMM Agent, 관리자 , 시스템이 수행한 단말 상태 변경을 일자별로 조회할 수 있습니다 . 비활성 시 사용된 오프라인 비활성화 인증코드는 Android 와 Wearable 단말의 경우에만 표시됩니다 .

단말 상태의 변경 이력을 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. 단말의 **마지막 업데이트** 항목을 클릭하세요.

단말 제어하기

사용자 , 조직 , 그룹 , 단말별로 여러 대의 활성화 단말에 제어 명령을 보낼 수 있습니다 . Knox 컨테이너 사용 단말의 경우 Knox 컨테이너를 선택한 후 제어합니다 .



단말 제어 명령 중 가장 자주 쓰이는 것들을 Frequently Used 영역에서 빠르게 선택할 수 있습니다 . 마지막 전송된 단말 제어를 단말 목록에서 확인할 수 있습니다 . 단말에 정상적으로 전송되지 못한 단말 제어 내역은 **서비스 현황 > 미처리 단말 제어**에서 확인할 수 있습니다 . 미처리 단말 제어 확인은 **설정 > 서비스 > 환경 설정**의 **단말 제어 방식**이 **Queue** 로 설정된 경우에만 가능합니다 . 단말 제어 명령별 전송 방법에 대한 자세한 내용은 431 페이지 18 장의 " 단말 제어 전송 방법 " 을 참고하세요 .

단말 제어 명령 보내기

단말 , 사용자 , 조직 , 그룹별로 단말을 제어하기 위하여 다음의 절차를 따르세요 .

1. 전송 대상에 따라 **단말 & 사용자 > 단말/ 사용자 & 조직/그룹**으로 이동하세요. 단말에 전송하려면, **단말 & 사용자 > 단말**로 이동하세요.
2. 제어하려는 단말을 검색한 다음 단말 제어 명령을 선택한 후 을 클릭하세요.
   - Knox 컨테이너를 사용하는 단말의 경우, 상단의 일반▼ 을 클릭한 후 Knox 컨테이너를 선택하세요.
3. "단말 제어" 창에서 명령을 선택한 후 **확인**을 클릭하세요.
4. **확인**을 클릭하세요.
5. 확인 팝업 메시지가 나타나면 **확인**을 클릭하세요.

단말 전송 단말제어 이력 조회하기

일자별로 전송된 단말제어 및 관련 audit 내역을 조회할 수 있습니다 . Audit 내역에서 단말에 전송된 단말 제어의 처리 성공 여부와 실패 상세 내역을 볼 수 있습니다 .

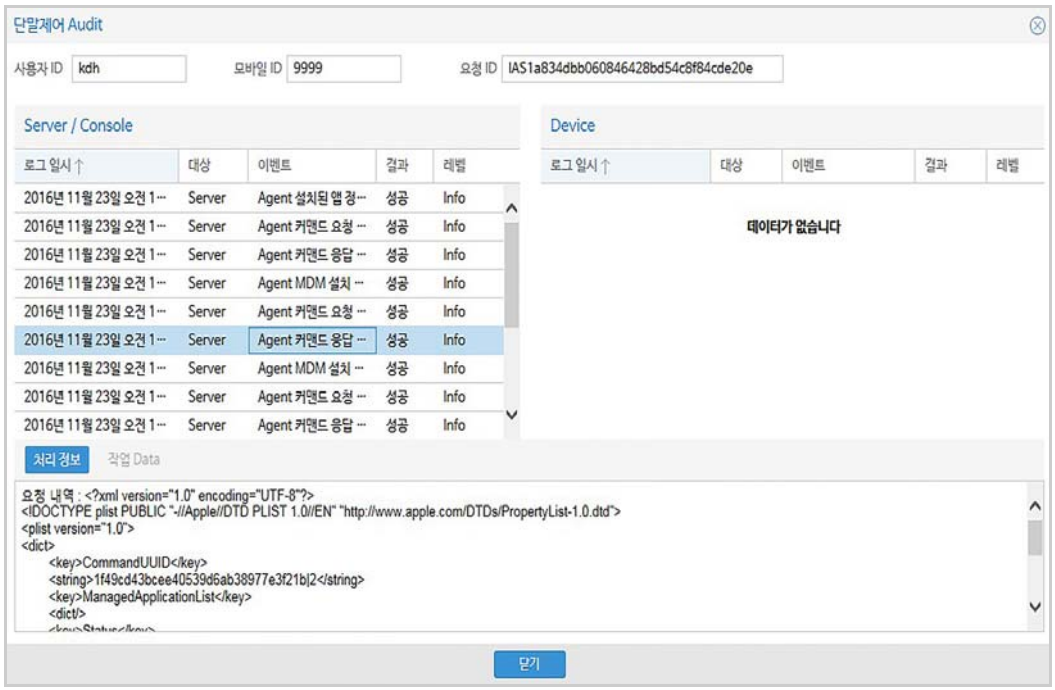
- Audit 로그 항목에 대한 자세한 내용은 58페이지 3장의 “단말 제어 Audit 조회하기"를 참고하세요.
- 동일한 내용을 **서비스 현황 > 로그 > Audit 로그**에서도 확인할 수 있습니다.

단말에 전송된 단말 제어의 내역을 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.
3. 단말의 **단말 이력** 항목의 을 클릭하세요.
4. **단말 제어** 탭을 클릭하세요.
5. 단말 제어 audit 결과를 조회하려면 **단말제어 타입**을 클릭하세요.

단말 실행 단말제어 이력 조회하기

“ 단말 제어 Audit” 창과 동일한 내용을 **서비스 현황 > 로그 > Audit 로그**에서도 확인할 수 있습니다 . 자세한 내용은 58 페이지 3 장의 “ 단말 제어 Audit 조회하기 " 를 참고하세요 .



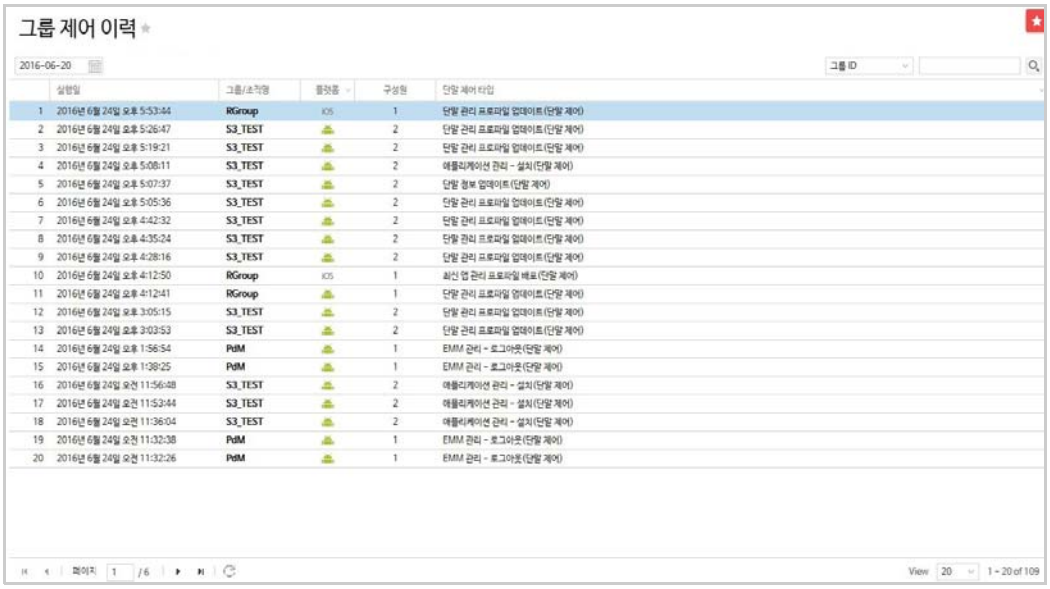
단말에서 실행된 단말 제어 이력을 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 이력 > 단말 제어 이력**으로 이동하세요.
2. **사용자 ID** 또는 **모바일 ID**를 입력한 후 을 클릭하세요.

3. 단말 제어 Audit의 상세 내역을 조회하려면 **단말 제어 타입** 항목을 클릭하세요.

그룹별 단말제어 이력 조회하기

그룹별 단말 제어 전송 이력을 조회하려면 다음의 절차를 따르세요 .



1. **단말 & 사용자 > 이력 > 그룹 제어 이력**으로 이동하세요.
2. **일자**, **그룹 ID**, **조직명**을 입력한 후 을 클릭하세요.
3. **그룹/조직명**을 클릭하세요.

단말 진단 로그 보기

단말의 진단 정보를 수집하거나 , 단말 잠금 또는 잠금 해제가 발생한 경우 관련 내용을 조회하고 다운로드할 수 있습니다 .

- 단말 진단 정보: 운영자가 단말 상태를 파악하려면 단말제어를 전송한 후 단말 진단 정보를 수집할 수 있습니다. 단말이 정상적으로 단말제어를 수신하면, 서버 관련 audit로그와 단말로그가 기록됩니다. 상세내용은 파일을 다운로드한 후 확인합니다. 단말 진단을 위한 audit 이벤트 목록의 자세한 내용은 54페이지 3장의 “Audit 이벤트"를 참고하세요.
- 단말 잠금/잠금해제 이력: 단말 위변조 사항 발견 시 단말은 자동으로 잠기게 됩니다. 이 경우 정책 위반 사유 미해결 상태에서 잠금 해제 명령을 전송하면 단말 잠금 상태를 해제할 수 있습니다. 단말 잠금 혹은 해제 시 이력 데이터를 audit 로그에 기록합니다.

단말 진단 로그 내역과 단말 잠금 이력을 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.

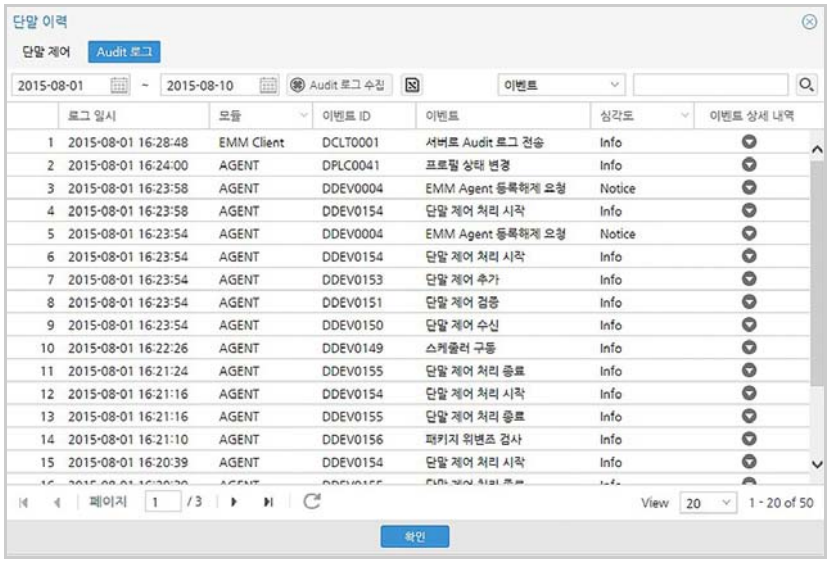
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.
3. 단말 진단 항목의 을 클릭한 후 "단말 진단" 창에서 진단 정보 탭을 선택하세요.
4. 진단 정보 **수집일**을 입력한 후 **진단 리스트**와 **진단 상세**를 확인하세요.
5. **확인**을 클릭하세요.

단말의 audit 로그 수집하기

활성 상태 단말의 Audit 로그를 수집하고 엑셀 파일로 저장할 수 있습니다 .

단말의 Audit 로그를 수집하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 을 클릭하세요.
3. 단말의 을 클릭한 후 "단말 이력" 창의 **Audit 로그** 탭을 클릭하세요.



4. 활성 단말의 로그를 수집하려면 **Audit 로그 수집**을 클릭하세요.
   단말에 로그 수집 단말 제어 명령이 전송됩니다.
5. 단말 Audit 로그를 Excel 파일로 저장하려면, 상단의 을 클릭하세요.

메시지 보내기

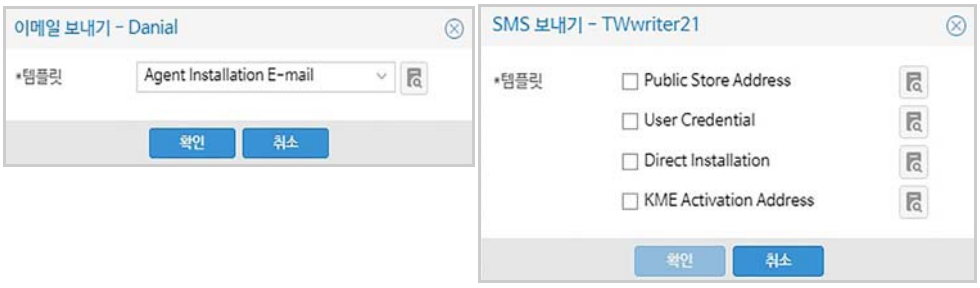
사용자 정보에 등록된 메일 주소 또는 전화번호로 이메일이나 메시지를 발송할 수 있습니다 . EMM 의 메시지 서비스는 SMTP 메일 전송 서비스를 사용하기 때문에 , 실제 메일이 수신자에게 전달되었는지는 알 수 없습니다 . 메일 발송 성공은 SMTP 서버까지 성공적으로 전달되었음을 의미합니다 . SMS 전송 시 , SMS 발송 여부만 EMM 서버에 기록되며 SMS 가 사용자 단말에 발송되었는지는 알 수 없습니다 .

메시지 발송 시 **설정 > 서비스 > 메시지 템플릿**에 등록된 템플릿을 이용합니다 .

사용자가 메시지를 수신하지 못한 경우 , 입력된 메일 주소나 전화번호가 정확한지 확인합니다 . 사용자 계정 정보에 이메일 주소나 전화번호가 등록되지 않은 경우 , 발송 버튼은 비활성화 됩니다 .

사용자에게 이메일이나 SMS 메시지를 보내려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직도에서 원하는 조직을 클릭하거나 검색 키워드를 입력한 후 을 클릭하세요.
3. 사용자의 또는 을 클릭하세요.



4. “이메일 보내기” 또는 “SMS 보내기” 창에 템플릿을 선택한 후 **확인**을 클릭하세요.

QR 코드 전송하기

EMM 은 사용자의 단말 활성화에 필요한 정보를 QR 코드로 생성하여 제공합니다 . QR 코드는 EMM 의 Tenant ID, 사용자 ID, 단말 ID, EMM 도메인 정보로 구성됩니다 .

운영자는 사용자에게 이메일로 QR 코드를 전송합니다 . 단말 사용자는 수신 이메일의 QR 코드를 단말의 EMM 초기 화면에 입력하여 활성화시킵니다 . 메일 발송 전에 QR 코드 전송 템플릿을 EMM 관리자 포털의 **설정 > 서비스 > 메시지 템플릿**에 먼저 등록합니다 . 메일 템플릿 등록 및 관리는 50 페이지 2 장의 “ 메시지 템플릿 관리하기 " 를 참고하세요 .

이메일을 통해 QR 코드를 전송하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 조직도에서 원하는 조직을 클릭하거나 검색 키워드를 입력한 후 을 클릭하세요.
   - 이메일 주소가 등록된 사용자만 이 활성화됩니다.
3. 사용자의 을 클릭하세요.
4. “이메일 보내기-사용자명”창에서 **템플릿**을 선택하세요.
5. 템플릿의 상세 정보를 조회하려면 을 클릭하세요.
6. “메시지 템플릿 조회”장에서 **확인**을 클릭하세요.
7. “이메일 보내기-사용자명”에서 **확인**을 클릭하세요.

8. 발송 확인 메시지 창에서 **예**를 클릭하세요.
   메일 관련 설정이 유효하지 않은 경우 경고 메시지가 나타납니다.

메시지 발송 이력 조회하기

사용자에게 발송한 SMS 와 이메일 정보를 조회합니다 . 메시지 전송 중 발생한 오류 내역은 서버 전송 결과 항목에서 확인할 수 있습니다 .

- SMTP 메일 전송 서비스를 사용하기 때문에, 실제 메일이 수신자에게 전달되었는지는 알 수 없습니다. 메일 발송 성공은 SMTP서버까지 성공적으로 전달되었음을 의미합니다.
- SMS 전송 시, SMS 발송 여부만 EMM 서버에 기록되며 SMS가 사용자 단말에 발송되었는지는 알 수 없습니다

이메일 또는 SMS 메시지 발송 이력을 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 이력 > 메시지 발송 이력**으로 이동하세요.
2. **수신인 ID**, **이메일, 전화번호**를 입력한 후 을 클릭하세요.이력의 다음 항목들을 확인하세요.
   - **로그일시**: 메일을 발송한 날짜와 시각
   - **제목**: 클릭 시 전송된 메일의 상세 내용 조회
   - **수신인 ID**: 메일 수신자의 사용자 ID
   - **발송 방법**: 발송된 방법, SMS 또는 이메일
   - **이메일/전화번호**: 발송된 이메일 또는 전화번호
   - **서버 전송 결과**: 메일의 SMTP 서버 전송 성공 여부
     - 전송 실패 메시지를 클릭하면 “상세 로그” 창에서 발송 실패 원인을 확인할 수 있습니다.
   - **발신인**: 발신한 운영자의 관리자 포털 로그인 ID

10 프로파일

EMM 은 카메라 , 스크린 캡처 , 마이크 , Wi-Fi, 블루투스 , GPS 등에 대한 단말 제어 정책과 분실에 대응하기 위한 비밀번호 , 공장 초기화 등과 같은 보안 정책을 프로파일에 설정하여 사용자 단말을 관리합니다 .

방문자 라이선스가 있는 경우 , 방문자 단말을 제어하기 위한 정책 프로파일을 방문자 관리 콘솔에 미리 설정하여 제공합니다 . 일반 사용자를 위한 정책과 마찬가지로 플랫폼별 (Android/iOS) 정책을 설정합니다 .

EMM 은 단말을 제어하기 위해 프로파일에 정의된 각종 정책 및 설정을 단말에 전송합니다 . 조직이나 그룹에 프로파일을 할당한 후 , **적용** 버튼을 클릭하여 프로파일을 배포하거나 **최신 단말 관리 프로파일 / 앱 정보 배포** 단말 제어 명령을 전송합니다 . 단말 제어 명령을 전송하는 방법은 128 페이지 9 장의 " 단말 제어 명령 보내기 " 를 참고하세요 .

프로파일은 다음의 두가지로 구성됩니다 .

- **단말 관리 프로파일:** 단말 플랫폼 별로 단말 제어 기능, 정책 스케줄 기능 등을 제공합니다. 단말 관리 프로파일은 단말 플랫폼, Knox, 이벤트로 구분되어 있으며, 해당 정책과 설정을 등록할 수 있습니다.
  - **정책**: 단말 기기에 대한 제어와 단말 설치 애플리케이션 및 데이터 제어를 위한 정책을 설정합니다. 단말의 EMM 영역에서 개인 영역으로의 데이터 유출을 방지하기 위해, 문자열 복사와 화면 캡처 기능을 제어할 수 있고 애플리케이션별 필수 설치 여부를 설정할 수 있습니다. 또한 Google이 제공하는 Android for Work 앱의 화면 캡처 및 문자열 복사 기능을 제어할 수 있습니다.
  - **설정**: 사용자가 단말에서 Wi-Fi, VPN, 인증서, 사내 메일 사용을 위한 Exchange 등을 사용할 수 있도록 하기 위한 기본 설정 항목을 등록합니다. 네트워크 관련 설정 및 인증서 설정을 포함한 프로파일을 할당받은 단말의 사용자는 단말에서 간단한 설정 과정을 통해 회사의 네트워크를 이용할 수 있게 됩니다. EMM은 이를 위해 인증서, Directory 서비스를 연동하여 사용자 인증을 하게 됩니다.
- **앱 관리 프로파일**: 애플리케이션, Android for Work, EMM Client의 비밀번호 정책, Secure Browser, mMail, SecuCamera, Knox Portal 등의 애플리케이션에 대한 제어 기능을 제공합니다.

하나의 단말이 여러 관리 단위에 소속되어 있을 경우 우선순위에 따라 전송될 프로파일이 결정됩니다 . 정책 및 설정에 대한 프로파일이 적용되는 우선순위는 다음과 같으며 , 그룹이 조직보다 우선순위가 높습니다 .

- 프로파일 그룹(단말) > 프로파일 그룹(사용자) > 조직

프로파일 만들기

EMM 프로파일은 신규로 등록하기 , 구성요소로 등록하기 , 프로파일을 Export 하여 파일로 저장한 후 Import 하여 생성할 수 있습니다 . 구성요소를 사용하는 방식으로 프로파일을 생성하는 경우 , 구성요소를 먼저 생성해야 합니다 . 등록한 프로파일은 수정 및 삭제할 수 있습니다 . 설정 삭제 시 , 단말의 Trusted Anchor Database 에서 해당 설정에서 등록된 인증서는 삭제됩니다 . Android 와 Knox 플랫폼의 경우 삭제하는 VPN 설정이 Cisco AnyConnect, StrongSwan 인 경우 , VPN 설정삭제 후 사용자 단말을 재부팅해야 합니다 .

신규 프로파일 등록하기

신규로 단말 관리 프로파일 또는 앱 관리 프로파일을 등록하려면 다음의 절차를 따르세요.

1. **프로파일 > 단말 관리 프로파일/앱 관리 프로파일**로 이동하세요.
2. ➕을 클릭한 후, **신규 등록**을 클릭하세요.
3. “신규 등록” 창에서 **프로파일명**과 **설명**을 입력하세요.

   - 이미 존재하는 프로파일과 동일한 프로파일명을 입력할 경우, 중복 알림 팝업 확인 메시지가 나타납니다.
   - 프로파일이 추가된 이후 프로파일명은 수정할 수 없습니다.
4. **다음**을 클릭하세요.
5. 확인 메시지가 나타나면, **예**를 클릭하세요.
6. 프로파일의 상세 설정 방법은 다음을 참고하세요.
   - 141페이지의 "단말 관리 프로파일 정책 설정하기"
   - 144페이지의 "단말 관리 프로파일 설정 추가하기"
   - 181페이지의 "앱 관리 프로파일 설정하기"
   - 191페이지의 "11 Knox 컨테이너"
   - 208페이지의 "12 이벤트"
7. 프로파일의 설명을 수정하려면 “단말 관리 프로파일” 창에서 프로파일명 옆의 ✏을 클릭하세요. 설명을 입력하고 저장을 클릭하세요.

8. 설정한 정책 및 설정을 조회하려면 “단말 관리 프로파일” 창에서 프로파일명 옆의 **프로파일 정책**을 클릭하세요. 플랫폼별 상세 정책이 조회됩니다.

구성요소 방식의 프로파일 등록하기

단말 관리 프로파일 또는 앱 관리 프로파일을 구성요소 등록 방식으로 생성합니다 . 생성된 프로파일에 여러 구성요소를 조합하여 사용할 수 있습니다 . 구성요소 사용을 위해서는 **프로파일 > 단말 관리 프로파일 구성요소 / 앱 관리 프로파일 구성요소**에 구성요소가 등록되어 있어야 합니다 . 구성요소를 등록하는 방법은 142 페이지의 " 단말 관리 프로파일의 정책 구성요소 등록하기 " 와 144 페이지의 " 단말 관리 프로파일의 설정 구성요소 등록하기 " 를 참고하세요 .

구성요소 방식의 프로파일을 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일/앱 관리 프로파일**로 이동하세요.
2. ➕을 클릭한 후, **구성요소 등록**을 클릭하세요.
3. “구성요소 등록” 창에서 **프로파일명**과 **설명**을 입력하세요.

   - 이미 존재하는 프로파일과 동일한 프로파일명을 입력할 경우, 중복 알림 팝업 확인 메시지가 나타납니다.
   - 프로파일이 추가된 이후 프로파일명은 수정할 수 없습니다.
4. **다음**을 클릭하세요.
5. 확인 메시지가 나타나면, **예**를 클릭하세요.
6. 구성요소를 등록하려는 단말 플랫폼을 “단말 관리 프로파일”창의 왼쪽 메뉴에서 클릭하세요.
7. 정책 구성요소를 등록하려면, **Android/iOS/Windows/Tizen Wearable > 정책**으로 이동하세요.
   가. 📝을 클릭하면 정책 구성요소 목록이 “정책” 팝업 화면에 조회됩니다.
   나. **구성요소 명**을 검색하거나 조회된 목록에서 등록하려는 구성 요소를 선택한 후 **저장**을 클릭합니다.
   목록에서 구성요소 명을 클릭하면 설정된 정책 항목이 조회됩니다.
   다. 등록된 정책 목록이 조회됩니다.
8. 설정 구성요소를 등록하려면, **Android/iOS/Windows > 설정**으로 이동하세요.
   가. ➕를 클릭하면 설정 구성요소 목록이 “설정” 팝업 화면에 조회됩니다.

나. **구성요소 명**을 검색하거나 조회된 목록에서 등록하려는 구성 요소를 선택한 후 **저장**을 클릭합니다.
목록에서 구성요소 명을 클릭하면 설정된 설정 항목이 조회됩니다.

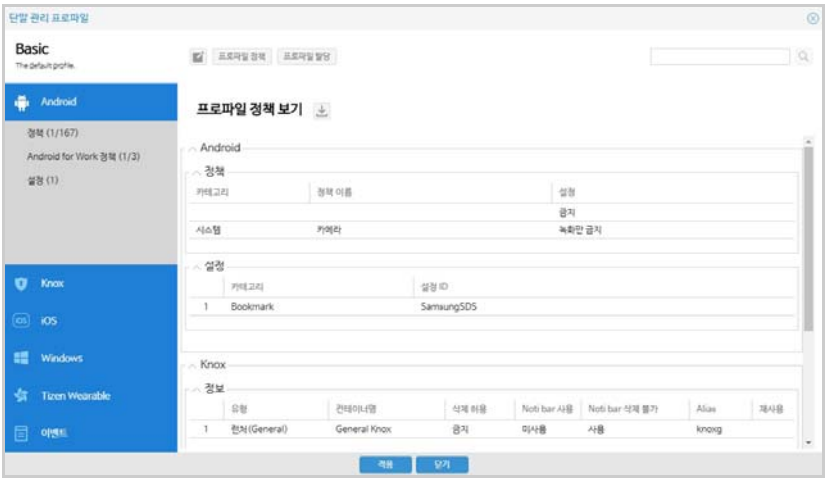
다. 등록된 설정 목록이 조회됩니다.

9. 구성요소 방식으로 등록된 단말 관리 프로파일은 구성요소 등록 항목이 Y로 표시됩니다.

프로파일 Export하기

등록된 프로파일을 Export 하여 파일로 저장한 후 , 동일 또는 다른 Samsung SDS EMM 서버에 해당 프로파일을 Import 하여 사용할 수 있습니다 . 구성요소로 등록한 프로파일은 Export 할 수 없습니다 . 프로파일을 Export 하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일/앱 관리 프로파일**로 이동하세요.
2. 프로파일 목록에서 Export하려는 프로파일명을 클릭하세요.
3. **프로파일 정책**을 클릭한 후 **프로파일 정책 보기** 우측의 을 클릭하여 파일을 Export하세요.



4. "확인" 창의 메시지를 확인하고 **예**를 클릭하면 로컬 PC에 저장됩니다.
   - Export된 단말 관리 프로파일은 .cea 파일로, 앱 관리 프로파일은 .cec 파일로 저장됩니다. 암호화된 내보내기 파일은 열람할 수 없으며 파일 등록을 통해서만 상세 내용 확인이 가능합니다.
   - 앱 관리 프로파일에의 애플리케이션, Android for Work, EMM Client의 Android 및 iOS 버전 제어, mMail 정보는 Export 되지 않습니다.

프로파일 Import하기

Export 된 파일을 Import 하여 단말 관리 프로파일을 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일/앱 관리 프로파일**로 이동하세요.
2. ➕을 클릭한 후, **파일 등록**을 클릭하세요.
3. "파일 등록" 창에서 **프로파일명**을 입력하고 파일을 선택한 후, **다음**을 클릭하세요.

4. "확인" 창에서 **예**를 클릭하세요.
   프로파일 목록에서 Import된 프로파일이 표시됩니다.
   - **Android/iOS/Windows/Knox 컨테이너 > 설정** 정보는 Import 되지 않습니다.
     그외 Import 되지 않는 정책은 다음과 같으며, 관리자는 추후 해당 항목들을 추가적으로 프로파일에 포함시켜야 합니다.

구분	정책
Android 정책	앱 • 앱 블랙/화이트 리스트 설정 Kiosk Wizard • Kiosk 앱 설정
iOS 정책	앱 • 앱 블랙/화이트 리스트 설정 • 자동 Single 앱 모드 허용 앱 목록 설정
Tizen Wearable 정책	앱 • 앱 블랙/화이트 리스트
Knox 정책	앱 • 앱 블랙/화이트 리스트 설정 • 앱 설치 권한 화이트 리스트 설정 • TIMA CCM 프로파일 앱 화이트리스트 설정 • 외장 SD 카드 사용 허용 앱 화이트리스트 설정 보안 • 비밀번호 정책 중 기업 ID 연동의 설치파일

Note: 향후 확장성을 고려하여 모든 정책과 설정 정보가 Export되지만, 사용자와 단말별 환경에 영향을 받는 정책과 설정 정보는 Import 제외 대상입니다.

조직 또는 그룹에 프로파일 할당하기

프로파일에 설정한 정책을 단말에 적용하려면 그룹 또는 조직에 프로파일을 할당해야 합니다. 프로파일을 할당하지 않아 제어할 수 없는 단말이 발생하는 것을 방지하기 위해, 최상위 조직인 회사 코드에 반드시 프로파일을 할당해야 합니다.

이미 프로파일이 할당된 그룹이나 조직에는 또 다른 프로파일을 할당할 수 없으며, 적용 중인 정책을 적용 취소하려면 그룹 또는 조직에 할당된 프로파일을 해제해야 합니다.

프로파일 > 단말 관리 프로파일 / 앱 관리 프로파일 조회 목록의 Actions 항목에서 또는 을 클릭하면 프로파일이 할당된 조직 또는 그룹을 확인할 수 있습니다.

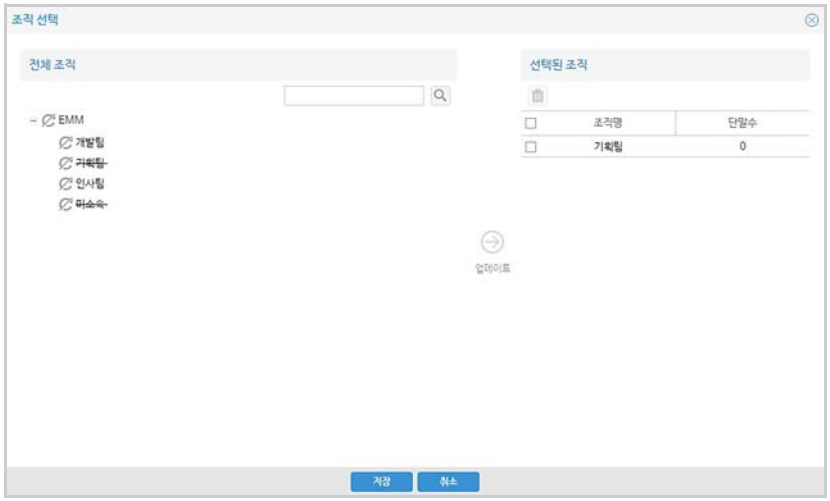
Note: 정책 및 설정 프로파일이 적용되는 우선순위는 그룹이 조직보다 우선순위가 높기 때문에 단말 관리 프로파일에 그룹 및 조직을 할당하는 경우 주의가 필요합니다.

- 프로파일 그룹(단말) > 프로파일 그룹(사용자) > 조직

프로파일을 조직에 할당하기

조직의 단말에 프로파일을 할당하려면 프로파일을 조직에 할당해야합니다. 프로파일을 조직에 할당하려면 다음의 절차를 따르세요.

1. **프로파일 > 단말 관리 프로파일/앱 관리 프로파일**로 이동하세요.
2. 프로파일 목록에서 조직을 할당할 프로파일 행의 을 클릭하세요.
3. 또는프로파일명을 클릭하면 "단말 관리 프로파일" 또는 "앱 관리 프로파일" 창이 나타납니다. 프로파일명 옆의 **프로파일 할당**을 클릭한 후 조직 옆의 을 클릭하세요. "조직 선택" 창의 **전체 조직**에서 해당 프로파일을 할당할 조직을 선택하고 을 클릭하세요.



- 하나의 프로파일을 여러 조직에게 할당할 수 있습니다.
- 조직은 하나의 프로파일만 할당받을 수 있으며, 이미 프로파일이 할당된 조직은 선택할 수 없습니다. 이미 프로파일이 할당된 조직에는 취소선이 그어져 있습니다.

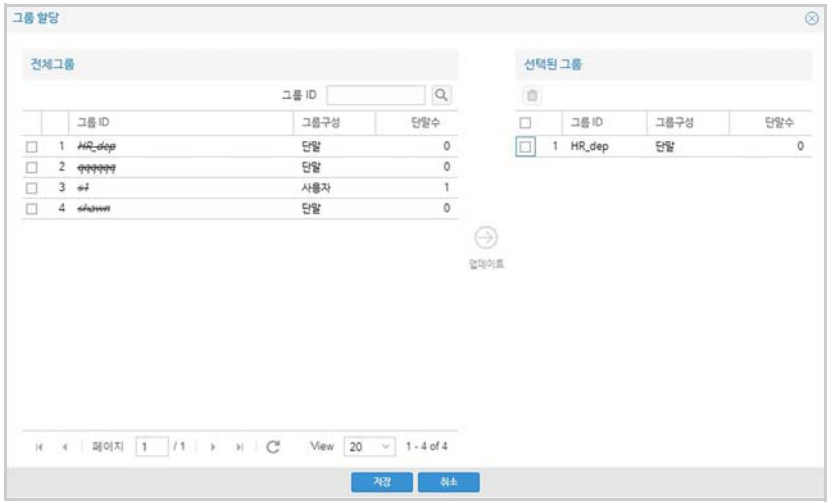
- **선택된 조직** 목록에서 프로파일을 해제할 그룹을 선택하고 을 클릭하면 해제됩니다.

4. **저장**을 클릭하세요.
5. 조직에 프로파일을 바로 배포하려면 "프로파일 배포" 팝업창에서 **예**를 클릭하세요.
6. 프로파일을 할당받은 조직에 설치된 Knox 컨테이너를 제어하려면, 194페이지 11 장의 "Knox 컨테이너 제어하기"를 참고하세요.

프로파일을 그룹에 할당하기

그룹의 단말에 프로파일을 할당하려면 프로파일을 그룹에 할당해야합니다 . 프로파일을 그룹에 할당하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일/앱 관리 프로파일**로 이동하세요.
2. 목록에서 그룹에 할당할 프로파일 행의 을 클릭하세요.
   - 또는 **단말 관리 프로파일**에서 프로파일명을 클릭하면 "단말 관리 프로파일" 또는 "앱 관리 프로파일" 창이 나타납니다. 프로파일명 옆의 **프로파일 할당**을 클릭한 후 그룹 옆의 을 클릭하세요.
3. "그룹 할당" 창의 **전체 그룹**에서 해당 프로파일을 할당할 그룹을 선택하고 을 클릭하세요.



   - 하나의 프로파일을 여러 그룹에게 할당할 수 있습니다.
   - 그룹에 하나의 프로파일만 할당할 수 있으며, 이미 프로파일이 할당된 그룹은 선택할 수 없습니다. 이미 프로파일이 할당된 그룹에는 취소선이 그어져 있습니다.
   - **선택된 그룹** 목록에서 프로파일을 해제할 그룹을 선택하고 을 클릭하면 해제됩니다.
4. **저장**을 클릭하세요.

5. 그룹에 프로파일을 바로 배포하려면 “프로파일 배포” 팝업창에서 **예**를 클릭하세요.
6. 프로파일을 할당받은 그룹에 설치된 Knox 컨테이너를 제어하려면, 194페이지 11장의 “Knox 컨테이너 제어하기"를 참고하세요.

단말 관리 프로파일 정책 설정하기

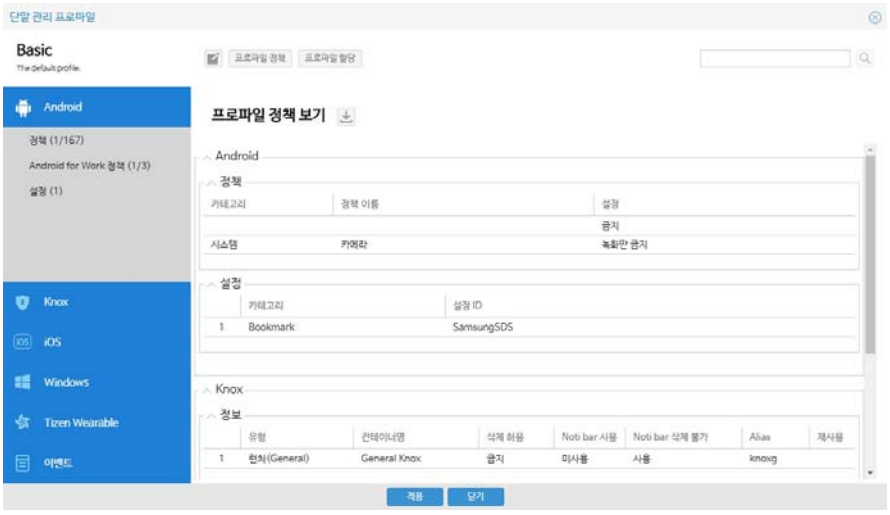
단말의 Android, iOS, Windows, Tizen Wearable 플랫폼에 단말 관리 프로파일 정책을 설정하여 단말을 제어할 수 있습니다 . 정책을 설정한 후 할당된 조직 또는 그룹에 프로파일을 바로 배포 할 수 있습니다 .

Note:
- 플랫폼별 제어 가능한 정책에 대한 자세한 내용은 344페이지 18장의 “정책 목록"을 참고하세요.
- Windows 플랫폼의 앱 블랙/화이트리스트 정책 설정을 위한 CSP 설정에 대한 자세한 내용은 298페이지 17장의 “CSP 설정하기"를 참고하세요.

정책 추가하기

단말 관리 프로파일의 정책을 추가하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 목록에서 정책을 추가하려는 프로파일명을 클릭하세요.
   - 프로파일명과 설명은 “단말 관리 프로파일”창의 왼쪽 상단에 표시됩니다.
3. 정책을 추가하려는 단말 플랫폼을 “단말 관리 프로파일”창의 왼쪽 메뉴에서 클릭하세요.
   - 정책을 검색하려면 우측 상단에 검색할 정책명을 입력한 후 엔터 또는 을 클릭하세요. 검색 결과에서 추가할 정책을 클릭하면 해당 설정 화면으로 이동합니다.



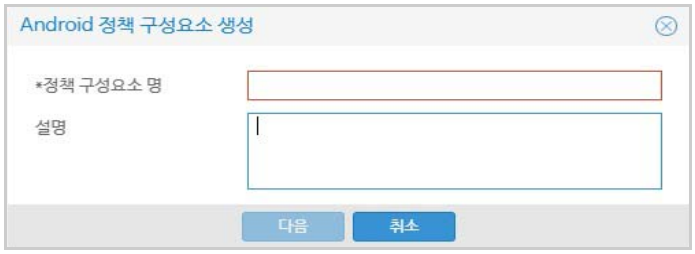
4. **Android/iOS/Windows/Tizen Wearable > 정책**으로 이동하세요.

5. 을 클릭하면 정책 수정 화면이 나타납니다.
   - Android 정책 중에서 삼성 단말에만 적용되는 정책명 옆에는 파란색 점으로 표시됩니다.
6. 정책을 설정한 후 **저장**을 클릭하세요.
   정책 상세 내용은 344페이지 18장의 "정책 목록"을 참고하세요.
7. 할당된 조직 또는 그룹에 속한 단말에 정책을 배포하려면 "단말 관리 프로파일" 창에서 **적용**을 클릭하세요. 확인 메시지가 나타나면 **예**를 클릭하세요.

단말 관리 프로파일의 정책 구성요소 등록하기

단말 관리 프로파일의 정책 구성요소를 추가하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일 구성요소**로 이동하세요.
2. 을 클릭한 후, **정책 등록** 아래 **Android**, **Android for Work**, **iOS**, **Windows**, **Tizen Wearable**, **Knox 컨테이너** 중 등록할 구성 요소를 선택하세요.



3. 해당 정책 구성요소 생성 창에서 **정책 구성요소 명**과 **설명**을 입력한 후 **다음**을 클릭하세요.
4. 상세 항목을 설정하고 **저장**을 클릭하세요.
   플랫폼별 제어 가능한 정책에 대한 자세한 내용은 344페이지 18장의 "정책 목록"을 참고하세요

단말 정책 업데이트 스케줄 등록하기

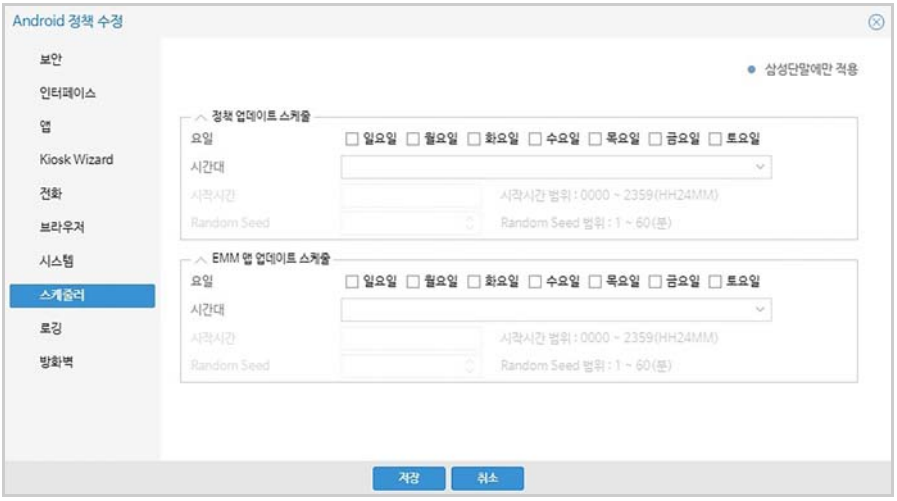
사용자의 단말에 정책 및 EMM 앱 업데이트 스케쥴을 등록할 수 있습니다 .

Android 단말의 경우 , 정책 그룹 중 스케줄러에서 업데이트 스케줄을 등록하면 , 단말에서 해당 시간에 서버로 정책 업데이트를 요청합니다 . 해당 기능은 삼성 갤럭시 단말에만 적용됩니다 .

프로파일이 할당된 전체 플랫폼 단말에 정책 업데이트를 요청하려면 , 215 페이지 12 장의 " 프로파일 업데이트 주기 설정하기 " 를 참고하세요 . 이벤트에서 설정하는 프로파일 업데이트 주기 설정은 서버에서 단말로 정책 업데이트를 요청합니다 . Android 정책과 이벤트 양쪽에 스케줄이 설정되어 있으면 삼성 갤럭시 단말은 각 스케줄에 따라 정책이 업데이트됩니다 .

Android 단말에 정책 업데이트 스케줄을 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 업데이트 하려는 프로파일명을 클릭하세요.
3. "단말 관리 프로파일" 창에서 **Android > 정책**으로 이동하세요.
4. Android 정책 옆의 을 클릭하세요.
5. “Android 정책 수정” 창에서 **스케줄러**를 클릭하세요.



6. 정책 업데이트를 위한 스케줄은 **정책 업데이트 스케줄** 영역에서, EMM 앱 업데이트를 위한 스케줄은 **EMM 앱 업데이트 스케줄** 영역에서, **요일**, **시간대**, **시작시간**, **Random Seed**를 설정하세요.
   - **Random Seed**: 정책 업데이트를 진행할 시간 범위를 설정합니다.
     예) Random Seed를 30분으로 설정하면, 설정한 시작 시간 후 30분 이내에 단말이 무작위로 업데이트됩니다.
   - 정책 업데이트 시간은 단말 시간을 기준으로 하기 때문에사용자의 시간대에 의해 정책 업데이트 시간이 변동될 수 있습니다.
7. **저장**을 클릭하세요.

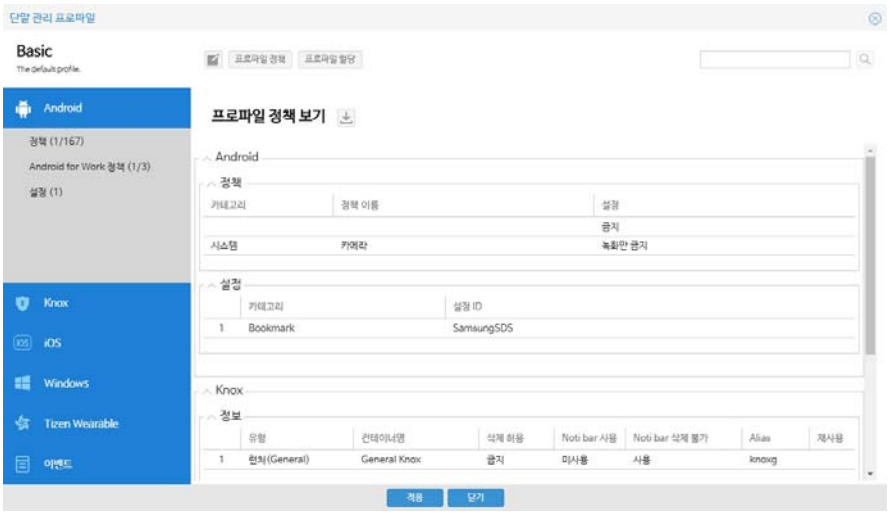
단말 관리 프로파일 설정 추가하기

단말의 Android, iOS, Windows 플랫폼에 단말 관리 프로파일 설정을 추가하여 사용할 수 있습니다 . 추가 및 변경된 설정을 단말에 적용하려면 " 단말 관리 프로파일 " 화면에서 **적용**을 클릭합니다 . 프로파일이 할당된 조직 또는 그룹의 사용자 단말에 최신 단말 관리 프로파일이 배포됩니다 .

설정 추가하기

단말 관리 프로파일의 설정을 추가하려면 다음의 절차를 따르세요 . 플랫폼 별 상세 설정 내용은 344 페이지 18 장의 " 정책 목록 " 을 참고하세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 목록에서 설정을 추가하려는 프로파일명을 클릭하세요.
3. 설정을 추가하려는 단말 플랫폼을 "단말 관리 프로파일"창의 왼쪽 메뉴에서 클릭하세요.



4. **Android/iOS/Windows > 설정**으로 이동하세요.
5. ➕을 클릭하면 설정 등록 화면이 나타납니다.
6. 설정을 등록한 후 **저장**을 클릭하세요.
7. 할당된 조직 또는 그룹에 속한 단말에 설정을 배포하려면 "단말 관리 프로파일" 창에서 **적용**을 클릭하세요. 확인 메시지가 나타나면 **예**를 클릭하세요.

단말 관리 프로파일의 설정 구성요소 등록하기

단말 관리 프로파일의 설정 구성요소를 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일 구성요소**로 이동하세요.
2. ➕을 클릭한 후, **설정 등록** 아래 **Android**, **iOS**, **Windows** 중 등록할 구성 요소를 선택하세요.

3. **카테고리** 목록에서 설정 대상을 “설정 등록” 창의 카테고리를 선택하세요.
   - Android, iOS, Windows에 따른 카테고리 목록이 보여집니다.
4. **설정 ID**와 상세 항목을 설정하세요.
   - 등록한 설정 ID가 단말 관리 프로파일 구성요소 목록에서 구성요소 명으로 조회됩니다.
   - 설정 등록 방법에 대한 자세한 내용은 144페이지의 "단말 관리 프로파일 설정 추가하기"를 참고하세요.
5. **저장**을 클릭하세요.

사용자 인증서 등록하기

단말에서 Wi-Fi, VPN, Exchange, Generic VPN 을 이용하기 위한 사용자 인증서 (.p12 또는 .pfx) 는 아래와 같이 2 가지 경우로 구분하여 입력됩니다 .

- EMM 서버에서 프로파일 내에 사용자 인증서를 포함하여 내려주는 경우
- Microsoft AD CS 발급에 필요한 템플릿 정보만을 내려주는 경우

단말 관리 프로파일에 Wi-Fi, VPN, Exchange 설정을 위한 사용자 인증서가 포함되어 단말에 전송되는 경우 , 단말은 해당 인증서를 설치하고 , 인증서에 대한 패스워드를 사용자로부터 입력받아 처리합니다 .

Microsoft AD CS 발급에 필요한 템플릿 정보가 단말 관리 프로파일에 포함되어 단말에 전송되는 경우 , Android 단말은 내려받은 템플릿 정보로 Microsoft AD CS 발급 Cert Lib 에 인증서 발급을 요청 후 인증서를 설치합니다 .

iOS 단말의 경우 , 서버에서 해당 템플릿 정보로 인증서를 발급하여 인증서를 단말 관리 프로파일에 포함하여 전송합니다 . 단말 관리 프로파일을 통해 내려받은 인증서 정보로 국제 인증규격인 X.509v3 인증서가 단말에 설치되며 , 설치된 인증서는 단말의 Trusted Anchor Database 에서 확인할 수 있습니다 .

또한 , EMM 은 Directory 서비스를 연동하여 사용자를 인증합니다 . 이를 위해 **설정 > 연동 시스템 > Directory** 메뉴에서 Directory 서비스를 사전에 등록해야 합니다 . Directory 서비스 등록 방법에 대한 263 페이지 16 장의 “Directory 서버 관리하기 " 를 참고하세요 . 인증서와 인증서 템플릿 등록에 대한 자세한 내용은 245 페이지의 "15 인증서 " 를 참고하세요 .

Android, iOS, Knox 영역에서 Wi-Fi, VPN, Exchange, Generic VPN 설정 등록 시 사용자 인증서를 입력하는 방법은 다음과 같습니다 .

- EMM 관리 인증서를 선택하면 나타나는 사용자 인증서에서 인증서를 선택하세요. **인증서> 외부 인증서**에서 등록한 인증서 중 용도에 따라 인증서가 조회됩니다.
  - Wi-Fi 설정시 인증서 용도가 Wi-Fi Certificate이며, 인증서 유형이 User Certificate인 Wi-Fi 인증서가 목록에 나타납니다.
  - VPN 설정시 인증서 용도가 VPN Certificate이며, 인증서 유형이 User Certificate인 VPN 인증서가 목록에 나타납니다.
  - Exchange 설정시 인증서 용도가 Exchange이며, 인증서 유형이 User Certificate인 Exchange 인증서가 목록에 나타납니다.
  - Generic VPN 설정시 인증서 용도가 Generic VPN Certificate이며, 인증서 유형이 User Certificate인 Generic VPN 인증서가 목록에 나타납니다.
- **커넥터 연동**을 선택하면 나타나는 **사용자 인증서 커넥터**에서 사용할 커넥터를 선택하세요. **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

외부 사용자 인증서를 선택하면 나타나는 **외부 사용자 인증서**에서 인증서 템플릿을 선택하세요 . **인증서 > 인증서 템플릿**에서 템플릿 타입이 **외부**로 등록된 인증서 템플릿이 목록에 나타납니다 . 선택한 인증서 템플릿은 프로파일에 포함되어 사용자 단말에 전송됩니다 . 단말 사용자는 해당 템플릿으로 인증서를 설치하게 됩니다 .

Android 설정 등록하기

Android 플랫폼에 단말 관리 프로파일의 설정을 등록하여 사용할 수 있습니다 . 입력 항목명 앞에 표시 (*) 는 필수 입력값이며 , 나머지는 선택 사항입니다 .

Wi-Fi 설정 등록하기

Android 설정 카테고리에서 Wi-Fi 를 선택한 후 , 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**, **네트워크명(SSID)**과 선택한 **보안 유형** 에 따른 설정 항목 입력하세요.
- **네트워크명(SSID)**: 연결할 무선 공유기의 식별자를 입력합니다. 특수 문자는 입력할 수 없습니다.
- **삭제 가능**: 단말 사용자가 Wi-Fi 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 Wi-Fi 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 Wi-Fi 설정을 삭제하는것이 금지됩니다. • 사용자 단말에서는 Wi-Fi 설정을 삭제하는 버튼이 비활성화됩니다.

- **보안 유형**을 선택 후, 선택한 보안 유형에 따라 나타나는 항목을 입력하세요.

항목	설명
없음	보안 설정을 하지 않습니다.
WEP	선택 시 WEP KEY 인덱스를 설정하여 사용합니다. • **WEP KEY 인덱스**: WEP KEY 1~WEP KEY 4 중 사용할 인덱스 선택합니다.

항목	설명
WPA/WPA2-PSK	선택 시 비밀번호를 설정하여 사용하며, 입력 범위는 최소 길이 8자입니다.
802.1xEAP	선택 시 아래 항목을 설정하여 사용합니다. • **EAP 방식**: 인증 프로토콜(PEAP,TLS, TTLS)을 선택합니다. • **2단계 인증**: 추가 인증 방법(PAP, MSCHAP, MSCHAPV2, GTC)을 선택합니다. • **사용자 정보 입력방법**: **직접 입력**을 선택하면 나타나는 **ID**와 **비밀번호**에 Wi-Fi 접속을 위한 사용자 ID와 비밀번호를 입력하거나, **커넥터 연동**을 선택하면 나타나는 **사용자 정보 커넥터** 항목에서 커넥터를 선택합니다. • **사용자 인증서 입력방법**은 147페이지의 "Android 설정 등록하기"를 참고하세요. • **CA인증서**에서 루트 인증서를 선택합니다. **인증서> 외부 인증서**에서 등록한 인증서 중, **인증서 용도**가 Wi-Fi Certificate이며, **인증서 유형**이 Root Certificate인 Wi-Fi 인증서가 목록에 나타납니다.

VPN설정 등록하기

Android 설정 카테고리에서 VPN 을 선택한 후 , 다음의 항목을 입력하세요 .

- **설정 ID**와 **설명**을 입력하세요.
- **VPN 이름**: 사용자의 단말에 표시될 VPN 이름을 입력하세요.
- **삭제 가능**: 단말 사용자가 VPN 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 VPN 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 VPN 설정을 삭제하는것이 금지됩니다. • 사용자 단말에서는 VPN 설정을 삭제하는 버튼이 비활성화 됩니다.

- **연결 유형**: VPN 서버 유형을 선택하세요.
- **서버 주소**: VPN 서버의 IP 주소, 호스트 명, 또는 URL을 입력하세요.
- **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **ID**, **비밀번호**에 VPN 접속을 위한 사용자의 ID와 비밀번호를 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

- 선택한 **연결 유형**에 따라 나타나는 해당 항목을 입력하세요.

항목	설명
PPTP	선택 시 **PPP 암호화(MPPE)** 여부를 선택하세요.
L2TP/IPSec PSK	선택 시 **L2TP 비밀 키**, **IPSec 식별자**, **IPSec 사전 공유 키**를 입력하세요. • Android용 VPN 설정시 단말이 CC 모드로 활성화 상태인 경우, **L2TP/IPSec PSK** 사용은 불가능합니다.
L2TP/IPSec RSA, IPSec Xauth RSA, IPSec Hybrid RSA	선택 시 • **사용자 인증서 입력방법**은 147페이지의 "Android 설정 등록하기"를 참고하세요. • **IPSec CA 인증서**에서 사용할 루트 인증서를 선택하세요. **인증서> 외부 인증서**에서 등록한 인증서 중, 인증서 용도가 VPN Certificate이며, **인증서 유형**이 Root Certificate인 VPN 인증서가 목록에 나타납니다.
IPSec Xauth PSK	선택 시 **IPSec 식별자, IPSec 사전 공유 키**를 입력하세요.

- **고급 옵션 표시**의 항목은 다음과 같습니다.

항목	설명
DNS 검색 도메인	사용할 DNS 검색 도메인의 이름을 설정하세요. • 예: example.com
DNS 서버	DNS 서버 주소를 IP 패턴에 맞게 입력하세요. • 예: 127.0.0.1
전달 경로	**서브넷 비트**를 선택하면 자동 입력됩니다.
서브넷 비트	없음, **/1~/30** 중 선택합니다.

Exchange 설정 등록하기

Android 설정 카테고리에서 Exchange 를 선택한 후 , 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **삭제 가능**: 단말 사용자가 Exchange 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 Exchange 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 Exchange 설정을 삭제하는것이 금지됩니다. • 사용자 단말에서는 Exchange 설정을 삭제하는 버튼이 비활성화됩니다.

- **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **이메일**, ID, **비밀번호**에 Exchange 서버 접속을 위한 사용자의 이메일, ID, 비밀번호을 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

- **도메인**, **Exchange 서버 주소**를 지정하세요.
- **과거 데이터 동기화 단위**: 1일, 3일, 1주일, 2주일, 1개월 중 선택하세요.
- **사용자 인증서 입력방법**은 147페이지의 "Android 설정 등록하기"를 참고하세요.
- 아래 항목에 대하여 동기화 여부를 설정하세요.
  - **일정 동기화**, **전화번호부 동기화**, **할 일 동기화**, **노트 동기화**
- 이메일 암호화 통신 방법으로 **SSL** 사용 여부를 선택하세요.
- **서명**: 사용할 이메일 서명을 입력하세요.

- 메일 도착시 **알림** 방법을 선택하세요.
  - **알림**, **항상 진동 알림**, **무음 알림**
- **첨부파일 용량(byte)**: 첨부파일의 제한 용량을 byte 단위로 입력하세요. 입력값의 범위는 1~52428800(50MB) 입니다.
- **메일 본문 용량(Kbyte)**: 메일의 본문 제한 용량을 Kbyte 단위로 입력하세요.

Certificate 설정 등록하기

Android 설정 카테고리에서 Certificate 를 선택한 후 , 다음의 항목을 설정하세요 .

- **설정 ID**, **설명**, **인증서분류**, **CA 인증서**를 입력하세요.
- **인증서분류**를 선택하세요.

항목	설명
CA 인증서	선택 시 나타나는 **CA 인증서**에서 사용할 인증서를 선택하세요. • **인증서> 외부 인증서**에서 등록한 인증서 중, **인증서 용도**가 CA Certificate이며, **인증서 유형**이 Root Certificate인 CA 인증서가 목록에 나타납니다.
사용자 인증서	선택 시 나타나는 **사용자 인증서**에서 사용할 인증서를 선택하세요. • **인증서> 외부 인증서**에서 등록한 인증서 중, **인증서 용도**가 CA Cert이며, **인증서 유형**이 User Certificate인 사용자 인증서가 목록에 나타납니다.

Generic VPN 설정 등록하기

Generic VPN 은 개인 영역 또는 Knox 영역 상관없이 단말에서 하나만 설치할 수 있습니다 . Android 설정 카테고리에 Generic VPN 을 선택한 후 , 다음의 항목을 설정하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **설정 ID**를 입력하세요.
- **VPN 이름**: 사용자의 단말에 표시될 VPN 이름을 입력하세요.
- **삭제 가능**: 단말 사용자가 Generic VPN 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 Generic VPN 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 Generic VPN 설정을 삭제하는것이 금지됩니다. • 사용자 단말에서는 Generic VPN 설정을 삭제하는 버튼이 비활성화됩니다.

- **VPN 벤더사**를 선택하세요. 선택한 VPN 벤더사에 따라 나타나는 입력하는 항목이 다를 수 있습니다.

항목	설명
VPN 클라이언트 벤더 패키지명	선택한 **VPN 벤더사**에 따라 설치된 Client 버전의 패키지명이 자동 입력이 되며, **VPN 벤더사**에서 직접입력을 선택한 경우 VPN 클라이언트 벤더 패키지명을 입력하세요.
VPN 타입	선택한 **VPN 벤더사**에 따라 자동 입력됩니다. **VPN 벤더사**가 직접입력인 경우 VPN 타입을 선택하세요.

- **Generic VPN 프로파일 입력 방법**: 직접입력, 프로파일 업로드 중 선택하세요. **VPN 벤더사**를 직접입력으로 선택한 경우 프로파일 업로드가 기본값입니다.

항목	설명
직접입력	선택 시 154페이지의 "Generic VPN 프로파일 직접 입력하기"를 참고하세요.
프로파일 업로드	선택 시 다음을 수행합니다. 1. **Generic VPN 프로파일 업로드** 옆의 ⊕을 클릭하세요. 2. "Generic VPN 프로파일" 창에서 Generic VPN 프로파일을 선택 후, **확인**을 클릭하세요. • Json 형태의 text 파일을 업로드하세요. Json 파일은 **VPN 벤더사, VPN 타입** 별로 내용이 달라집니다. • 파일 업로드시 156페이지의 "Generic VPN 프로파일 업로드를 위한 파일 샘플"을 참고하세요. 3. "확인" 창에서 Generic VPN 프로파일을 확인한 후, **확인**을 클릭하세요.

- 선택한 **VPN 벤더사**, **VPN 타입**, 프로파일 직접 입력시 선택한 연결방식에 따라 다음의 항목은 다를 수 있습니다.

항목	설명
사용자 인증서 입력 방법	147페이지의 "Android 설정 등록하기"를 참고하세요.
OCSP Url	CA서버에서 인증서의 폐기 여부를 체크하기 위한 OCSP Url을 입력하세요.
CA인증서	**루트 인증서**를 선택하세요. • **인증서 > 외부 인증서**에서 등록한 인증서 중, 인증서 용도가 Generic VPN Certificate이며, **인증서 유형**이 Root Certificate인 VPN 인증서가 목록에 나타납니다.
서버 인증서	**서버 인증서**를 선택합니다. • **인증서 > 외부 인증서**에서 등록한 인증서 중, **인증서 용도**가 Generic VPN Certificate이며, **인증서 유형**이 Server Certificate인 VPN 인증서가 목록에 나타납니다.
FIPS 모드	사용 여부를 설정하세요.
접속 에러시 재접속	재접속 여부를 설정하세요.

- **앱별 VPN Route Type**: 애플리케이션별 또는 일반 영역의 전체 패키지에 대해 VPN을 사용할지 여부를 설정하세요.

항목	설명
앱별	애플리케이션 선택하여 해당 애플리케이션 구동시 설정된 VPN을 사용합니다. • **앱별 VPN 적용 패키지명** 옆의 ⊕을 클릭하여 "앱 목록" 창에서 애플리케이션 선택 후 **확인을** 클릭하세요.
일반 영역 전체 패키지	일반 영역의 모든 애플리케이션 구동시 설정된 VPN이 사용됩니다.

Generic VPN 프로파일 직접 입력하기

Generic VPN 프로파일 입력 방법을 **직접입력**으로 선택한 경우 , **Generic VPN 프로파일** 영역에서 아래의 항목을 입력하세요 .

- **VPNrouteEnable**은 per-app vpn으로, 특정 앱이 구동 시 VPN 터널링을 자동으로 사용하게 됩니다.
- **서버 주소**: VPN 서버의 IP 주소, 호스트 명, 또는 URL을 입력하세요.
- **User 인증**: 사용자 인증 여부를 선택합니다. 사용 선택 시 다음을 입력하세요.
  - **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **ID**, **비밀번호**에 VPN 접속을 위한 사용자의 ID와 비밀번호를 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

- **VPN 벤더사**가 **StrongSwan**일 때, 구성되는 항목은 다음과 같습니다.
  - 선택한 **연결 유형**에 따라 나타나는 해당 항목을 입력하세요.

항목	설명
PPTP	**PPP 암호화(MPPE)** 여부를 선택하세요.
L2TP/IPSec PSK	**L2TP 비밀 키**, **IPSec 식별자**, **IPSec 사전 공유 키**를 입력하세요.
L2TP/IPSec RSA	**L2TP 비밀 키**를 입력하세요.
IPSec Xauth PSK	**IPSec 식별자**, **IPSec 사전 공유 키**를 입력하세요.
IPSec Xauth RSA	**사용자 인증서 입력 방법**, **CA 인증서**, **서버 인증서**를 입력하세요.
IPSec Hybrid RSA	**CA 인증서**, **서버 인증서**를 입력하세요.
IPSec IKE2 PSK	**식별자**, **사전 공유 키**를 입력하세요.
IPSec IKE2 RSA	**사용자 인증서 입력 방법**, **OCSP Url, CA 인증서**, **서버 인증서**를 입력하세요.

  - **고급 옵션 표시**의 항목은 다음과 같습니다.

항목	설명
DNS 검색 도메인	사용할 DNS 검색 도메인의 이름을 설정하세요. • 예: example.com
DNS 서버	DNS 서버 주소를 IP 패턴에 맞게 입력하세요. • 예: 123.0.0.4
전달 경로	**서브넷 비트**를 선택하면 자동 입력하세요.
서브넷 비트	**없음**, **/1~/30** 중 선택하세요.

- **연결 방식**:

항목	설명
KEEP On	VPN 접속을 계속 유지합니다.
On Demand	요청시 VPN 접속을 합니다.

- **체이닝** 방식을 선택하세요.
- **UID PID** 사용여부를 선택하세요.

Generic VPN 프로파일 업로드를 위한 파일 샘플

다음은 VPN 벤더사가 Cisco 이며 , VPN 타입이 IPSec 인 경우의 파일 샘플입니다 .

```
{     "KNOX_VPN_PARAMETERS":{
                "profile_attribute":{
                          "profileName":"c1",
                          "host":"12.3.456.78",
                     "isUserAuthEnabled":true,
                          "vpn_type":"ipsec",
                          "vpn_route_type":1 },
        "ipsec":{
                "basic":{
                            "username":"",
                            "password":"",
                            "authentication_type":1,
                            "psk":"",
                            "ikeVersion":1,
                            "dhGroup":0,
                            "p1Mode":2,
                            "identity_type":0,
                          "identity":"test@sta.com",
                            "splitTunnelType":0,
                            "forwardRoutes":
                              {
                                        "route":""
                                    }
                            ] },
                  "advanced":{
                                "mobikeEnabled":false,
                                "pfs":true,
                                "ike_lifetime":"10",
                                "ipsec_lifetime":"25",
                                "deadPeerDetect":true
                  },
                  "algorithms":{
                }},
        "knox":{
          "connectionType":"keepon",
          "chaining_enabled":"-1",
          "uidpid_search_enabled":"0" },
        "vendor":{
                    "setCertCommonName":"space",
                    "SetCertHash":"pluto",
                    "certAuthMode":"Automatic"}
    }
}
```

다음은 VPN 벤더사가 Cisco 이며 , VPN 타입이 SSL 인 경우의 파일 샘플입니다 .

```
{
       "KNOX_VPN_PARAMETERS":{
                 "profile_attribute":{
                   "profileName":"c3",
                   "host":"cisco-asa.gnawks.com",
                   "isUserAuthEnabled":true,
                   "vpn_type":"ssl",
                   "vpn_route_type":1
         },
         "ssl":{
                   "basic":{
                            "username":"demo",
                            "password":"samsung",
                            "authentication_type":1,
                            "splitTunnelType":0,
                            "forwardRoutes":
                                     {
                                          "route":""
                                     }
                            ]
                    },
                    "algorithms":{
                            "ssl_algorithm":0
                    }
        },
        "knox":{
                    "connectionType":"keepon",
                    "chaining_enabled":"-1",
                    "uidpid_search_enabled":"0"
          },
          "vendor":{
                    "setCertCommonName":"space",
                    "SetCertHash":"pluto",
                    "certAuthMode":"Automatic"
        }
   }
}
```

APN 설정 등록하기

Android 설정 카테고리에서 APN 을 선택한 후 , 다음의 항목을 설정하세요 .

- **표시명**, **설명**을 입력하세요.
- **표시명**: 단말에 표시할 APN의 명칭을 입력하세요.
- **삭제 가능**: 단말 사용자가 VPN 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 APN 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 APN 설정을 삭제하는것이 금지됩니다. 사용자 단말에서는 APN 설정을 삭제하는 버튼이 비활성화 됩니다.

- **액세스 포인트 이름 (APN)**: 네트워크 연결 지점으로 사용하려는 Access Point Name을 입력하세요.
- **APN 유형**의 항목은 다음과 같습니다.

항목	설명
Default	
MMS	멀티미디어 메시징 서비스
Supl	IP 기반으로 GPS 위성 신호를 수신하는 프로토콜

- **모바일 국가 코드 (MCC)**: APN을 사용하는 국가 코드를 입력하세요.
- **모바일 네트워크 코드 (MNC)**: APN을 사용하는 통신사 네트워크 코드를 입력하세요.
- **MMS 서버 (MMSC)**: 멀티미디어 메시지 전송에 사용되는 서버 정보를 입력하세요.

  - MMSC와 MMS 메시지 송수신에 사용되는 **MMS 프록시 서버**와 **MMS 프록시 서버 포트**를 입력하세요.
- **서버**: WAP 게이트웨이 서버를 입력합니다. 스마트 폰 및 단말에서 사용하지 않는 기능입니다.
  - **프록시 서버**와 **프록시 서버 포트**를 입력하세요.
- 통신사에서 데이터에 접근하기 위한 **사용자 이름**과 **비밀번호**를 입력하세요.
  - 일반적으로 사용되지 않습니다.
- **인증 방식**은 다음과 같습니다.

항목	설명
None	인증 방식을 사용하지 않는 경우
PAP	사용자 이름과 비밀번호를 입력하여 인증하는 방식입니다.
CHAP	Challenge 문자열을 이용하여 암호화하는 인증 방식입니다.
PAP or CHAP	PAP 또는 CHAP 인증 방식을 사용하는 경우

- **APN 적용 여부**: APN 설정을 단말에 적용할지 여부를 지정하세요.

Bookmark 설정 등록하기

Android 의 삼성 단말에서 사용되는 기본 브라우저인 S 브라우저의 북마크를 등록 , 수정 및 삭제합니다 .

Bookmark 사용 시 제약 사항은 다음과 같습니다 .

- 단말에서 인터넷 브라우저를 모두 종료한 후 재실행해야 변경된 설정이 반영됩니다.
- 사용자가 등록된 북마크를 수정하거나 동일한 URL과 이름으로 북마크를 등록하더라도 북마크 설정 삭제 시 삭제되지 않습니다.
- 삼성 단말의 기능 제약으로 인해 설정된 Bookmark를 사용자가 브라우저에서 임의로 삭제하더라도 EMM 앱에서는 여전히 설치되어 있는 것으로 보일 수 있습니다. 이 경우 단말 관리 프로파일 설정에서 해당 북마크 삭제 후 재 설정을 해야 합니다.

북마크를 설정하려면 Android 설정 카테고리에서 북마크를 선택한 후 , 다음의 항목을 설정하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **설치 영역**: 북마크가 설치될 위치를 설정합니다.
  - Bookmark: S 브라우저의 북마크 내에 설정됩니다.
  - ShortCut: 단말의 바탕화면에 북마크 URL로 바로가기가 설정됩니다. ShortCut 설치 영역을 선택한 경우 ShorCut 이미지를 선택하세요.
- **ShortCut 이미지**: ShortCut 설치 영역을 선택한 경우 사용자의 단말에 생성될 ShortCut 아이콘을 선택하세요.
- **북마크 페이지 URL**: 북마크 선택 시 이동할 웹 사이트 주소를 입력하세요.
  - http:// 또는 https:// 로 시작해야하며, 입력 가능한 특수 문자는 도메인 명에는 _, -, + 입력 가능하며, 도메인 외 디렉토리명에는 _만 가능합니다.
    예) http://www.n_-+test.com/_test
- **북마크 이름**: 북마크에서 제목으로 표시될 북마크 이름을 입력하세요.

Email Account 설정 등록하기

Android 설정 카테고리에서 Email Account 를 선택한 후 , 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **삭제 가능**: 단말 사용자가 Knox 영역의 Email Account 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 Email Account 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 Email Account 설정을 삭제하는것이 금지됩니다. • 사용자 단말에서는 Email Account 설정을 삭제하는 버튼이 비활성화 됩니다.

- **기본 계정**: 기본 계정 사용 여부를 설정하세요.
- **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **이메일**에 Email 접속을 위한 사용자의 이메일을 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

- **수신 서버 프로토콜**을 선택하세요.
  - POP3 (pop3)
  - IMAP (imap)
- **발신 서버 프로토콜**은 **SMTP**로 설정되어 있습니다.

- **수신 관련 설정**은 다음과 같습니다.

항목	설명
수신 서버 주소/포트	입력 형식에 맞게 입력
수신 서버 ID	
수신 서버 비밀번호	
수신 SSL	수신 암호화 방법으로 SSL 사용 여부를 설정

- **발신 관련 설정**은 다음과 같습니다.

항목	설명
발신 서버 주소/포트	입력 형식에 맞게 입력
발신 서버 ID	
발신 서버 비밀번호	
발신 SSL	발신 암호화 방법으로 SSL 사용 여부를 설정

- **알림**: 사용자 단말에서 이메일 수신시 알림 방법을 설정하세요.

항목	설명
Enable Notify	알림 활성화하기
Enable Always Vibrate Notify	항상 진동으로 알림
Disable Notify	알림 비활성화하기

- **수신 인증서** 허용 여부를 설정하세요.
- **발신 인증서** 허용 여부를 설정하세요.
- **서명**: 사용할 이메일 서명 입력하세요.
- **계정 이름**, **발신인 이름**을 입력하세요.

iOS 설정 등록하기

iOS 플랫폼에 단말 관리 프로파일의 설정을 등록하여 사용할 수 있습니다. 입력 항목명 앞에 표시 (*) 는 필수 입력값이며, 나머지는 선택 사항입니다.

Wi-Fi 설정 등록하기

iOS 설정 카테고리에서 Wi-Fi 를 선택한 후 다음의 항목을 입력하세요.

- **설정 ID**, **설명**을 입력하세요.
- **네트워크명(SSID)**: 연결할 무선 공유기의 식별자 입력, 특수 문자는 입력할 수 없습니다.
- **보안 유형**: 선택한 보안 유형에 따라 입력 항목 다릅니다.

항목	설명
없음	보안을 적용 하지않습니다.
WEP	선택 시 비밀번호는 다음과 같이 설정하세요. • 대소문자를 구분하는 영문 5자 • 13자의 문자 또는 숫자 • 10자 또는 26자의 16진수 문자
WPA/WPA2	선택 시 비밀번호는 다음과 같이 설정하세요. • 대소문자를 구분하는 8~63자의 문자 또는 숫자 • 64자의 16진수 문자
모든 개인용	선택 시 비밀번호는 다음과 같이 설정하세요. • 대소문자를 구분하는 영문 5자 • 13자의 문자 또는 숫자 • 대소문자를 구분하는 8~63자의 문자 또는 숫자 • 64자의 16진수 문자
기업용 WEP	선택 시 나타나는 **프로토콜**, **인증**, **신뢰** 탭에서 해당 항목을 설정하세요.
기업용 WPA/WPA2	선택 시 나타나는 **프로토콜**, **인증**, **신뢰** 탭에서 해당 항목을 설정하세요.
모든 기업용	선택하면 나타나는 **프로토콜**, **인증**, **신뢰** 탭에서 해당 항목을 설정하세요.

- **핫스팟 사용 여부**를 선택하면 Wi-Fi 로밍 서비스인 Wi-Fi Hotspot 2.0 기능을 이용할 수 있으며, iOS 7 이상에서 사용 가능합니다.

항목	설명
핫스팟 도메인명	단말에 표시될 Wi-Fi Hotspot 서비스 식별자
로밍 서비스 제공자 연결 허용	로밍 서비스 제공자와의 연결 허용 여부 지정
오퍼레이터명	단말에 표시될 네트워크 공급자 이름
로밍 컨소시엄 OI	단말에서 연결할 로밍 컨소시엄 조직 ID 입력 • ∨을 클릭하여 로밍 컨소시엄 OI 입력 후 ⊕을 클릭
네트워크 접근 ID	네트워크 접근을 인증하기 위한 ID • ∨을 클릭하여 네트워크 접근 ID 입력 후 ⊕을 클릭
핫스팟 통신사 코드	Mobile Country Code(MCC, 국가코드), Mobile Network Configuration(MNC, 모바일 네트워크 코드) 입력 • ∨을 클릭하여 핫스팟 통신사 코드 입력 후 ⊕을 클릭 • 핫스팟 통신사 코드는 숫자 6자임

- **Hidden 네트워크**: 네트워크 숨기기 여부를 설정하세요.
- **자동 연결(iOS 5이상)**: Wi-Fi 자동 연결 여부를 설정하세요.
- **보안 유형**이 **기업용 WEP, 기업용 WPA/WPA2, 모든 기업용**일 경우 **프로토콜** 탭에서 Wi-Fi 네트워크에 적용할 프로토콜을 다음과 같이 설정하세요.

항목	설명
허용된 EAP 유형	TLS, LEAP, EAP-FAST, TTLS, PEAP, EAP-SIM 중 한 개 이상 선택 • **TTLS**를 선택하면 나타나는 **내부 신원 인증 프로토콜**에서 사용할 프로토콜 선택
EAP-FAST	• **PAC 사용**: PAC 사용 여부 선택 • **PAC 공급**: **PAC 사용**을 선택하면 설정 가능 • **익명으로 PAC 공급**: **PAC 공급**을 선택하면 설정 가능
사용자에 의한 인증서 신뢰	사용 여부 설정
직접 연결 허용 (프록시 URL)	사용 여부 설정

- **보안 유형**이 **기업용 WEP, 기업용 WPA/WPA2, 모든 기업용**일 경우 **인증** 탭에서 Wi-Fi 사용자 인증 방법을 다음과 같이 설정하세요.

항목	설명
연결당 비밀번호 사용	Wi-Fi 연결할 때마다 사용자로부터 비밀번호를 입력받을지 설정하세요. • 선택하면 **자동 연결(iOS 5 이상)** 자동 해제 • 해제하면 **자동 연결(iOS 5 이상)** 자동 선택
사용자 정보 입력방법	• **직접입력**을 선택하면 나타나는 **ID**, **비밀번호**에 Wi-Fi 접속을 위한 사용자 ID와 비밀번호 입력 • **커넥터 연동**을 선택하면 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택

항목	설명
외부 ID	**프로토콜** 탭의 **허용된 EAP 유형** 중 TTLS, PEAP 또는 EAP-FAST 선택 시 사용 가능
사용자 인증서 입력 방법	147페이지의 "Android 설정 등록하기"를 참고하세요.

- **보안 유형**이 **기업용 WEP, 기업용 WPA/WPA2, 모든 기업용**일 경우 **신뢰** 탭에서 다음 항목을 설정하세요.

항목	설명
신뢰할 수 있는 인증서 명	을 클릭하여 인증서명 입력 후 을 클릭
Root 인증서	인증서 선택

- **프록시 설정(iOS 5 이상)**

항목	설명
없음	
수동	선택 시 **IP 주소** 및 **Port**, **사용자 이름**, **비밀번호** 항목 설정
자동	선택 시 **프록시 서버 URL** 항목 입력

VPN 설정 등록하기

iOS 설정 카테고리에서 VPN 을 선택한 후 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.

- **연결 유형**: L2TP, PPTP, IPSec (Cisco), Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Aruba VIA, Check Point Mobile VPN, OpenVPN, IKEv2
  - **IKEv2** 선택 시 167페이지의 "연결 유형이 IKEv2인 VPN 설정하기"를 참고하세요.
- **서버 주소**: VPN 서버의 IP 주소, 호스트 명, 또는 URL 입력하세요.
- **VPN 앱 할당**: 특정 애플리케이션 구동시 VPN 자동 연결을 위해 설정하세요.
  - ⊕을 클릭하여 "앱 목록" 창에서 앱 선택 후, **확인**을 클릭
- **Safari 도메인**: Safari에서 특정 URL 이동시 VPN 자동 연결을 위해 설정하세요.
  - 도메인명 입력 후, ⊕ 을 클릭
- **앱별 VPN 제공 타입**을 **packet-tunnel**과 **app-proxy** 중에 선택하세요.
- **사용자 연결 인증 유형**을 비밀번호와 RSA SecurID 중에 선택하세요.
- **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **ID**, **비밀번호**에 VPN 접속을 위한 사용자의 ID와 비밀번호를 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

- 선택한 **연결 유형**에 따라 나타나는 다음 항목을 설정하세요.

항목	설명
L2TP	선택 시 **공유 보안**, **모든 트랙픽 보내기** 설정
PPTP	선택 시 **암호화 단계**, **모든 트랙픽 보내기** 설정
IPSec(Cisco)	선택 시 다음 항목을 설정합니다. **장비 인증**에서 **인증서**를 선택한 경우 • **주문형 VPN**: **도메인/호스트 패턴**, **동작** 설정 후 ⊕을 클릭 • **사용자 인증서 입력방법**은 147페이지의 "Android 설정 등록하기"를 참고하세요. • **사용자 PIN 포함**: 장비 인증 시 사용자 PIN 포함 여부 선택 **장비 인증**에서 **공유 보안/그룹 이름**을 선택한 경우 • **그룹 이름** • **혼합 인증 사용** • **비밀번호 요청**: 연결 시 비밀번호 요청 여부 선택 • **공유 보안** 입력
Cisco AnyConnect	선택 시 **그룹 이름** 항목 입력
Juniper SSL	선택 시 **영역**, **역할** 항목 입력 • Juniper SSL을 선택 시 신규 VPN인 Pulse secure VPN이 지원됨, 이전 Juniper Pulse는 지원되지 않음
SonicWALL Mobile Connect	선택 시 **로그인 그룹** 또는 **도메인** 항목 입력

- **프록시 설정**은 다음과 같습니다.

항목	설명
없음	
수동	선택 시 **IP 주소** 및 **Port**, **사용자 이름**, **비밀번호** 항목 설정
자동	선택 시 **프록시 서버 URL** 항목 입력

연결 유형이 IKEv2인 VPN 설정하기

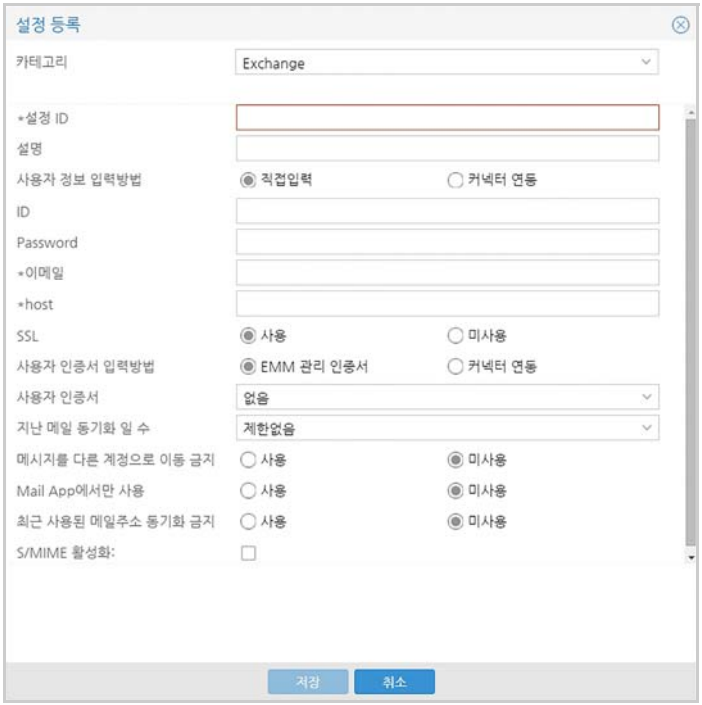
- **연결 유형**에서 **IKEv2** 선택 시 **VPN 상시 연결** 정보를 다음과 같이 설정합니다.
  - **VPN 상시 연결(감독 승인 장비만 가능)**을 선택하면 단말에서 VPN 비활성화가 금지됩니다.
  - 사용자가 자동 연결을 비활성화하도록 허용을 선택 또는 해제하세요.
  - 셀룰러와 Wi-Fi에 동일한 터널을 구성하려면 **셀룰러 및 Wi-Fi에 대해 동일한 터널 구성 사용** 확인란을 선택한 후 공통으로 사용될 VPN 연결 정보를 입력하세요.
    셀룰러와 Wi-Fi에 다른 터널을 구성하려면 **셀룰러**, **Wi-Fi** 탭을 선택한 후 VPN 연결 정보를 입력하세요
  - 하나의 단말 관리 프로파일 안에 **VPN 상시 연결**이 선택된 VPN 설정이 두 개 이상이면, 단말 관리 프로파일은 단말에 설치되지 않습니다.

항목	설명
서버 주소	VPN 서버의 IP 주소, 호스트 명, 또는 URL을 입력하세요.
로컬 식별자	IKEv2 Client를 식별하기 위한 값으로, 다음의 형식에 맞게 입력하세요. • FQDN, UserFQDN, Address, ASN1DN
원격 식별자	다음의 형식에 맞게입력하세요. • FQDN, UserFQDN, Address, ASN1DN
시스템 인증	시스템 인증 방법을 선택하세요. **공유 보안** 선택 시 **공유 보안 비밀번호**를 입력하세요. **인증서** 선택 시 다음을 입력하세요. • **사용자 인증서 입력방법**을 선택하세요. 사용자 인증서 입력방법은 147페이지의 "Android 설정 등록하기"를 참고하세요. • 서버 인증서 발급자 일반 이름 • 서버 인증서 일반 이름
EAP 활성화	활성화 여부를 선택하고 EAP 활성화 선택 시 **EAP 인증**의 사용자 인증 방법을 선택하세요. • **인증서** 선택 시 **사용자 인증서 입력방법**을 선택합니다. 사용자 인증서 입력방법은 147페이지의 "Android 설정 등록하기"를 참고하세요. • **비밀번호** 선택 시 사용자의 **ID**와 **비밀번호**를 입력하세요.

항목	설명
Dead Peer Detection 속도	VPN 장비와의 유용성을 확인하기 위한 주기를 설정합니다. (리소스가 변경되어야 하는지, 내용을 수정해야하는지 선택) • 사용안함, 30분마다, 10분마다, 1분마다
기기가 잠자기 모드인 동안 NAT 킵얼라이브 활성화	선택 시 기기가 잠자기 모드인 동안 NAT 킵얼라이브를 활성화하고 NAT 킵 얼라이브 간격을 설정하세요. • 지원 플랫폼: iOS 9
NAT 킵얼라이브 간격	NAT 킵 얼라이브 간격을 초 단위로 설정합니다. 기본값은 20초 입니다. • 지원 플랫폼: iOS 9
IPv4/IPv6 내부 서브넥 속성 사용	선택 시 IKEv2의 IPv4/IPv6 내부 서브넥 속성 사용이 가능합니다. • 지원 플랫폼: iOS 9
휴대성 및 멀티호밍 비활성화	선택 시 휴대성 및 멀티호밍(MOBIKE)을 비활성화합니다. • 지원 플랫폼: iOS 9
리다이렉트 비활성화	선택 시 IKEv2 커넥션의 리다이렉트가 비활성화합니다. • 지원 플랫폼: iOS 9
완벽한 전달 보안 활성화	선택 시 완벽한 전달 보안(PFS)이 활성화됩니다. • 지원 플랫폼: iOS 9
암호화 알고리즘	암호화 알고리즘을 선택합니다. • **IKE SA**: DES, 3DES, AES-128, AES-256, AES-128-GCM, AES-256-GCM • **하위 SA**: DES, 3DES, AES-128, AES-256, AES-128-GCM, AES-256-GCM
무결성 알고리즘	무결성 알고리즘을 선택합니다. • **IKE SA**: SHA1-96, SHA1-160, SHA2-256, SHA2-384, SHA2-512 • **하위 SA**: SHA1-96, SHA1-160, SHA2-256, SHA2-384, SHA2-512
Diffie Hellman 그룹	Diffie Hellman 알고리즘 사용시 사용할 그룹을 선택합니다. • **IKE SA**: 0, 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21 • **하위 SA**: 0, 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
시간(분 단위)	세션 만료 기간을 입력합니다. • **IKE SA**: 입력 범위는 10~14440이며, 기본값은 14440입니다. • **하위 SA**: 입력 범위는 10~14440이며, 기본값은 14440입니다.

Exchange 설정 등록하기

iOS 설정 카테고리에서 Exchange 를 선택한 후 다음의 항목을 입력하세요 .



- **설정 ID**, **설명**을 입력하세요.
- **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **ID**, **비밀번호**에 VPN 접속을 위한 사용자의 ID와 비밀번호를 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

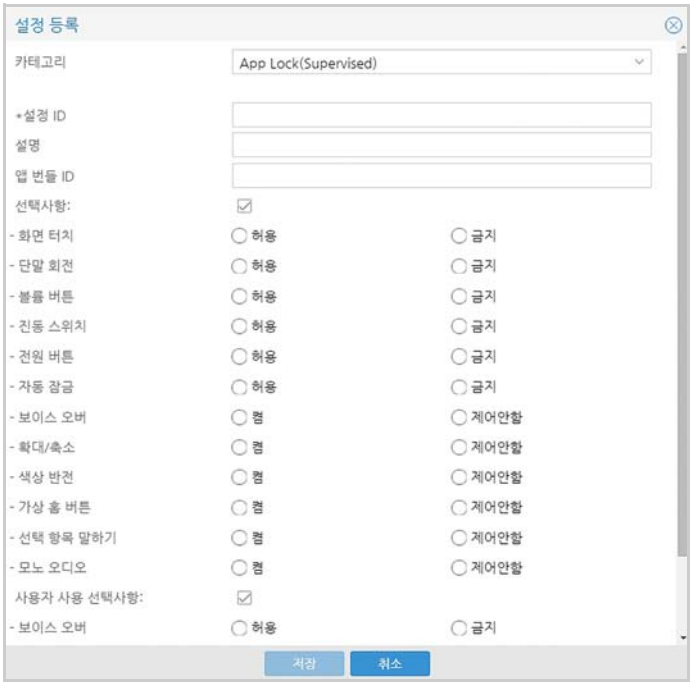
- **host**: 필수 입력 항목인 이용할 이메일 서버의 호스트 명을 입력하세요.
- **SSL** 사용 여부를 지정하세요.
- **사용자 인증서 입력방법**은 147페이지의 "Android 설정 등록하기"를 참고하세요.
- **지난 메일 동기화 일 수**: 제한없음, 1일, 3일, 1주일, 2주일, 1개월 중 선택
- **메시지를 다른 계정으로 이동 금지** 여부를 설정하세요.
- **Mail App에서만 사용** 여부를 설정하세요.
- **최근 사용된 메일주소 동기화 금지** 여부를 설정하세요.

- **S/MIME 활성화**를 다음과 같이 설정하세요.

항목	설명
S/MINE 서명 인증서 입력방법	선택 시 **S/MINE 서명 인증서** 또는 **S/MINE 서명 인증서 커넥터**를 선택하세요.
S/MIME 암호화 인증서 입력방법	선택 시 **S/MINE 암호화 인증서** 또는 **S/MINE 서명 인증서 커넥터**를 선택하세요.
메시지당 S/MIME 활성화 스위치 사용	사용 여부 선택

App Lock 설정 등록하기

단말을 싱글앱 모드로 설정하려면 App Lock 을 설정해야합니다 . 이 기능은 iOS 6.0 이상인 단말에 적용할 수 있습니다 . iOS 설정 카테고리에서 **App Lock (Supervised)** 을 선택한 후 , 다음의 항목을 입력하세요 .



- **설정 ID**, **설명**을 입력하세요.
- **앱 번들 ID**: 애플리케이션의 번들 ID를 입력하세요.
- **선택사항:** iOS 7.0 이상인 단말에 적용할 수 있는 기능으로, 아래 항목에 대하여 허용 여부를 설정하세요.
  - 화면 터치, 단말 회전, 볼륨 버튼, 진동 스위치, 전원 버튼, 자동 잠금, 보이스 오버, 확대/축소, 색상 반전, 가상 홈 버튼, 선택 항목 말하기, 모노 오디오
- **사용자 사용 선택사항:** iOS 7.0 이상인 단말에 적용할 수 있는 기능으로, 아래 항목에 대하여 허용 여부를 설정하세요.
  - 보이스 오버, 확대/축소, 색상 반전, 가상 홈 버튼

SSO 설정 등록하기

단말 사용자가 한 번의 로그인으로 추가 인증 없이 다른 앱에 엑세스할 수 있게 해주는 SSO(Single Sign On) 서비스를 설정할 수 있습니다 . iOS 설정 카테고리에서 **SSO** 를 선택한 후 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **계정명을** 입력하세요.
- **주체자를** 입력하세요.
- **영역**: SSO을 통해 이용할 수 있는 서비스 범위가 되는 도메인 명을 대문자로 입력하세요.
- **URL 접두어**: ∨을 클릭하여 다음과 같이 설정하세요.

항목	설명
URL 접두어	SSO을 통해 이용할 수 있는 URL 리스트 입력 후, ⊕을 클릭합니다. • 'http', 'https'와 같은 URL 프리픽스를 반드시 포함하여 입력 • URL 마지막에 '/' 포함하여 입력 • 예:http://www.example.com/, https://www.example.com/

- **앱 식별자**: ∨을 클릭하여 다음과 같이 설정하세요.

항목	설명
URL 접두어	SSO을 통해 이용할 수 있는 애플리케이션 리스트 입력 후, ⊕을 클릭하세요. • 애플리케이션 번들 ID를 입력하여 추가 • 애플리케이션 리스트에 추가된 항목이 없으면 모든 애플리케이션이 대상

Cellular 설정 등록하기

통신 네트워크 설정을 하는 카테고리입니다 . APN 설정이 이미 적용된 경우 Cellular 설정은 적용되지 않습니다 . Cellular 설정은 iOS 7 이상인 단말에 적용할 수 있습니다 . iOS 설정 카테고리에서 **Cellular** 를 선택한 후 , 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **AttachAPN** 영역을 설정하세요.

항목	설명
이름	해당 설정에 대한 이름 입력
인증 방식	**PAP, CHAP** 중 인증 방식 선택
사용자명	사용자 인증을 위한 단말 사용자명 입력
비밀번호	사용자 인증을 위한 단말 사용자의 비밀번호 입력

- **APNs** 영역을 설정하세요.

항목	설명
이름	해당 설정에 대한 이름 입력
인증 방식	**PAP, CHAP** 중 인증 방식 선택
사용자명	사용자 인증을 위한 단말 사용자명 입력
비밀번호	사용자 인증을 위한 단말 사용자의 비밀번호 입력
프록시 서버	프록시 서버의 IP 주소 입력
프록시 서버 포트	프록시 서버의 포트 입력

Airprint 설정 등록하기

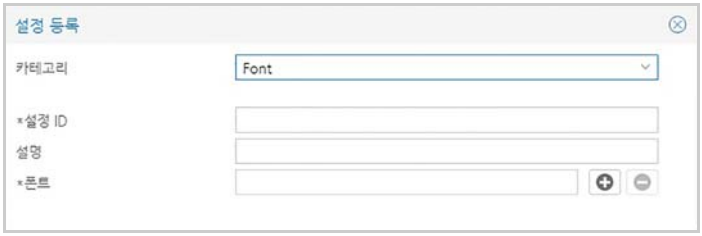
사용자 단말의 AirPrint 목록에 프린터를 추가하여, 서로 다른 개별 네트워크에 존재하는 단말과 프린터의 환경 설정을 보다 용이하게 도와줍니다 . iOS 설정 카테고리에서 **Airprint** 를 선택한 후 , 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **AirPrint Printers**: ∨을 클릭하여 **IP Address**, **Resource Path** 항목 입력 후, ⊕을 클릭하세요.

항목	설명
IP Address	AirPrint 기기의 IP 주소를 IP 패턴에 맞게 입력 • 예: 127.0.0.1
Resource Path	프린터의 리소스 경로를 다음과 같이 입력 • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer

Font 설정 등록하기

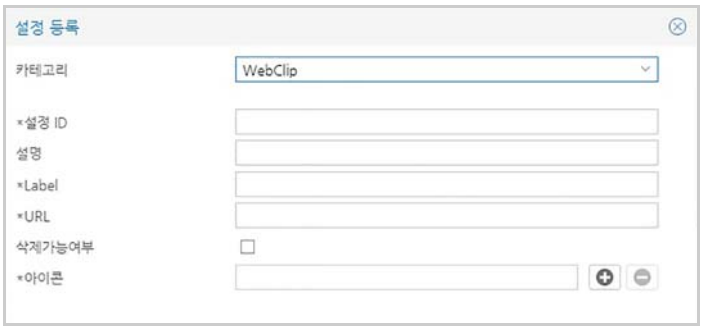
사용자 단말에 Font 를 추가하려면 iOS 설정 카테고리에서 **Font** 를 선택한 후 다음의 항목을 입력하세요 .



- **설정 ID**, **설명**을 입력하세요.
- **폰트**: ⊕을 클릭하면 나타나는 "폰트" 창에서 폰트를 추가하세요.

WebClip 설정 등록하기

사용자 단말의 홈 화면에 WebClip 을 추가하려면 iOS 설정 카테고리에서 **WebClip** 을 선택한 후 다음의 항목을 입력하세요 .



- **설정 ID**, **설명**을 입력하세요.
  - 입력 항목명 앞에 표시(*)는 필수 입력값이며, 나머지는 선택 사항입니다.
- **Label**: 홈 화면에 표시될 웹클립 이름을 입력하세요.
- **URL**: HTTP 또는 HTTPS로 시작하는 웹클립 URL을 입력하세요.
- **삭제가능여부**: 웹클립 삭제 허용 여부를 설정합니다.
  - 체크박스를 선택하면 단말 사용자가 삭제하는 것을 허용
  - 체크박스를 선택하지 않으면 사용자는 해당 웹클립을 삭제할 수 없지만, 해당 프로파일이 해제되면 설정한 웹클립도 삭제됨
- **아이콘**: 사용자 단말의 홈 화면에 표시될 아이콘을 ⊕을 클릭하여 추가하세요.
  - 파일 형식: PNG
  - 사이즈: 59 x 60 (px)
  - 아이콘을 지정하지 않으면 흰 사각형이 표시됨

AirPlay 설정 등록하기

AirPlay 설정은 iOS 7.0 이상의 단말에 적용할 수 있습니다 . AirPlay 를 설정하려면 iOS 설정 카테고리에서 **AirPlay** 를 선택한 후 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **화이트리스트(Supervised)**에 등록된 AirPlay 기기만이 사용자 단말 목록에 나타납니다.

항목	설명
화이트리스트 (Supervised)	∨을 클릭하여 장치 ID 입력 후 ⊕을 클릭 • 예: MAC 주소 패턴 a0:b1:c2:d4:e5:f6 에 맞게 입력

- **암호**: AirPay 기기에 대한 비밀번호를 입력하세요.

항목	설명
암호	∨을 클릭하여 **장치 이름**, **비밀 번호** 입력 후 ⊕을 클릭

전역 HTTP 프록시 설정 등록하기

iOS 설정 카테고리에서 **HTTP 프록시 (Supervised)** 를 선택한 후 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
  - 입력 항목명 앞에 표시(*)는 필수 입력값이며, 나머지는 선택 사항입니다.

- **프록시 유형**에 따라 해당 항목을 입력하세요.

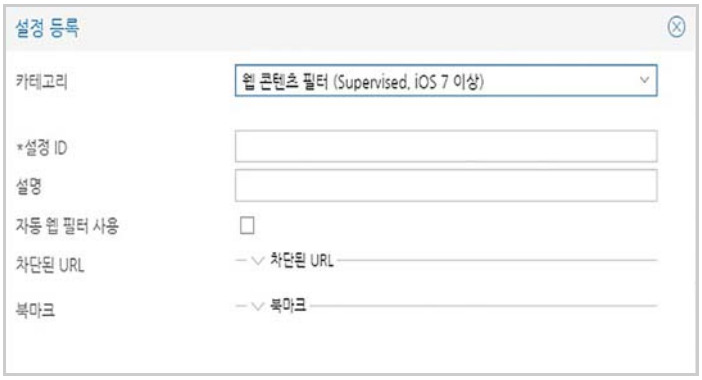
항목	설명
수동	• **프록시 서버 및 포트** 입력 • **사용자 이름**에 프록시 서버에서 인증할 단말 사용자 이름 입력 • **비밀번호**에 프록시 서버에서 인증할 단말 사용자의 비밀번호 입력
자동	• **프록시 PAC URL**에 자동 프록시 구성 파일인 PAC의 URL 입력 • **PAC 연결 실패시 직접 연결 허용 (iOS 7 이상)**을 선택하면 사용자 단말이 직접 연결하는 것을 허용

- **캡티브 네트워크 접근 허용 (iOS 7 이상)** 을 선택하면 프록시 서버를 통과하게 되어, 캡티브 네트워크에 대한 로그인 페이지를 보여줍니다.

웹 콘텐츠 필터 설정 등록하기

특정 URL 에 대하여 화이트리스트 또는 블랙리스트로 설정하는 카테고리입니다 .

iOS 단말에 웹 콘텐츠 필터를 설정하려면 iOS 설정 카테고리에서 **웹 콘텐츠 필터 (Supervised, iOS 7 이상**) 를 선택한 후 다음의 항목을 입력하세요 .



- **설정 ID**, **설명**을 입력하세요.
- **자동 웹 필터 사용**을 선택하여 **허용된 URL**을 추가하세요.

항목	설명
허용된 URL	∨을 클릭하여 허용할 URL 입력한 후 ⊕을 클릭

- **차단된 URL**: ∨을 클릭하여 차단할 URL 입력한 후 ⊕을 클릭
- **북마크:** ∨을 클릭하여 북마크 URL 입력한 후 ⊕을 클릭

Managed Domains 설정 등록하기

Managed domains 설정은 iOS 8.0 이상의 단말에 적용할 수 있습니다 . iOS 설정 카테고리에서 **Managed Domains (iOS 8 이상)** 를 선택한 후 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **Email 도메인:** ∨을 클릭하여 접속 가능한 Email 도메인을 입력한 후⊕을 클릭하세요.
- **Web 도메인:** ∨을 클릭하여 접속 가능한 Web 도메인을 입력한 후 ⊕을 클릭하세요.

네트워크 사용 규칙 설정 등록하기

iOS 9 단말에서 애플리케이션의 데이터 로밍 허용 여부와 셀룰러 데이터 사용의 허용 여부에 대한 네트워크 규칙을 설정합니다 . iOS 설정 카테고리에서 **네트워크 사용 규칙**을 선택한 후 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **Managed 앱 네트워크 설정**에 허용하려는 애플리케이션과 셀룰러 데이터 및데이터 로밍 허용 여부를 설정하세요.
  - **애플리케이션:** 🔍을 클릭하여 적용하려는 애플리케이션을 선택하세요.
  - **셀룰러 데이터:** ∨을 클릭하여 셀룰러 데이터 사용의 허용 및 금지를 선택하세요.
  - **데이터 로밍:** ∨을 클릭하여데이터 로밍의 허용 및 금지를 선택 **후** ⊕을 클릭하여 애플리케이션, 셀룰러 데이터, 데이터 로밍을 추가하세요.
  - 추가한 애플리케이션, 셀룰러 데이터, 데이터 로밍을 삭제하려면 우측의 **X**를 클릭하세요.

Windows 설정 등록하기

Windows 플랫폼에 단말 관리 프로파일의 설정을 등록하여 사용할 수 있습니다 . 입력 항목명 앞에 표시 (*) 는 필수 입력값이며 , 나머지는 선택사항입니다 .

Wi-Fi 설정 등록하기

Windows 설정 카테고리에서 **Wi-Fi** 를 선택한 후 다음의 항목을 입력하세요 .

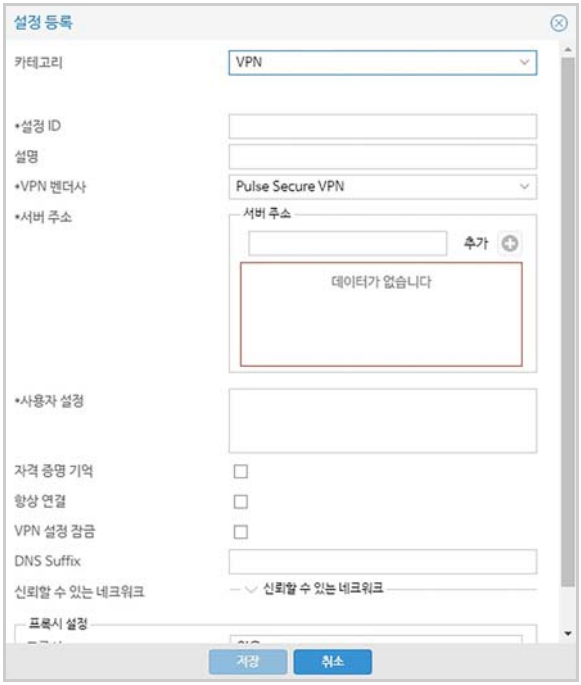
- **설정 ID**, **설명**을 입력하세요.
- **네트워크명(SSID)**: 연결할 무선 공유기의 식별자 입력, 특수 문자는 입력할 수 없습니다.
- **보안 유형**: 선택한 보안 유형에 따라 입력 항목 다릅니다.

항목	설명
Open	비밀번호 입력없이 Wi-Fi 연결이 가능합니다.
WEP	선택 시 비밀번호를 설정하여 사용합니다. • 비밀번호는 5– 13자리의 영문, 숫자(0-9, A-Z, a-z) 또는 10 – 26자리의 16진수(0-9, A-F, a-f)만 입력이 가능합니다.
WPA2 Personal	선택 시 비밀번호를 설정하여 사용합니다. • 비밀번호는 6– 63자리의 영문, 숫자, 특수 문자로 입력되어야 합니다. 입력 불가한 특수문자는 <,>,\,/,',” 입니다.
EAP	선택 시 **설정 XML** 코드를 입력하여 사용하세요.

- **자동 연결**: Wi-Fi 자동 연결 여부를 설정하세요.
- **숨김 여부**: 설정한 Wi-Fi를 단말에서 공개할지 여부를 설정하세요.
- **프록시 서버 및 포트**: 프록시 IP 주소 및 Port 번호를 설정하세요.

VPN 설정 등록하기

Windows 설정 카테고리에서 **VPN** 을 선택한 후 다음의 항목을 입력하세요 .



- **설정 ID**, **설명**을 입력하세요.
- **VPN 벤더사**를 선택하세요.
- **서버 주소**: VPN 서버의 IP 주소, 호스트 명, 또는 URL 입력하세요.
- **사용자 설정**: VPN 벤더사별 설정값을 XML 형태로 입력하세요.
- **자격 증명 기억, 항상 연결, VPN 설정 잠금 여부**를 설정하세요.
- **DNS Suffix**를 입력하세요.
- **신뢰할 수 있는 네크워크**에 IP 주소, 호스트 명, 또는 URL을 입력하세요.
- **프록시 설정**은 다음과 같습니다.

항목	설명
없음	
수동	선택 시 **프록시 서버 주소** 항목 입력
자동	선택 시 **프록시 서버 URL** 항목 입력

Exchange 설정 등록하기

Windows 설정 카테고리에서 **VPN** 을 선택한 후 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **이메일, ID, 비밀번호**에 Exchange 서버 접속을 위한 사용자의 이메일, ID, 비밀번호을 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

- **도메인**, **Exchange 서버 주소**를 지정하세요.
- **서버이름**: Exchange 서버명을 입력하세요.
- **Diagnostic Logging**의 로깅 수준을 선택하세요.

항목	설명
Logging off	이벤트 뷰어 로그에 기록을 남기지 않습니다.
Basic logging	기본 진단 로그 정보를 구성합니다.
Advanced logging	주요 보안 관련 이벤트 진단 로그 정보를 구성합니다.

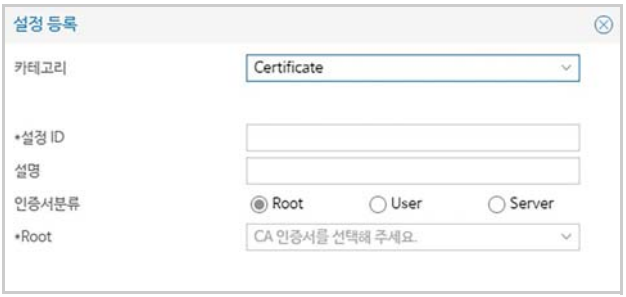
- **동기화 스케쥴**: Email 받을때, 수동, 15분, 30분, 60분 중 선택하세요.
- **과거 데이터 동기화 단위**: 제한없음, 3일, 1주일, 2주일, 1개월 중 선택하세요.
- **사용자 인증서 입력방법**은 147페이지의 "Android 설정 등록하기"를 참고하세요.
- 아래 항목에 대하여 동기화 여부를 설정하세요.

- 일정 동기화, 전화번호부 동기화, Email 동기화, 할 일 동기화

- 이메일 암호화 방법으로 **SSL** 사용 여부를 선택하세요.

Certificate 설정 등록하기

Windows 설정 카테고리에서 **Certificate** 을 선택한 후 다음의 항목을 입력하세요 .



- **설정 ID**, **설명**을 입력하세요.
- **인증서분류를 선택**하세요.

항목	설명
CA 인증서	선택 시 나타나는 **CA 인증서**에서 사용할 인증서를 선택하세요. • **인증서> 외부 인증서**에서 등록한 인증서 중, **인증서 유형**이 Root Certificate인 CA 인증서가 목록에 나타납니다.
사용자 인증서	선택 시 나타나는 **사용자 인증서**에서 사용할 인증서를 선택하세요. • **인증서> 외부 인증서**에서 등록한 인증서 중, **인증서 유형**이 User Certificate인 사용자 인증서가 목록에 나타납니다.
서버 인증서	선택 시 나타나는 **서버 인증서**에서 사용할 인증서를 선택하세요. • **인증서> 외부 인증서**에서 등록한 인증서 중, **인증서 유형**이 Server Certificate인 사용자 인증서가 목록에 나타납니다.

앱 관리 프로파일 설정하기

앱 관리 프로파일은 애플리케이션 , Android for Work, EMM Client, Secure Browser, mMail, SecuCamera, Knox Portal 로 구성되어 있습니다 .

- 애플리케이션: 업무용 애플리케이션 설치에 대한 필수 여부와 문자열 복사, 프린트, 공유, 화면 캡처 허용 여부를 설정합니다.
- Android for Work: Google이 제공하는 Android for Work 앱의 화면 캡처, 문자열 복사 허용 여부를 설정합니다.
- EMM Client: EMM 앱의 비밀번호와 화면 잠금에 대한 정책, 플랫폼별 버전 선택 정책을 설정합니다.
- Secure Browser: EMM 사용자에 한해 특정 사이트로 접근하기 위한 Secure Browser의 화이트리스트, 블랙리스트 등의 보안 정책을 관리합니다. Secure Browser 정책은 플랫폼에 따라 기능별 제약이 있습니다.
- mMail: 기업용 Exchange ActiveSync Client로서 메일, 일정, 연락처에 대한 기본적인 ActiveSync 기능을 제공합니다. mMail에 대한 접근 방법 및 동기화 조건 등을 설정합니다.
- SecuCamera: EMM 사용자가 단말에서 사진 촬영 시 지정된 서버나 메일로 바로 전송하여 외부 유출을 막는 동시에 편의성을 제공하는 카메라 보안 기능을 제공합니다
- Knox Portal: MDM 2.0의 경우 업무 애플리케이션의 보안 정책을 설정합니다.

앱 관리 프로파일은 관리 콘솔의 **프로파일 > 앱 관리 프로파일**에서 설정합니다 . 조직이나 그룹에 최신 정책이 적용되도록 앱 관리 프로파일 화면에서 **적용**을 클릭합니다 . 앱 관리 프로파일 등록 시 미리 등록해 놓은 앱 관리 프로파일 구성요소를 사용할 수 있습니다 . 앱 관리 프로파일 구성요소 등록은 EMM 라이선스상의 상품 기능에 따라 EMM Client, Secure Browser, mMail, SecuCamera, Knox Portal 에 대하여 가능하며앱 관리 프로파일을 구성요소로 등록하여 **구성요소 등록** 항목이 Y 로 표시된 프로파일에 정책 구성요소를 설정하는 방식입니다 . 앱 관리 정책 구성요소는 1 개만 등록 가능하기 때문에 추가하는 신규 구성요소로 교체됩니다 . 이미 설정되어 있는 구성요소는 목록에서 취소선으로 표시되며 선택할 수 없습니다 .

애플리케이션 정책 설정하기

애플리케이션 영역에서 업무용 애플리케이션 설치에 대한 필수 여부와 문자열 복사 , 프린트 , 공유 , 화면 캡처 허용 여부를 설정합니다 . 적용할 수 있는 제어 정책은 애플리케이션 종류에 따라 다를 수 있습니다 .

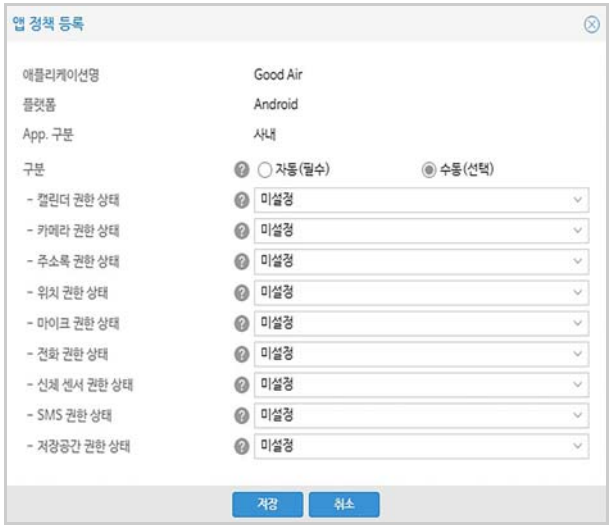
애플리케이션에서 추가할 수 있는 앱 목록은 **애플리케이션 > 사내 애플리케이션** 또는 **애플리케이션 > 외부 애플리케이션**에서 관리합니다 . 애플리케이션을 추가하는 방법은 223

페이지 14 장의 " 사내 애플리케이션 등록하기 " 와 226 페이지 14 장의 " 외부 애플리케이션 등록하기 " 를 참고합니다. 사내 애플리케이션 영역에서 추가한 애플리케이션은 EMM 내 앱 스토어에 보여지게 됩니다. 애플리케이션 정책은 수정 및 삭제 가능하며 앱 관리 프로파일에서 삭제된 애플리케이션은 해당 프로파일에서만 삭제되며, **애플리케이션** 메뉴에서 조회 가능합니다.

Note: Android 외부 애플리케이션과 Tizen Wearable 애플리케이션은 수정할 수 없으니, 앱 관리 프로파일에서 삭제한 후 추가하여 사용합니다.

애플리케이션을 추가하여 앱 정책을 등록하려면 다음의 절차를 따르세요.

1. **프로파일 > 앱 관리 프로파일**로 이동하세요.
2. 목록에서 애플리케이션 설정을 추가하려는 프로파일명을 클릭하세요.
   - 프로파일명과 설명은 "앱 관리 프로파일"창의 왼쪽 상단에 표시됩니다.
3. "앱 관리 프로파일" 창에서 **애플리케이션**을 클릭하세요.
4. 팝업창 우측에 있는 **애플리케이션** 옆의 ➕을 클릭하세요.
   "앱 목록" 창이 나타납니다.
5. 추가할 애플리케이션을 선택한 후 **다음**을 클릭하세요.
6. "앱 정책 등록" 창의 정보를 입력한 후 **저장**을 클릭하세요.
   추가한 애플리케이션은 **애플리케이션** 목록에 보여집니다.



- **구분**: 선택한 애플리케이션의 필수 설치 여부를 설정하세요. 플랫폼 및 애플리케이션별 설정 가능 항목은 다음의 표를 확인하세요.
  - **자동(필수)**: Knox Manage에 반드시 설치되어야 하는 앱으로, Knox 컨테이너가 설치된 단말에서 필수 애플리케이션이 설치되는 영역을 **Knox 생성 시 앱 설치 영역**에서 Knox, 일반, Knox+일반 중 선택하세요.
  - **수동(선택)**: Knox Manage에 해당 앱 설치가 가능합니다. 사용자가 단말에서 직접 설치를 진행해야 합니다.

- 앱 권한 설정: Android의 사내 앱을 선택하는 경우 앱에서 사용하는 단말의 접근 권한을 설정하세요.
  애플리케이션의 서비스를 제공하기 위하여 사용자의 단말에 접근하는 권한을 관리자가 제어할 수 있습니다. 앱 관리 프로파일에서 Android 단말의 사내 애플리케이션 등록 시, 권한 상태에 기본,허용,금지 3가지 권한을 설정할 수 있습니다.

항목	설명
권한 상태	캘린더, 카메라, 주소록, 위치, 마이크, 전화, 신체 센서, SMS, 저장공간
지원 단말	Android 6.0(Marshmallow) 이상의 삼성 단말
권한 설정	• 기본: 사용자가 단말에서 앱 접근 권한에서 허용/금지를 선택 • 허용: 앱에서 요구하는 단말의 리소스 권한을 관리자가 허용하며, 사용자는 단말에서 선택할 수 없음 • 금지: 앱에서 요구하는 단말의 리소스 권한을 관리자가 금지하며, 사용자는 단말에서 선택할 수 없음 **Note:** 구분값을 설치가능으로 선택한 경우, 설정된 권한 상태가 단말의 일반/Knox 영역에 모두 적용되며, 구분값을 필수로 선택한 경우, Knox 생성 시 앱 설치 영역(Knox, 일반, Knox+일반)에서 설정한 영역에만 설정된 권한 상태가 적용됩니다.
반영 방법	앱 관리 프로파일에 설정했지만, 단말에 적용할 때에는 **최신 단말 관리 프로파일/앱 정보 배포** 또는 **사내 애플리케이션 최신 정보 배포** 단말 제어를 전송

- 앱 정책 설정: 앱내에서 제어할 수 있는 정책을 설정하세요. 플랫폼 및 애플리케이션별 설정 가능 항목은 다음의 표를 확인하세요.

플랫폼	애플리케이션	구분	정책 설정
Android	사내	필수/설치가능	• SDK 사용 앱/ App Wrapping 앱: O • 일반 앱: X
Android	외부	설치가능	X
iOS	사내	필수/설치가능	O
iOS	외부	필수/설치가능	X
Tizen Wearable	사내	필수	X

- **문자열 복사**: 해당 앱에서 문자열 복사를 허용할지 여부를 설정하세요.
- **화면 캡처**: 해당 앱에서 화면 캡처를 허용할지 여부를 설정하세요.
- **프린트**: 해당 앱에서 프린트 사용을 허용할지 여부를 설정하세요.
- **공유**: 해당 앱에서 공유를 허용할지 여부를 설정하세요.
- **설정파일**: 해당 앱에서 설정 파일을 적용할지 여부를 설정하세요. 사내 애플리케이션 등록 시 **App Wrapping 사용** 확인란을 선택한 경우에 설정 할 수 있습니다.
  - **파일 업로드**: **Browser**를 클릭하여 .INI 형태의 앱 설정파일을 등록하세요. 파일 사이즈는 최대 500KB까지 가능하며 1개만 등록 가능합니다. 등록한 설정 파일을 삭제하려면 **X**를 클릭합니다.

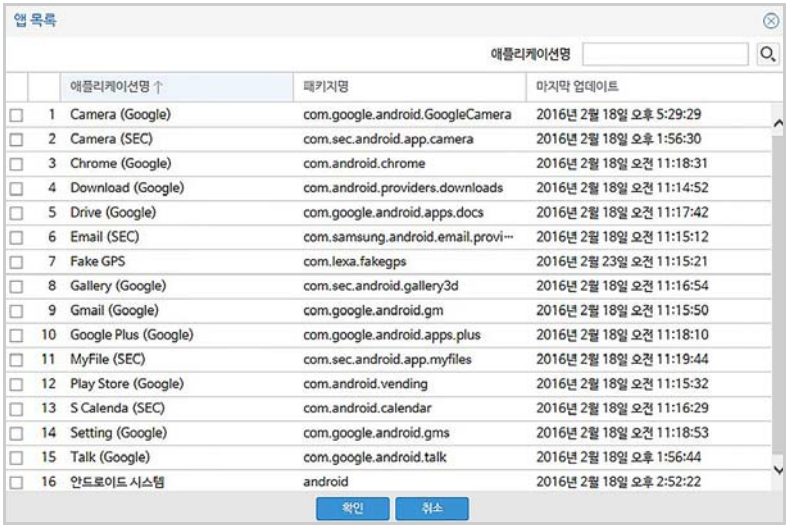
7. 앱 관리 프로파일의 설명을 수정하려면 “앱 관리 프로파일” 창에서 프로파일명 옆의 을 클릭하세요. 설명을 입력하고 저장을 클릭하세요.
8. 설정한 정책을 조회하려면 “단말 관리 프로파일” 창에서 프로파일명 옆의 **프로파일 정책**을 클릭하세요. 플랫폼별 상세 정책이 조회됩니다.

Android for Work 앱 설정하기

Android for Work 앱은 Android 단말에서 업무용 및 개인 데이터를 분리하여 안전하게 데이터를 보호 및 관리합니다 . Android for Work 앱의 정책은 Google 정책을 따르며 , EMM 은 Android for Work 앱의 화면 캡처 및 문자열 복사의 허용 여부를 제어합니다 . **Android for Work** 에서 제어 정책을 적용하려는 앱은 **애플리케이션 > 제어 애플리케이션**에서 등록합니다 . Android for Work 앱 등록에 대한 자세한 내용은 228 페이지 14 장의 “ 제어 애플리케이션 등록하기 " 를 참고하세요 .

Android for Work 앱을 추가하려면 다음의 절차를 따르세요 . 수정을 불가능하기 때문에 삭제 후 Android for Work 앱을 추가하세요 .

1. **프로파일 > 앱 관리 프로파일**로 이동하세요.
2. 목록에서 Android for Work 앱을 설정하려는 프로파일명을 클릭하세요.
3. “앱 관리 프로파일” 창에서 **Android for Work**을 클릭하세요.
4. Android for Work 앱을 추가하려면 팝업창 우측에 있는 **Android for Work** 옆의 을 클릭하세요. “앱 목록” 팝업창이 나타납니다.



5. 앱 목록에서 애플리케이션을 선택 후 **확인**을 클릭하세요.
   - 애플리케이션은 다중 선택이 가능합니다.

EMM Client 정책 설정하기

단말에 설치된 EMM 애플리케이션에 대한 정책을 설정합니다 . 사용자가 EMM 을 실행할 때 , 해당 정책을 받고 단말을 제어하게 됩니다 . 로그인 , 화면 잠금 , 컴플라이언스 각 항목에 대한 정책 설정을 추가하거나 수정할 수 있습니다 .

정책에 대한 자세한 내용은 407 페이지 18 장의 “EMM Client 애플리케이션 정책 " 을 참고하세요 .

EMM Client 정책을 설정하려면 다음의 절차를 따르세요 .

1. **프로파일 > 앱 관리 프로파일**로 이동하세요.
2. 목록에서 EMM Client 설정을 추가하려는 프로파일명을 클릭하세요.
3. “앱 관리 프로파일” 창에서 **EMM Client**를 클릭하세요.
4. 팝업창 우측 **EMM Client 정책** 옆의 을 클릭하세요.
   “EMM Client 정책 수정” 창이 나타납니다.

5. “EMM Client 정책 수정” 창의 정보 입력 후 **저장**을 클릭하세요.
   - 수정한 정책을 **EMM Client 정책** 목록에서 확인하세요.
6. **확인**을 클릭하세요.

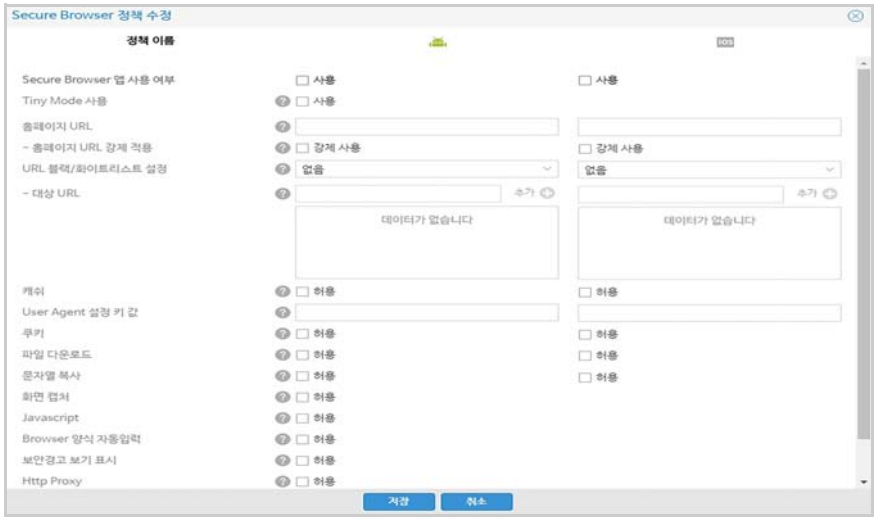
Secure Browser 정책 설정하기

Secure Browser 란 EMM 사용자에 한해 특정 사이트로 접근하도록 하기 위해 제공되는 브라우저입니다 . 다른 애플리케이션과 마찬가지로 브라우저 실행 시 해당 정책을 받고 제어하게 됩니다 . 사용자에게 URL 요청을 받은 후 해당 URL 이 화이트리스트 또는 블랙리스트에 해당되는 URL 인지 확인 후 동작 여부를 결정하게 됩니다 . Secure Browser 를 사용하려면 **애플리케이션 > EMM 애플리케이션** 메뉴에서 해당 앱을 등록해야합니다.

정책의 기능별 자세한 내용은 409 페이지 18 장의 “Secure Browser 애플리케이션 관리 정책 " 을 참고하세요 .

Secure Browser 정책을 설정하려면 다음의 절차를 따르세요 .

1. **프로파일 > 앱 관리 프로파일**로 이동하세요.
2. 목록에서 Secure Browser 설정을 추가하려는 프로파일명을 클릭하세요.
3. “앱 관리 프로파일” 창에서 **Secure Browser**를 클릭하세요.
4. 팝업창 우측 **Secure Browser 정책** 옆의 을 클릭하면 “Secure Browser 정책 수정 ” 창이 나타납니다.



5. “Secure Browser 정책 수정” 창에서 정책 설정 후 **저장**을 클릭하세요.

mMail 정책 설정하기

기업용 Exchange ActiveSync Client 인 Samsung SDS mMail 에 대한 접근 방법 및 동기화 조건 등을 설정합니다 . **mMail** 정책 설정은 EMM 라이선스 관리 서버 (LMS) 에서 발급된 라이선스가 있을 경우 사용 가능합니다 . 정책의 기능별 자세한 내용은 411 페이지 18 장의 “mMail 애플리케이션 관리 정책 " 을 참고하세요 .

mMail 정책을 설정하려면 다음의 절차를 따르세요 .

1. **프로파일 > 앱 관리 프로파일**로 이동하세요.
2. 목록에서 mMail 설정을 추가하려는 프로파일명을 클릭하세요.
3. “앱 관리 프로파일” 창에서 **mMail**을 클릭하세요.

4. 팝업창 우측 **mMail 정책** 옆의 을 클릭하세요.
   "mMail 정책 수정" 창이 나타납니다.

5. "mMail 정책 수정" 창에서 정책 설정 후 **저장**을 클릭하세요.
6. **확인**을 클릭하세요.

SecuCamera 정책 설정하기

SecuCamera 는 EMM 사용자가 단말에서 사진 촬영 시 지정된 서버나 메일로 바로 전송하여 외부 유출을 막는 보안 카메라입니다 . SecuCamera 는 EMM 이 운영되는 장소에서만 사용이 가능하며 , 이외 장소에서는 실행되지 않습니다 . SecuCamera 를 사용하려면 **설정 > 서비스 > 라이선스 정보**에서 SecuCamera 라이선스가 필요하고 , **애플리케이션 > EMM 애플리케이션** 메뉴에서 해당 앱을 등록해야합니다 .

SecuCamera 정책을 설정하거나 앱 사용여부를 취소하려면 다음의 절차를 따르세요 .

1. **프로파일 > 앱 관리 프로파일**로 이동하세요.
2. 목록에서 SecuCamera 설정을 추가하려는 프로파일명을 클릭하세요.
3. "앱 관리 프로파일" 창에서 **SecuCamera**를 클릭하세요.
4. 팝업창 우측 **SecuCamera 정책** 옆의 을 클릭하세요.
   "SecuCamera 정책 수정" 창이 나타납니다.
5. "SecuCamera 정책 수정" 창에서 **SecuCamera 앱 사용 여부**의 **사용** 확인란을 선택한 후 **저장**을 클릭하세요.
   - 사용자의 이메일은 EMM에 사용자 등록 시 설정합니다.
6. SecuCamera 정책을 취소하려면 **사용** 확인란에 선택을 해제한 후 **저장**을 클릭하세요.

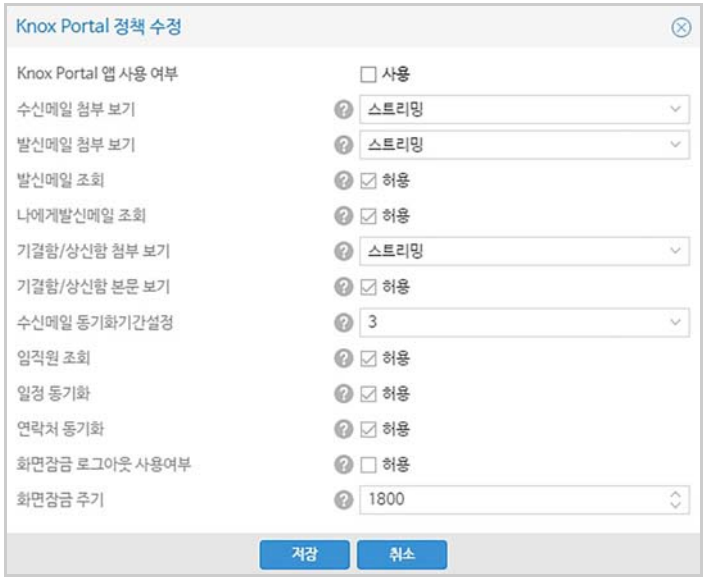
Knox Portal 정책 설정하기

해당 정책은 삼성그룹향 라이선스인 경우에만 사용 가능합니다 . 라이선스 확인 방법은 **설정 > 서비스 > 라이선스 정보**의 **삼성그룹향**에서 사용 여부를 확인합니다 .

삼성 그룹사에서 사용하는 업무용 앱인 Knox Portal 애플리케 0 이션에 대한 정책을 설정합니다 . 메일 , 결재 , 임직원 정보 등에 대한 정책 설정을 추가하거나 수정할 수 있습니다 . EMM 사용자가 Knox Portal 애플리케이션 실행 시 해당 정책을 받고 단말을 제어하게 됩니다 . 정책에 대한 자세한 설명은 413 페이지 18 장의 “Knox Portal 애플리케이션 관리 정책 " 을 참고하세요 .

Knox Portal 정책을 설정하거나 앱 사용 여부를 취소하려면 다음의 절차를 따르세요 .

1. **프로파일 > 앱 관리 프로파일**로 이동하세요.
2. 목록에서 Knox Portal을 설정하려는 프로파일명을 클릭하세요.
3. “앱 관리 프로파일” 창에서 **Knox Portal**을 클릭하세요.
4. 팝업창 우측에 있는 **Knox Portal 정책** 옆의 을 클릭하세요.
   “Knox Portal 정책 수정” 창이 나타납니다.



5. “Knox Portal 정책 수정” 창에 정보 입력 후 **저장**을 클릭하세요.
   - 수정한 정책은 Knox Portal 정책 목록에서 확인합니다.
   - Knox Portal **정책을 취소하려면 사용 확인란에 선택을 해제한 후 저장을 클릭**하세요.

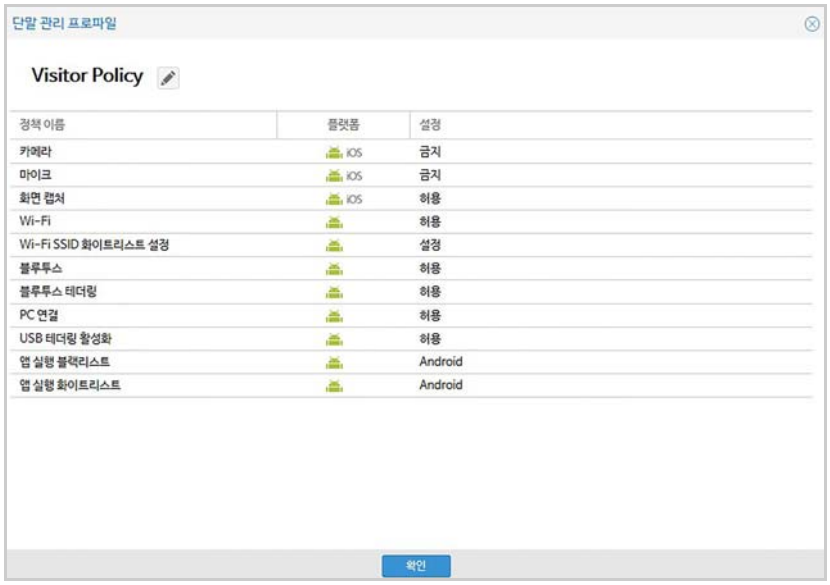
방문자 정책 설정하기

방문자의 단말을 관리하기 위해 EMM 관리 콘솔에서 방문자 정책을 설정합니다 . EMM 라이선스 관리 서버 (LMS) 에서 발급된 라이선스가 있는 경우 , 별도의 Tenant ID 로 로그인하여 방문자의 단말을 관리합니다 .

프로파일 > 단말 관리 프로파일에 기본적으로 제공되는 방문자 프로파일인 **Visitor Policy** 에서 방문자 정책을 설정합니다 . 해당 방문자 정책은 삭제할 수 없습니다 . 방문자 정책에 대한 상세한 내용은 414 페이지의 " 방문자 정책 " 을 참고하세요 .

방문자 정책을 설정하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 목록에서 방문자 관리 프로파일인 **Visitor Policy**를 클릭하세요.
3. "단말 관리 프로파일" 창에서 **방문자 정책** 옆의 를 클릭하세요.



4. “방문자 정책 수정” 창에서 정책을 수정하세요.
5. **저장**을 클릭하세요.

앱 관리 프로파일의 구성요소 등록하기

프로파일에 등록된 구성요소는 삭제가 불가능하기 때문에 구성요소를 삭제하려면 프로파일에서 해제한 후 삭제해야 합니다 . 앱 관리 프로파일의 구성요소를 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 앱 관리 프로파일 구성요소**로 이동하세요.
2. ➕을 클릭한 후, **정책 등록** 아래 EMM Client, Secure Browser, mMail, SecuCamera 중 선택하세요.

3. 해당 정책 구성요소 생성 창에서 **정책 구성요소 명**과 **설명**을 입력하고 **다음**을 클릭하세요.
   - Secure Browser 정책 구성요소를 생성하는 경우에는 플랫폼 목록에서 Android 또는 iOS를 선택하세요.
   - "기본 정보" 탭의 **정책 구성요소 명**은 수정할 수 없습니다.
4. 해당 정책 수정 창에서 앱 관리 정책을 설정하세요.
   상세 정책 설정 방법에 대한 자세한 내용은 다음을 참고하세요.
   - EMM Client 앱 정책 설정: 185페이지의 "EMM Client 정책 설정하기"
   - Secure Browser 앱 정책 설정: 185페이지의 "Secure Browser 정책 설정하기"
   - mMail 앱 정책 설정: 186페이지의 "mMail 정책 설정하기"
   - SecuCamera 앱 정책 설정: 187페이지의 "SecuCamera 정책 설정하기"
   - Knox Portal 앱 정책 설정: 188페이지의 "Knox Portal 정책 설정하기"
5. **저장**을 클릭하세요.

11 Knox 컨테이너

Knox 컨테이너는 단말에서 개인 공간으로부터 업무 데이터 및 앱을 분리하기 위하여 제공되는 가상의 모바일 보안 환경입니다 .

삼성 단말에서 Knox 컨테이너를 사용하려면 Knox 컨테이너를 등록하고 Knox 컨테이너에 적용할 정책과 설정을 구성합니다 . EMM 에서 지원하는 Knox 컨테이너는 다음과 같은 두가지 유형이 있으며 , 컨테이너는 유형에 상관없이 1 개만 생성할 수 있습니다 .

- 런처(General): 단말에서 일반 영역과 가상 분할하여 사용하는 Knox 컨테이너로 개인 영역으로 이동이 가능합니다.
- 폴더(LightWeight): 단말에 폴더 형태로 생성되는 Knox 컨테이너로, 일반 영역 간의 이동이 General 유형보다 편리합니다.

Note:
- Knox 영역에서 GCM(Google Cloud Messaging)을 통한 Samsung SDS Push를 깨우는 명령을 수행할 수 없습니다. 따라서 Knox 내 설치된 애플리케이션의 경우 Samsung SDS Push 수신이 지연될 수 있습니다.
- Public Push를 사용하는 경우 컨테이너 only 유형은 사용할 수 없습니다.

Knox 컨테이너 만들기

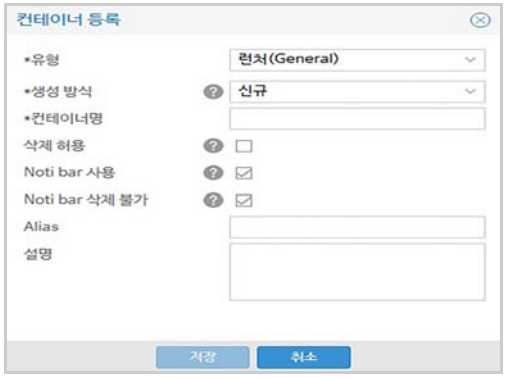
단말 관리 프로파일을 신규로 생성한 후 Knox 컨테이너를 등록 , 수정 , 삭제할 수 있습니다 . 단말 관리 프로파일을 등록하려면 135 페이지 10 장의 " 신규 프로파일 등록하기 " 또는 136 페이지 10 장의 " 구성요소 방식의 프로파일 등록하기 " 을 참고하세요 . 추가 및 변경된 Knox 컨테이너 정보를 단말에 적용하기 위해서 , 조직이나 그룹에 프로파일을 할당한 후 , **적용** 버튼을 클릭하여 프로파일을 배포합니다 . 또는 **최신 단말 관리 프로파일 / 앱 정보 배포** 단말 제어 명령을 조직별 , 그룹별 또는 개별 전송합니다 .

신규 Knox 컨테이너 등록하기

Knox 컨테이너를 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 프로파일명을 클릭하세요. "단말 관리 프로파일" 창이 나타납니다.
3. "단말 관리 프로파일" 창에서 **Knox > 컨테이너 관리**로 이동하세요.

4. **컨테이너 관리** 옆의 ➕을 클릭하세요. “컨테이너 등록” 창이 나타납니다.



5. **유형**과 **생성 방식**을 선택한 후, **컨테이너 명**, **삭제 허용**, **Alias**, **설명** 입력 후 **저장**을 클릭하세요.
   - **컨테이너명**은 수정할 수 없습니다.
   - **생성 방식**을 **재사용**으로 선택하면, **컨테이너명**과 **Alias**는 기본값으로 설정되며 수정 불가합니다. 기본 컨테이너를 사용하는 경우, 사용자 단말에 새로운 단말 관리 프로파일로 변경하더라도 기존의 Knox 컨테이너가 삭제되지 않고 유지된 상태에서 정책 및 설정만 변경됩니다. 재사용을 선택하면 Noti bar 알림이 사용으로 선택되고 삭제는 불가능합니다.
   - 사용자가 임의로 Knox 컨테이너를 삭제할 수 없게하려면, **삭제 허용**을 선택하지 않습니다. **삭제 허용**을 선택한 경우, 사용자의 단말에 Knox 컨테이너를 삭제하는 버튼이 활성화되며 Knox 컨테이너의 삭제가 가능합니다.
   - **Noti bar 사용**을 선택하면, 설치할 컨테이너가 있는 경우 사용자의 단말 상단의 알림바에 Knox 컨테이너 설치 알림이 표시됩니다. 기본 값은 알림 사용입니다.
   - Knox 컨테이너 설치 알림 메시지를 삭제하지 못하게 하려면 **Noti bar 삭제 불가**를 선택합니다. Knox 컨테이너가 생성되면 알림 메시지가 사라집니다. 기본 값은 알림 삭제 불가 입니다.
6. 생성한 Knox 컨테이너 정책 또는 설정을 등록하세요. 195페이지의 "Knox 컨테이너 정책 및 설정 추가하기"를 참고하세요.
7. 할당된 조직 또는 그룹에 속한 단말에 Knox 컨테이너를 배포하려면 “단말 관리 프로파일” 창에서 **적용**을 클릭하세요. 확인 메시지가 나타나면 **예**를 클릭하세요.

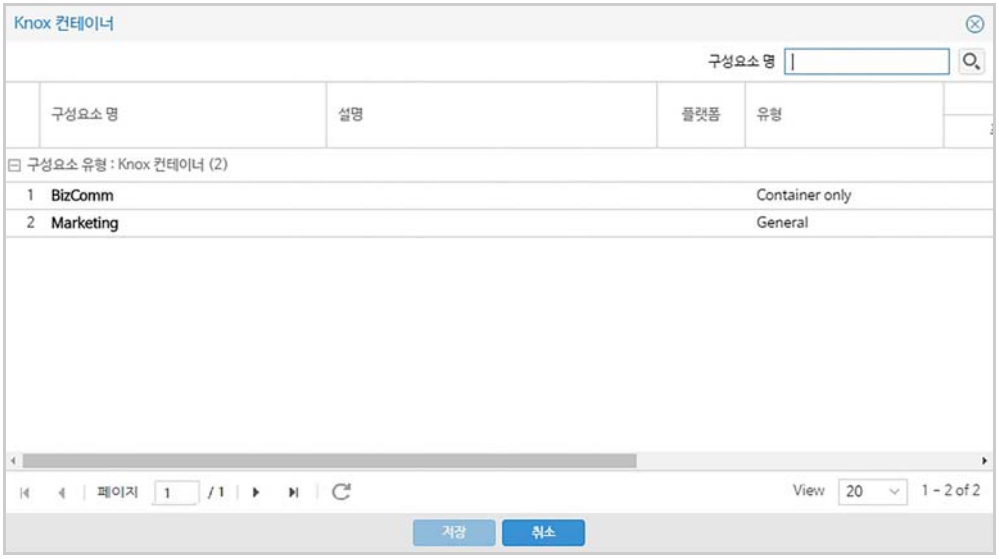
Note: OS 위변조를 한 단말의 경우, Knox 컨테이너를 생성할 수 없습니다.

구성요소 방식의 Knox 컨테이너 등록하기

단말 관리 프로파일을 구성요소로 등록하여 **구성요소 등록** 항목이 Y 로 표시된 프로파일에 Knox 컨테이너 구성요소를 추가하는 방법입니다. Knox 컨테이너 구성요소를 생성할 경우에는 생성 방식은 재사용이 아닌 신규로만 가능합니다 .Knox 컨테이너 구성요소를 등록한 후 정책 및 설정 구성요소를 등록해야 합니다 . Knox 컨테이너의 정책 및 설정 구성요소 등록 방법에 대한 자세한 내용은 196 페이지의 "Knox 정책 구성요소와 설정 구성요소 추가하기 " 를 참고하세요 .

Knox 컨테이너 구성요소를 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 프로파일명을 클릭하세요. “단말 관리 프로파일” 창이 나타납니다.
3. “단말 관리 프로파일” 창에서 **Knox > 컨테이너 관리**로 이동하세요.
4. **컨테이너 관리** 옆의 ➕을 클릭하세요. “Knox 컨테이너 조회” 창이 나타납니다.



5. **구성요소 명**을 검색하거나 조회된 목록에서 등록하려는 구성요소를 선택하고 **저장**을 클릭하세요.
6. 생성한 Knox 컨테이너 정책 또는 설정을 설정하세요. 195페이지의 "Knox 컨테이너 정책 및 설정 추가하기"를 참고하세요.
7. “단말 관리 프로파일” 창에서 **확인**을 클릭하세요.

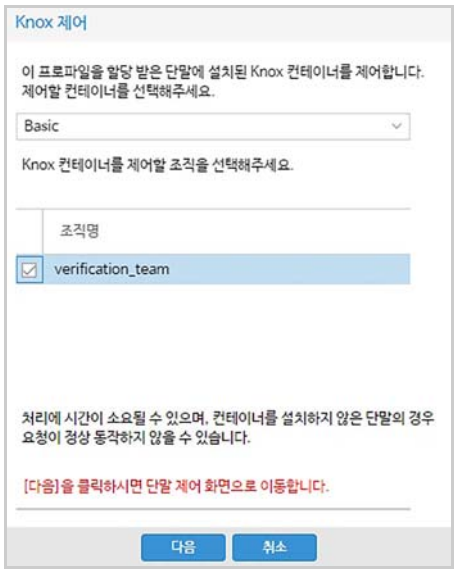
Note:
- OS 위변조를 한 단말의 경우, Knox 컨테이너를 생성할 수 없습니다.
- 구성요소로 등록한 Knox 컨테이너의 삭제는 해당 프로파일에서만 삭제되며, **프로파일 > 단말 관리 프로파일 구성요소**에서 조회 가능합니다.

Knox 컨테이너 제어하기

프로파일이 할당된 조직이나 그룹에 설치된 Knox 컨테이너를 단말 제어 명령으로 제어할 수 있습니다 . 단말 제어 명령은 Knox 컨테이너와 조직 및 그룹을 선택한 후 전송하며 , Knox 컨테이너가 설치되지 않은 단말에는 적용되지 않습니다 . 프로파일을 할당받은 조직 및 그룹의 단말에 설치된 Knox 컨테이너를 제어하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 프로파일 목록에서 Knox 컨테이너를 제어하려는 프로파일명을 클릭하세요.
3. Knox 컨테이너를 제어하려면 "단말 관리 프로파일" 창에서 프로파일명 옆의 **프로파일 할당**을 클릭하세요.

4. **조직** 또는 **그룹** 우측의 Knox 을 클릭하세요.
5. "Knox 제어" 창에서 제어하려는 **Knox 컨테이너**와 **조직명** 및 **그룹 ID**를 선택하고, **다음**을 클릭하세요.



- 그룹을 선택한 경우, 그룹에 속한 모든 사용자 단말이 제어됩니다.

- 조직을 선택한 경우, 조직내 속한 그룹의 사용자 단말은 제어되지 않습니다.
- Knox 컨테이너가 설치되지 않은 단말의 경우, Knox 컨테이너 제어가 적용되지 않습니다.

6. “단말 제어 - Knox 컨테이너명” 창에서 단말 제어 명령을 전송하세요.
   해당 Knox 컨테이너의 조직 및 그룹에 최신 정책이 적용됩니다. 단말 제어 명령 전송 방법에 대한 자세한 내용은 128페이지 9장의 “단말 제어 명령 보내기"를 참고하세요.

Knox 컨테이너 정책 및 설정 추가하기

Knox 컨테이너에 적용할 정책과 설정을 등록, 수정, 삭제합니다. 추가 및 변경된 Knox 정책를 단말에 적용하기 위해서, **적용** 버튼을 클릭하여 프로파일을 배포하거나 **최신 단말 관리 프로파일/앱 정보 배포** 단말 제어 명령을 조직별, 그룹별 또는 개별 전송합니다.

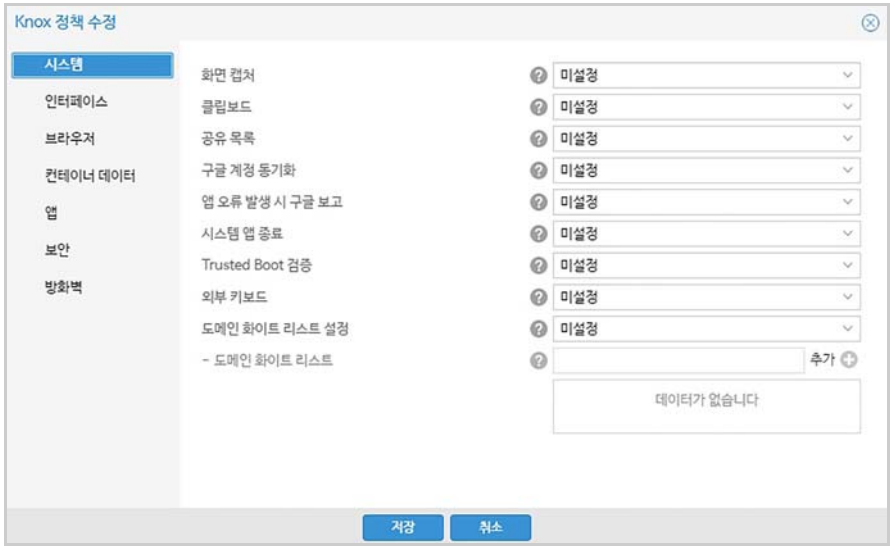
Knox 컨테이너의 설정 삭제 시 , 단말의 Trusted Anchor Database 의 해당 설정에서 등록된 인증서가 삭제됩니다 . 또한 삭제하는 VPN 설정이 Cisco AnyConnect, StrongSwan 인 경우 , VPN 설정 삭제 후 사용자 단말을 재부팅해야 합니다 . 제어 가능한 정책의 상세 내용은 390 페이지 18 장의 “Knox 영역 단말 관리 정책 " 설명을 참고하세요

Knox 컨테이너에 정책을 추가하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 프로파일명을 클릭하세요. "단말 관리 프로파일" 창이 나타납니다.
3. "단말 관리 프로파일" 창에서 **Knox** 탭을 클릭하세요.
4. 정책을 추가할 컨테이너를 클릭하세요.

5. 선택한 컨테이너명 아래의 **정책**을 클릭하세요.
6. **Knox 정책** 옆의 을 클릭하세요.

7. “Knox 정책 수정” 창에서 정책을 설정하고 **저장**을 클릭하세요.



8. 할당된 조직 또는 그룹에 속한 단말에 Knox 컨테이너 정책을 배포하려면 “단말 관리 프로파일” 창에서 **적용**을 클릭하세요. 확인 메시지가 나타나면 **예**를 클릭하세요.

Knox 정책 구성요소와 설정 구성요소 추가하기

단말 관리 프로파일을 구성요소로 등록하여 **구성요소 등록** 항목이 Y 로 표시된 프로파일에 정책 및 설정 구성요소를 추가하는 방법입니다 . 정책 구성요소는 Knox 컨테이너별 1 개만 등록 가능하기 때문에 추가하는 신규 구성요소로 교체됩니다 . 설정 구성요소는 여러개 선택 가능하며 이미 설정되어 있는 구성요소는 목록에서 취소선으로 표시되며 선택할 수 없습니다 . Knox 정책 구성요소와 설정 구성요소를 추가하려면 다음의 절차를 따르세요 .

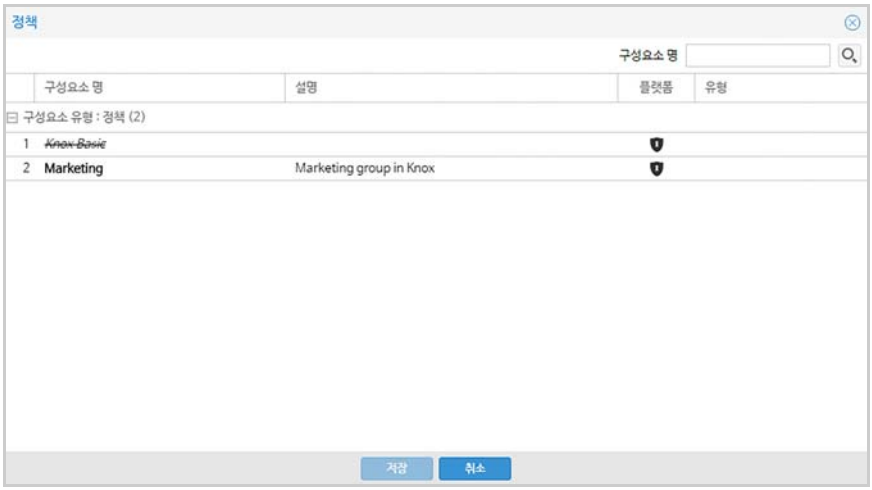
1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 프로파일명을 클릭하세요."단말 관리 프로파일" 창이 나타납니다.
3. "단말 관리 프로파일" 창에서 **Knox**를 클릭하세요.
4. 정책 및 설정을 추가할 컨테이너를 클릭하세요.

- Knox의 정책을 설정하려면 선택한 컨테이너명 아래의 **정책**을 클릭하세요.

  가. **Knox 정책** 옆의 을 클릭하세요. “정책” 창에서 구성요소 유형이 정책이며 Knox 컨테이너 플랫폼으로 등록된 구성요소 목록이 조회됩니다.

  - 설정된 상세 내용을 조회하려면 구성요소명을 클릭하세요.

나. 설정할 구성요소를 선택한후 **저장**을 클릭하세요.



- Knox의 설정을 추가하려면 선택한 컨테이너명 아래의 **설정**을 클릭하세요.

  가. **Knox 설정** 옆의 ➕을 클릭하세요. "Knox 설정" 창에서 구성요소 유형이 설정이며 Knox 컨테이너 플랫폼으로 등록된 구성요소 목록이 조회됩니다.

  - 설정된 상세 내용을 조회하려면 구성요소명을 클릭하세요.

  나. 설정할 구성요소를 선택한 후 **저장**을 클릭하세요.

Knox 설정 등록하기

Knox 플랫폼에 단말 관리 프로파일의 설정을 등록하여 사용할 수 있습니다 . Knox 컨테이너의 설정 삭제 시 , 단말의 Trusted Anchor Database 의 해당 설정에서 등록된 인증서가 삭제됩니다 . 또한 삭제하는 VPN 설정이 Cisco AnyConnect, StrongSwan 인 경우 , VPN 설정 삭제 후 사용자 단말을 재부팅해야 합니다 .

Knox 설정을 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 프로파일명을 클릭하세요. "단말 관리 프로파일" 창이 나타납니다.
3. "단말 관리 프로파일" 창에서 **Knox**를 클릭하세요.
4. 설정을 추가할 컨테이너명을 클릭하세요.
5. 선택된 컨테이너명 하단의 **설정**을 클릭하세요.
6. **Knox 설정** 우측의 ➕을 클릭하세요.
7. "Knox 설정 등록" 창의 **카테고리** 목록에서 추가할 항목을 선택한 후 해당 카테고리의 정보를 입력하세요. 카테고리별 설정 정보에 대한 자세한 내용은 아래의 내용을 참고하세요.
   - 입력 항목명 앞에 표시(*)는 필수 입력값이며, 나머지는 선택사항입니다.
8. **저장**을 클릭하세요.
   등록된 설정 목록이 조회됩니다.

9. 할당된 조직 또는 그룹에 속한 단말에 Knox 컨테이너 정책을 배포하려면 "단말 관리 프로파일" 창에서 **적용**을 클릭하세요. 확인 메시지가 나타나면 **예**를 클릭하세요.

Email Account 설정 등록하기

Knox 설정 카테고리에서 Email Account 를 선택한 후 , 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **삭제 가능**: 단말 사용자가 Knox 영역의 Email Account 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 Email Account 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 Email Account 설정을 삭제하는것이 금지됩니다. • 사용자 단말에서는 Email Account 설정을 삭제하는 버튼이 비활성화 됩니다.

- **기본 계정**: 기본 계정 사용 여부를 설정하세요.
- **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **이메일**에 Email 접속을 위한 사용자의 이메일을 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

- **수신 서버 프로토콜**을 선택하세요.
  - POP3 (pop3)
  - IMAP (imap)

- **발신 서버 프로토콜**은 **SMTP**로 설정되어 있습니다.
- **수신 관련 설정**은 다음과 같습니다.

항목	설명
수신 서버 주소/포트	입력 형식에 맞게 입력
수신 서버 ID	
수신 서버 비밀번호	
수신 SSL	암호화 방법으로 SSL 사용 여부 선택

- **발신 관련 설정**은 다음과 같습니다.

항목	설명
발신 서버 주소/포트	입력 형식에 맞게 입력
발신 서버 ID	
발신 서버 비밀번호	
발신 SSL	암호화 방법으로 SSL 사용 여부 선택

- **알림**: 사용자 단말에서 이메일 수신시 알림 방법을 설정하세요.

항목	설명
Enable Notify	알림 활성화하기
Enable Always Vibrate Notify	항상 진동으로 알림
Disable Notify	알림 비활성화하기

- **수신 인증서** 허용 여부를 설정하세요.
- **발신 인증서** 허용 여부를 설정하세요.
- **서명**: 사용할 이메일 서명 입력하세요.
- **계정 이름**, **발신인 이름**을 입력하세요.

Exchange ActiveSync 설정 등록하기

Knox 설정 카테고리에서 **Exchange ActiveSync**를 선택한 후, 다음의 항목을 입력하세요.

- **설정 ID**, **설명**을 입력하세요.
- **삭제 가능**: 단말 사용자가 Knox 영역의 Exchange ActiveSync 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 Exchange ActiveSync 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 Exchange ActiveSync 설정을 삭제하는것이 금지됩니다. • 사용자 단말에서는 Exchange ActiveSync 설정을 삭제하는 버튼이 비활성화 됩니다.

- **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **이메일, ID**, **비밀번호**에 Exchange 서버 접속을 위한 사용자의 이메일, ID, 비밀번호를 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

- **도메인**: Exchange 서버의 도메인 명을 입력하세요.
- **Exchange 서버 주소**: Exchange 서버의 IP 주소, 호스트 명, 또는 URL을 입력하세요.
- **과거 데이터 동기화 단위**: 1일, 3일, 1주일, 2주일, 1개월 중 선택하세요.

- **사용자 인증서 입력방법**은 147페이지 10장의 "Android 설정 등록하기"를 참고하세요.
- 동기화와 관련된 다음 항목의 사용 여부를 설정하세요.
  - 일정 동기화, 전화번호부 동기화, 할 일 동기화, 노트 동기화
- 이메일 암호화 통신 방법으로 **SSL** 사용 여부를 선택하세요.
- **서명**: 사용할 이메일 서명을 입력하세요.
- 메일 도착시 알림 방법을 선택하세요.
  - 알림, 항상 진동 알림, 무음 알림
- **첨부파일 용량(byte)**: 첨부파일의 제한 용량을 byte 단위로 입력하세요.
- **메일 본문 용량(Kbyte)**: 메일의 본문 제한 용량을 Kbyte 단위로 입력하세요.

Generic VPN 설정하기

Knox VPN 설정에서 IT 관리자가 애플리케이션별로 VPN 사용을 구성하고 공급 , 관리할 수 있습니다 . 이 기능을 통해 기업은 특정 기업용 애플리케이션에만 VPN 사용을 적용할 수 있습니다 . Knox 설정 카테고리에서 **Generic VPN** 을 선택한 후 , 다음의 항목을 입력하세요 .

- Knox 컨테이너의 유형이 컨테이너 Only의 경우 Cisco AnyConnect VPN을 생성할 수 없습니다.
- Generic VPN은 개인 영역 또는 Knox 영역 상관없이 단말에서 하나만 설치할 수 있습니다.

Knox 영역에 Generic VPN 을 설정하려면 Knox 설정 카테고리에서 **Generic VPN** 을 선택한 후 , 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **VPN 이름**: 사용자의 단말에 표시될 VPN 이름을 입력하세요.
- **삭제 가능**: 단말 사용자가 Knox 영역의 Generic VPN 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 Generic VPN 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 Generic VPN 설정을 삭제하는것이 금지됩니다. • 사용자 단말에서는 Generic VPN 설정을 삭제하는 버튼이 비활성화 됩니다.

- **VPN 벤더사**를 선택하세요. 선택한 VPN 벤더사에 따라 입력 항목이 다를 수 있습니다.

항목	설명
VPN 클라이언트벤더 패키지명	선택한 **VPN 벤더사**에 따라 자동 입력됩니다. • **VPN 벤더사**에서 직접입력을 선택한 경우 VPN 클라이언트 벤더 패키지명을 입력합니다.
VPN 타입	선택한 **VPN 벤더사**에 따라 자동 입력됩니다. • **VPN 벤더사**가 직접입력인 경우 VPN 타입을 선택합니다.

- **Generic VPN 프로파일 입력 방법**: 직접입력, 프로파일 업로드 중 선택하세요. **VPN 벤더사**가 직접입력인 경우 프로파일 업로드가 기본값입니다.

항목	설명
직접입력	선택 시 203페이지의 "Knox Generic VPN 프로파일 직접 입력하기"를 참고하세요.
프로파일 업로드	선택 시 다음을 수행합니다. **Generic VPN 프로파일 업로드** 옆의 ⊕을 클릭하세요. 1. “Generic VPN 프로파일” 창에서 Generic VPN 프로파일을 선택 후, **확인**을 클릭하세요. - Json 형태의 text 파일을 업로드합니다. Json 파일은 VPN 벤더사, VPN 타입 별로 내용이 달라집니다. - 파일 업로드시 156페이지 10장의 “Generic VPN 프로파일 업로드를 위한 파일 샘플" 참고하세요. 2. “확인” 창에서 Generic VPN 프로파일을 확인 후, **확인**을 클릭하세요.

- **인증방식**: 선택한 **VPN 벤더사**, **VPN 타입**, **인증방식**, 프로파일 직접 입력 시 선택한 **연결유형**에 따라 다음의 항목은 다를 수 있습니다.

항목	설명
사용자 인증서 입력방법	147페이지 10장의 “Android 설정 등록하기"를 참고하세요.
OCSP Url	CA서버에서 인증서의 폐기 여부를 체크하기 위한 OCSP Url을 입력하세요.

항목	설명
CA인증서	**CA인증서**에서 루트 인증서를 선택하세요. • **인증서> 외부 인증서**에서 등록한 인증서 중, 인증서 용도가 Knox Generic VPN Certificate이며, **인증서 유형**이 Root Certificate인 VPN 인증서가 목록에 나타납니다.
서버 인증서	**서버 인증서**를 선택하세요. • **인증서> 외부 인증서**에서 등록한 인증서 중, 인증서 용도가 Knox Generic VPN Certificate이며, **인증서 유형**이 Server Certificate인 VPN 인증서가 목록에 나타납니다.

- **FIPS 모드**: FIPS 모드 사용 여부를 설정하세요.
- **접속 에러시 재접속** 여부를 설정하세요.
- **앱별 VPN Route Type**: 애플리케이션별 또는 Knox 컨테이너 내의 전체 패키지에 대해 VPN을 사용할지 여부를 설정하세요.

항목	설명
앱별	애플리케이션 선택하여 해당 애플리케이션 구동시 VPN을 사용합니다. • **앱별 VPN 적용 패키지명** 옆의 ⊕을 클릭하여 "앱 목록" 창에서 애플리케이션 선택 후 **확인**을 클릭하세요.
컨테이너의 전체 패키지	Knox 컨테이너 내 모든 애플리케이션 구동 시 VPN이 사용됩니다.

- **Wide VPN**: 사용자가 Knox영역에서 일반영역으로 이동할 경우, Knox 영역에서 연결된 VPN을 일반 영역에서도 사용하도록 하기 위한 설정입니다. 해당 설정은 **VPN 벤더사**가 Strong Swan이며, **앱별 VPN Route Type**으로 **Container의 전체 패키지**를 선택한 경우 나타나는 항목입니다.
  - 해당 프로파일의 Android 설정에서 Strong Swan에 대한 Generic VPN을 설정한 경우, 사용자 단말에서 Wide VPN을 사용할 수 없습니다. Wide VPN을 사용하려면, Android 설정 영역에서 Strong Swan에 대한 Generic VPN을 설정을 삭제 후 Knox 영역에서 Wide VPN을 설정하세요.
- **VPN 벤더사**가 Mocana, NCP engineering GmbH일때 다음 항목을 설정하세요.

항목	설명
Knox	∨을 클릭하여 Knox 키와 값을 입력 후 ⊕을 클릭하세요.
vendor	벤더 키와 값을 입력 후 ⊕을 클릭하세요.

Knox Generic VPN 프로파일 직접 입력하기

Generic VPN 프로파일 입력방법에서 직접입력을 선택하는 경우 Generic VPN 프로파일 영역에서 입력해야하는 항목은 다음과 같습니다 .

- **VPNroute 타입**은 per-app vpn으로, 특정 앱이 구동될 시 VPN 터널링을 자동적으로 사용하게 하는 것입니다.
- **서버 주소**: VPN 서버의 IP 주소, 호스트 명, 또는 URL을 입력하세요.
- **User 인증**: 사용자 인증 여부를 선택합니다. 사용 선택 시 다음을 입력하세요.

- **사용자 정보 입력방법**은 다음과 같습니다.

항목	설명
직접 입력	선택 시 나타나는 **ID**, **비밀번호**에 VPN 접속을 위한 사용자의 ID와 비밀번호를 입력
커넥터 연동	선택 시 나타나는 **사용자 정보 커넥터** 항목에서 커넥터 선택 • **설정 > 커넥터 > Directory**에서 등록한 커넥터가 목록에 나타납니다.

- **VPN 타입**이 SSL일때 **SSL 알고리즘**에 서버에서 필요로 하는 SSL 알고리즘을 입력하세요.
- **VPN 타입**이 IPSec이며**, VPN 벤더사**가 Mocana, NCP engineering GmbH 일 때 구성되는 항목은 다음과 같습니다.

항목	설명
IKE 버전	IKEv1, IKEv2 중 선택하세요.
DH 그룹 설정	Diffie Hellman 알고리즘 사용 시 사용할 그룹을 선택하세요. • 0, 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
IKE Phase1 모드	Main 모드, Aggressive 모드 중 선택하세요.
IPsec Group ID Type	**IPsec Group ID Type**에서 선택한 항목에 따라 구성되는 항목을 설정하세요. • Default • IPv4 Address • FQDN, User FQDN, IKE Key ID을 선택하면 나타나는 **IPsec Group ID** 항목을 입력하세요.
MobIke Option	Mobike 프로토콜 사용 여부를 설정하세요.
PFS	PFS 기능 활성화 여부를 설정하세요.
DeadPeerDetection	IPsec Peer 유용성 확인 기능을 활성화할지 여부를 설정하세요.
IKE lifetime	
IPsec 암호화 알고리즘	서버에서 필요로하는 IPSEC 암호화 알고리즘을 입력하세요.
IPsec 무결성 알고리즘	서버에서 필요로하는 IPSEC 무결성 알고리즘을 입력하세요.
IKE 암호화 알고리즘	서버에서 필요로하는 IKE 암호화 알고리즘을 입력하세요.
IKE 무결성 알고리즘	서버에서 필요로하는 IKE 무결성 알고리즘을 입력하세요.

- **VPN 벤더사**가 StrongSwan일때, 구성되는 항목은 다음과 같습니다.
  - 선택한 **연결 유형**에 따라 나타나는 해당 항목을 입력하세요.

항목	설명
PPTP	**PPP 암호화(MPPE)** 여부를 선택하세요.
L2TP/IPSec PSK	**L2TP 비밀 키**, **IPSec 식별자**, **IPSec 사전 공유 키**를 입력하세요
L2TP/IPSec RSA	**L2TP 비밀 키**를 입력합니다.

항목	설명
IPSec Xauth PSK	**IPSec 식별자**, **IPSec 사전 공유 키**를 입력하세요.
IPSec Xauth RSA	**사용자 인증서 입력 방법, CA 인증서, 서버 인증서**를 입력하세요.
IPSec Hybrid RSA	**CA 인증서, 서버 인증서**를 입력하세요.
IPSec IKE2 PSK	**식별자**, **사전 공유 키**를 입력하세요.
IPSec IKE2 RSA	**사용자 인증서 입력 방법,OCSP Url, CA 인증서, 서버 인증서**를 입력하세요.

- **고급 옵션 표시**의 항목은 다음과 같습니다.

항목	설명
DNS 검색 도메인	사용할 DNS 검색 도메인의 이름을 설정하세요. • 예: example.com
DNS 서버	DNS 서버 주소를 IP 패턴에 맞게 입력하세요. • 예: 123.0.0.4
전달 경로	**서브넷 비트**를 선택하면 자동 입력됩니다.
서브넷 비트	없음, /1~/30 중 선택하세요.

- **연결 방식**을 선택하세요.

항목	설명
KEEP On	VPN 접속을 계속 유지합니다.
On Demand	요청시 VPN 접속을 합니다.

- **체이닝** 방식을 선택하세요.
- **UID PID** 사용여부를 선택하세요.
- **Logon Mode 사용여부 선택**: **VPN 벤더사**가 **F5**일 경우 선택하는 항목입니다.
  - **Logon Mode 정보**는 native가 기본값입니다.

SSO 설정 등록하기

단말 사용자가 한 번의 로그인으로 추가 인증 없이 다른 앱에 엑세스할 수 있게 해주는 SSO (Single Sign On) 서비스를 설정할 수 있습니다 . SSO 타입의 설정은 1 개만 생성할 수 있습니다 . Knox 설정 카테고리에서 **SSO** 를 선택한 후 다음의 항목을 입력하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **삭제 가능**: 단말 사용자가 Knox 영역의 SSO 설정을 삭제하는것을 허용할지 여부를 지정하세요.

항목	설명
허용	사용자가 단말에서 SSO 설정을 삭제하는것이 허용됩니다.
금지	사용자가 단말에서 SSO 설정을 삭제하는것이 금지됩니다. • 사용자 단말에서는 SSO 설정을 삭제하는 버튼이 비활성화 됩니다.

- **SSO 타입**을 선택하세요.
- **SSO 화이트 패키지 리스트**: SSO을 통해 엑세스할 수 있는 애플리케이션을 추가하세요.
  - ⊕을 클릭하여 “앱 목록” 창에서 추가할 애플리케이션을 선택하세요. 다중 선택이 가능합니다.
- **Authenticator 설치파일**: Knox 2.4 버전 이상부터는 단말에 사전 설치되었던 SAMSUNG SSO Authenticator 서비스 APK가 제외되었습니다. Knox 2.4 이상 단말 (예를 들어, 삼성전자 갤럭시 S6)에서 SSO 서비스를 사용하기 위해서는 추가적인 SAMSUNG SSO Authenticator을 등록이 필요합니다.
  - ⊕을 클릭하여 사용자 계정의 안전 유지를 위한 인증자 앱을 **앱 목록**에서 선택합니다. 해당 설치 파일은 **애플리케이션 > 사내 애플리케이션** 또는 **애플리케이션 > 외부 애플리케이션**에 먼저 등록해야, **앱 목록**에서 선택할 수 있습니다.

  - SSO 타입이 SAMSUNG SSO일 때 옵션 입력 항목입니다.
- **SSO KRB5**: ⊕을 클릭하여 KRB5 설정 파일을 추가하세요.
  - **SSO 타입**이 SAMSUNG SSO 타입일 때 필수 입력 항목입니다.
- **SSO SAML 설정**: **SSO 타입**이 SAMSUNG SSO 타입일 때 필수 입력 항목입니다.
- **SSO Customer 로고**: ⊕을 클릭하여 로고를 추가하세요.
- **SSO Customer 이름**을 입력하세요.

Bookmark 설정 등록하기

Android 의 삼성 단말에서 사용되는 기본 브라우저인 S 브라우저의 북마크를 등록 , 수정 및 삭제합니다 .

Bookmark 사용 시 제약 사항은 다음과 같습니다 .

- 단말에서 인터넷 브라우저를 모두 종료한 후 재실행해야 변경된 설정이 반영됩니다.
- 사용자가 등록된 북마크를 수정하거나 동일한 URL과 이름으로 북마크를 등록하더라도 북마크 설정 삭제 시 삭제되지 않습니다.
- 삼성 단말의 기능 제약으로 인해 설정된 Bookmark를 사용자가 브라우저에서 임의로 삭제하더라도 EMM 앱에서는 여전히 설치되어 있는 것으로 보일 수 있습니다. 이 경우 단말 관리 프로파일 설정에서 해당 북마크 삭제 후 재 설정을 해야 합니다.

북마크를 설정하려면 Knox 설정 카테고리에서 북마크를 선택한 후 , 다음의 항목을 설정하세요 .

- **설정 ID**, **설명**을 입력하세요.
- **북마크 페이지 URL**: 북마크 선택 시 이동할 웹 사이트 주소를 입력하세요.
- **북마크 이름**: 북마크에서 제목으로 표시될 북마크 이름을 입력하세요.

12 이벤트

정책을 적용할 수 있는 이벤트 유형(Event type)은 시간, 애플리케이션, Wi-Fi SSID, SIM 변경, 로밍, 사용자별 예외 정책, 사용자 지정, 입출문, Cell 으로 분류되어 있어, 이벤트 유형에 따라 운영자가 정책을 정의할 수 있습니다.

- 입출문 유형으로 정책을 설정하면, 입문 시 단말에 정책이 적용되며, 출문 시 단말에 적용된 정책은 해제됩니다.
- 시간, 애플리케이션, Cell 유형으로 정의된 이벤트는 단말 통신 상태가 온라인이 아니더라도 이벤트 발생 시 단말에 적용되도록 설정할 수 있습니다.
- 사용자 지정 유형으로 정책을 설정하면, 필요에 따라 단말 제어 명령을 보내 기본 정책보다 우선 적용합니다. 이벤트 해제 또한 단말 제어 명령을 통해 이루어집니다.
- SIM 변경, 로밍 유형을 제외한 모든 이벤트 유형은 하나의 프로파일에 하나의 이벤트 유형으로 여러 개의 이벤트를 등록할 수 있습니다. 즉, SIM 변경, 로밍 유형은 하나의 프로파일에 하나의 이벤트만 등록할 수 있습니다.
- 또한, 하나의 이벤트에 여러 개의 개별 정책들로 구성할 수 있습니다. 즉, 플랫폼별 정책과 설정, Knox 컨테이너별 정책과 설정을 정의할 수 있습니다. 이벤트가 여러 개일 경우 우선 순위를 설정하여 우선 순위에 따라 단말에 적용합니다.

이벤트를 단말에 적용하려면 단말 관리 프로파일에 조직이나 그룹을 할당한 후, **적용** 버튼을 클릭하여 프로파일을 배포해야 합니다. 또는 **최신 단말 관리 프로파일 배포** 단말 제어 명령을 전송합니다.

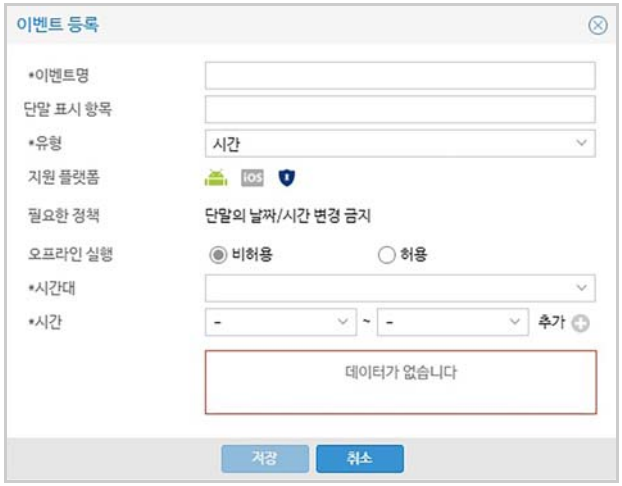
또한 KeepAlive 설정과 프로파일 업데이트 주기를 프로파일 별로 설정하여, 프로파일을 할당받은 단말을 관리할 수 있습니다. EMM 의 전체 단말에 설정하려면 **설정 > 서비스 > 환경 설정**에서 설정할 수 있으며, 프로파일 설정의 우선순위가 환경 설정보다 더 높습니다.

이벤트 추가하기

이벤트를 추가하려면 다음의 절차를 따르세요.

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 이벤트를 추가할 프로파일명을 선택하세요.
   - 프로파일을 신규 생성한 후 이벤트를 추가하려면 ➕을 클릭하세요.
3. "단말 관리 프로파일" 창에서 **이벤트 > 이벤트 관리**로 이동하세요.
4. **이벤트관리** 우측의 ➕을 클릭하세요. “이벤트 등록” 창이 나타납니다.

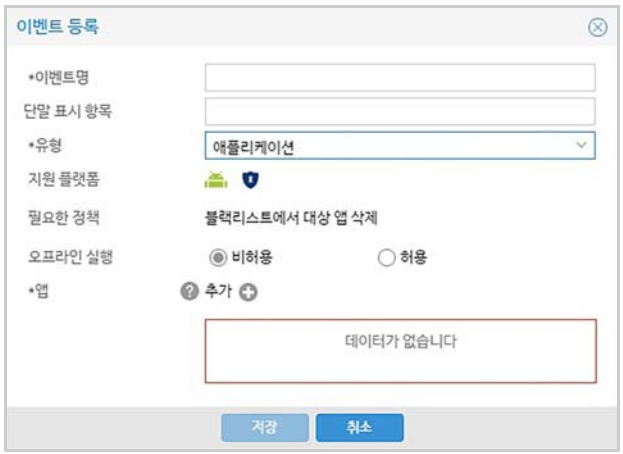
5. **이벤트명**, **단말 표시 항목**을 입력한 후 **유형**을 선택하세요.
   - 입력 항목명 앞에 표시(*)는 필수 입력값이며, 나머지는 선택 사항입니다.
   - 이벤트 명과 유형은 추가된 후 수정 할 수 없으며, 수정하려면 삭제 후 다시 생성해야 합니다.
6. 이벤트 유형에 따른 다음의 항목들을 입력한 후 **저장**을 클릭하세요.
   - **유형**이 **시간**인 경우: 특정 시간대에 사용자 단말을 제어합니다.



     - **오프라인 실행** 여부를 선택하세요.
     - 시간 이벤트를 적용할 기준이 되는 **시간대**를 선택하세요.
     - **시작 시간**과 **종료 시간** 설정한 후 ⊕를 클릭하여 추가하세요.

> **Note:**
> - 시간 이벤트를 적용하려면 날짜, 시간 변경 제어가 금지되어야 합니다. 해당 프로파일의 **Android > 정책 > 시스템** 에서 **날짜**, **시간 변경** 항목을 **금지**로 설정합니다.
> - iOS 단말의 경우 정책 업데이트를 위한 스케줄러가 따로 없으므로, 시간 이벤트를 이용하여 최신 정책을 업데이트합니다.

   - **유형**이 **애플리케이션**인 경우: 사용자의 단말에서 특정 애플리케이션이 실행될 때 단말을 제어합니다. 해당 이벤트는 Samsung SDS가 배포한 SDK로 개발되거나 AppWrapper 툴 또는 애플리케이션 등록 시 **AppWrapper 사용**을 선택하여 변환된 애플리케이션에 적용할 수 있습니다.

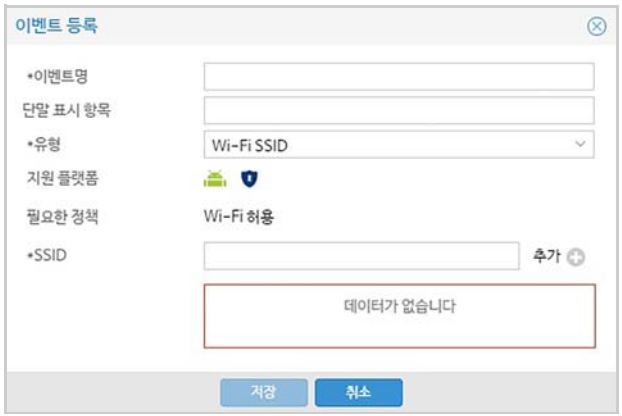


     - **오프라인 실행** 여부를 선택하세요.

- **앱**의 ⊕를 클릭하면 나타나는 **앱 목록**에서 앱을 선택 후 **확인**을 클릭하세요. 앱 목록에는 안드로이드 플랫폼을 지원하는 사내 애플리케이션과 EMM 애플리케이션만 조회됩니다.

Note:
- 애플리케이션 이벤트를 적용하려면 해당 애플리케이션을 블랙리스트로 지정하면 안됩니다.
- 사내 SecuCamera 애플리케이션을 지정할 경우, 입출문 이벤트보다 우선 순위가 높아야 합니다. 해당 이벤트 정책 설정 시 보안에 문제가 생기지 않도록 주의합니다.

- **유형**이 **Wi-Fi SSID**인 경우: 사용자 단말이 특정 Wi-Fi SSID에 연결시 단말을 제어합니다. 특정 Wi-Fi SSID 접속 해제 시 적용된 이벤트 정책은 해제됩니다.



- **SSID**에 Wi-Fi SSID를 입력한 후 ⊕ 클릭하여 추가하세요.

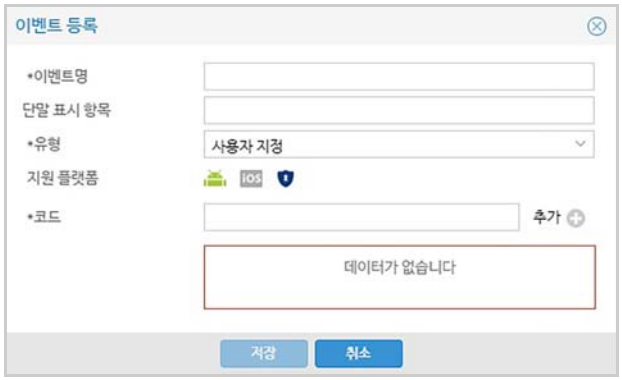
Note: Wi-Fi SSID 이벤트를 적용하려면 Wi-Fi가 허용되어야 합니다. Android 또는 Knox 정책의 인터페이스 그룹에서 확인합니다.

- **유형**이 **SIM 변경**인 경우: EMM에서 인증되지 않은 SIM이 사용자의 단말에 장착되었을때 단말을 제어합니다. SIM 변경 유형으로 이벤트 등록 시 미리 정해놓은 정책을 적용하거나, 운영자가 정책을 설정하는것을 선택할 수 있습니다. EMM에서 인증받은 SIM으로 다시 장착되면, SIM 변경 이벤트 발생으로 적용된 정책은 해제됩니다. SIM 변경 이벤트는 수정이 불가능하며, 삭제 후 다시 추가해야 합니다.

- **변경시** 적용할 정책을 선택하세요.

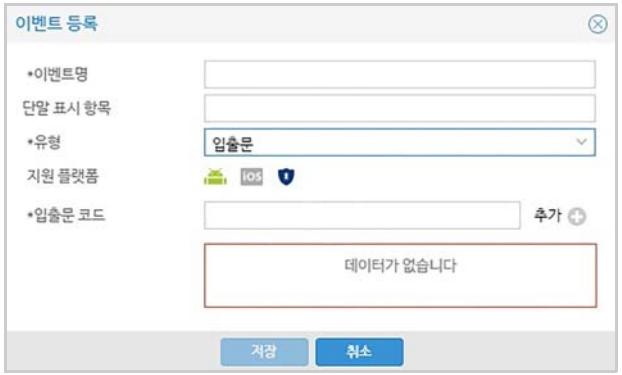
항목	설명
이벤트 정책 적용	운영자가 정책을 설정합니다.
단말 잠금	미리 정해놓은 정책 집합을 적용합니다. • 카메라 사용 금지 • 블루투스 사용 금지 • 블루투스 테더링 사용 금지 • PC 연결 금지 • USB 테더링 금지 • USB 디버깅 금지 • USB Host Storage OTG(On-the-go) 금지 • Microphone 금지

- **유형**이 **로밍**인 경우: 사용자가 해외에서 국내 통신사의 USIM으로 로밍을 하는 경우 단말을 제어합니다. 로밍으로 인하여 일시적으로 서버와 통신을 할 수 없으면 비행기 모드 해제 또는 단말 재부팅 시점 등 네트워크 통신이 가능한 시기에 적용됩니다.
- **유형**이 **사용자별 예외 정책**인 경우: 특정 사용자에게 일정 기간 동안 예외 정책을 적용합니다. 기간별 상세 정책 설정을 하려면 **프로파일 > 사용자별 예외 정책 관리**에서 사용자별 기간을 설정하고 Android 정책 구성요소, iOS 정책 구성요소, Knox Portal 정책 구성요소를 등록합니다. 자세한 내용은 216페이지의 "사용자별 예외 정책 설정하기"를 참고하세요.
- **유형**이 **사용자 지정**인 경우: 기본 정책보다 우선적으로 적용되는 정책입니다.



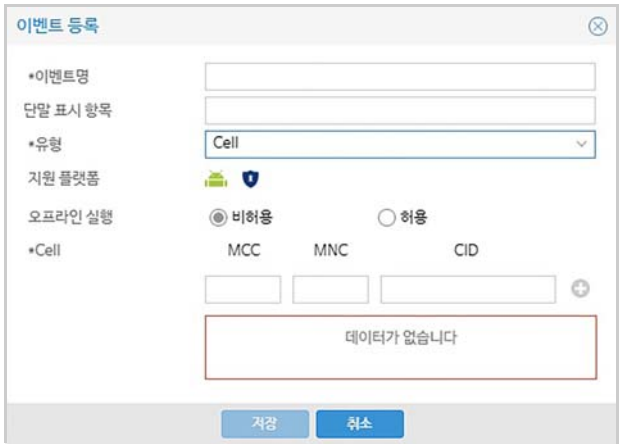
- **코드**에 기간계 시스템에서 정의한 값을 입력한 후 ⊕을 클릭하세요.
- 사용자 지정 이벤트를 실행시키는 방법은 431페이지 18장의 “단말 제어 전송 방법"을 참고하세요.

- **유형**이 **입출문**인 경우: 출입 시 사용자 단말을 제어합니다.



  - 입출문 코드를 입력한 후 ⊕을 클릭하세요.

- **유형**이 **Cell**인 경우: 사용자 단말이 통신사 기지국의 서비스 셀내에 위치하는 경우, 단말을 제어합니다.



  - **오프라인 실행** 여부를 선택하세요.
  - **MCC/MNC/CID**에 Cell 정보를 입력한 후, ⊕을 클릭하여 추가하세요.
    - 필수 항목: Cell ID(CID)에는 0~268435455자리의 숫자만 입력합니다.
    - 옵션 항목: 모바일 국가 코드(MCC), 모바일 네트워크 코드(MNC)는 옵션 항목입니다.

7. **이벤트** 메뉴 아래에 생성된 신규 이벤트의 플랫폼(Android, iOS), Knox 컨테이너 정책을 설정하세요. 이벤트 유형에 따라 지원하는 플랫폼은 다음과 같습니다.

   - Android, iOS, Knox 영역의 정책 설정 방법과 동일합니다. 정책을 설정하는 방법은 141페이지 10장의 "단말 관리 프로파일 정책 설정하기"를 참고하세요.

이벤트 유형	지원 플랫폼			프로파일당 등록 제한 갯수
	Android	iOS	Knox	
시간	O	O	O	X
애플리케이션	O	X	O	X
Wi-Fi SSID	O	X	O	X
SIM 변경	O	X	O	1개
로밍	O	X	O	1개

이벤트 유형	지원 플랫폼			프로파일당 등록 제한 갯수
	Android	iOS	Knox	
사용자별 예외 정책	O	O	X	1개
사용자 지정	O	O	O	X
입출문	O	O	O	X
Cell	O	X	O	X

구성요소 방식의 이벤트 추가하기

단말 관리 프로파일을 구성요소로 등록하여 **구성요소 등록** 항목이 Y 로 표시된 프로파일에 이벤트 구성요소를 추가하는 방법입니다 . 이벤트 구성요소는 미리 등록되어 있어야 하며 자세한 내용은 214 페이지의 " 이벤트 구성요소 등록하기 " 를 참고하세요 . 이미 설정되어 있는 구성요소는 목록에서 취소선으로 표시되며 선택할 수 없습니다 . 구성요소로 등록한 이벤트의 삭제는 해당 프로파일에서만 삭제되며 , **프로파일 > 단말 관리 프로파일 구성요소**에서 조회 가능합니다 .

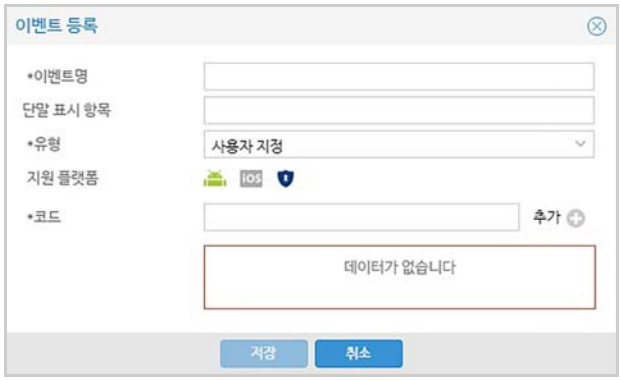
이벤트 구성요소를 추가하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 이벤트를 추가할 프로파일명을 선택하세요.
   - 신규 프로파일에 이벤트를 정의하려면 ➕을 클릭하여 프로파일을 신규 생성한 후 이벤트를 추가하세요.
3. "단말 관리 프로파일" 창에서 **이벤트 > 이벤트 관리**로 이동하세요.
4. **이벤트 관리** 우측의 ➕을 클릭하세요.“이벤트” 창에 이벤트 구성요소 목록이 나타납니다.
   - 설정된 상세 내용을 조회하려면 구성요소명을 클릭하세요.
5. 설정할 구성요소를 선택한 후 **저장**을 클릭하세요.
6. 플랫폼별 정책이 필요한 이벤트의 경우, **이벤트** 메뉴 아래에 생성된 신규 이벤트의 정책을 설정하세요.
   - 플랫폼별 단말 관리 정책 구성요소를 설정하는 방법과 동일합니다.
7. "단말 관리 프로파일" 창에서 **확인**을 클릭하세요.
8. 이벤트를 적용하려는 조직 또는 그룹을 할당한 후, “단말 관리 프로파일” 창에서 **적용**을 클릭하여 이벤트를 단말에 배포하세요. 확인 메시지가 나타나면 **예**를 클릭하세요.

이벤트 구성요소 등록하기

단말 관리 프로파일의 이벤트 구성요소를 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일 구성요소**로 이동하세요.
2. ➕을 클릭한 후, **이벤트 등록**을 클릭하세요.



3. “이벤트 등록” 창에서 각 항목의 값을 입력하세요.
   이벤트 유형별 상세 설정에 대한 자세한 내용은 208페이지의 "이벤트 추가하기"를 참고하세요.
4. **저장**을 클릭하세요.

이벤트 우선순위 정하기

이벤트가 여러개인 경우에는 이벤트 정책의 우선순위를 정해야하고 , 우선순위에 따라 정책이 적용됩니다 . 이벤트 목록에서 우선순위가 높을수록 상위에 보여집니다 .

이벤트의 우선순위를 정하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 이벤트의 우선순위를 정할 프로파일명을 선택하세요.
3. **이벤트 > 이벤트 관리**로 이동하세요.

4. 우선순위를 변경하려면 이벤트명을 클릭한후 ⬆⬇을 클릭하세요. 또는 변경할 위치에 이벤트명을 마우스로 끌어다 놓으세요.
5. 💾을 클릭하세요.
6. "단말 관리 프로파일" 창에서 **확인**을 클릭하세요.

KeepAlive 설정하기

Knox Manage 서버와 단말 간의 연결 상태를 확인하기 위해 KeepAlive 를 설정합니다 . Knox Manage 서버는 설정한 KeepAlive 주기마다 서버와 단말의 연결 상태를 확인합니다 .

단말 관리 프로파일에서 KeepAlive 를 설정하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. KeepAlive를 설정하려는 프로파일명을 선택하세요.
3. **이벤트 > KeepAlive 설정**으로 이동한 후, **KeepAlive 설정** 옆의 을 클릭하세요 .
4. **KeepAlive 활성화 설정**을 **설정**으로 변경한 후, 항목 값을 입력하세요.
   - KeepAlive 기한 (일): 3-365 숫자만 입력이 허용되며, 단말과 서버의 연결 상태가 끊어진 채로 설정된 기한을 넘기면 단말 상태를 시스템 차단으로 변경한 후, Audit 로그를 남깁니다.
   - KeepAlive 체크 주기 (시간): 서버와 단말 간의 연결 상태를 확인하는 시간 주기입니다.

5. **저장**을 클릭하세요.
6. KeepAlive 설정을 단말에 배포하려면 **적용**을 클릭하세요.

프로파일 업데이트 주기 설정하기

EMM 서버는 주기적으로 단말 관리 프로파일의 정책을 단말에 전송합니다 . 다음과 같이 프로파일 업데이트 주기를 설정하면 프로파일을 할당받은 전체 단말 플랫폼에 정해진 스케줄에 따라 정책 업데이트가 실행됩니다 .

프로파일 업데이트 주기를 설정하려면 다음의 절차를 따르세요 .

1. **프로파일 > 단말 관리 프로파일**로 이동하세요.
2. 업데이트 주기를 설정할 프로파일명을 선택하세요.
3. **이벤트 > 프로파일 업데이트 주기 설정**으로 이동한 후, **프로파일 업데이트 주기 설정** 옆의 을 클릭하세요.

4. **요일**, **시간대**, **시작시간**을 설정하세요.
   - **시작 시간**: HHMM의 4자리로 입력하며 0000-2359까지 입력 가능합니다.

5. **저장**을 클릭하세요.
6. 프로파일 업데이트 주기 설정을 단말에 배포하려면 **적용**을 클릭하세요.

사용자별 예외 정책 설정하기

그룹 및 조직 단위로 단말 및 앱 관리 프로파일을 배포함과 동시에 특정 사용자의 단말에 기간을 설정하여 예외 정책을 적용하여 사용할 수 있습니다 .

사용자별 예외 정책을 사용하려면 다음의 절차를 따르세요 .

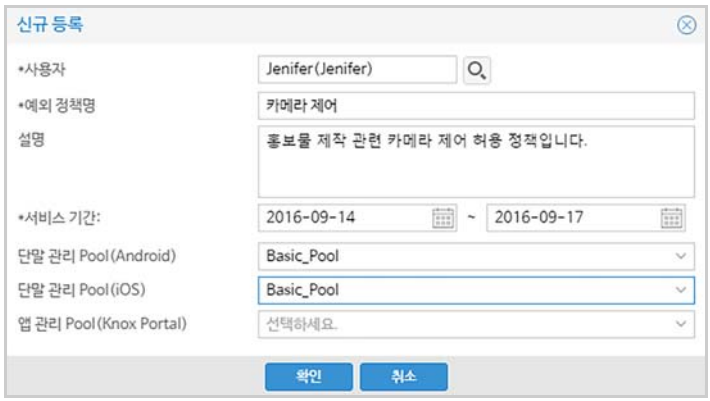
1. 예외적으로 적용할 정책 구성요소를 등록하세요.
   적용 가능한 예외 정책은 다음과 같으며 자세한 내용은 142페이지 10장의 “단말 관리 프로파일의 정책 구성요소 등록하기"와 188페이지 10장의 “Knox Portal 정책 설정하기"를 참고하세요.
   - 단말 관리 프로파일의 Android 정책 구성요소, iOS 정책 구성요소
   - 앱 관리 프로파일의 Knox Portal 정책 구성요소
2. **프로파일 > 사용자별 예외 정책**에서 사용자를 선택한 후 예외 정책으로 적용할 구성요소를 선택하세요.
3. 예외 정책 사용자에게 할당된 단말 관리 프로파일의 이벤트 항목에서 사용자별 예외 정책 이벤트를 추가해야 합니다.

사용자별 예외 정책 등록하기

사용자별 예외 정책은 수정이 불가합니다 . 삭제 후 신규 등록하여 사용합니다 . 사용자에게 적용할 예외 정책을 등록하려면 다음의 절차를 따르세요 .

1. **프로파일 > 사용자별 예외 정책**으로 이동하세요.

2. ➕을 클릭한 후 “신규 등록” 창에 예외 정보를 입력하세요.



- 사용자: 🔍를 클릭하면 “사용자 조회” 창이 조회됩니다. 검색 조건 목록에서 **사용자 이름**, **사원 번호**, **이메일**, **사용자 ID**, **조직**을 선택한 후, 검색어를 입력하고 **검색**을 클릭합니다. 사용자 목록에서 예외 처리할 사용자를 선택하고 **확인**을 클릭하세요.
- 예외 정책명: 한글, 알파벳, 숫자와 ‘_’ 문자만 허용하며 20자까지 입력 가능합니다.
- 서비스 기간: 📅를 클릭하여 예외 정책을 적용하려는 시작 일자와 종료 일자를 입력하세요.
  - 예외 정책 적용 시간을 설정하려면 **설정 > 서비스 > 환경 설정**으로 이동하여 **예외정책 적용/해제 스케쥴 시각**을 설정하세요. 기본 설정값은 자정(00시) 10분입니다. 자세한 내용은 19페이지 2장의 “환경 설정하기"를 참고하세요.
- **단말 관리 프로파일 구성요소(Android)**: 등록된 단말 관리의 Android 정책 구성요소 목록에서 선택하세요.
- **단말 관리 프로파일 구성요소(iOS)**: 등록된 단말 관리의 iOS 정책 구성요소 목록에서 선택하세요.
- **앱 관리 프로파일 구성요소(Knox Portal)**: 등록된 앱 관리의 Knox Portal 정책 구성요소 목록에서 선택합니다. EMM이 삼성그룹향 라이선스이며 Knox Portal 앱이 사용 가능한 경우에 설정할 수 있습니다.

3. **확인**을 클릭하세요. 등록한 정책 갯수만큼의 예외 정책이 생성되며 목록에서 조회됩니다.
   - 사용자별 예외 정책은 하나의 사용자에 최대 5개까지 등록 가능합니다.
   - 사용자별 예외 정책에 할당된 구성요소는 **프로파일 > 단말 관리 프로파일 구성요소/앱 관리 프로파일 구성요소** 목록에서 **사용자별 예외 정책** 항목에 갯수로 표시됩니다. 숫자를 클릭하면 할당된 사용자별 예외 정책 목록이 조회됩니다.

사용자별 예외 정책 우선 순위 정하기

사용자별 하나의 플랫폼에 여러개의 예외 정책이 설정되어 있는 경우 등록된 예외 정책 중에서 적용 우선 순위를 조정할 수 있습니다 . 우선 순위를 정하려면 다음의 절차를 따르세요 .

1. **프로파일 > 사용자별 예외 정책**으로 이동하세요.
2. 목록에서 우선 순위를 변경할 사용자를 클릭하세요.
   예외 정책창이 조회됩니다.
3. 검색 조건 목록에서 **구성요소 정책명**, **예외 정책명**, **등록자**를 선택한 후 검색어를 입력하고 **검색**을 클릭하세요.
4. 우선순위를 변경할 예외 정책을 클릭한 다음 ↑ ↓을 클릭한 후 우선 순위를 지정하고 을 클릭하세요.
5. **확인**을 클릭하세요.

13 E-FOTA 그룹

Firmware Over The Air (FOTA) 서비스는 단말의 펌웨어를 무선으로 업그레이드하는 기능입니다. EMM 에서는 제품, 모델, 통신사, 언어별 그룹을 생성하고 그룹별로 특정 펌웨어 버전을 설정하여 해당 버전으로 강제 업데이트를 진행하는 Enterprise FOTA (E-FOTA) 서비스를 제공합니다. 사용자의 단말에 설치된 펌웨어가 설정한 버전보다 상위일 경우에는 해당 버전에서 더 이상 상위 버전으로 업데이트 하는 것을 방지합니다. E-FOTA 그룹별로 서비스가 적용된 단말의 상태를 확인합니다.

- E-FOTA 적용 가능 단말: Android 7.0 (Nougat) 이상의 삼성 단말

E-FOTA 서비스를 운용하기 위한 순서는 다음과 같습니다.

1. E-FOTA 사용을 위한 사전 준비가 필요합니다.
   - **설정 > 서비스 > 환경 설정 > E-FOTA 설정**에서 E-FOTA 연결 정보를 설정하세요. 설정 항목의 자세한 내용은 40페이지 2장의 “E-FOTA 설정하기"을 참고하세요.
   - **설정 > 서비스 > 라이선스 정보**에서 E-FOTA 라이선스 등록하세요.
2. 특정 제품, 모델, 통신사의 단말에서 E-FOTA 실행을 위해 **단말 & 사용자 > E-FOTA 그룹**에서 E-FOTA 그룹을 생성하세요.
   자세한 내용은 220페이지의 "E-FOTA 그룹 등록하기"을 참고하세요.
3. E-FOTA 정책 적용을 위해 E-FOTA 정책을 프로파일에 설정한 후, 프로파일을 사용자의 단말에 배포하세요.
   - **프로파일 > 단말 관리 프로파일**에서 설정할 프로파일을 선택한 후, **Android > 정책 > 시스템**에서 **EnterpriseFOTA** 정책을 **사용**으로 설정하세요.
   - 프로파일 정책을 적용할 조직 또는 그룹에 해당 프로파일을 할당한 후, **적용**을 클릭하여 프로파일을 배포하세요.
4. 사용자의 단말에 펌웨어 업데이트를 다음의 두가지 방법으로 적용하세요. E-FOTA 를 통한 펌웨어 업데이트는 E-FOTA 그룹에 속한 단말만 펌웨어 업데이트가 실행됩니다.
   - 단말 제어 업데이트: **단말 & 사용자 > 단말**에서 단말을 선택한 후  을 클릭하여 **단말 관리**의 **업데이트 E-FOTA 펌웨어 버전** 단말 제어를 전송합니다.
     단말 제어를 전송하면 즉시 사용자의 단말에 펌웨어 업데이트가 요청되며, 사용자가 단말에서 소프트웨어 업데이트를 실행해야 적용됩니다.
   - 강제 업데이트: **단말 & 사용자 > E-FOTA 그룹**에서 강제업데이트를 수행합니다.
     자세한 내용은 222페이지의 "강제 업데이트하기"을 참고하세요.

E-FOTA 서비스는 삼성 전자의 E-FOTA API(Application Programming Interface) 를 사용하여 제공되며 , API 에러 코드는 462 페이지 18 장의 “E-FOTA API" 를 참고하세요 .

E-FOTA 그룹 등록하기

E-FOTA 그룹은 단말의 모델명과 통신사 코드로 구성된 그룹이며 , 강제 펌웨어 업데이트는 E-FOTA 그룹 단위로 수행됩니다 .

모델명과 통신사 코드가 동일한 FOTA 그룹은 중복 생성이 불가능합니다 . 단말에서 통신사 코드 및 현재 펌웨어 버전을 확인하는 방법은 221 페이지의 " 현재 펌웨어 버전 확인하기 " 를 참고하세요 .

E-FOTA 그룹을 설정하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > E-FOTA 그룹**으로 이동하세요.
2. ➕을 클릭하세요.

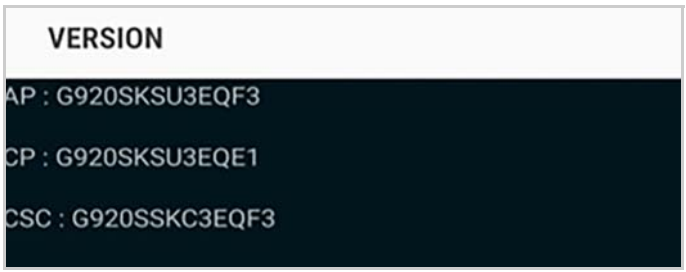
3. “E-FOTA 신규 등록” 창에서 생성할 그룹 정보를 입력하세요.
   - **E-FOTA 이름**: E-FOTA 그룹 이름을 입력하세요.
   - **제품명**: 단말의 제품명을 선택하세요.
   - **모델 이름**: 단말의 모델 이름을 선택하세요.
   - **통신사 코드**: 통신 서비스를 제공하는 이동 통신사 코드를 선택하세요.
     - 통신사 코드를 직접 입력하려면 직접 입력을 선택한 후 오른쪽에 통신사 코드를 입력하세요.
   - **언어 코드**: 펌웨어 업데이트를 제어할 언어를 목록에서 선택하세요.
   - **현재 펌웨어 버전**: 현재 펌웨어 버전을 입력하세요. 선택 입력사항이며 **대상 버전** 목록 조회 시, 현재 버전보다 상위의 펌웨어 버전이 보여집니다. 현재 펌웨어 버전 미입력 시, 해당 단말에 적용 가능한 전체 펌웨어 버전이 조회됩니다.
   - **대상 버전**: 🔍을 클릭하면 “펌웨어 목록” 창이 조회됩니다. 입력한 모델과 통신사 코드에 해당하는 펌웨어 목록이 Samsung FOTA 서버를 통해 조회됩니다. 단말에 업데이트할 특정 펌웨어 버전을 선택하고 **확인**을 클릭하세요. E-FOTA 그룹 수정 시, 대상 버전만 수정할 수 있습니다.

4. **저장**을 클릭하세요.

현재 펌웨어 버전 확인하기

단말에서 현재 펌웨어 버전 및 통신사 코드를 확인하려면 **전화 > 키패드**를 탭한 후 , *#1234# 을 입력합니다 . 아래의 예시같이 버전 정보가 조회되며 , E-FOTA 그룹에서 현재 펌웨어 버전은 AP/CSC/CP 순서로 입력해야 합니다 .

예시)



- 펌웨어 버전: G920SKSU3EQF3/G920S**SKC**3EQF3/G920SKSU3EQE1
- 통신사 코드: CSC 값에서 앞 5자리인 모델명 뒤의 3자리 코드(굵은 글씨로 표시한 SKC)

E-FOTA 그룹 조회하기

E-FOTA 그룹 정보와 설정된 펌웨어 정보가 목록에서 조회됩니다 . E-FOTA 그룹을 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > E-FOTA 그룹**으로 이동하세요.
2. 검색 조건 목록에서 **E-FOTA 이름**, **등록자**를 선택한 후, 검색어를 입력하고 **검색**을 클릭하세요. 등록된 E-FOTA 그룹 목록이 조회됩니다.
   - E-FOTA 이름을 클릭하면 E-FOTA 그룹의 기본 정보가 조회됩니다. 해당 팝업에서 수정 버튼을 클릭한 후 대상 버전을 수정할 수 있습니다.
   - **대상 펌웨어 버전**을 클릭하면 대상 펌웨어 버전으로 적용할 수 있는 현재 펌웨어 버전 목록이 조회됩니다. 단말이 현재 펌웨어 버전과 다르면 에러를 발생하며 업데이트가 불가능합니다.

E-FOTA 적용 단말 조회하기

E-FOTA 그룹의 단말에 설정한 펌웨어 적용 여부가 조회됩니다 . 적용 단말을 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > E-FOTA 그룹**으로 이동하세요.

2. 목록에서 조회할 E-FOTA 그룹 목록 좌측의 을 클릭하세요.
   "적용 단말 목록" 창이 조회되며 선택한 E-FOTA 그룹에 적용되는 단말 목록이 조회됩니다.
   - 적용 단말별 펌웨어 업데이트의 결과가 적용 또는 미적용으로 **상태**에 표시되며 상세 원인 등의 정보가 **상세 설명**에 조회됩니다.
3. 확인 메시지가 나타나면 **예**를 클릭하세요.

강제 업데이트하기

설정한 스케쥴에 따라 사용자의 동의없이 단말의 펌웨어를 업데이트를 할 수 있습니다.

펌웨어를 강제로 업데이트하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > E-FOTA 그룹**으로 이동하세요.
2. 목록에서 업데이트 할 E-FOTA 그룹 목록 좌측의 을 클릭하세요.
   - 펌웨어가 설정되지 않은 E-FOTA 그룹은 강제 업데이트가 불가능합니다.
3. "펌웨어 강제 업데이트"창에 E-FOTA 그룹 정보가 조회됩니다.
   강제 업데이트를 진행할 시작일시와 종료일시를 입력하고 **확인**을 클릭하세요.
   - 적용 일자는 GMT+0 기준으로 설정합니다.
   - 일자 기준으로 시작일과 종료일의 최대 기간은 7일이며, 시간 기준으로 시작 시간과 종료 시간의 범위는 12시간을 넘지 말아야 합니다.
4. 확인 메시지가 나타나면 **예**를 클릭하세요.
   E-FOTA 그룹 목록에서 을 클릭하여 적용된 단말 정보를 확인할 수 있습니다.

14 애플리케이션

EMM 에서 관리하는 애플리케이션의 종류는 다음과 같습니다 .

- **사내 애플리케이션**: 기업 내 사용을 위해 배포되는 업무용 애플리케이션
- **외부 애플리케이션**: Google Play Store 및 Apple App Store를 통해 배포되는 애플리케이션
- **Kiosk 애플리케이션**: 단말에서 Kiosk 모드로 실행되는 애플리케이션
- **제어 애플리케이션**: 블랙리스트 또는 화이트리스트로 등록된 후 제어되는 애플리케이션과Google의 Android for Work 앱을 통해 배포 가능한 업무용 애플리케이션
- **EMM 애플리케이션**: EMM 사용을 위해 단말에 필수적으로 설치되어야 하는 애플리케이션

사용자는 단말의 EMM 앱 스토어에서 사내 , 외부 애플리케이션을 다운로드 할 수 있습니다 . 사내 애플리케이션은 EMM 에서 관리되는 기업용 애플리케이션을 , 외부 애플리케이션은 Google Play Store 및 Apple App Store 의 애플리케이션을 지칭합니다 . 운영자가 EMM 관리자 포털에서 사내 / 외부 애플리케이션을 활성화 또는 비활성화하여 사용자의 애플리케이션 다운로드와 실행 여부를 제어합니다 . 애플리케이션 관련 정책 관리는 181 페이지의 " 앱 관리 프로파일 설정하기 " 를 참고하세요 . 단말 애플리케이션 관리는 122 페이지의 " 단말 애플리케이션 관리하기 " 를 참고하세요 .

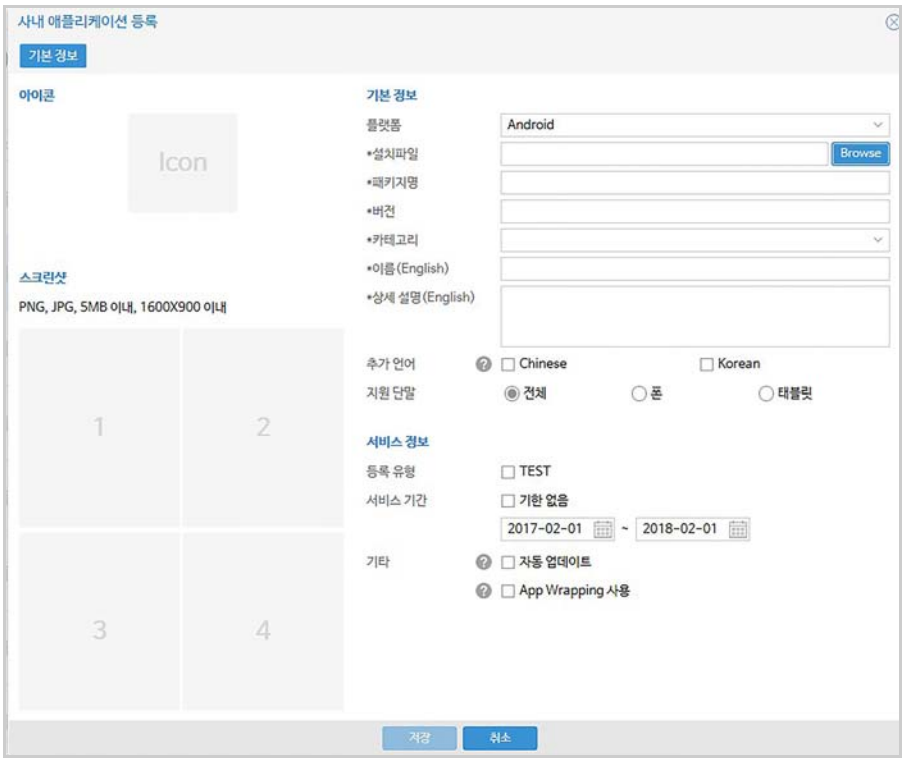
사내 애플리케이션 등록하기

사내 애플리케이션 파일을 등록하고 기본 정보와 자동 업데이트 , App wrapping, iOS managed App 의 기타 기능을 설정할 수 있습니다 . 동일한 패키지 또는 번들을 갖는 애플리케이션을 여러 버전으로 등록할 수 있습니다 .

사내 애플리케이션을 등록하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > 사내 애플리케이션**으로 이동하세요.
2. ➕을 클릭하세요.

3. “사내 어플리케이션 등록” 창에 기본 정보를 입력하세요.



항목	설명
아이콘	5MB 이하의 JPG, PNG 형식 파일로서 설치 파일 선택 시 자동 입력됩니다.
기본 정보	• **플**랫폼: Android, iOS, Tizen Wearable 중 선택 • **Android 패키지명 (iOS의 경우 번들ID), 버전**: 파일 선택 시 자동 추출됩니다. - 동일한 패키지(번들)를 갖는 애플리케이션을 여러 버전으로 등록 가능 • **설치파일**: **Browse**를 클릭하여 Android용은 APK, iOS용은 IPA형식 파일을 입력합니다. 선택한 파일의 다음의 정보가 자동 입력됩니다. - APK 파일: 이름 (English), 패키지명, OS, 버전 - IPA 파일: 이름 (English), 번들ID, 번들명, URL Scheme, OS, 버전 • **이름 (English)**: 선택된 파일의 영문명이 자동 입력됩니다. • **카테고리**: 카테고리 목록에서 선택하세요. • **상세설명 (English)**: 애플리케이션의 **이름**, **개요**, **상세 설명**, **사용법** 등의 정보를 입력하세요. • **추가 언어**: 애플리케이션 이름과 상세 설명 항목을 Chinese, Korean으로 추가 입력하세요. 단말 설정 언어에 따라 애플리케이션 설명이 나타납니다. **지원 단말**: 전체, 폰, 테블릿 중 선택하세요.

항목	설명
스크린샷	선택 항목이며 애플리케이션 관련 화면을 최대 4개까지 입력하세요.
서비스 정보	• **등록 유형**: Test 애플리케이션의 경우, **TEST**를 클릭하세요. Android만 지원합니다. - **Test 앱**: 애플리케이션 개발 편의성을 위하여, 무결성 확인을 위한 CRC 체크를 하지 않는 애플리케이션 • **서비스 기간**: 애플리케이션 서비스 기간을 설정. 기한없음 선택 또는 시작일과 종료일을 입력하세요. • **기타**: - **자동 업데이트**: 클릭 시, 단말에 설치된 애플리케이션의 버전을 체크하여 최신 버전으로 업데이트하고 이를 사용자에게 알립니다. - **App Wrapping 사용**: EMM SDK로 개발 가능한 사용자 인증, 화면 캡쳐, 화면 잠금, 단말 copy & paste 차단 기능을 사내 애플리케이션에 추가할 수 있습니다. Android만 지원합니다. EMM App Wrapper에 대한 자세한 내용은 225페이지의 "App Wrapping에 대하여"를 참고하세요. - **iOS Managed App 설정 사용**: MDM설정을 변경할 용도의 애플리케이션을 개발하여 등록하는 경우 클릭하세요.

4. **저장**을 클릭하세요.

App Wrapping에 대하여

EMM 의 App Wrapper 를 이용하여 사내 애플리케이션에 기능을 추가할 수 있습니다 . App Wrapper 를 사용하면 , EMM SDK 로 구현 가능한 기능들을 추출하여 사내 애플리케이션에 포함시킬 수 있으므로 , 플랫폼에 대한 전반적인 개발 지식 없이도 빠른 시간에 새로운 기능을 추가 개발 할 수 있는 장점이 있습니다 . 또한 wrapping 시 파일 암호화도 가능합니다 .

App wrapping 시의 유의사항은 다음과 같습니다 .

- App Wrapper를 이용한 변환은 사내 애플리케이션에 한정합니다. 외부 애플리케이션의 변환은 저작권 이슈의 문제가 있을 수 있습니다.
- Kiosk 변환 기능과 App wrapping 기능을 동시에 사용할 수 없습니다.
- Signing키를 체크하는 보안 로직 적용 앱의 경우에는 wrapping할 수 없습니다.
- EMM SDK를 사용한 앱은 wrapping할 수 없습니다.

App Wrapper 로 구현 가능한 EMM SDK 의 기능으로는 사용자 인증 , 화면 캡쳐 , 화면 잠금 , 단말 copy & paste 차단 등이 있습니다 . 사용자 단말에서는 기존 사내 애플리케이션과 Wrapping 된 사내 애플리케이션이 아이콘으로 구분되어 나타납니다 .

App wrapping 된 애플리케이션에 INI 파일이 필요한 경우 , 앱 관리 프로파일에 설정한 후 단말에 앱정책을 적용하면 단말의 data storage 에 저장됩니다 . Wrapping 된 애플리케이션에 필요한 INI 파일 등록 방법에 대해서는 181 페이지의 " 애플리케이션 정책 설정

하기 " 를 참고하세요 .

iOS Managed App 설정 사용 예시

iOS7 이상 단말의 MDM 설정을 변경하고자 하는 경우에만 사용합니다 . 개발자로 부터 MDM 설정 변경을 위해 별도로 개발된 애플리케이션을 전달 받습니다 . 운영자는 이 애플리케이션을 사내 애플리케이션으로 등록하면서 단말 설정 변경을 위한 Key 와 Value 값을 입력합니다 . 설정 내용에 따른 Key 와 Value 값은 개발자에게 문의합니다 .

예시) iOS 설정 변경용 앱을 이용하여 단말초기 URL 이 http://www.samsungsds.com 이 되도록 설정하려면 , 다음의 절차를 따르세요 .

1. 개발자로부터 애플리케이션 파일을 전달 받으세요.
2. 해당 파일을 **애플리케이션 > 사내 애플리케이션**에 등록하세요.
3. "사내 애플리케이션 등록" 창에서 **iOS Managed App 설정 사용**을 클릭하세요.
4. **Managed App 설정** 탭을 클릭하세요.
5. "사내 애플리케이션 등록" 창의 **Managed App 설정** 탭의 key값을 serverURL로, value값을 http://www.samsungsds.com으로 입력하세요.
6. **단말 & 사용자 > 단말**에서 **사내 애플리케이션 설치** 단말 제어 명령을 전송하세요.
7. 사용자는 단말에 해당 앱이 설치 된 후, 기본 URL이 http://www.samsungsds.com 임을 확인하세요.

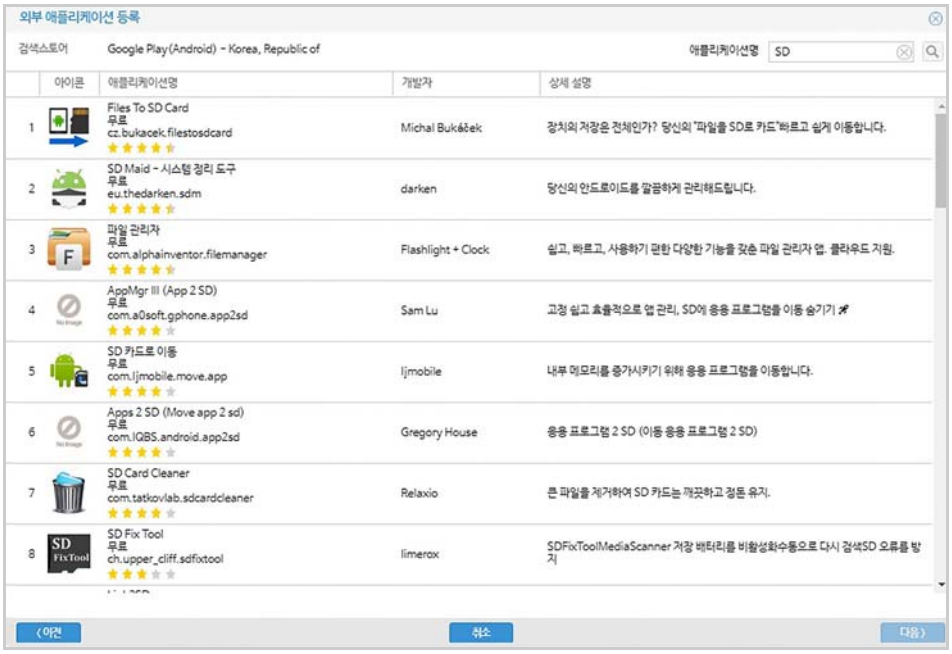
외부 애플리케이션 등록하기

Google Play (Android) 또는 App Store(iOS) 가 제공하는 애플리케이션을 국가별로 검색하여 등록할 수 있습니다 . **설정 > 서비스 > 환경 설정**의 **기본 국가코드**에 설정된 국가로 앱 스토어에서 검색이 되며 , 그 외의 국가로도 검색할 수 있습니다 .
외부 애플리케이션을 추가하려면 다음의 절차를 따르세요 .

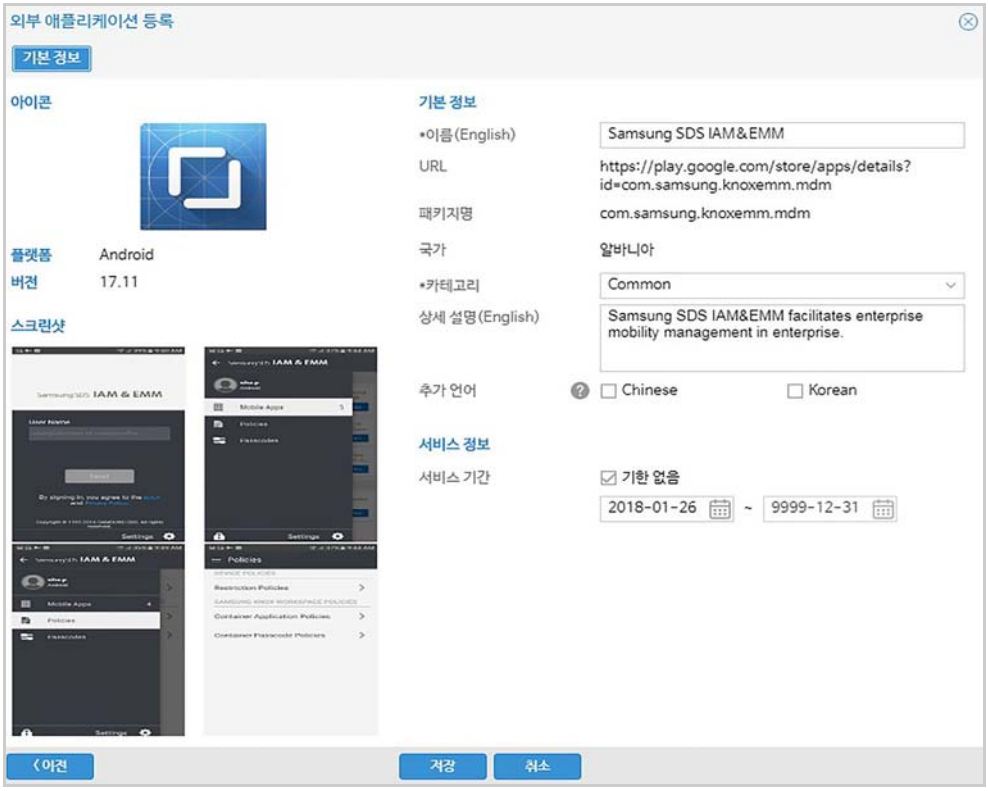
1. **애플리케이션 > 외부 애플리케이션**으로 이동하세요.
2. 외부 애플리케이션을 추가하려면 ➕을 클릭하세요.
3. "외부 애플리케이션 등록" 창에서 다음 항목을 입력하세요.

- **검색 스토어**: 앱스토어 종류를 **Google Play (Android)** 또는 **App Store (iOS)** 중에서 선택하세요. 앱스토어는 국가별로 애플리케이션을 등록하고 관리하여 정보를 제공합니다.
- **국가 설정**: 기본 이외 국가의 앱 스토어를 이용하려면 **국가 설정**을 클릭한 후 **국가**를 선택하세요.

4. **검색**을 클릭하세요.



5. "외부 애플리케이션 추가" 창에서 애플리케이션을 선택한 후, **다음**을 클릭하세요.



6. 애플리케이션 기본 정보를 입력하세요.

- **아이콘**, **Version.**, **이름(English)**, **패키지명**, **URL**: 앱 스토어가 제공하는 정보가 자동으로 입력됩니다.
- **카테고리**: 애플리케이션이 속하게 될 카테고리로서 단말상에 해당 카테고리에 애플리케이션이 보이게 됩니다.
- **상세 설명(English)**: 애플리케이션의 이름, 개요, 상세 설명, 사용법등의 정보를 입력하세요.
- **추가 언어**: Chinese 또는 Korean 으로 **이름**과 **상세 설명** 항목을 입력하세요.
- **서비스 기간**: 애플리케이션 서비스 기간을 기한없음 선택 또는 시작일과 종료일로 입력하세요.
- **스크린샷**: 앱 스토어가 제공하는 이미지 파일이 자동으로 입력되며 변경할 수 없습니다.

7. **저장**을 클릭하세요.

제어 애플리케이션 등록하기

단말에 설치할 애플리케이션을 프로파일에 설정하여 제어할 수 있습니다 . 이러한 애플리케이션을 제어 애플리케이션이라 칭하며 그 종류는 다음과 같습니다 .

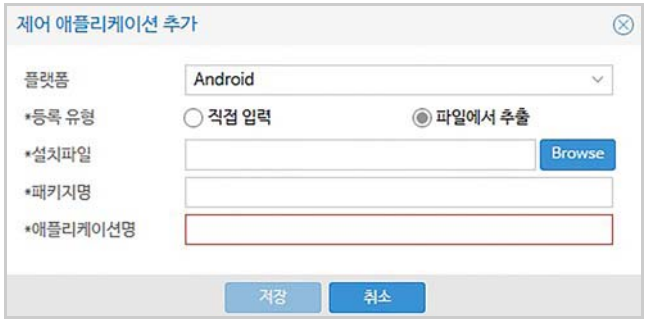
- 블랙 리스트와 화이트 리스트
- 단말 EMM 설치 시 기본으로 제공되는 애플리케이션
- Google Android for Work을 통해 배포 가능한 업무용 애플리케이션

EMM 내의 애플리케이션을 블랙리스트 또는 화이트리스트로 설정할 수 있습니다 . 블랙리스트는 단말에 설치되거나 실행되면 안되는 애플리케이션 , 화이트리스트는 단말에 설치 가능한 애플리케이션과 설치된 후 삭제되어서는 안 되는 애플리케이션을 말합니다 . 블랙리스트 또는 화이트리스트로 설정하고자 하는 애플리케이션을 제어 애플리케이션이라 하며 관리자 포털의 **애플리케이션 > 제어 애플리케이션**에서 등록 , 수정 , 삭제할 수 있습니다 . EMM 설치 시 기본으로 함께 설치되어야 하는 애플리케이션이 있는 경우 , 제어 에플리케이션에 등록합니다 . Google 의 Android for Work 앱을 통해 배포가능한 업무용 애플리케이션도 제어 애플리케이션에 등록하여 관리합니다 . 사내 , 외부 , EMM 애플리케이션으로 등록된 애플리케이션은 제어 애플리케이션으로 등록할 수 없습니다 .

제어 애플리케이션을 등록하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > 제어 애플리케이션**으로 이동하세요.

2. 제어 애플리케이션을 등록하려면 ➕을 클릭하세요.



- **플랫폼**: Android, iOS, Windows, Tizen Wearable 중 선택하세요.
- **등록 유형**: 플랫폼에 따라 **직접 입력**, **파일에서 추출**, **URL 검색**을 통해 등록하세요.

플랫폼	설명
Android, iOS	애플리케이션 정보를 **직접 입력**하거나 **파일에서 추출**하세요. • **직접 입력**의 경우: **패키지명**과 **애플리케이션명**을 입력하세요. - Android 플랫폼을 선택한 경우: 패키지명 입력 시 와일드카드를 입력할 수 있습니다. 패키지명 '.' 을 기준으로 다음 예제와 같이 중간 또는 끝에 위치할 경우에만 적용됩니다. 예: com.*.emm / com.sds.* / com.*.emm.* • **파일에서 추출**의 경우: 해당 설치파일 입력 시 **패키지명, 번들 ID**, **번들명**, **애플리케이션명**이 자동 입력됩니다.
Tizen Wearable	애플리케이션의 **패키지명**과 **애플리케이션명**을 입력하세요.
Windows	애플리케이션 정보를 **직접 입력**하거나 **URL검색**을 통하여 입력하세요. • 직접 입력의 경우: 패키지명, 게시자, 애플리케이션명을 입력하세요. • **URL 검색**의 경우: - **애플리케이션 ID**를 검색을 통해 찾아 입력하세요. - 정확한 **애플리케이션 ID** 입력 시, 해당 **패키지명**, **게시자**, **애플리케이션명**은 자동 입력됩니다. • **Preload 앱**: Windows플랫폼의 경우, 해당 앱을 Preload 앱으로 지정할 지 선택하세요.

3. **저장**을 클릭하세요.

단말 애플리케이션을 제어 애플리케이션으로 등록하기

단말에 설치된 애플리케이션 정보를 조회한 후 , 원하는 애플리케이션을 제어 애플리케이션으로 등록하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. **사용자 이름**, **사원 번호**, **이메일**, **모바일 ID**, **모델명**을 입력한 후 🔍을 클릭하세요.
3. 목록에서 상세 조회하려는 **모바일 ID**를 클릭하세요.
4. "단말 상세" 창의 **앱** 탭을 클릭하세요.

5. 목록에서 원하는 애플리케이션을 선택한 후 상단의 ➡을 클릭하세요.
6. 확인 메시지 팝업 창에서 **예**를 클릭하세요.

EMM 애플리케이션 등록하기

단말에서 EMM 을 사용하려면 운영자가 등록해 놓은 EMM 애플리케이션이 사용자 단말에 설치되어야 합니다 . EMM 애플리케이션은 필수로 설치해야 할 System 애플리케이션과 그 밖의 애플리케이션으로 이루어집니다 . System 애플리케이션에는 EMM Agent, EMM Client, Push Agent 가 있습니다 . 단 , Windows 플랫폼의 경우 Push Agent 는 설치되지 않습니다 .

Tizen Wearable 플랫폼의 경우 , EMM Agent, EMM Client, EMM Widget 을 Wearable EMM 하나의 파일로 제공합니다 . EMM 애플리케이션의 EMM Agent 항목에 대표로 Wearable EMM 앱 정보를 등록합니다 .

애플리케이션 > EMM 애플리케이션에 등록된 앱은 사용자가 단말에서 삭제할 수 없도록 EMM 삭제 방지 애플리케이션 리스트에 자동 등록됩니다 .

EMM 상품 종류에 따라 Secure Browser, mMail, SecuCamera, Knox Portal, Kiosk Browser 의 설치가 필요합니다 . 필수로 설치하고자 하는 경우 , 앱 관리 프로파일에 설정하여 정책에 반영합니다 .

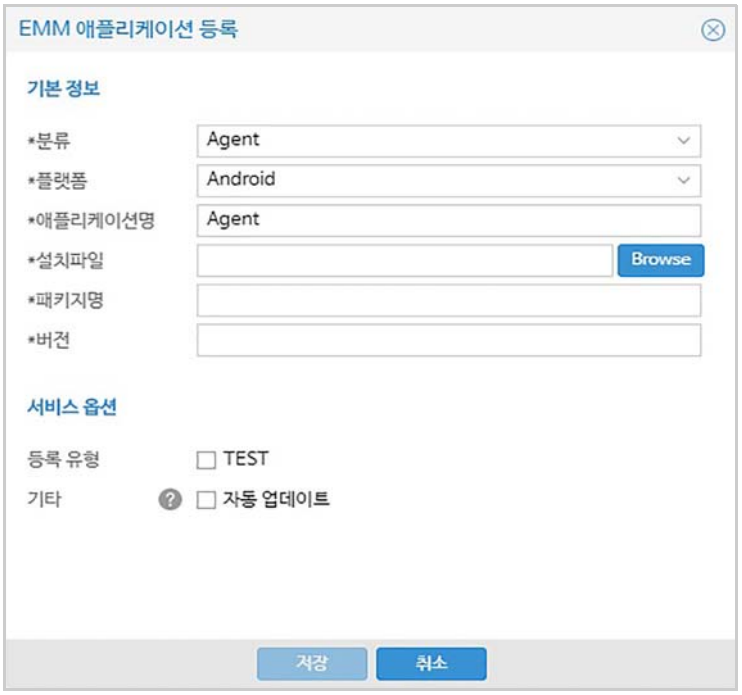
운영자는 Tenant 별로 EMM 애플리케이션을 등록하여 관리합니다 . EMM 애플리케이션으로 등록할 수 있는 파일의 유형과 수는 플랫폼별로 다음과 같이 제한됩니다 .

- Agent: Android 다수 등록 가능, Tizen Wearable 1개 등록 가능
  - Tizen Wearable Agent 등록 시, 패키지명은 “com.sds.emm.wearable”로 입력
- Client: Android, iOS, Windows 각 1개 씩 등록 가능
- Push Agent: Android 1개 등록 가능
- Secure Browser, mMail: Android, iOS 각 1개 등록 가능
- Kiosk Browser: Android 1개 등록 가능
- SecuCamera: Android 1개 등록 가능
- Knox Portal (Agent, UI) : Android 각 1개 등록 가능

EMM 애플리케이션 등록 및 수정 시 , 설치파일의 패키지명이 **설정 > 서비스 > 기준정보**의 **EMMPackageName** 과 동일해야 합니다 . 패키지명을 다르게 하려면 기준정보의 EMM PackageName 값을 변경해야 합니다 . 변경 방법에 대한 자세한 내용은 33 페이지의 " 사용자 동의서 설정하기 " 를 참고하세요 .

EMM 애플리케이션을 입력하여 등록하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > EMM 애플리케이션**으로 이동하세요.
2. EMM 애플리케이션을 추가하려면 ➕을 클릭한 후 **신규 등록**을 선택하세요.



3. "EMM 애플리케이션 추가"창에 정보를 입력하세요.
   - **분류**: Agent, Client, Push Agent, Secure Browser, mMail, SecuCamera, Knox Portal UI, Knox Portal Agent, Kiosk Browser
   - **애플리케이션명**: EMM 애플리케이션 이름
   - **설치파일**: APK, IPA, APPX형식의 파일
   - **플랫폼**: 선택된 분류에 따라 입력 가능한 플랫폼이 Android, iOS, Windows, Tizen Wearable 중 보여짐
   - 버전 및 패키지명 (Android 패키지명, iOS의 경우 번들ID)
     - APK 파일을 등록 시 플랫폼, 패키지명, 버전은 자동으로 입력됩니다.
     - iOS Secure Browser, mMail의 경우 url scheme을 등록해야합니다.
   - **유형**: Test 애플리케이션 등록 시 체크박스를 클릭하세요.
     - Test 애플리케이션은 개발 편의성을 위해 무결성 확인을 위한 CRC 체크를 하지 않는 애플리케이션입니다.
   - **기타**: **자동 업데이트**를 클릭 시 단말에 설치된 애플리케이션의 버전을 체크한 뒤 최신 버전 업데이트 알림을 사용자 단말에 내려줍니다.
4. **저장**을 클릭하세요.

EMM 애플리케이션 복사 등록하기

운영자가 여러 Tenant 관리 시 , 기존에 등록된 다른 Tenant 의 EMM 애플리케이션을 불러와 등록할 수 있습니다 . 복사 등록 시 정보 수정은 불가능합니다 . 수정 사항이 있는 경우에는 , 등록 후 해당 Tenant ID 로 접속하여 EMM 애플리케이션 메뉴에서 수정합니다 .

EMM 애플리케이션을 복사 등록하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > EMM 애플리케이션**으로 이동하세요.
2. EMM 애플리케이션을 추가하려면 ➕을 클릭한 후 **불러오기**를 선택하세요.

3. **Tenant ID**를 입력하세요.
   - 등록 오류 방지를 위해 Tenant ID는 전체 이름을 정확하게 입력하세요.
4. "EMM애플리케이션 등록" 창의 EMM 애플리케이션을 확인한 후 **저장**을 클릭하세요.
   - 불러온 EMM애플리케이션의 선택 저장은 불가능합니다.

Note:
- EMM 애플리케이션 복사 등록 시, 동일 서버에 있는 Tenant의 애플리케이션만 불러올수 있습니다.
- iOS 플랫폼의 경우, 같은 iDep 및 APNS 인증서를 사용하는 Tenant끼리만 복사 등록이 가능합니다.
- 현 Tenant의 EMM애플리케이션 보다 낮은 버전으로 복사할 수 없습니다.

애플리케이션 관리하기

사용자가 단말의 EMM App Store 를 통해 다운로드 받아 사용할 수 있도록 사내 애플리케이션을 EMM 관리자 포털에 등록합니다 . 사내 애플리케이션이 iOS 용인 경우 iOS 7 이상 단말의 MDM 설정을 변경하기 위해 설정값을 등록할 수 있습니다 . 사내 애플리케이션 등록 화면의 iOS Managed App 에서 가능합니다 . 설정 내용은 사용자가 단말에서 EMM 로그인 시 자동으로 적용됩니다 .

Google Play Store 나 Apple App Store 에 등록된 애플리케이션을 외부 애플리케이션이라 합니다 . EMM 관리자 포털에서 Google Play Store 또는 Apple App Store 의 애플리케이션을 검색하여 외부 애플리케이션으로 등록할 수 있습니다 . 외부 애플리케이션 등록 시 , 앱스토어는 해당 애플리케이션 관련 이름 , 아이콘 , URL, 플랫폼 , 패키지명 , 버전 정보 등을 최신 정보로 제공합니다 .

Tizen Wearable 앱에 대하여

EMM 을 통해 기어 단말에 Tizen Wearable 앱을 배포하려면 기어 앱 스토어 가입 후 앱 등록을 반드시 해야합니다 . 앱 등록을 위한 심사에 시간이 소요되기 때문에 미리 진행을 해야합니다 . 추가적으로 Standalone 모드에서 앱 설치를 위해서 기어 앱 스토어에 등록 앱에 Stub API 권한을 삼성전자로부터 부여 받아야합니다 . 앱 설치 시 , 삼성 계정이 필요하다는 메시지가 나오면 Stub API 권한이 없기 때문입니다 .

Note: 웨어러블 단말에서는 아래의 두가지 모드가 가능하며, B2B 사용 환경에서는 Standalone 모드를 권장합니다.

- Standalone 모드: 초기화된 기어 단말에서 모바일 폰과 블루투스 페어링 없이 사용하도록 설정된 모드
- Compainion 모드: 한번이라도 모바일 폰과 블루투스로 페어링하여 기어 매니저를 통한 설정이 된 모드

사내/외부 애플리케이션 활성화하기

사내 / 외부 애플리케이션은 EMM 관리자 포털에 등록 시 서비스 상태입니다 . 서비스 종료 상태의 애플리케이션의 경우 단말제어를 하려면 해당 애플리케이션을 서비스 상태로 활성화합니다 .

사내 , 외부 애플리케이션을 활성화하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > 사내 애플리케이션** 또는 **애플리케이션 > 외부 애플리케이션**으로 이동하세요.
2. 서비스 상태가 종료인 애플리케이션을 선택한 후 **서비스 상태** 항목을 클릭하세요.
3. “상태 변경” 창에서 서비스 기간을 입력하세요.
4. **확인**을 클릭하세요.

사내/외부 애플리케이션 비활성화하기

서비스 중인 사내 / 외부 애플리케이션을 서비스 종료 상태로 변경하면 , 사용자는 해당 애플리케이션을 다운로드 또는 실행할 수 없습니다 . 프로파일에 설정되어 서비스 중인 상태를 서비스 종료 상태로 변경 하는 경우 , 해당 애플리케이션은 프로파일에서도 삭제됩니다 .

사내 , 외부 애플리케이션을 비활성화하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > 사내 애플리케이션**으로 이동하세요.
2. 서비스 중인 애플리케이션을 선택한 후 **서비스 상태** 항목을 클릭하세요.
3. 상태 변경 확인 팝업 메시지가 나타나면 **예**를 클릭하세요.

외부 애플리케이션 업데이트하기

외부 애플리케이션 정보를 Google Play Store 또는 Apple App Store 의 최신 정보로 업데이트하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > 외부 애플리케이션**으로 이동하세요.
2. 업데이트하고자 하는 애플리케션의 을 클릭하세요..
3. "외부애플리케션 수정" 창에서 **버전 우측**의 을 클릭하세요.

제어 애플리케이션을 프로파일에 설정하기

프로파일 > 단말 관리 프로파일 메뉴에서 애플리케이션 관련 정책 설정시 제어 애플리케이션이 보여지며 , 화이트리스트 , 블랙리스트로 설정 가능합니다 . **프로파일 > 단말 관리 프로파일**에서 프로파일명을 클릭한후 " 프로파일 보기 " 창 **설정** 탭의 앱 블랙 / 화이트 리스트 설정에서 프로파일화하여 단말에 적용할 수 있습니다 . 자세한 내용은 141 페이지의 " 단말 관리 프로파일 정책 설정하기 " 를 참고하세요 .

Google Android for Work 을 통해 배포 가능한 업무용 애플리케이션들은 , **프로파일 > 앱 관리 프로파일 > Android for work** 메뉴에서 Work profile 에 적용할 앱 선택 시 보여집니다 . **프로파일 > 앱 관리 프로파일 > Android for work** 메뉴에서의 work profile 설정 관련하여 141 페이지의 " 단말 관리 프로파일 정책 설정하기 " 를 참고하세요 . Work profile 에 적용된 preloaded 앱이 단말에 정상적으로 설치되지 않은 경우 , 이에 대한 내용을 Audit 기록에서 확인할 수 있습니다 . Audit 로그 확인에 대한 자세한 내용은 54 페이지 3 장의 "Audit 이벤트 " 를 참고하세요 .

EMM 애플리케이션 삭제하기

EMM 애플리케이션이 프로파일에 설정되어 있는 경우 삭제 할 수 없습니다 . 삭제하기 전에 프로파일에서 EMM 애플리케이션을 제거한 후 삭제해야 합니다 . 시스템 애플리케이션을 삭제하면 단말 EMM 에 오류가 발생할 수 있습니다 .

EMM 애플리케이션을 삭제하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > EMM 애플리케이션**으로 이동하세요.
2. 목록에서 삭제할 EMM 애플리케이션의 을 클릭하세요.
   EMM애플리케이션이 설정된 프로파일 목록이 보여집니다.
3. 삭제 확인 팝업 메시지가 나타나면 **예**를 클릭하세요.

EMM 애플리케이션 삭제 및 위변조 방지하기

EMM 은 사용자 단말에 설치된 EMM 애플리케션에 대한 삭제 방지 기능과 위변조 방지 기능을 제공합니다 . EMM 의 System 애플리케이션인 EMM Agent, EMM Client, Push Agent 는 사용자가 단말에 설치한 후 직접 삭제하는 것이 불가능합니다 . EMM 애플리케이션인 Secure Browser, mMail, Secure Camera, Kiosk Browser 는 삭제 방지를 위해 운영자가 다음과 같이 설정할 수 있습니다 .

- 삭제 방지하기: Secure Browser, mMail, SecuCamera, Kiosk Browser의 삭제 방지를 원하는 경우, **프로파일 > 앱 관리 프로파일**에서 EMM 애플리케이션을 필수로 설정하는 정책을 추가합니다. 필수로 설정된 EMM 애플리케이션은 자동 설치 리스트와 삭제 방지 리스트에 자동으로 추가됩니다.
- 위변조 방지하기: EMM 관리자 포털의 **애플리케이션 > EMM 애플리케이션**에 등록되어 있는 EMM 애플리케이션과 사용자 단말에 설치되어 있는 EMM 애플리케이션은 일치해야 합니다. 사용자 로그인 시 단말 EMM의 signature를 서버의 signature와 비교하여 일치하지 않는 경우 위변조 된 앱으로 판단하고 단말에서 자동 삭제합니다. Signature는 TMS에서 관리합니다.

사내 애플리케이션 버전, 다운로드, 평가 이력 조회하기

사내 애플리케이션의 **버전** , **다운로드** , **평가 항목**에 대한 상세 이력을 확인할 수 있습니다 .

Tizen Wearable 플랫폼은 버전 이력만 조회가능합니다 .

조회하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > 사내 애플리케이션**으로 이동하세요.
2. 목록에서 선택한 애플리케이션의 **버전**, **다운로드**, **평가** 항목을 클릭하세요.

항목	설명
버전 이력	한국어, 영어, 중국어 지원 • 버전: 애플리케이션 버전 정보 • 업데이트 내용: 해당 버전의 주요 특징 • 날짜: 버전 등록일
다운로드 이력	사내 애플리케이션 버전별 다운로드 횟수 및 사용자 목록 조회 • 버전: 사내 애플리케이션 버전 정보 • 다운로드: 사내 애플리케이션의 다운로드 총 횟수. 다운로드 후 애플리케이션을 사용하지 않는 경우도 포함 • 사용자 ID: 사내 애플리케이션을 다운로드한 사용자 ID • 사용자 이름: 사내 애플리케이션을 다운로드한 사용자 이름 • 날짜: 애플리케이션 다운로드 날짜
평가	사내 애플리케이션 사용자의 사용 후기 • 날짜, 버전, 사용자 ID, 사용자 이름, 평점, 사용후기

EMM애플리케이션 버전 조회하기

EMM 애플리케이션의 버전 항목 클릭 시 해당 상세 이력이 조회됩니다 . 단 , Agent 는 여러 개 등록 가능하므로 버전 이력이 제공되지 않습니다 .

EMM 애플리케이션 버전을 조회하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > EMM 애플리케이션**으로 이동하세요.
2. 목록에서 선택한 애플리케이션의 **버전** 항목을 클릭하세요.

애플리케이션 카테고리

사용자 단말의 사내 애플리케이션과 외부 애플리케이션은 카테고리별로 분류 가능합니다 . 운영자는 애플리케이션의 카테고리를 최대 15 개까지 등록할 수 있습니다 . 카테고리 순서를 변경할 수 있으며 , 지정한 순서대로 단말에 카테고리가 나열됩니다 . 사내 애플리케이션과 외부 애플리케이션 등록 시 기본 카테고리를 등록한 뒤 , 필요에 따라 카테고리를 변경합니다 . 카테고리 이름은 영문 , 국문 , 중문으로 가능합니다 . 운영자는 **설정 > 서비스 > 기준정보**에서 필수 언어를 설정할 수 있습니다 .

카테고리 등록하기

1. **애플리케이션 > 카테고리 관리**로 이동하세요.
2. 카테고리를 추가하려면 ＋을 클릭하세요.
3. 카테고리의 **이름**, **상세 설명**을입력한 후 **저장**을 클릭하세요.
   - 영문, 국문, 중문 중 영문은 필수 입력 항목입니다.

카테고리 순서 변경하기

사용자의 단말에 보여지는 애플리케이션 카테고리의 순서를 변경하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > 카테고리 관리**로 이동하세요.
2. 이동하려는 카테고리를 선택하세요.
3. 위로 이동하려면 ↑을 클릭하세요.
   또는 아래로 이동하려면 ↓을 클릭하세요.
4. 변경한 순서를 고정하려면 을 클릭하세요.

애플리케이션의 카테고리 변경하기

사내 애플리케이션과 외부 애플리케이션의 기본 카테고리는 애플리케이션 등록 시 설정됩니다 . 카테고리를 변경하려면 해당 애플리케이션 정보에서 변경하거나 카테고리 관리에서 변경합니다 .

1. **애플리케이션 > 카테고리 관리**로 이동하세요.
2. 목록에서 조회할 카테고리의 **앱수**를 클릭하세요.
   해당 카테고리에 속한 애플리케이션정보가 조회됩니다.
   - 아이콘, 애플리케이션명, 플랫폼, 유형, 지원 단말, 서비스 상태, 버전, 다운로드
3. "애플리케이션 조회" 창에서 카테고리를 변경할 애플리케이션을 선택한 후 ➡을 클릭하세요.
4. "카테고리 변경" 창에서 애플리케이션을 이동시킬 **카테고리**를 선택한 후 **확인**을 클릭하세요.

Kiosk 애플리케이션

Android 단말에 특정 애플리케이션만 실행하려면 Kiosk 애플리케이션을 만들어 사용합니다 . Kiosk 모드의 런처를 제작하려면 Kiosk Wizard 를 사용합니다 . Kiosk Wizard 를 정상적으로 운영하려면 해당 PC 또는 노트북에 다음의 권장 사양이 충족되어야 합니다 .

- CPU: i5, 2.X GHz 이상
- 메모리: 4G 이상
- HDD: 500G 이상
- OS: Windows 7 이상

Kiosk 애플리케이션은 다음 세 가지 모드로 생성이 가능합니다 . 멀티 애플리케이션 Kiosk 생성에 Kiosk Wizard 가 사용됩니다 .

- 멀티 애플리케이션 모드: Kiosk Wizard로 제작된 런처를 통해 하나 이상의 애플리케이션이 실행됩니다.
- 싱글 애플리케이션 모드: 애플리케이션이 Kiosk 런처 홈을 거치치 않고 실행된 상태로 유지됩니다.
- Kiosk Browser 모드: 웹 페이지 실행을 위한 키오스크인 Kiosk Browser의 전용 Secure Browser가 Kiosk 런처 홈을 거치지 않고 실행됩니다. 실행될 웹 홈페이지의 URL을 운영자가 지정할 수 있습니다.

EMM 의 사내 , 외부 , 제어 애플리케이션 및 EMM 애플리케이션을 멀티 또는 싱글 애플리케이션 Kiosk 로 만들 수 있습니다 . Kiosk 런처 사용 시 , 운영자는 Kiosk Wizard 로 사용자의 단말 화면 , 배너 , 로고 및 다양한 위젯과 EMM 애플리케이션을 구성할 수 있습니다 . 운영자는 Kiosk 애플리케이션을 프로파일의 애플리케이션 관리에 설정하여 단말에서 사용 가능하도록 합니다 . 또한 단말의 Kiosk 애플리케이션 업데이트 및 제어가 단말 제어 명령 전송으로 가능합니다 .

Kiosk 애플리케이션에 대한 정책은 356 페이지 18 장의 “Kiosk Wizard 그룹 " 을 참고하세요 . 정책 설정 방법에 관한 내용은 141 페이지의 " 단말 관리 프로파일 정책 설정하기 " 를 참고하세요 .

멀티 애플리케이션 Kiosk 만들기

운영자는 Kiosk Wizard 를 이용하여 멀티 애플리케이션 Kiosk 를 만들 수 있습니다 . 멀티 애플리케이션 Kiosk 에는 다음의 애플리케이션과 위젯을 추가할 수 있습니다 .

- 애플리케이션: EMM의 사내, 외부, 제어 애플리케이션과 EMM 애플리케이션 (EMM Client, EMM Secure Browser)
- 위젯: 폴더, 배너, 텍스트, 월달력, 시계, 메모, 북마크

Kiosk 파일을 프로파일에 설정하고 단말에 적용하면 자동 설치됩니다 . 프로파일에 설정하는 방법에 대한 자세한 내용은 141 페이지의 " 단말 관리 프로파일 정책 설정하기 " 를 참고하세요 .

Kiosk Wizard 를 실행하여 멀티 애플리케이션 Kiosk 를 만들려면 다음의 절차를 따르세요 .

1. **애플리케이션 > Kiosk 애플리케이션**으로 이동하세요.
2. 화면 좌측 상단의 ➕을 클릭한 후 **멀티 애플리케이션**을 클릭하세요.
3. “멀티 애플리케이션 추가” 창의 Kiosk Wizard를 이용하여 Kiosk 런처를 구성하세요.
   - Kiosk Wizard 요소별 자세한 내용은 240페이지의 "● 쿠키 정책 설정: 웹 페이지의 쿠키 관련 설정을 변경할 수 있습니다."를 참고하세요.
4. APK 파일 생성을 위해 **빌드**를 클릭하세요.

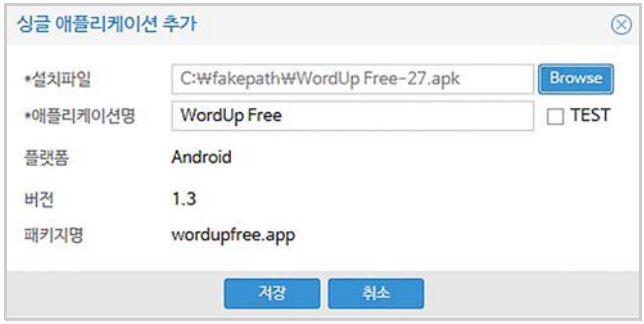
Note: 문제가 발생한 Kiosk 파일의 을 클릭 시 파일 오류 메시지가 나타납니다. 에러가 발생한 Kiosk 애플리케이션은 사용할 수 없으므로 재등록하거나 새로 생성합니다.

싱글 애플리케이션 Kiosk 만들기

APK 파일을 이용하여 Kiosk 애플리케이션을 만들려면 다음의 절차를 따르세요 .

1. **애플리케이션 > Kiosk 애플리케이션**으로 이동하세요.

2. 좌측 상단 ➕을 클릭한 후 **싱글 애플리케이션**을 클릭하세요.



- **설치파일**: APK 파일을 선택하려면 **Browse**를 클릭하세요. 선택된 파일의 플랫폼과 버전, 패키지명이 표시됩니다.
  - 키오스크 애플리케이션은 Android 단말에서만 지원됩니다.
- **애플케이션명**: Kiosk 애플리케이션 이름을 입력하세요.
- **TEST**: 애플리케이션 개발 편의성을 위하여, 무결성 확인을 위한 CRC 체크를 하지 않는 애플리케이션인 경우 클릭하세요.
- **플랫폼**: 등록한 파일의 플랫폼 정보입니다.
- **버전**: Kiosk 애플리케이션의 버전입니다. Kiosk 애플리케이션의 APK 파일에서 추출하여 보여집니다.
- **패키지명**: Kiosk 애플리케이션의 패키지 이름입니다.

3. **저장**을 클릭하세요.

Kiosk 애플리케이션 복사하기

기존의 Kiosk 애플리케이션 패키지를 복사하여 새로운 Kiosk 애플리케이션을 만들 수 있습니다 . Kiosk 복사 기능은 멀티 애플리케이션에만 가능합니다 .

Kiosk 애플리케이션을 복사하려면 다음의 절차를 따르세요 .

1. **애플리케이션 > Kiosk 애플리케이션**으로 이동하세요.
2. Kiosk 애플리케이션을 선택한 후 을 클릭하세요.
3. “Kiosk 애플리케이션 복사” 창에서 정보를 수정하세요.
   - **버전**: 복사 대상의 버전에 상관 없이 1.0.0이 초기값이며 버전을 자유로이 조정하여 입력할 수 있습니다.
   - **잠금 비밀번호**: 복사 대상의 잠금 비밀번호에 상관 없이 미사용이 초기값이며 잠금 비밀번호를 자유로이 조정하여 입력할 수 있습니다.
   - **화면전환**: 화면모드 전환 시 Grid 설정 및 현재 화면 설정이 모두 초기화됩니다.
   - **Grid**: 6x6이상 선택 시 스마트폰에서는 화면이 정상적으로 보이지 않을 수 있습니다.

- **위치변경**: 단말에서도 편집허용 선택 시, 사용자가 단말의 홈 화면에서 아이콘 위치 변경이 가능하세요.
- **포인트 색상**: 런처 내부의 아이콘 및 페이지 인디케이터 등에 적용될 포인트 컬러를 선택하세요.
- **페이지**: 순환 선택 시 마지막 페이지에서 swipe 시 첫번째 페이지로 이동하게 됩니다. 효과는 페이지 swipe 시에 적용되는 효과로 밀기, 카드, 상자, 밀어내기, 코너 중 선택하세요.
- **배경**: 배경 이미지는 5장까지 등록할 수 있습니다. 등록된 순서대로 화면 잠금 해제 시마다 배경화면이 변경되며, 랜덤 설정을 선택하면 무작위로 변경됩니다.

4. **빌드**를 클릭하세요.

Kiosk Browser 등록하기

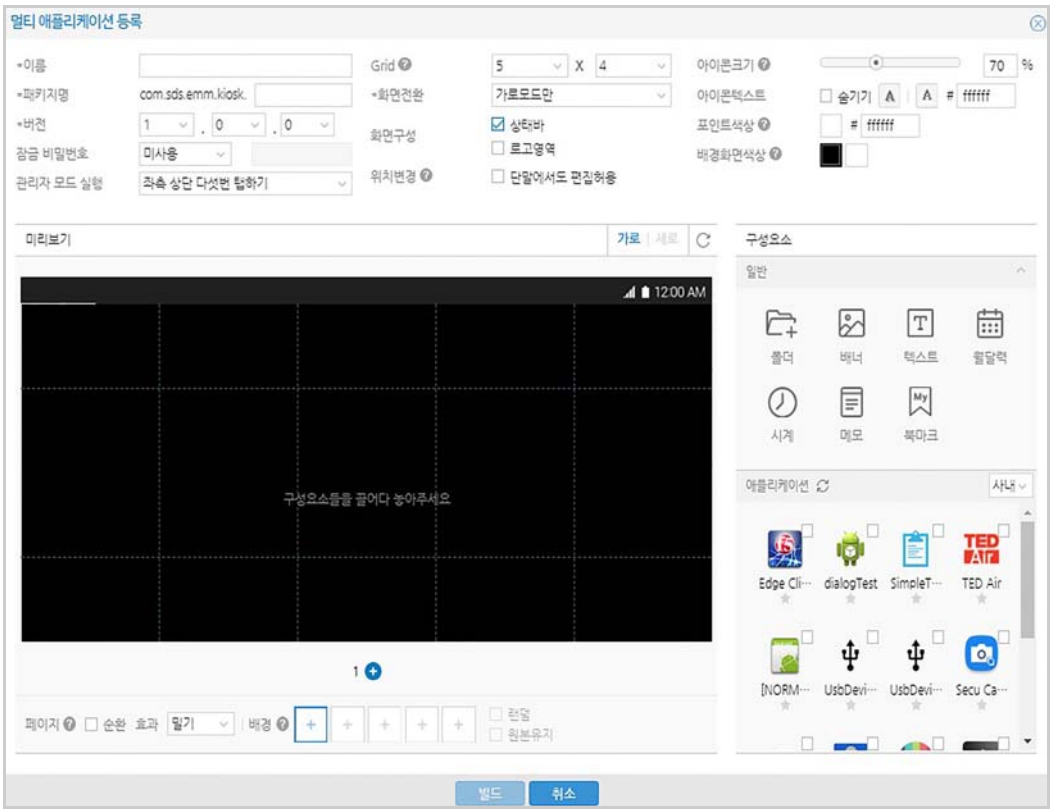
웹 전용 Kiosk 애플리케이션인 Kiosk Browser 는 단말 전용 Secure Browser 를 통해 실행됩니다 . Kiosk Browser 파일은 EMM 이 기본으로 제공하며 **애플리케이션 > EMM 애플리케이션**에서 확인 가능합니다 . 단말 프로파일에 Kiosk 정책을 설정하면 프로파일이 단말에 적용되는 시점에 자동으로 설치 또는 업데이트됩니다 . Kiosk Browser 를 통해 단말에서는 지정된 웹 홈페이지의 URL 만이 실행됩니다 .

Kiosk Browser 가 다음의 기능을 하도록 프로파일에 설정할 수 있습니다 .

- 자동 세션 종료: 설정 시간(초) 동안 단말을 사용하지 않는 경우, Kiosk Browser 사용자 정보(Cache, Cookie 등)를 삭제하고 기본 페이지 URL로 이동합니다.
- Privacy 보호
  - 로그인 ID와 비밀번호의 저장을 막을 수 있습니다.
  - 자동 세션 종료 시 사용자 계정은 자동 로그아웃되며 모든 개인 정보는 삭제됩니다.
  - 웹 사용 관련 모든 형태의 데이터는 삭제됩니다.
- 쿠키 정책 설정: 웹 페이지의 쿠키 관련 설정을 변경할 수 있습니다.

Kiosk Wizard 살펴보기

Kiosk Wizard 는 **애플리케이션 > Kiosk 애플리케이션**에서 화면 좌측 상단의 ➕을 클릭한 후 멀티 애플리케이션 선택 시 실행됩니다 . Kiosk Wizard 에서는 폴더 , 배너 , 텍스트 , 월달력 , 시계 , 메모 , 북마크 위젯과 애플리케이션을 원하는 Kiosk 미리보기 페이지로 끌어다놓아 화면을 구성합니다 . Kiosk Wizard 는 다음과 같이 구성되어 있습니다 .



- Kiosk Wizard 메뉴: Kiosk 애플리케이션 관련 설정 항목입니다.
- Kiosk 미리보기: Kiosk 애플리케이션 실행 시의 첫 화면을 미리보기 위한 화면입니다.
- 구성요소: Kiosk 애플리케이션에 추가 가능한 위젯과 애플리케이션이 제공됩니다.

Kiosk Wizard 메뉴

Kiosk 애플리케이션 관련 설정 항목입니다 . Kiosk 애플리케이션 정보를 구성하고 잠금 비밀번호를 설정합니다 . 화면 전환 , Grid 설정 , 화면 구성 , 위치 변경 , 아이콘과 포인트 색상 및 관리자 모드 실행을 위한 액션을 설정합니다 .

- **애플리케이션명**: Kiosk 애플리케이션의 이름을 입력합니다.

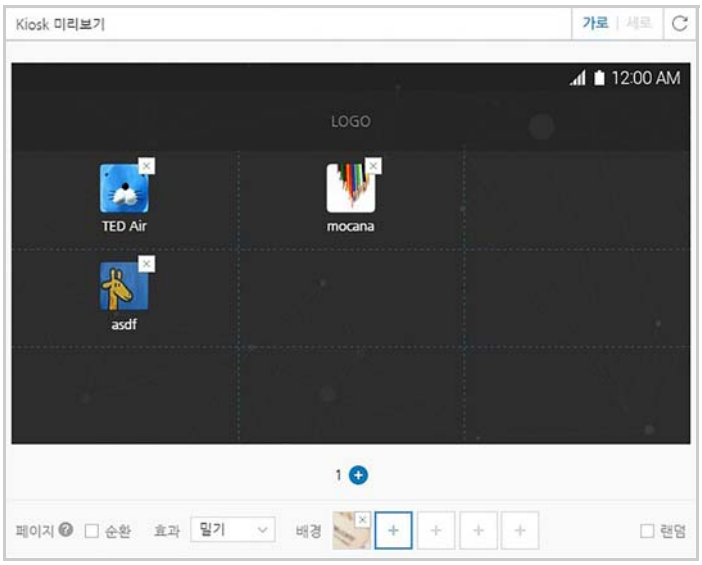
- **패키지명**: Kiosk 애플리케이션의 패키지 이름을 입력합니다.
- **버전**: Kiosk 애플리케이션의 버전으로 최초 등록시 기본값은 1.0.0입니다.
  - 기존 버전이 있는 경우 상위 버전을 입력합니다. 하위 버전 입력 시 "현재 버전보다 상위 버전을 입력해 주세요."라는 메시지가 표시됩니다.
- **잠금 비밀번호**: Kiosk 애플리케이션의 잠금 비밀 번호입니다.
  - 미사용 또는 4자리 숫자, 영문 + 숫자를 선택 후 비밀번호를 입력합니다.
  - 운영자는 Kiosk 애플리케이션 관리를 위해 비밀번호를 설정할 수 있으며 비밀번호 수정 시 Kiosk 애플리케이션을 재빌드 후 단말에 다시 배포해야 합니다.
- **관리자 모드 실행**: Kiosk 모드 사용 중 단말과 서버간 통신 불가로 원격 제어가 불가능한 경우, 관리자 모드를 실행하여 Kiosk 모드를 비활성화시킬 수 있습니다. 잠금 비밀번호를 설정한 경우에는 단말의 Kiosk 홈 화면의 좌측 하단에 위치한 ℹ을 탭하여 관리자 모드 진입 액션을 수행할 수 있습니다.
  사용자 단말에서 관리자 모드 실행 방법은 다음과 같습니다. 관리자 모드로 변경 진입을 위한 단말의 터치 액션을 선택합니다.

  가. 단말 홈 버튼의 좌측 메뉴를 터치하면 단말 화면에 About 메뉴가 표시됩니다. About을 탭하여 관리자가 Kiosk 애플리케이션 생성 시 정의한 터치 액션을 수행합니다. 예: 좌측 상단 다섯번 탭하기

  나. EMM 서비스의 오프라인 비활성화 코드를 관리자에게 요청하여 입력하면 Kiosk 모드가 비활성화되며 EMM 서비스도 비활성화 됩니다.
- **화면 전환**: 화면 전환 모드를 선택합니다.
  - 가로모드만 (기본값), 세로모드만, 모두지원 중 선택합니다.
- **Grid**: 화면 전환에 선택한 값에 따라 Grid 옵션을 선택합니다.
  - **가로**: 정방향과 가로특화 그리드를 지원합니다.
  - **세로**: 정방향과 세로특화 그리드를 지원합니다.
  - **모두지원**: 정방향만 지원합니다
- **화면 구성**: 상태바또는 로고영역을 클릭하면 Kiosk 미리보기 화면에 상태바와 로고영역이 표시됩니다.
  - **로고영역**을 클릭하면 "로고 이미지 등록" 창으로 이동합니다. 로고 등록이 완료되면 **확인**을 클릭합니다.
- **위치 변경**: **단말에서도 편집허용**을 클릭하면 사용자는 단말의 Kiosk 애플리케이션에서 아이콘 위치 변경이 가능합니다.
- **아이콘 크기**: 아이콘 크기를 조정합니다.
  - 선택 범위는 최소 50 ~ 100%입니다.
- **아이콘 텍스트**: 텍스트 숨기기, 그림자 사용 여부, 색상을 선택합니다.
  - 숨기기를 클릭하면 아이콘 텍스트 입력이 불가능합니다.
- **포인트 색상**: 런처 내부의 아이콘 및 페이지 인디케이터 등에 적용될 포인트 컬러를 설정합니다.
- **배경화면 색상**: Kiosk 배경 이미지 외의 남은 공간이 있는 경우, 검정색 또는 흰색으로 채워집니다.

Kiosk 애플리케이션 미리보기

Kiosk 미리보기는 폴더 , 배너 , 텍스트 , 월달력 , 시계 , 메모 , 북마크 위젯 , EMM 애플리케이션을 원하는 Kiosk 미리보기 페이지로 끌어다놓아 구성해보는 화면입니다 . Kiosk 에 사용되는 모든 이미지는 PNG 파일을 권장합니다 .



- **가로 / 세로**: Kiosk 메뉴의 화면 전환에서 선택한 모드만 활성화됩니다. 모두지원 모드인 경우 가로, 세로 미리보기가 가능합니다.
- : 클릭하면 현재까지 구성된 화면이 모두 삭제됩니다.
- **- / +**: Kiosk 미리보기 하단의 - 또는 +를 클릭하면 페이지를 삭제하거나 추가할 수 있습니다. Kiosk 페이지는 최대 9장까지 추가할 수 있습니다.
- **페이지 순환**: 순환을 클릭하면 사용자가 손으로 Kiosk 마지막 페이지를 넘길 시 자동으로 첫번째 페이지로 이동합니다.
- **페이지 효과**: 손으로 Kiosk 페이지를 넘길 때 적용할 효과를 선택합니다.
  - 밀기, 카드, 상자, 밀어내기, 코너
- **배경**: 배경 화면 설정을 위해 이미지를 업로드합니다. **+**를 클릭하면 "배경 이미지 등록" 창으로 이동합니다. 배경 이미지는 최대 5개까지 등록 가능하며 등록된 순서대로 배경 화면이 전환됩니다. 배경 등록이 완료되면 **확인**을 클릭합니다.
  - **랜덤**: 배경 화면 등록 순서와 상관없이 랜덤하게 보여집니다.
  - **원본유지**: 이미지 크기 조정없이 원본 크기가 유지됩니다.

구성요소

구성요소는 폴더 , 배너 , 텍스트 및 월달력 , 시계 , 메모 , 북마크 위젯의 일반영역과 사내 , 외부 , 제어 , EMM 애플리케이션 영역으로 구분되며 구성요소의 각 컨텐츠들을 Kiosk 미리보기 화면으로 끌어다놓아 화면을 구성합니다 .

- **폴더**: EMM 애플리케이션을 관리하기 위한 폴더입니다.
  - 폴더명은 수정이 가능하고 애플리케이션을 끌어다놓아 폴더에 추가하는 경우 썸네일로 애플리케이션이 표시됩니다. 또한 폴더를 더블 클릭하여 나타난 "폴더" 창에 애플리케이션을 추가, 삭제, 위치변경을 할 수 있습니다.
- **배너**, **텍스트**, **월달력**, **시계**, **메모**: 화면에 해당 컨텐츠를 설정할 수 있습니다. 컨텐츠를 끌어다놓으면 "등록" 창으로 이동합니다. 등록이 완료되면 **확인**을 클릭합니다.
  - 텍스트의 폰트 사이즈, 색상, 위치 변경이 가능합니다.
- **북마크**: 특정 웹페이지를 북마크로 지정하기 위한 위젯입니다. 북마크 위젯을 끌어다놓으면 "북마크 등록" 창으로 이동합니다. 북마크 등록이 완료되면 **확인**을 클릭합니다.
- **애플리케이션**: Kiosk 화면에 애플리케이션을 등록할 수 있습니다. 우측 리스트 박스에서 사내, 외부, 제어, EMM을 선택하면 현재 서비스 중인 관련 애플리케이션들이 하단에 썸네일로 표시됩니다. 애플리케이션을 끌어다놓거나 체크박스를 클릭하면 미리보기 화면에 추가됩니다.
  - **필수 애플리케이션**: 필수로 설치되어야하는 사내 애플리케이션의 경우, 썸네일 상단 별표를 클릭합니다. 필수로 선택된 사내 애플리케이션은 Kiosk 애플리케이션이 단말에 설치되는 경우 자동으로 설치됩니다. 또한 필수 사내 애플리케이션을 삭제한 경우 단말에 Empty 아이콘으로 표시되며 사용자가 재설치해야 합니다.
  - **필수 설치가 아닌 애플리케이션**: 단말에 Kiosk 애플리케이션 설치 시 해당 애플리케이션은 Empty 아이콘으로 제공되며, 사용자가 Empty 아이콘을 탭하여 선택적으로 설치할 수 있습니다.

15 인증서

일반적으로 공개키 기술을 적용하는 애플리케이션의 경우 보안 강화를 위해 인증서를 발급하고 관리합니다. EMM 에는 Wi-Fi, VPN, Exchange, APNS 등과 같은 네트워크 사용을 위한 외부 인증서가 있습니다. 운영자는 발급한 인증서 목록를 관리자 포털에서 조회할 수 있으며, 유효하지 않은 인증서는 삭제할 수 있습니다. EMM 에서 관리 가능한 인증서의 종류, 용도 및 상태 구분은 다음과 같습니다.

인증서 종류

구분	설명
Wi-Fi	• Wi-Fi용 AP와 연결 및 사용을 위한 인증서 • Wi-Fi 장비 설정 확인 요함 • Subject 이름, 즉 인증서의 CN값으로 MAC address 사용 시 iOS에서는 발급 불가
Generic VPN	• 삼성 전자 단말에 특화된 VPN 인증서 • VPN 장비 설정 확인 요함
VPN	• MDM등록시 단말 VPN암호화 통신을 위한 인증서 • VPN 장비 설정 확인 요함
Exchange	• Exchange에서 사용자 인증 및 서비스를 위한 인증서 • Subject이름, 즉 인증서의 CN값으로 E-maill address 사용
APNS	Apple의 Push 알림 서비스를 받기 위한 인증서
CA Cert	사용자 공개키로 요청해 CA에서 발급받은 인증서
iOS Sign Cert	iOS 단말에 다운받아 서버에서 단말로의 데이터 전달이 안전함을 증명하는 인증서
Knox Generic VPN	• Knox 사용 단말 VPN 암호화 통신을 위한 인증서 • VPN 장비 설정 확인 요함
mobile Mail	mMail 서비스를 위한 단말 인증서

인증서 유형

구분	설명
Root	Root CA(Certificate Authority) 식별을 위한 인증서 체인 상의 최상위 인증서
User	단말, 애플리케이션, 서비스 등 일반 목적으로 발행된 인증서
Server	일반 목적으로 발행된 서버용 인증서

인증서 상태

구분	설명
Generated	정상적으로 발급되어 사용중인 상태
Deleted	운영자에 의해 삭제되어 EMM에서 사용될 수 없는 상태
Revoked	CA서버에서 폐기되어 사용될 수 없는 상태

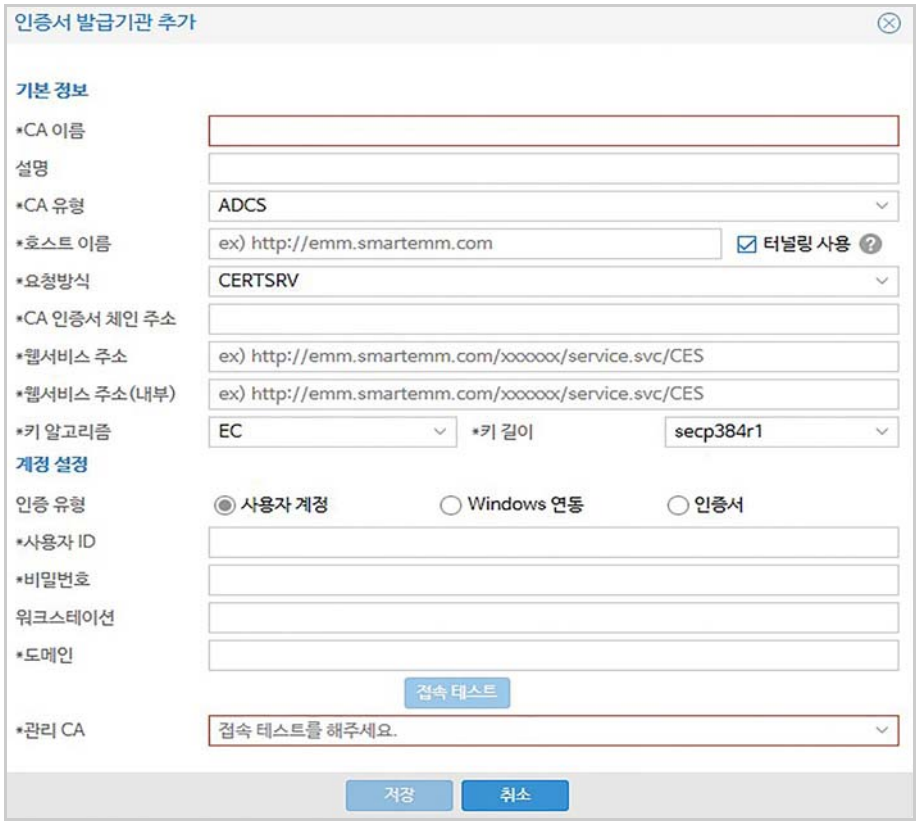
인증서 발급기관(CA) 등록하기

EMM의 인증서 서비스를 사용하기 위해서 ADCS, Generic SCEP, NDES, CertAgent, EST 유형의 CA 를 등록하여 관리합니다 . SCEP 를 지원하는 CA 로부터 CA root 인증서를 다운로드할 수 있고 , 단말 인증서 및 외부 인증서를 발급할 수 있습니다 . CA 등록 시 접속 테스트 기능을 제공합니다 . CA 삭제는 사용 중인 템플릿이 없는 경우에만 가능합니다 . 최초 등록된 CA Root 인증서 이외의 Root 인증서 등록은 CA 수정 시 가능합니다 .

인증서 발급기관을 등록하려면 다음의 절차를 따르세요 .

1. **인증서 > 인증서 발급기관(CA)**으로 이동하세요.
2. ➕을 클릭하세요.
3. 인증서 발급기관 정보를 입력하세요.
   - **CA이름**: CA서버와 연결하여 사용할 CA 이름을 입력하세요.
   - **CA유형**: 회사 기간계 시스템에서 사용하는 CA제품 유형으로 ADCS, Generic SCEP, NDES, CertAgent, EST 중 선택하세요.

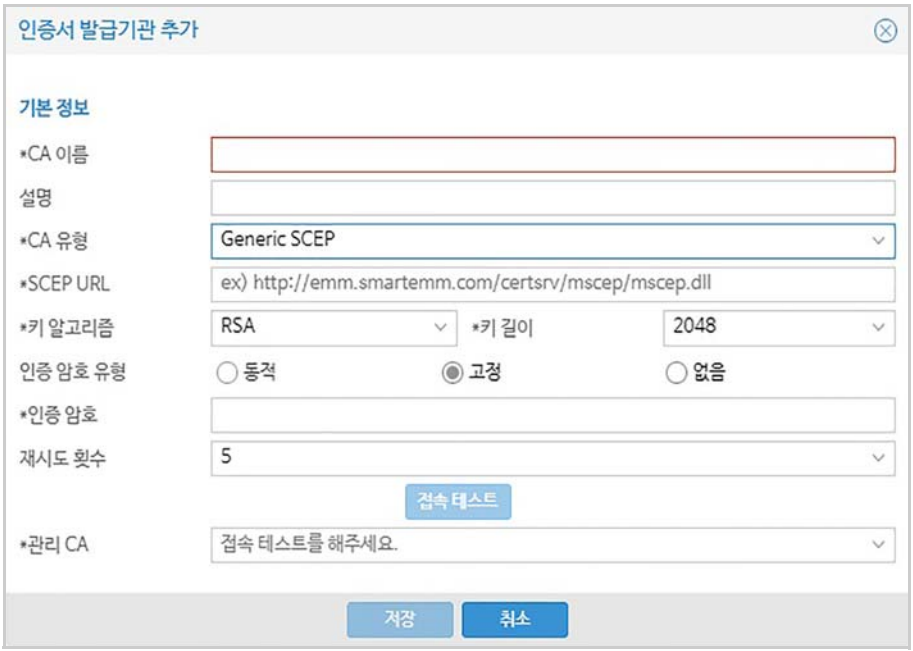
- CA 유형이 ADCS인 경우



항목	설명
호스트 이름	CA서버 호스트의 URL 주소. 예: https://emm.smartemm.com/
터널링 사용	• ADCS CA 연결 시 터널링 사용할 경우 체크 • **웹서비스 주소(내부)**: 터널링 사용 시 터널링 서버의 호스트와 포트가 포함된 내부에서 호출하는 웹서비스 주소를 입력
요청방식	인증 기관에 인증서 유효성 확인을 요청하는 방식으로 CERTSRV와 URL방식 중 선택 • CERTSRV: 사용자 단말 로그인 시 CRL체크 방식에 의해 유효성 확인 • URL: 사용자 단말 로그인 시 OCSP 체크 방식에 의해 유효성 확인
CA인증서 체인 주소	Root인증서와 Server 인증서를 포함하는 인증서 체인이 위치하는 CA 서버상의 주소 요청 방식이 CERTSRV 일 경우, 호스트 이름의 값에 '/certsrv'를 추가하여 자동입력 예: https://emm.smartemm.com/certsrv
웹서비스 주소	해당 인증기관 서비스가 제공되는 웹 주소로써 CA와 웹서비스를 하기 위해 등록된 Certificate Enrollment Web Service (CES) 주소를 입력
웹서비스 주소 (내부)	터널링 사용 시 터널링 서버 호스트와 포트가 포함된 내부에서 호출할 웹서비스 주소
키 알고리즘	RSA, EC중 선택

항목	설명
키 길이	키 알고리즘에 따라 적절한 값 선택 • 키 알고리즘이 RSA일 경우: 2048, 3072, 4096 중 선택 • 키 알고리즘이 EC일 경우: secp256r1, secp384r1 중 선택
인증 유형	인증 방식은 사용자 계정, Windows연동, 인증서 방식 중 선택할 수 있습니다. 사용자 ID, 비밀번호, 워크스테이션, 도메인은 세 가지 방식 공통 입력 항목이며, 유형에 따라 아래의 항목을 추가로 입력하세요. • Windows 연동: Window 통합 인증 방식으로 Auth Type은 NT LAN Manager(NTLM) 과 NEGOTIATE (Kerberos) 중 선택하여 입력 • 인증서: Client에서 사용할 인증서 선택 후 암호 입력. 인증서 타입, 인증서 경로, 인증서 비밀번호 입력
관리 CA	회사 내 CA 서버 명칭

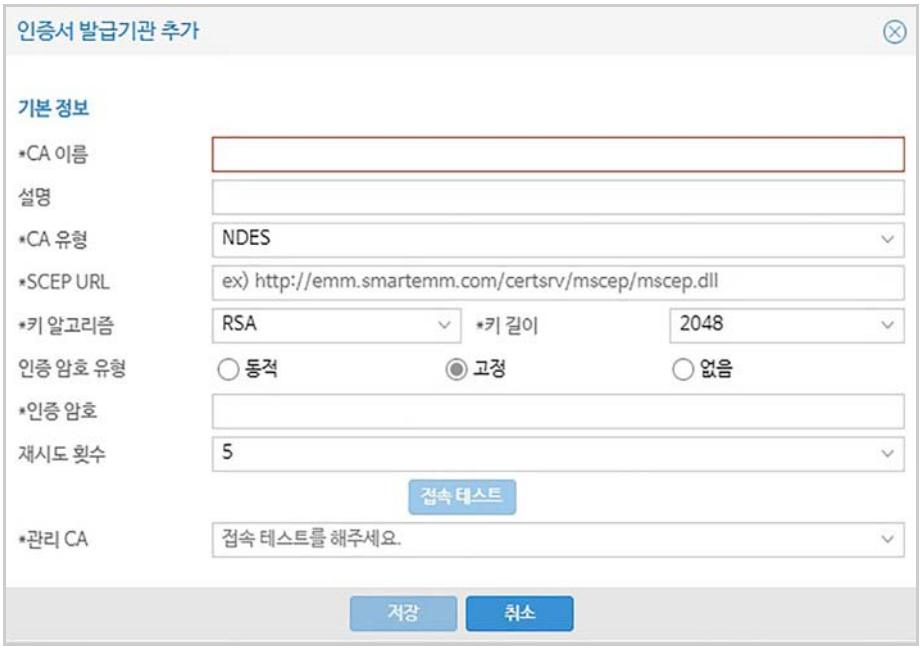
- CA 유형이 Generic SCEP인 경우



항목	설명
호스트 이름	CA서버 호스트의 URL주소. 예: https://emm.smartemm.com/
SCEP URL	인증 기관에 인증서 유효성 확인 요청을 보낼 SCEP IP 또는 URL 주소. 예: http://emm.smartemm.com/certsrv/mscep/mscep.dll
키 알고리즘	RSA만 지원됨
키 길이	2048, 3072, 4096중 선택
인증 암호 유형	Generic SCEP 유형의 CA를 인증하기 위한 암호 • **고정**: 인증 암호에 입력한 암호가 사용됨 • **없음**: 인증 암호를 사용하지 않음

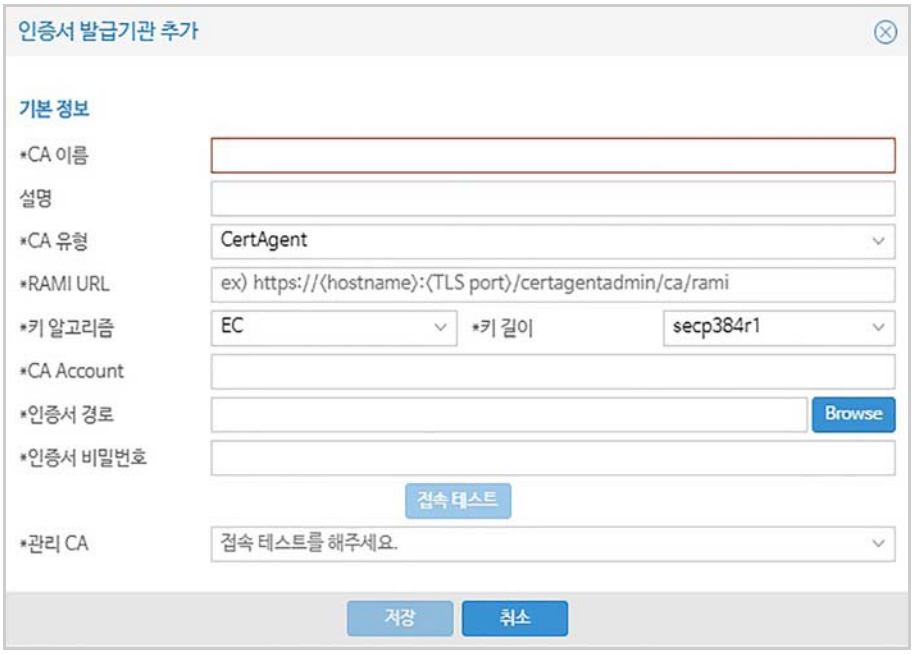
항목	설명
재시도 횟수	인증서 발급 지체 시 재시도 횟수 • 기본값: 5, • 입력 가능 값: 1 ~ 10
관리 CA	회사 내 CA 서버 명칭

- CA 유형이 NDES인 경우



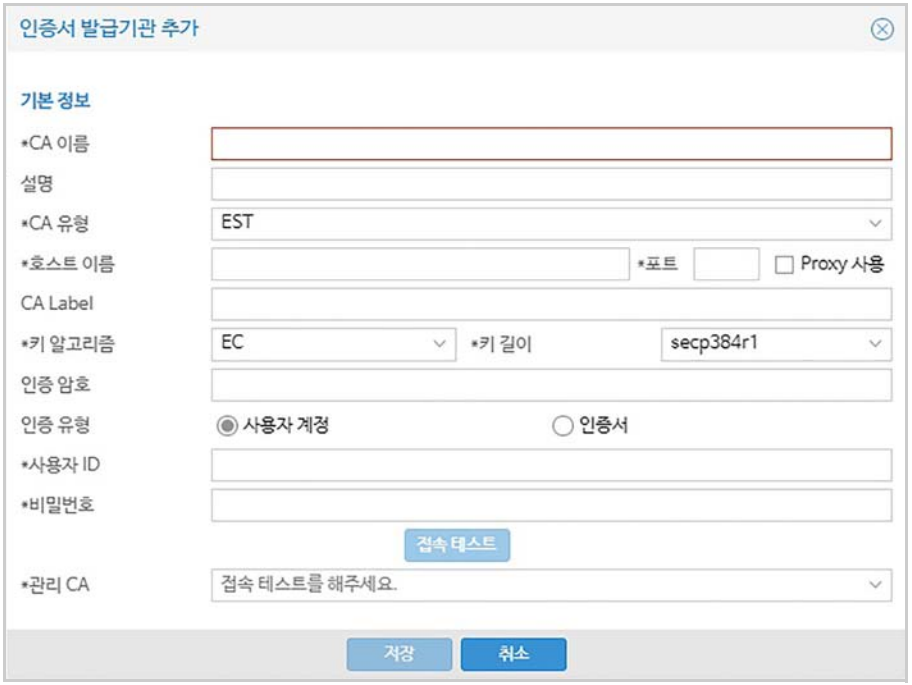
항목	설명
호스트 이름	CA서버 호스트의 URL주소. 예: https://emm.smartemm.com/
SCEP URL	인증 기관에 인증서 유효성 확인 요청을 보낼 SCEP IP 또는 URL 주소. 예: http://emm.smartemm.com/certsrv/mscep/mscep.dll
키 알고리즘	RSA만 지원됨
키 길이	2048, 3072, 4096 중 선택
인증 암호 유형	인증서 발급 요청이 발생한 경우, Generic SCEP 유형의 CA를 인증하기 위해 설정하는 암호 방식 • 동적: EMM 서버에 설정된 사용자 ID, 비밀번호, 도메인, Challenge URL 등의 인증 정보 입력 • **고정**: 인증 암호에 입력한 암호를 고정적으로 사용 • **없음**: 별도의 인증 암호를 사용하지 않음
재시도 횟수	인증서 발급 지체 시 재시도 횟수 • 기본값: 5, • 입력 가능 값: 1 ~ 10
관리 CA	회사 내 CA 서버 명칭

- CA 유형이 CertAgent인 경우



항목	설명
RAMI URL	인증 기관에 인증서 유효성 확인 요청을 보낼 RAMI IP 또는 URL 주소. 예:https://emm.smartemm.com/certagentadmin/ca/rami
키 알고리즘	RSA, EC 중 선택
키 길이	2048, 3072, 4096 중 선택
사용자 ID	CA 관리자의 CA 서버 로그인 ID
인증서 경로	인증서 발급 요청이 발생한 경우, CertAgent 유형의 CA를 인증하기 위해 사용되는 인증서 파일의 위치
인증서 비밀번호	CertAgent 유형의 CA를 인증하기 위해 사용되는 인증서 비밀번호
관리 CA	회사 내 CertAgent CA 서버 명칭

- CA 유형이 EST인 경우



항목	설명
호스트 이름	CA서버 호스트의 URL주소. 예: testrfc7030.cisco.com
포트	CA서버 호스트의 포트 번호
Proxy 사용	CA서버 Proxy 사용 여부
CA Label	CA서버의 Label 입력. CA 서버 관리자에게 문의 후 입력
키 알고리즘	RSA, EC중 선택
키 길이	키 알고리즘에 따라 적절한 값 선택 • 키 알고리즘이 RSA일 경우: 2048, 3072, 4096 중 선택 • 키 알고리즘이 EC일 경우: secp256r1, secp384r1 중 선택
인증 암호	CA서버 인증 시 필요한 암호 입력
인증 유형	인증 방식은 사용자 계정, 인증서 방식 중 선택 • 사용자 계정: 사용자 계정의 ID와 비밀번호를 입력 • 인증서: 인증서 발급 요청이 발생한 경우, EST유형의 CA를 인증하기 위해 사용되는 인증서 파일의 위치를 인증서 경로에 입력. 해당 인증서의 비밀번호 입력
관리 CA	회사 내 CertAgent CA 서버 명칭

4. 입력한 정보를 확인하기 위해 **접속 테스트**를 클릭하세요.
5. **저장**을 클릭하세요.

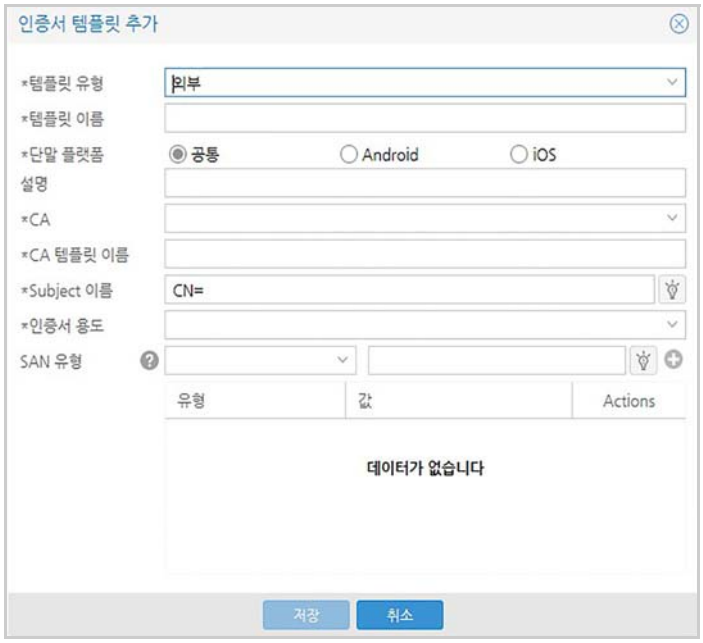
인증서 템플릿 등록하기

CA 서버는 인증서 유형을 템플릿화하여 관리합니다 . 템플릿화된 인증서 양식에 따라 인증서 설정 항목들을 간소화 , 표준화하여 효율적인 인증서 발급이 가능합니다 .

외부 유형의 템플릿을 생성하여 Wi-Fi, VPN, Exchange 인증을 위해 사용합니다 . 템플릿은 사용자 인증을 위한 프로파일 설정 시 사용됩니다 . 프로파일 설정 시의 사용자 인증서 입력 방법에 대한 자세한 내용은 147 페이지의 " Android 설정 등록하기 " 를 참고하세요 .

인증서 템플릿을 등록하려면 다음의 절차를 따르세요 .

1. **인증서 > 인증서 템플릿**으로 이동하세요.
2. ➕을 클릭한 후 템플릿 정보를 입력하세요.



- 템플릿 유형: Wi-Fi, VPN, exchange 인증을 위한 탬플릿 유형인 외부를 입력하세요.
- 템플릿 이름: 템플릿에 부여할 이름을 입력하세요.
- **단말 플랫폼**: 공통, Android, iOS 중에서 인증서를 발급하고자 하는 단말의 플랫폼을 선택하세요.
  - 공통: Android, iOS 구분없이 단일 템플릿을 사용하는 경우
  - Android, iOS: Android 또는 iOS 플랫폼에 따라 다른 템플릿을 사용하는 경우
- **CA**: 기등록된 인증서 발급기관 목록에서 선택하세요.
  - CertAgent 유형의 CA인 경우: 프로파일 ID를 입력할 수 있습니다. 입력 하지 않는 경우 master profile이 사용됩니다.
  - EST 유형의 CA인 경우: CA Label을 입력할 수 있습니다. 입력하지 않는 경우, **인증서 > 인증서 발급기관(CA)**에 등록된 **CA Label**이 사용됩니다.
    CA의 **인증 유형**이 **사용자 인증**인 경우 SAN 값을 다음과 같이 입력하세요.
    - **SAN 유형**: 목록에서 Email Address를 선택하세요.
    - **SAN 값**: 을 클릭한 후, “참조 항목” 창에서 **사용자 이름**을 선택한 다음 을 클릭하세요.
- **CA 템플릿 이름**: CA가 제공하는 템플릿 사용 시, 템플릿 이름을 입력하세요.

  - Generic SCEP, NDES, CertAgent, EST유형의 CA는 단일 템플릿을 제공하므로, **CA 템플릿 이름**은 등록할 필요 없습니다.
- **Subject 이름**: 인증서 용도에 따라 CN= {Subject 이름값}의 형태로 입력하세요.
- **인증서 용도**: 외부 인증서의 경우 단말 플랫폼에 따라 아래와 같이 입력하세요.
  - **공통, iOS**: Wifi, VPN, Exchange 중 선택
  - **Android**: Wifi, VPN, Exchange, Knox Generic VPN, Generic VPN 중 선택
- **SAN 유형**: X.509의 extension으로서 인증서와 관련된 다양한 값이 허용된 규격.
  - **유형**에서 Email Address, DNS Name,Directory Name, URL, IP Address, Registered ID, User Principal Name 중 선택하고 우측 SAN 값을 목록에서 선택한 후 +를 클릭하세요.
  - 선택한 SAN값이 multi-byte (예:한글)인 경우 인증서 발급이 되지 않습니다.
  - 인증을 위한 Certificate Signing Request (CSR) 생성 시 사용

3. **저장**을 클릭하세요.

인증서 템플릿 삭제하기

프로파일에 설정된 인증서의 템플릿은 삭제할 수 없습니다 . 사용 중인 탬플릿의 삭제는 단말 관리 프로파일의 Android, iOS 설정을 삭제한 후에 가능합니다 .

인증서 템플릿을 삭제하려면 다음의 절차를 따르세요 .

1. **인증서 > 인증서 템플릿**으로 이동하세요.
2. 전체 목록 중 삭제하려는 템플릿의 을 클릭하세요.
   - 사용 중인 템플릿은 삭제 불가 메시지가 나타납니다.

외부 인증서 등록하기

인증서를 CA 로부터 발급 받지 않고 , 인증서 파일을 등록하여 EMM 서버에서 관리할 수 있습니다 .

1. **인증서 > 외부인증서**로 이동하세요.
2. ➕을 클릭한 후 인증서를 추가하세요.
3. “외부 인증서 추가” 창에서 정보를 입력하세요.

- **이름**: 외부 인증서의 이름을 입력하세요.
- **용도**: Wifi, Generic VPN, VPN, Exchange, CA, iOS Sign, Knox Generic VPN, Mobile Mail 중 선택하세요.
- **유형**: Root, User, Server 중 선택하세요.
- **파일**: Browse 클릭하여 검색 후 입력하세요.
  - 외부 인증서 파일은 CER, DER, PFX, P12 형태만 가능합니다.
- **비밀번호**: 외부 인증서의 비밀번호를 입력하세요.
- **설명**: 외부 인증서에 대한 간단한 설명을 입력하세요.

4. **저장**을 클릭하세요.

외부 인증서 수정하기

외부 인증서의 용도와 유형은 수정할 수 없고 , 외부 인증서 파일을 다른 파일로 갱신할 수 있습니다 .

외부 인증서 정보를 수정하려면 다음의 절차를 따르세요 .

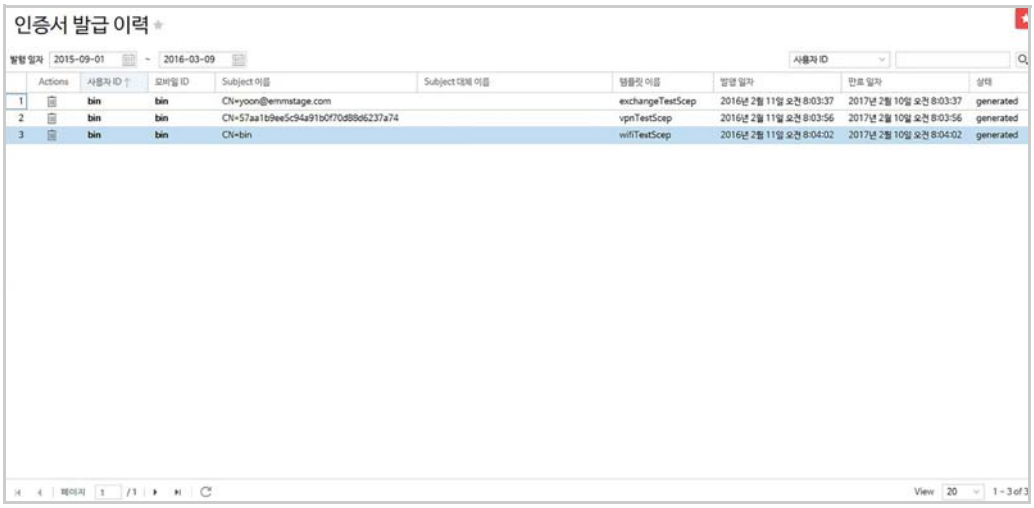
1. **인증서 > 외부인증서**로 이동하세요.
2. 수정을 위해 을 클릭하세요.
3. "외부 인증서 수정" 창에서 정보를 수정하세요.
   - **갱신**: 선택 시, 새로운 외부 인증서 파일을 Browse하여 입력하세요.
   - **비밀번호**: 인증서 암호를 입력하세요.
4. **저장**을 클릭하세요.

인증서 발급 이력 조회하기

CA 서버에서 발급된 모든 인증서의 발급 이력을 조회할 수 있습니다 . EMM 의 인증서 상태는 다음과 같이 구분됩니다 .

- Generated: 정상적으로 발급되어 사용 중인 상태
- Deleted: 운영자에 의해 삭제되어 EMM에서 사용 불가인 상태

발급된 인증서는 사용자 요청에 의해 또는 만기 도래 시에 갱신이 가능합니다 . Android 단말의 경우 사용자가 직접 인증서를 갱신할 수 있으며 , iOS 단말의 경우 만기된 인증서에 대해 서버에서 자동으로 갱신합니다 . 단말 비활성화 시 단말 내의 모든 인증서는 폐기처리되며 단말에서 삭제됩니다 . 운영자는 EMM 서버에서 더 이상 사용 불가능한 인증서를 관리자 포털에서 삭제할 수 있습니다 .



해당 인증서의 사용자와 단말 정보를 조회하려면 다음의 절차를 따르세요 .

1. **인증서 > 인증서 발급 이력**으로 이동하세요.
2. **발행 일자**, **사용자 ID**, **모바일 ID**, **템플릿 이름**을 입력한 후 을 클릭하세요.해당 인증서의 **사용자 ID**, **모바일 ID** 클릭 시 상세 정보가 조회됩니다.
   - 단말 상세 화면은 단말 상태가 Activated 또는 Blocked by System인 경우에만 조회됩니다.

인증서 삭제하기

운영자는 EMM 단말에서 사용 중인 Wi-Fi, VPN, Exchange 인증서를 삭제할 수 있습니다 . 단 , ADCS 유형의 CA 에서 발급한 Android 용 인증서는 삭제할 수 없습니다 . 인증서를 삭제하려면 다음의 절차를 따르세요 .

1. **인증서 > 인증서 발급 이력**으로 이동하세요.
2. **사용자 ID**, **모바일 ID**, **템플릿 이름을** 입력한 후 을 클릭하세요.
3. 삭제하려는 인증서의 을 클릭하세요.
4. 삭제 확인 팝업 메시지가 나타나면 **확인**을 클릭하세요.

Note: 인증서가 폐기된 단말을 사용하려면 단말을 재등록해야합니다.

16 연동 서비스

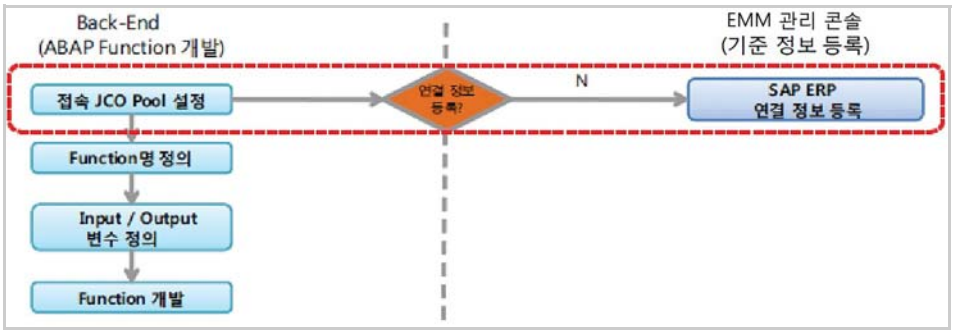
EMM 은 회사내 기간계 시스템과 연계가 가능한 다양한 연동 서비스를 제공합니다. 또한 연동 시스템에 등록된 서버들의 서비스를 제공하기 위해 커넥터를 설정합니다 . 연동 시스템은 서비스 그룹을 만들어 커넥터를 관리하며 , 역할을 부여하여 커넥터 서비스에 접근이 가능한 사용자만 서비스를 사용할 수 있도록 설정할 수 있습니다 .

Note:
- 연동 시비스 및 커넥터는 라이선스 유무에 따라 EMM의 메인 메뉴에서 보여지는 것이 다르며, 라이선스는 **설정 > 서비스 > 라이선스 정보**에서 확인합니다.

SAP ERP

SAP ERP 는 기업 내 모든 자원을 최적으로 통합 관리하여 업무의 효율을 극대화한 시스템으로 EMM 은 SAP ERP 와 연계를 통해 기업내 사용자 , 조직 , 그룹 단말에 대한 관리 및 제어로 단말 기기 , 애플리케이션 , 데이터의 통합적인 보안 관리가 가능합니다 .

SAP ERP 서비스와 연동하려면 SAP ERP 서버에 접속하기 위한 연결 정보를 등록하고 SAP 에서 제공하는 자바 커넥션 JCO 설정이 필요합니다 .



SAP ERP 서버 관리하기

EMM 은 SAP ERP 서버와 다음과 같은 설정을 통해 연계할 수 있으며 , 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 .

SAP ERP 서버와 연결하려면 다음의 절차를 따르세요 .

1. **설정 > 연동 시스템 > SAP ERP**로 이동하세요.

2. SAP ERP 연결을 추가하려면 ＋을 클릭하세요.

3. “SAP ERP 추가” 창에 연결 정보를 입력하세요. 각 항목에 대한 설명은 다음과 같습니다. 입력 항목 앞에 표시(*)는 필수 입력 값이며, 나머지는 선택사항입니다.
   - **Pool 이름**: SAP ERP 관리를 위한 Pool 이름입니다.
   - **Pool 크기**: 데이터 Pool의 최대 크기입니다.
   - **서버**: SAP ERP 서버의 주소입니다.
   - **클라이언트**: SAP ERP 클라이언트 정보입니다.
   - **사용자 ID**: SAP ERP CPIC 사용자 ID입니다.
   - **비밀번호**: SAP ERP CPIC 사용자 비밀번호입니다.
   - **언어**: 사용하는 언어를 입력합니다.
   - **시스템 번호**: SAP ERP 시스템 번호입니다.
   - **저장소**: Repository ID입니다.
   - **R3 명칭**: SAP ERP 버전입니다.
   - **그룹**: 그룹 정보를 입력합니다.
   - **상세 설명**: SAP ERP 연결 정보에 대한 상세 설명입니다.
4. **저장**을 클릭하세요.

> **Note:**
> - 이미 등록된 SAP ERP 서버의 정보를 복사하여 추가로 등록하는 경우, 동일한 Pool 이름으로는 등록이 불가능합니다.
> - 등록된 SAP ERP 서버 정보를 삭제하는 경우, SAP ERP 서비스가현재 사용 중이면 “사용 중인 서비스가 있습니다.”라는메시지와함께 삭제되지 않습니다.

SAP ERP 서버 연결 재설정하기

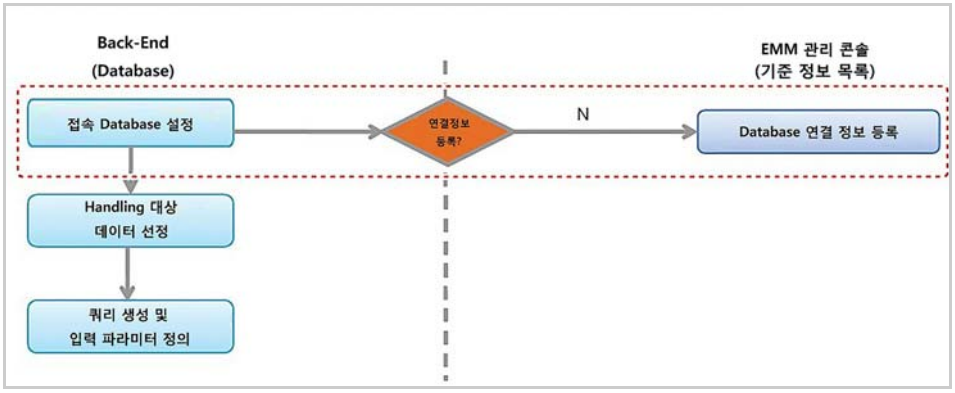
기존에 사용중인 SAP ERP 서버와의 연결을 초기화하려면 다음의 절차를 따르세요 .

1. **설정 > 연동 시스템 > SAP ERP**로 이동하세요.
2. 초기화하려는 SAP ERP 항목을 선택한 후, **재설정**을 클릭하세요.
3. “Pool 재설정” 창에서 **예**를 클릭하세요.

데이터베이스

데이터베이스는 기업 내 모든 자원과 조직을 운영하기 위해 필요한 데이터를 수집 및 저장하는 통합 데이터 시스템으로 EMM 은 데이터베이스와 연계를 통해 기업내 데이터베이스에 등록된 사용자의 단말에 대한 관리 및 제어가 가능합니다 .

데이터베이스와 연동하려면 데이터베이스 서버에 접속하기 위한 연결 정보를 등록하고 DB Pool 에 대한 설정이 필요합니다 .

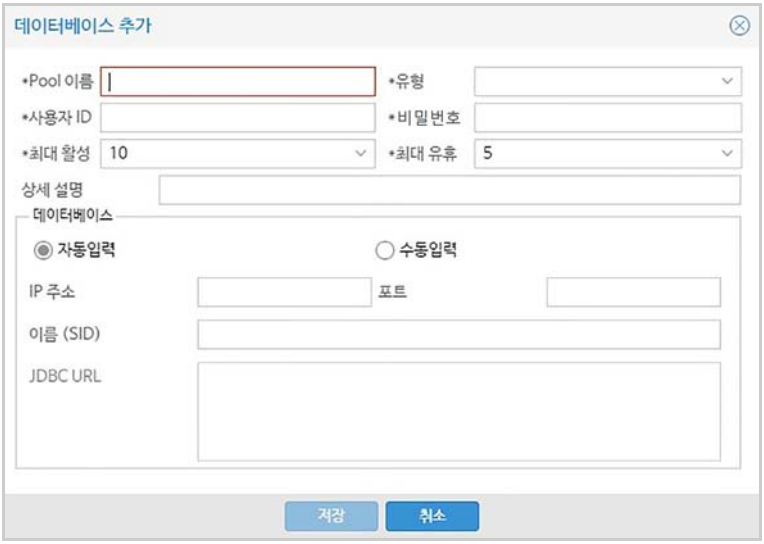


데이터베이스 서버 관리하기

EMM 은 데이터베이스 서버와 다음과 같은 설정을 통해 연계가 가능할 수 있으며 , 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 .

데이터베이스 서버와 연결하려면 다음의 절차를 따르세요 .

1. **설정 > 연동 시스템 > 데이터베이스**로 이동하세요.
2. 데이터베이스 연결을 추가하려면 ＋을 클릭하세요.



3. "데이터베이스 추가" 창에 연결 정보를 입력하세요. 각 항목에 대한 설명은 다음과 같습니다.
   입력 항목 앞에 표시(*)는 필수 입력 값이며, 나머지는 선택사항입니다.

항목	설 명
Pool 이름	데이터베이스 관리를 위한 Pool 이름입니다.
유형	등록하려는 데이터베이스의 유형(ORACLE, MSSQL, MYSQL)을 선택합니다.
사용자 ID	데이터베이스의 사용자 ID입니다.
비밀번호	데이터베이스의 사용자 비밀번호입니다.
최대 활성	활성 가능한 최대 커넥션 수입니다.(10~50)
최대 유휴	유휴 상태가 가능한 최대 커넥션 수입니다.(0~30)
데이터베이스	데이터베이스 연결 정보는 **자동입력** 또는 **수동입력**으로 입력할 수 있습니다. • 자동입력: IP 주소와 포트를 입력하면 JDBC URL이 자동 기록됩니다. • 수동입력: JDBC URL를 직접 입력합니다. - IP 주소: 데이터베이스 IP 주소입니다. - 포트: 데이터베이스의 포트 번호입니다. - 이름(SID): 데이터베이스 이름 또는 SID입니다. - JDBC URL: 데이터베이스 식별을 위한 JDBC URL입니다.

4. **저장**을 클릭하세요.

Note:
- 이미 등록된 데이터베이스 서버의 정보를 복사하여 추가로 등록하는 경우, 동일한 Pool 이름으로는 등록이 불가능합니다.
- 등록된 데이터베이스 서버 정보를 삭제하는 경우, 데이터베이스 서비스가현재 사용 중이면 "사용 중인 서비스가 있습니다."라는 메시지와함께 삭제되지 않습니다.

데이터베이스 서버 연결 상태 확인하기

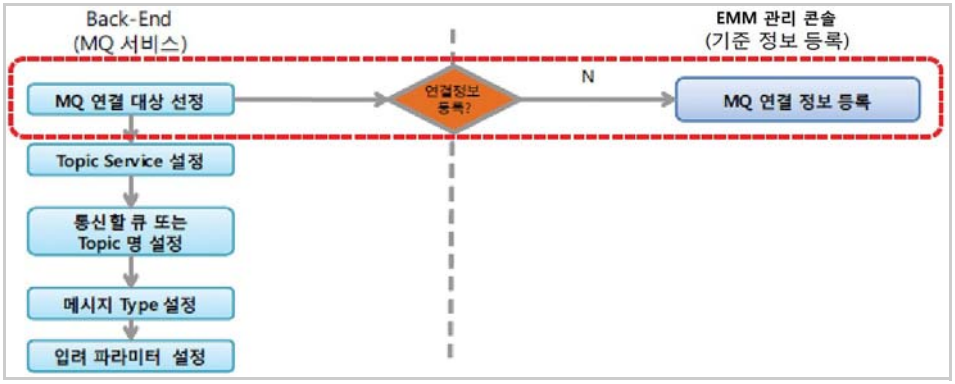
데이터베이스의 연결 상태를 확인하려면 다음의 절차를 따르세요 .

1. **설정 > 연동시스템 > 데이터베이스**로 이동하세요.
2. 연결 상태를 확인하려는 데이터베이스를 선택한 후, **데이터베이스 상태 확인**을 클릭하세요.
   - "데이터베이스 상태 확인" 창에 "데이터베이스 상태 확인이 완료 되었습니다. 연결 상태값을 확인하세요." 메시지가 표시됩니다.
   - 연결 상태는 연결 상태 필드에서 Connected, Disconnected로 확인합니다.

MQ

메시지 지향 미들 웨어 (Message Oriented Middleware: MOM) 는 비 동기 메시지를 사용하는 응용 프로그램 사이에서 데이터의 송수신을 의미합니다 . 이러한 MOM 을 구현한 시스템을 MQ(Message Queue) 라고 합니다 . MQ 는 메시지 처리를 위해 대기 중인 온라인 메시지 행렬을 통해 데이터 공정 작업을 연기 할 수 있는 유연성을 제공합니다 .

EMM 은 MQ 서비스와 연계를 통해 기업내 사용자의 단말에 데이터 전송 및 제어가 가능합니다 . MQ 서비스와 연동하려면 MQ 연결 대상에 대한 정보 설정이 필요합니다 .



MQ 서비스 관리하기

EMM 은 MQ 서비스와 다음과 같은 설정을 통해 연계할 수 있으며 , 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 . MQ 서비스와 연결하려면 다음의 절차를 따르세요 .

1. **설정 > 연동 시스템 > MQ**로 이동하세요.
2. MQ 연결을 추가하려면 ＋을 클릭하세요.

3. “MQ 추가” 창에 연결 정보를 입력하세요. 각 항목에 대한 설명은 다음과 같습니다. 입력 항목 앞에 표시(*)는 필수 입력 값이며, 나머지는 선택사항입니다.
   - **MQ ID**: MQ의 연결 정보 관리를 위한 ID입니다.
   - **시간 제한(초)**: 연결 제한 시간으로 30~600초까지 선택 가능합니다.
   - **MQ 이름**: MQ의 연결 정보 이름입니다.(예: ActiveMQ, RabbitMQ, OpenMQ)
   - **JNDI ICF**: 서버에 Lookup될 MQ 클래스명입니다.(MQ에 따라 다를 수 있음)

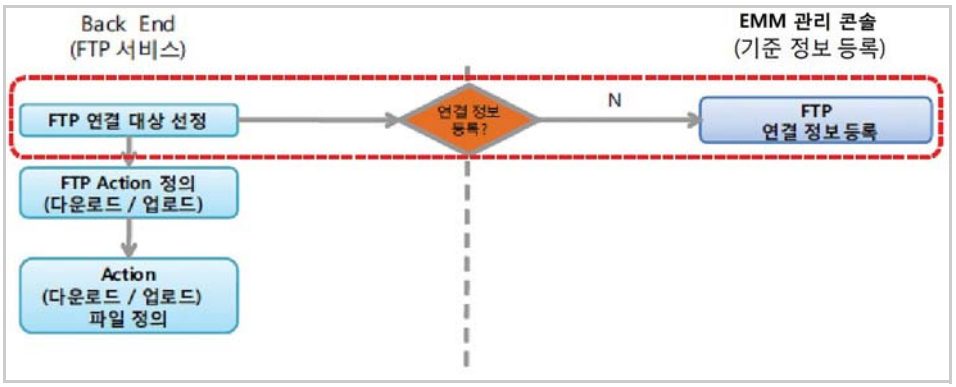
- **Provider URL**: MQ의 Provider URL입니다.
- **사용자 ID**: MQ의 사용자 ID입니다.
- **비밀번호**: MQ의 사용자 비밀번호입니다.
- **상세 설명**: 연결 정보에 대한 상세 설명입니다.

4. **저장**을 클릭하세요.

> **Note:**
> - 이미 등록된 MQ의 정보를 복사하여 추가로 등록하는 경우, 동일한 MQ ID로는 등록이 불가능합니다.
> - 등록된 MQ 정보를 삭제하는 경우, MQ 서비스가 현재 사용 중이면 "사용 중인 서비스가 있습니다."라는 메시지와 함께 삭제되지 않습니다.

FTP

EMM 은 FTP 서비스와 연계가 가능합니다 . FTP 서비스와 연동하려면 FTP 서버에 대한 정보 설정이 필요합니다 .

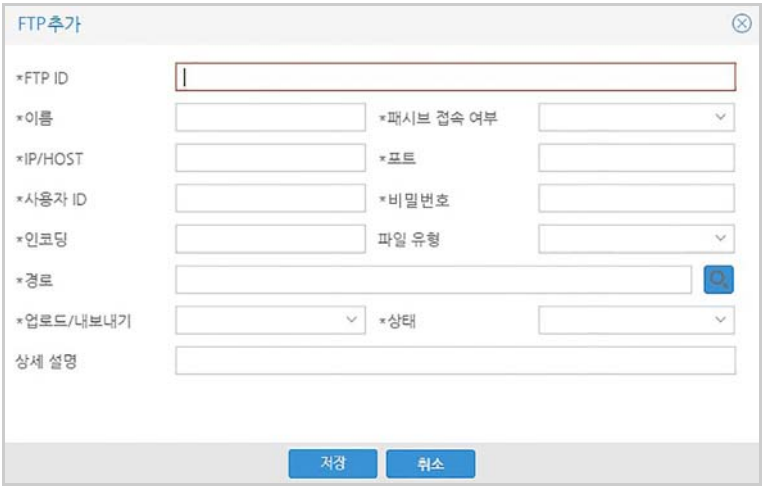


FTP 서버 관리하기

EMM 은 FTP 서버와 다음과 같은 설정을 통해 연계할 수 있으며 , 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 . FTP 서버와 연결하려면 다음의 절차를 따르세요 .

1. **설정 > 연동 시스템 > FTP**로 이동하세요.

2. FTP 연결을 추가하려면 ＋을 클릭하세요.



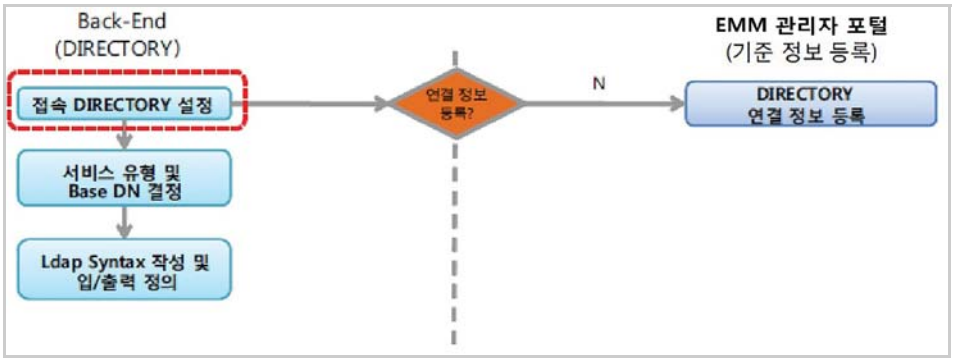
3. “FTP 추가” 창에 연결 정보를 입력하세요. 각 항목에 대한 설명은 다음과 같습니다. 입력 항목 앞에 표시(*)는 필수 입력 값이며, 나머지는 선택사항입니다.
   - **FTP ID**: FTP 연결 정보 관리를 위한 ID입니다.
   - **이름**: 연결 정보 이름입니다.
   - **패시브 접속 여부**: FTP 접속시 패시브모드로 접속 여부를 선택합니다.(ON, OFF)
   - **IP/HOST**: FTP 서버 주소입니다.
   - **포트**: FTP 포트 번호입니다.
   - **사용자 ID**: FTP 서버 사용자 ID입니다.
   - **비밀번호**: FTP 서버 사용자 비밀번호입니다.
   - **인코딩**: FTP 접속시 사용할 인코딩 방식입니다.
   - **파일 유형**: 파일 업로드,다운로드시 파일 유형을 선택합니다.(BINARY, ASCII)
   - **경로**: FTP 서버에 업로드, 다운로드할 파일의 절대 경로 위치를 선택합니다.
   - **업로드/내보내기**: 업로드 또는 다운로드 여부를 선택합니다.(DOWNLOAD, UPLOAD)
   - **상태**: FTP 서버 상태를 선택합니다.(비활성, 활성)
   - **상세 설명**: FTP 연결 정보에 대한 상세 설명입니다.
4. **저장**을 클릭하세요.

Note:
- 이미 등록된 FTP 서버의 정보를 복사하여 추가로 등록하는 경우, 동일한 FTP ID로는 등록이 불가능합니다.
- 등록된 FTP 서버의 정보를 삭제하는 경우, FTP 서버가 현재 사용 중이면 “사용 중인 서비스가 있습니다.”라는메시지와 함께 삭제되지 않습니다.

Directory

EMM 은 AD/LADP 연계를 통해 회사 내 사용자 및 조직을 등록하고 특정 주기로 기간계 시스템에 접근하여 갱신된 정보를 자동으로 동기화시키는 기능을 제공합니다 .

Directory 서버와 연동하려면 Directory 서버에 접속하기 위한 연결 정보 설정이 필요합니다 .



Directory 서버 관리하기

EMM 은 Directory 서버와 다음과 같은 설정을 통해 연계할 수 있으며 , 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 .

Directory 서버와 연동하려면 다음의 절차를 따르세요 .

1. **설정 > 연동 시스템 > Directory**로 이동하세요.
2. Directory 서버의 연결을 추가하려면 ➕을 클릭하세요.
3. “Directory 추가” 창에서 **기본 설정** 탭 정보를 입력하고, 선택한 인증 방식에 따라 **인증 상세** 탭을 입력하세요.
   - **기본 설정**과 **인증 상세** 탭 항목에 대한 자세한 내용은 94페이지 6장의 “동기화 서비스 등록하기"를 참고하세요.

4. **저장**을 클릭하세요.

Directory 서버의 연결 상태 확인하기

Directory 의 연결 상태를 확인하려면 다음의 절차를 따르세요 .

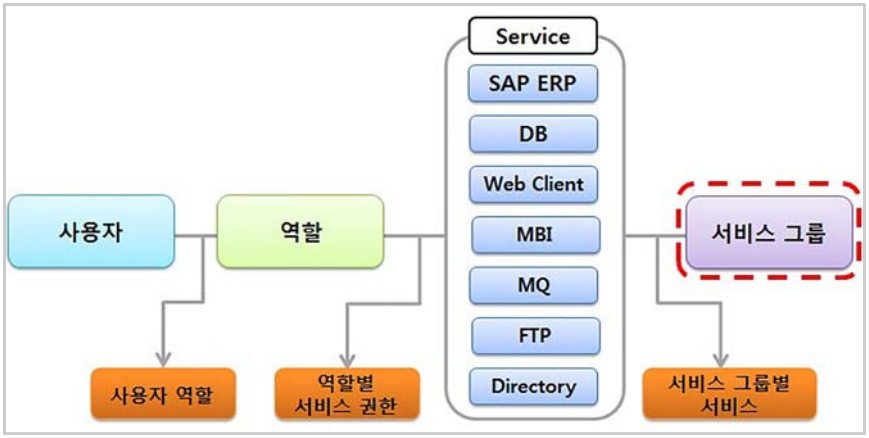
1. **설정 > 연동 시스템 > Directory**로 이동하세요.
2. 연결 상태를 확인하려는 항목을 선택한 후, **디렉터리 상태 확인**을 클릭하세요.
3. **연결 상태** 필드에서 Connected 또는 Disconnected를 확인하세요.

커넥터 설정하기

EMM은 연동 서비스에 등록된 서버들의 다양한 서비스를 제공하기 위해 커넥터를 설정합니다. 또한 커넥터를 설정하기 전에 서비스 그룹을 등록하고 역할을 부여하여 커넥터 서비스를 편리하게 이용할 수 있도록 도와줍니다 . 커넥터 서비스에 대한 접근 제어는 접근이 가능한 권한을 할당하여 권한이 할당된 사용자만 서비스를 사용할 수 있도록 설정합니다 .

커넥터 사용을 위한 서비스 그룹 관리하기

서비스 그룹은 커넥터 서비스를 그룹핑하여 커넥터를 관리하기 위해 설정하며 , 서비스 그룹 생성 시 그룹에 역할을 부여하고 사용자는 부여받은 역할에 연결된 서비스 그룹의 서비스만 사용이 가능합니다 .

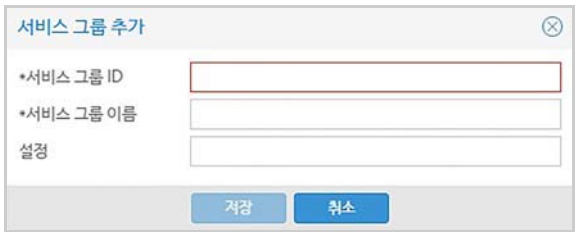


커넥터 서비스를 그룹핑하여 커넥터를 관리하기 위해 서비스 그룹을 설정할 수 있습니다 . 서비스 설정은 필요에 따라 추가 , 수정 및 삭제가 가능합니다 .

서비스 그룹을 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > 서비스 그룹**으로 이동하세요.

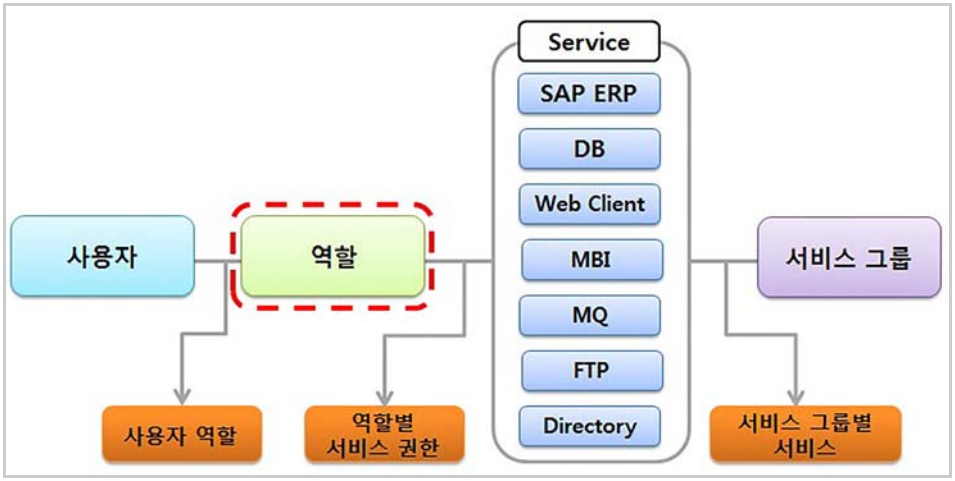
2. 새로운 서비스 그룹을 추가하려면 ＋을 클릭하세요.



3. "서비스 그룹 추가" 창에 **서비스 그룹 ID**, **서비스 그룹 이름**, **설정**을 입력하세요.
4. **저장**을 클릭하세요.

커넥터 사용을 위한 역할 관리하기

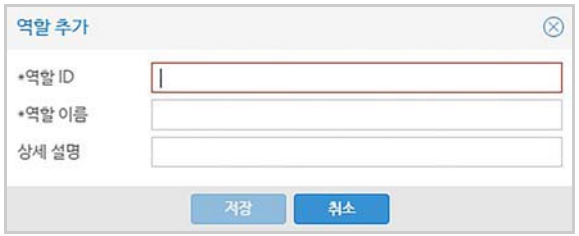
역할 설정은 커넥터를 사용하는 특정 사용자들을 그룹핑하여 권한을 제어하기 위해 설정합니다 . 즉 , 역할을 설정한 사용자만 지정한 커넥터의 접근이 가능하게 합니다 .



특정 사용자들을 그룹핑하여 권한을 제어하기 위해 역할을 설정합니다 . 역할 설정은 필요에 따라 추가 , 수정 및 삭제가 가능합니다 .

역할 설정을 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > 역할 관리**로 이동하세요.
2. 새로운 역할을 추가하려면 ＋을 클릭하세요.



3. "역할 추가" 창에 **역할 ID**, **역할 이름**, **상세 설명**을 입력하세요.

4. **저장**을 클릭하세요.

> **Note:** 기본 역할로 지정된 역할은 삭제가 불가능합니다. 만약, 해당 역할을 삭제하는 경우, "기본 역할을 삭제할 수 없습니다." 라는 메시지와 함께 삭제되지 않습니다.

사용자에게 역할 부여하기

역할을 등록한 후 , 사용자에게 역할 권한을 부여하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 사용자 & 조직**으로 이동하세요.
2. 역할을 설정하려는 **사용자**를 선택한 후, "사용자 수정" 창의 서비스 역할 필드 좌측 **추가** ⊕를 클릭하세요.
3. "서비스 역할 선택" 창에서 권한을 부여하려는 역할을 선택한 후, **확인**을 클릭하세요.
   - 역할은 다중 선택이 가능합니다.

커넥터 서비스 운영하기

커넥터 서비스 관리는 **설정 > 커넥터** 하위 메뉴의 서비스 그룹 , SAP ERP, 데이터베이스 , 웹 클라이언트 , MBI, MQ, FTP, Directory 서비스에서 각 커넥터 서비스의 정상적인 운영을 위해 설정합니다 . 또한 **커넥터 서비스**의 **시뮬레이션** 탭은 연동 시스템과 연결 없이 서비스 동작 여부를 테스트하기 위해 사용되며 , 시뮬레이션 시 단말로 보내려는 메시지를 전송할 수 있습니다 .

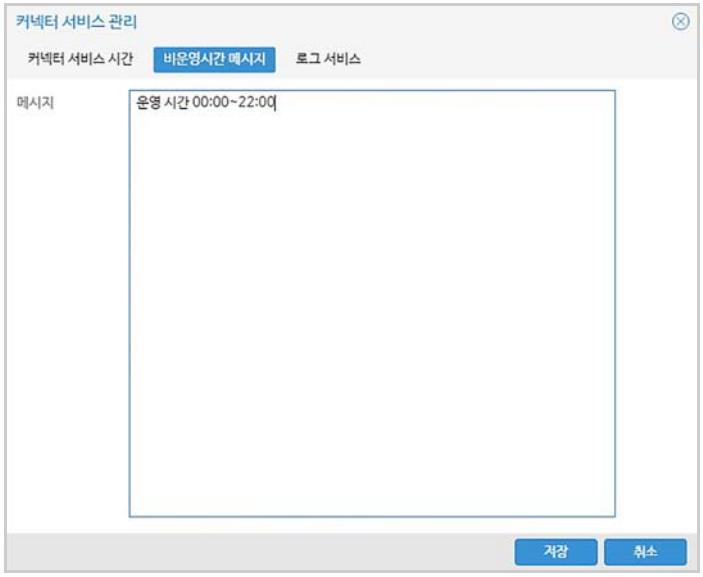
커넥터 서비스의 운영을 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > 서비스 그룹**으로 이동하세요.
   - SAP ERP, 데이터베이스, 웹 클라이언트, MBI, MQ, FTP, Directory 메뉴도 동일합니다.
2. 목록에서 **서비스 그룹 ID** 또는 **서비스 ID**를 선택한 후, **커넥터 서비스**를 클릭하세요.
3. "커넥터 서비스" 창의 **커넥터 서비스 시간** 탭을 클릭한 후, **기본**이나 **개별**을 선택하여 서비스 시간을 설정하고 **확인**을 클릭하세요.

- **커넥터 서비스 시간 탭**: 커넥터 서비스의 운영 시간을 설정합니다.

항목	설명
기본	**일~토(00:00~24:00)**로 설정된 시간으로 서비스가 운영됩니다. • 서비스 운영 시간은 서비스 그룹의 커넥터 서비스 시간에 설정된 운영 시간이 우선 적용되며, 서비스 그룹의 커넥터 서비스 시간이 설정되어 있지 않을 경우 전체 서비스 운영 시간이 적용됩니다. 전체 서비스 운영 시간은 **설정 > 서비스 > 환경 설정** 메뉴를 클릭한후, **관리**를 클릭하여 설정합니다.
개별	개별에서 선택한 날짜와 시간으로 서비스가 운영됩니다. • 요일과 시간을 선택한 후, ↓을 클릭하세요. 요일과 시간은 다중 설정이 가능합니다. • 설정한 요일과 시간을 삭제하려면 하단의 요일과 시간을 선택한 후, ↑을 클릭합니다. • **시간표보기**: 시간표 보기를 클릭하면 개별에서 설정한 요일과 시간이 표 형식으로 표시됩니다.

- **비운영 시간 메시지** 탭: 커넥터 서비스가 운영되지 않는 시간을 단말에 안내할 경우, 하단에 메시지를 입력합니다.



- **로그 서비스** 탭: 커넥터 서비스에 대한 로그 기록 여부를 설정합니다.

항목	설명
기본	커넥터 서비스에 대한 로그가 기본설정대로 기록됩니다. • 로그 기록은 서비스 그룹의 로그 서비스 기본 설정이 우선 적용되며, 서비스 그룹의 로그 서비스가 설정되어 있지 않을 경우, 시스템의 기본 설정이 적용됩니다. 시스템 기본 설정은 **설정 > 서비스 > 환경 설정**의 **관리**를 클릭하여 **로그 서비스** 탭에서 설정합니다.
개별	트랜잭션 로그 기록 사용 여부를 선택합니다. • **커넥터 서비스 트랜잭션 로그 기록 사용**을 클릭한 경우, **서비스 현황 > 로그 > 커넥터 로그**에서 커넥터 서비스에 대한 트랙잭션 추적이 가능합니다.

SAP ERP 커넥터

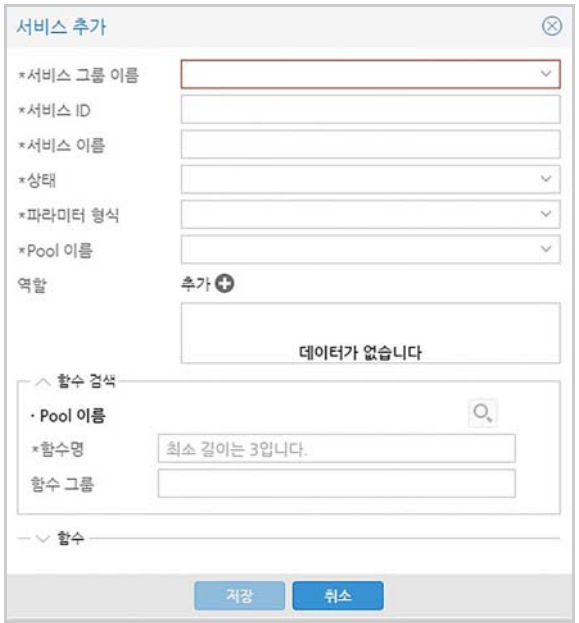
SAP ERP 커넥터는 시스템의 비즈니스 로직에 대한 서비스를 제공합니다 . 다음은 SAP ERP 커넥터를 설정 및 관리하는 방법에 대해 설명합니다 .

SAP ERP 서비스 관리하기

설정 > 연동시스템 > SAP ERP 에 등록한 SAP ERP 서버의 설정을 이용하여 커넥터를 설정합니다 . 커넥터 설정은 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 .

SAP ERP 서비스를 추가하려면 다음의 절차를 따르세요 .

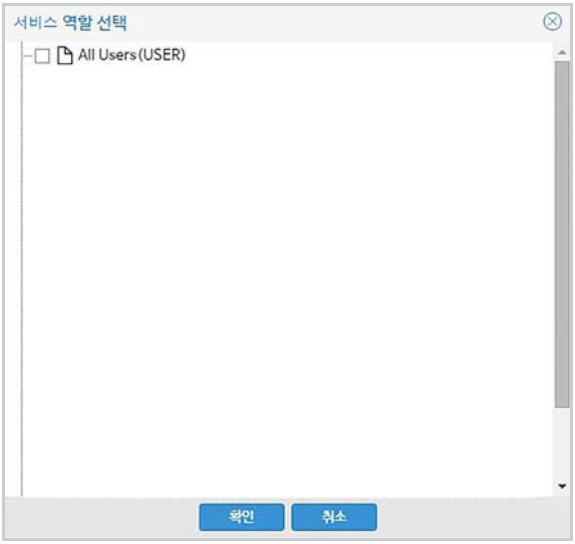
1. **설정 > 커넥터 > SAP ERP**로이동하세요.
2. SAP ERP 서비스를 추가하려면 ＋을 클릭하세요.



3. “서비스 추가” 창에 서비스 정보를 입력하세요.
   - **서비스 그룹 이름**: **설정 > 커넥터 > 서비스 그룹**에 등록된 서비스 그룹 중 SAP ERP 서비스를 추가할 서비스 그룹을 선택합니다.
   - **서비스 ID**: SAP ERP 서비스 관리를 위한 ID입니다.
   - **서비스 이름**: SAP ERP 서비스 이름입니다.

- **상태**: 활성, 비활성, 시뮬레이션 중 서비스 상태를 선택합니다.
- **파라미터 형식**: XML, NVP 중 단말의 파라미터 형식을 선택합니다.
- **Pool 이름**: SAP ERP 관리를 위해 설정한 Pool 이름을 선택합니다.

4. 서비스 관리를 위해 역할을 설정하려면 ⊕을 클릭한 후, "서비스 역할 선택" 창에서 역할을 선택하고 **확인**을 클릭하세요. 역할은 다중 선택이 가능합니다.



5. **함수 검색** 영역에서 **함수명** 또는 **함수 그룹**을 입력한 후, **Enter** 키를 누르거나 🔍을 클릭하세요.
6. **함수** 영역에서 사용하려는 함수를 선택한 후, **저장**을 클릭하세요.

> **Note:** 이미 등록된 SAP ERP 서버의 커넥터 정보를 복사하여 추가로 등록하는 경우, 동일한 서비스 ID로는 등록이 불가능합니다.

SAP ERP 서비스 테스트하기

SAP ERP 의 서비스가 정상적으로 연결 및 동작하는지 서비스 테스트를 통해 확인할 수 있습니다 . 서비스 테스트를 통해 연결 동작을 확인하려면 다음의 절차를 따르세요 .

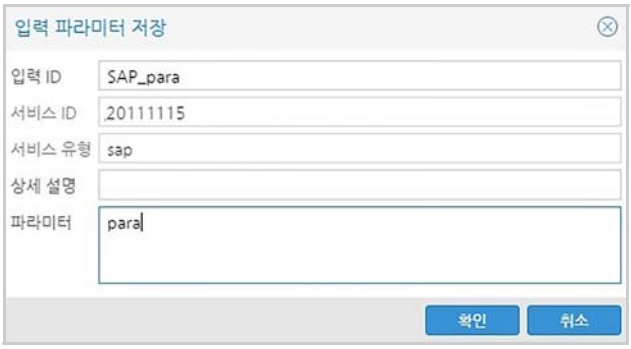
> **Note:** SAP ERP, 데이터베이스, 웹 클라이언트, MBI, MQ, FTP, Directory 메뉴의 서비스 테스트 방법은 모두 동일합니다.

1. **설정 > 커넥터 > SAP ERP**로 이동하세요.
2. 테스트하려는 항목을 선택한 후, ▶을 클릭하세요.

3. "테스트" 창에 테스트 정보를 입력하세요.

- **URL**: 서비스 호출 시 테스트를 위해 사용되는 URL을 입력합니다. 우측의 드롭박스에서 테스트 후, 출력값으로 표시되는 형식을 XML, JSON 중 선택합니다.
- **파라미터 불러오기**: 파라미터 입력을 위해 **불러오기**를 클릭합니다. 클릭 시 "입력값 리스트" 창이 나타납니다. "입력값 리스트" 창의 저장 ID에서 입력 파라미터로 사용하려는 파라미터 값을 클릭하여 파라미터로 보내고 **확인**을 클릭합니다.

- **파라미터 저장**: 입력 파라미터로 사용할 파라미터를 설정할 수 있습니다. **저장** 클릭 시 나타나는 "입력 파라미터 값 저장" 창에 파라미터값을 입력하고 저장하려면 **확인**을 클릭합니다.



  - **입력 ID**: 입력 파라미터 ID입니다.
  - **서비스 ID**: 입력 파라미터의 서비스 ID로 자동 입력됩니다.
  - **서비스 유형**: 입력 파라미터의 서비스 유형으로 자동 입력됩니다.(예: sap, db)
  - **상세 설명**: 입력 파라미터에 대한 상세설명입니다.
  - **파라미터**: 불러오기에서 설정한 입력 파라미터가 자동 입력됩니다.

4. 서비스 동작이 정상인지 테스트하려면 **보내기**를 클릭하세요. 테스트 결과는 결과값 영역에서 형식화 결과와 결과 메시지를 확인합니다. 트리형태로 결과값이 마지막 노드까지 확장하여 표시됩니다.
   - **형식화 결과**: 결과값이 트리 형태로 표시됩니다.
   - **결과 메시지**: 단말로 보낼 XML, JSON 타입의 메시지 형식이 표시됩니다.
5. **닫기**를 클릭하세요.

SAP ERP 서비스 운영하기

설정 > 커넥터 > SAP ERP 의 **커넥터 서비스**에서는 커넥터 서비스 운영 시간을 설정하고 서비스 비운영시간을 안내하는 메시지를 단말에 보내거나 서비스에 대한 로그 기록을 설정할 수 있습니다 .

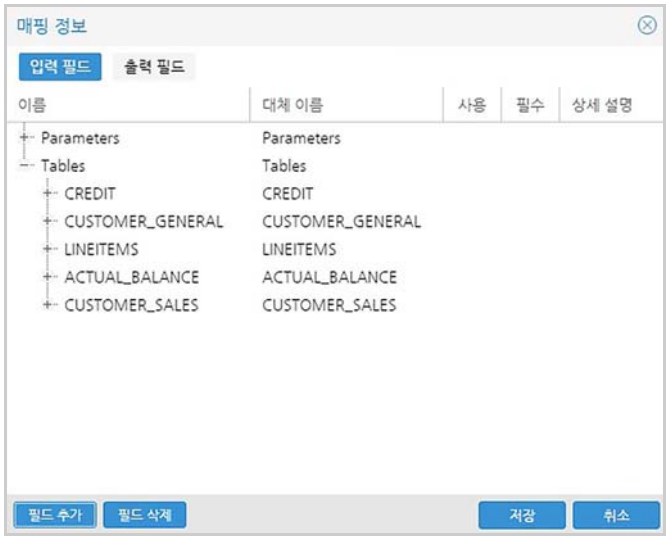
커넥터 서비스에 대한 자세한 내용은 266 페이지의 " 커넥터 서비스 운영하기 " 를 참고하세요 .

SAP ERP 매핑 정보 설정하기

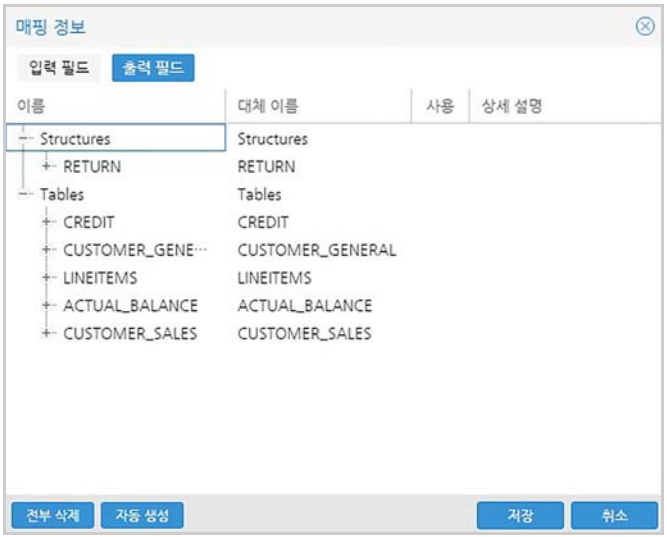
서비스 매핑 정보에서는 서비스의 입력 및 출력 파라미터에 대한 매핑 정보를 자동 생성하거나 임의로 추가 및 수정 , 삭제할 수 있습니다 .

서비스를 위한 매핑정보의 입력 또는 출력 필드를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > SAP ERP**로 이동하세요.
2. 목록에서 서비스 매핑 정보를 확인하려는 항목을 선택한 후, **매핑 정보**를 클릭 시 “매핑 정보” 창이 나타납니다.
3. “매핑 정보” 창의 **입력 필드** 탭을 클릭하세요. 입력 필드는 서비스 호출 시 입력 파라미터로 사용되는 필드의 정보입니다.
   - 입력 필드의 대체 이름과 상세 설명은 클릭하여 변경할 수 있습니다.
   - 입력 필드를 추가 하려면 **필드 추가**를, 추가한 필드 삭제하려면 **필드 삭제**를 클릭합니다.



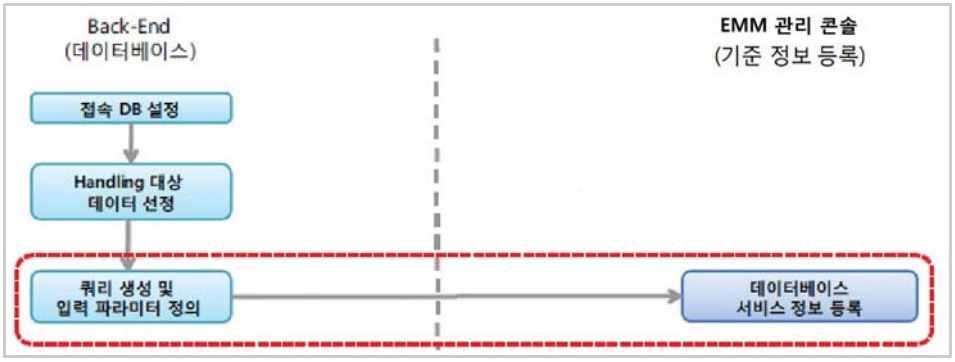
4. “매핑 정보” 창의 **출력 필드** 탭을 클릭하세요. 출력 필드는 서비스 응답시 출력 파라미터로 사용되는 필드의 정보입니다.
   - 출력 필드의 대체 이름과 상세 설명은 클릭하여 변경할 수 있습니다.



5. 출력 필드로 사용하려는 필드의 체크 박스를 선택한 후, **저장**을 클릭하세요.
   - 등록된 출력 필드를 모두 삭제하려면 **전부 삭제**를 클릭합니다.
   - 서비스를 수정하여 BAPI가 변경되었거나 연동 시스템에서 해당 BAPI의 필드가 변경되었을경우, 기존 매핑 정보를 초기화하려면 **자동 생성**을 클릭합니다. 기존의 매핑 정보가 초기화되어 다시 매핑이 가능합니다.

데이터베이스 커넥터

데이터베이스 커넥터는 데이터베이스 서버에 연결하여 데이터를 확인하고 검색하는 등의 서비스를 제공합니다. 다음은 데이터베이스 커넥터를 설정 및 관리하는 방법에 대해 설명합니다 .

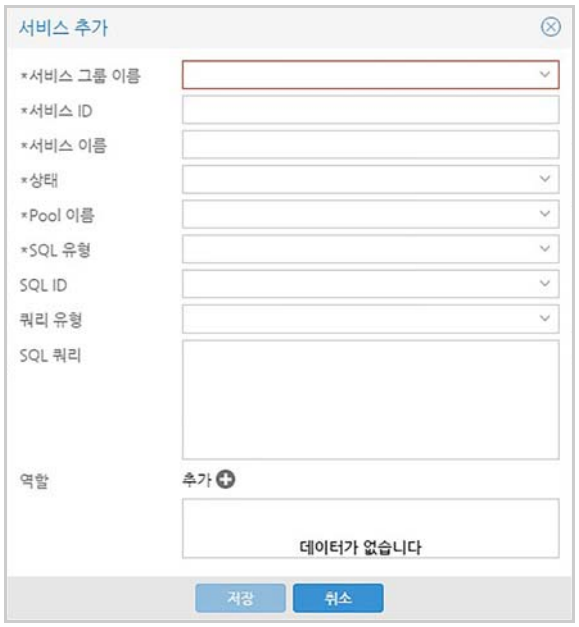


데이터베이스 서비스 관리하기

설정 > 연동시스템 > 데이터베이스에서 등록한 데이터베이스 서버의 설정을 이용하여 커넥터를 설정합니다 . 커넥터 설정은 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 .

데이터베이스 서비스를 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > 데이터베이스**로 이동하세요.
2. 데이터베이스 서비스를 추가하려면 ＋을 클릭하세요.



3. "서비스 추가" 창에 서비스 정보를 입력하세요.
   - **서비스 그룹 이름**: **설정 > 커넥터 > 서비스 그룹**에 등록된 서비스 그룹 중 데이터베이스 서비스를 추가할 서비스 그룹을 선택합니다.
   - **서비스 ID**: 데이터 베이스 서비스 관리를 위한 ID를 입력합니다.
   - **서비스 이름**: 데이터 베이스 서비스 이름을 입력합니다.
   - **상태**: 활성, 비활성, 시뮬레이션 중 서비스 상태를 선택합니다.
   - **Pool 이름**: 데이터 베이스 관리를 위해 설정한 Pool 이름을 선택합니다.
   - **SQL 유형**: MYBATIS 또는 QUERY 중 SQL 유형을 선택합니다.
   - **MYBATIS**: MYBATIS 선택 시 EMM의 MYBATIS SQL Map 파일에 등록되어있는 QUERY를 사용할 수 있습니다.
   - **QUERY**: QUERY 선택 시 SQL 쿼리 텍스트 박스에 직접 쿼리를 입력할 수 있습니다.
   - **SQL ID**: SQL 유형을 MYBATIS으로 선택한 경우, SQL ID를 선택합니다.
   - **쿼리 유형**: SQL 유형을 MYBATIS으로 선택한 경우, 쿼리 유형을 선택합니다.
   - **SQL 쿼리**: SQL 유형을 QUERY로 선택한 경우, 사용하려는 SQL 쿼리를 직접 입력합니다.
4. 서비스 관리를 위해 역할을 설정하려면 ⊕을 클릭한 후, "서비스 역할 선택" 창에서 역할을 선택하고 **확인**을 클릭하세요. 역할은 다중 선택이 가능합니다.
5. **저장**을 클릭하세요.

> **Note:** 이미 등록된 데이터베이스 서버의 커넥터 정보를 복사하여 추가로 등록하는 경우, 동일한 서비스 ID로는 등록이 불가능합니다.

데이터베이스 서비스 테스트하기

데이터베이스 서비스가 정상적으로 연결 및 동작하는지 서비스 테스트를 통해 확인할 수 있습니다. **설정 > 커넥터 > 데이터베이스** 내의 ▶을 클릭하여 각 서비스를 테스트할 수 있으며, 자세한 내용은 270 페이지의 " SAP ERP 서비스 테스트하기 " 를 참고하세요.

데이터베이스 서비스 운영하기

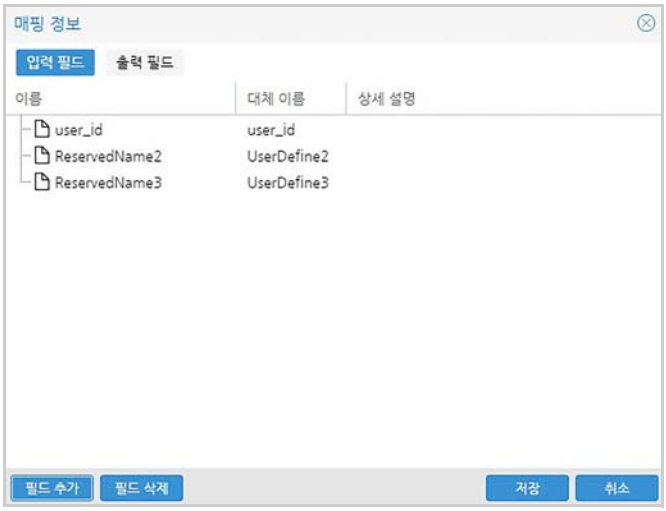
설정 > 커넥터 > 데이터베이스의 커넥터 서비스에서는 커넥터 서비스 운영 시간을 설정하고 서비스 비운영시간을 안내하는 메시지를 단말에 보내거나 서비스에 대한 로그 기록을 설정할 수 있습니다. 커넥터 서비스에 대한 자세한 내용은 266 페이지의 " 커넥터 서비스 운영하기 " 를 참고하세요.

데이터베이스 매핑 정보 설정하기

서비스 매핑 정보에서는 서비스의 입력 및 출력 파라미터에 대한 매핑 정보를 자동 생성하거나 임의로 추가 및 수정, 삭제할 수 있습니다.

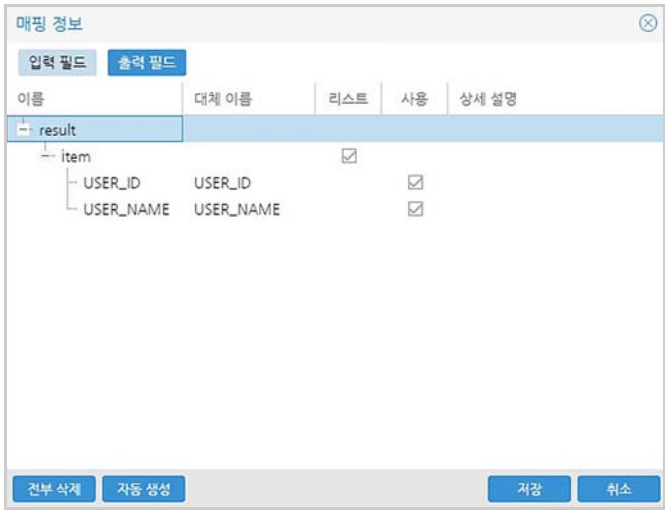
서비스를 위한 매핑정보의 입력 또는 출력 필드를 설정하려면 다음의 절차를 따르세요.

1. **설정 > 커넥터 > 데이터베이스**로 이동하세요.
2. **SQL 유형**을 **QUERY**로 선택시 **매핑 정보**를 클릭하세요.
3. "매핑 정보" 창에 **입력 필드**와 **출력 필드**가 표시됩니다.
4. **입력 필드** 탭을 클릭하세요.
   - 입력 필드는 서비스 호출시 입력 파라미터로 사용되는 필드의 정보입니다.
   - 입력 필드의 대체 이름과 상세 설명은 클릭하여 변경할 수 있습니다.
   - 입력 필드를 추가 하려면 **필드 추가**를, 추가한 필드 삭제하려면 **필드 삭제**를 클릭합니다.



5. "매핑 정보" 창의 **출력 필드** 탭을 클릭하세요.

- 출력 필드는 서비스 응답시 출력 파라미터로 사용되는 필드의 정보입니다.
- 출력 필드의 대체 이름과 상세 설명은 클릭하여 변경할 수 있습니다.

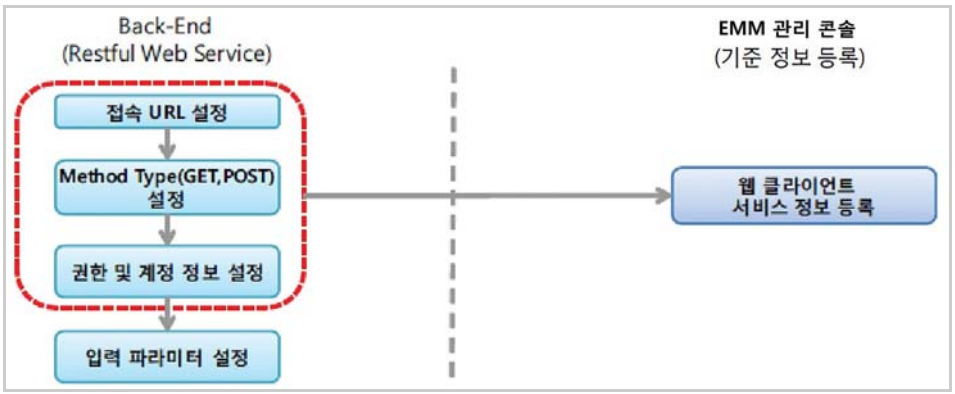


6. 출력 필드로 사용하려는 필드의 체크 박스를 선택한 후, **저장**을 클릭하세요.
   - 등록된 출력 필드를 모두 삭제하려면 **전부 삭제**를 클릭합니다.
   - **전부 삭제**를 클릭하여 출력 필드를 모두 삭제하면, 매핑없이 연동 시스템에 전달된 내용 그대로 단말에 전송됩니다.
   - 출력 필드가 구성되어 있지 않거나 SQL 쿼리가 변경된 경우, 출력 필드를 재 구성하려면 **자동 생성**을 클릭합니다.
   - 이전의 매핑 정보가 삭제되고 서비스를 직접 호출한 XML이나 JSON 형태의 결과를 분석하여 출력 필드를 재구성 합니다.

웹 클라이언트 커넥터

웹 클라이언트는 HTTP 로 서비스를 제공하는 Back-End 서버에 대한 서비스를 제공합니다 .

다음은 웹 클라이언트 커넥터를 설정 및 관리하는 방법에 대해 설명합니다 .

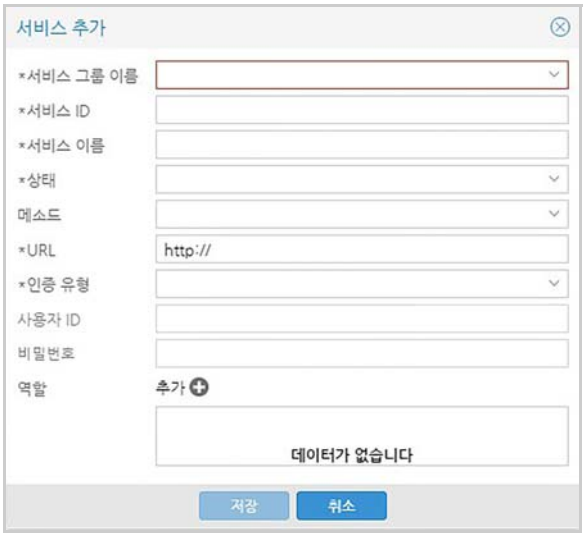


웹 클라이언트 서비스 관리하기

웹 클라이언트 서비스 사용을 위해 커넥터를 설정합니다 . 커넥터 설정은 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 .

웹 클라이언트의 서비스를 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > 웹 클라이언트**로 이동하세요.
2. 웹 클라이언트 서비스를 추가하려면 ＋을 클릭하세요.



3. “서비스 추가” 창에 서비스 정보를 입력하세요.
   - **서비스 그룹 이름**: **설정 > 커넥터 > 서비스 그룹**에 등록된 서비스 그룹 중 웹 클라이언트 서비스를 추가할 서비스 그룹을 선택합니다.
   - **서비스 ID**: 웹 클라이언트 서비스 관리를 위한 ID입니다.
   - **서비스 이름**: 웹 클라이언트 서비스 이름입니다.
   - **상태**: 활성, 비활성, 시뮬레이션 중 서비스 상태를 선택합니다.
   - **메소드**: GET, POST, POST_JSON, POST_XML, PUT, DELETE 중 REST 호출을 위한 HTTP 메소드를 선택합니다.
   - **URL**: 호출하려는 URL을 입력합니다.
   - **인증 유형**: BASIC, CLIENT_BASIC, NONE 중 인증 유형을 선택합니다.
   - **사용자 ID**: 인증 유형을 BASIC으로 선택한 경우, 인증을 위한 사용자 ID입니다.
   - **비밀번호**: 인증 유형을 BASIC으로 선택한 경우, 인증을 위한 사용자 비밀번호입니다.
4. 서비스 관리를 위해 역할을 설정하려면 ⊕을 클릭한 후, “서비스 역할 선택” 창에서 역할을 선택하고 **확인**을 클릭하세요. 역할은 다중 선택이 가능합니다.
5. **저장**을 클릭하세요.

> **Note:** 이미 등록된 웹 클라인트 서비스의 커넥터 정보를 복사하여 추가로 등록하는 경우, 동일한 서비스 ID로는 등록이 불가능합니다.

웹 클라이언트 서비스 테스트하기

웹 클라이언트 서비스가 정상적으로 연결 및 동작하는지 서비스 테스트를 통해 확인할 수 있습니다 . **설정 > 커넥터 > 웹 클라이언트** 내의 ▶을 클릭하여 각 서비스를 테스트할 수 있으며, 자세한 내용은 270페이지의 " SAP ERP 서비스 테스트하기 "를 참고하세요.

웹 클라이언트 서비스 운영하기

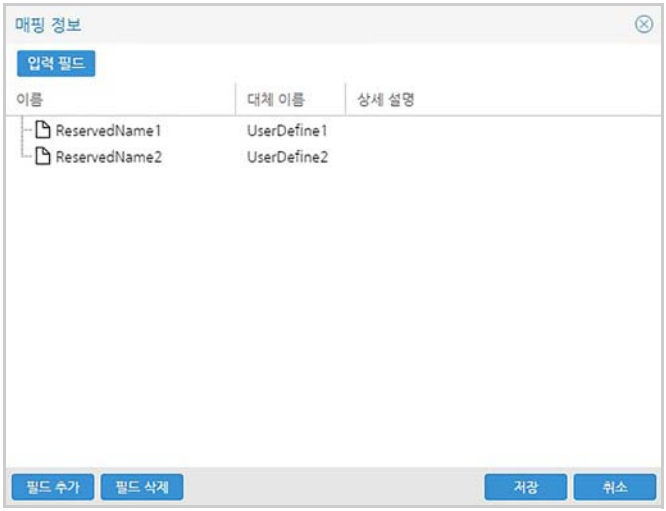
설정 > 커넥터 > 웹 클라이언트의 커넥터 서비스에서는 커넥터 서비스 운영 시간을 설정하고 서비스 비운영시간을 안내하는 메시지를 단말에 보내거나 서비스에 대한 로그 기록을 설정할 수 있습니다 . 커넥터 서비스에 대한 자세한 내용은 266 페이지의 " 커넥터 서비스 운영하기 " 를 참고하세요 .

웹 클라이언트 매핑 정보 설정하기

서비스 매핑 정보에서는 서비스의 입력 파라미터에 대한 매핑 정보를 추가 및 수정, 삭제할 수 있습니다 .

서비스를 위한 매핑정보의 입력 필드를 설정하려면 다음의 절차를 따르세요 .

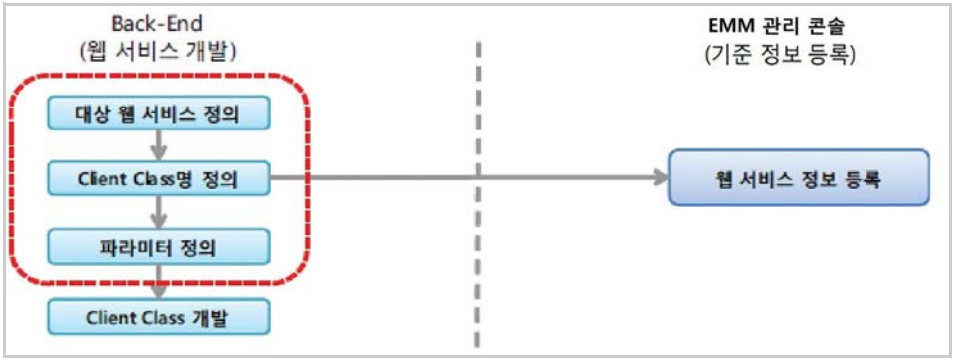
1. **설정 > 커넥터 > 웹 클라이언트**로 이동하세요.
2. 목록에서 서비스 매핑 정보를 확인하려는 항목을 선택한 후, **매핑 정보**를 클릭 시 “매핑 정보” 창이 나타납니다.
3. “매핑 정보” 창에 **입력 필드**가 표시됩니다.
4. **입력 필드** 탭을 클릭하세요.
   - 입력 필드는 서비스 호출시 입력 파라미터로 사용되는 필드의 정보입니다.
   - 입력 필드의 대체 이름과 상세 설명은 클릭하여 변경할 수 있습니다.
   - 입력 필드를 추가 하려면 **필드 추가**를, 추가한 필드 삭제하려면 **필드 삭제**를 클릭합니다.



5. **저장**을 클릭하세요.

MBI 커넥터

MBI(Mobile Business Integrator) 는 기존의 커넥터로 지원할 수 없는 프로토콜 또는 비즈니스 로직을 지원하는 인터페이스를 말합니다 . 다음은 JAVA 클래스 기반의 비즈니스 로직을 처리하는 웹 서비스 또는 커스텀 커넥터를 설정 및 관리하는 방법에 대해 설명합니다 .



MBI 서비스 관리하기

MBI 서비스 사용을 위해 커넥터를 설정합니다 . 커넥터 설정은 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 .

MBI 서비스를 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > MBI**로 이동하세요.
2. MBI 서비스를 추가하려면 ＋을 클릭하세요.

3. “서비스 추가” 창에 서비스 정보를 입력하세요.
   - **서비스 그룹 이름**: **설정 > 커넥터 > 서비스 그룹**에 등록된 서비스 그룹 중 MBI 서비스를 추가할 서비스 그룹을 선택합니다.
   - **서비스 ID**: 서비스 관리를 위한 ID입니다.

- **서비스 이름**: 서비스 이름입니다.
- **상태**: 활성, 비활성, 시뮬레이션 중 서비스 상태를 선택합니다.
- **클래스**: 서비스에서 사용하려는 커스텀 클래스의 패키지를 포함한 클래스 이름입니다.
- **시간 제한(초)**: 서비스 제한 시간으로 5~600초까지 선택 가능합니다.

4. 서비스 관리를 위해 역할을 설정하려면 ⊕을 클릭한 후, "서비스 역할 선택" 창에서 역할을 선택하고 **확인**을 클릭하세요. 역할은 다중 선택이 가능합니다.
5. **저장**을 클릭하세요.

> **Note:** 이미 등록된 MBI 서비스의 커넥터 정보를 복사하여 추가로 등록하는 경우, 동일한 서비스 ID로는 등록이 불가능합니다.

MBI 서비스 테스트하기

MBI 서비스가 정상적으로 연결 및 동작하는지 서비스 테스트를 통해 확인할 수 있습니다 . **설정 > 커넥터 > MBI** 내의 ▶을 클릭하여 각 서비스를 테스트할 수 있으며 , 자세한 내용은 270 페이지의 " SAP ERP 서비스 테스트하기 " 를 참고하세요 .

MBI 서비스 운영하기

설정 > 커넥터 > MBI 의 커넥터 서비스에서는 커넥터 서비스 운영 시간을 설정하고 서비스 비운영시간을 안내하는 메시지를 단말에 보내거나 서비스에 대한 로그 기록을 설정할 수 있습니다 . 커넥터 서비스에 대한 자세한 내용은 266 페이지의 " 커넥터 서비스 운영하기 " 를 참고하세요 .

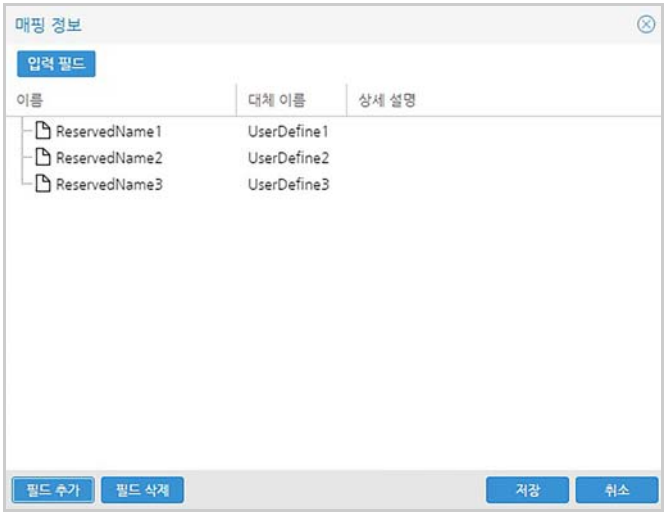
MBI 매핑 정보 설정하기

서비스 매핑 정보에서는 서비스의 입력 파라미터에 대한 매핑 정보를 추가 및 수정, 삭제할 수 있습니다 .

서비스를 위한 매핑정보의 입력 필드를 설정하려면 다음의 절차를 따르세요 .

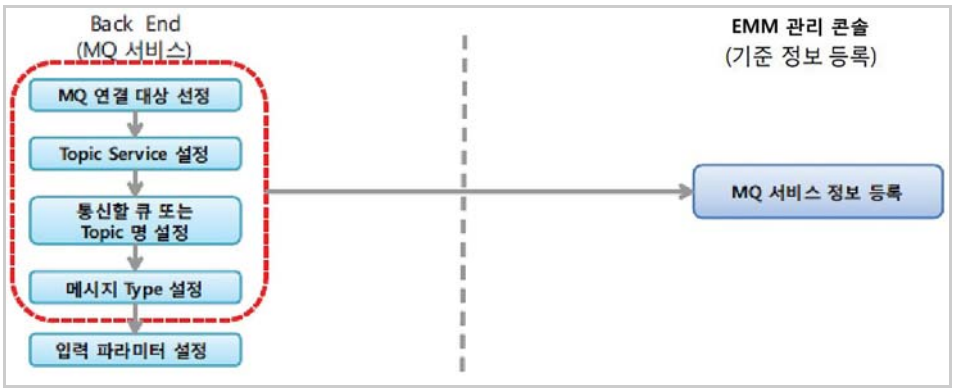
1. **설정 > 커넥터 > MBI**로 이동하세요.
2. 목록에서 서비스 매핑 정보를 확인하려는 항목을 선택한 후, **매핑 정보**를 클릭 시 "매핑 정보" 창이 나타납니다.
3. "매핑 정보" 창에 **입력 필드**가 표시됩니다.
4. "매핑 정보" 창의 **입력 필드** 탭을 클릭하세요.
   - 입력 필드는 서비스 호출시 입력 파라미터로 사용되는 필드의 정보입니다.
   - 입력 필드의 대체 이름과 상세 설명은 클릭하여 변경할 수 있습니다.

- 입력 필드를 추가 하려면 **필드 추가**를, 추가한 필드 삭제하려면 **필드 삭제**를 클릭합니다.



MQ 커넥터

MQ(Message Queue) 는 메시지 처리를 위해 대기 중인 온라인 메시지 행렬로 , MQ 를 통해 데이터를 전달하는 서비스입니다 . 다음은 IBM JMS 제공툴의 하나인 MQ 커넥터에 대한 설정 및 관리에 대한 설명입니다 .



MQ 서비스 관리하기

설정 > 연동시스템 > MQ 에서 등록한 MQ 서비스의 설정을 이용하여 커넥터를 설정합니다 . 커넥터 설정은 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다

MQ 서비스를 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > MQ**로 이동하세요.

2. MQ 서비스를 추가하려면 ＋을 클릭하세요.

3. "서비스 추가" 창에 서비스 정보를 입력하세요.

- **서비스 그룹 이름**: **설정 > 커넥터 > 서비스 그룹**에 등록된 서비스 그룹 중 MQ 서비스를 추가할 서비스 그룹을 선택합니다.
- **서비스 ID**: MQ 서비스 관리를 위한 ID입니다.
- **서비스 이름**: 서비스 이름입니다.
- **상태**: 활성, 비활성, 시뮬레이션 중 서비스 상태를 선택합니다.
- **MQ ID**: MQ 연결 정보에 등록된 MQ ID입니다.
- **Subject**: Topic/Queue의 명칭을 입력합니다.(예: Destination 명칭)
- **Topic/Queue**: Topic 또는 Queue를 선택합니다.
- **Consumer/Producer**: Consumer 또는 Producer 서비스를 선택합니다.
  - **Consumer**: 메시지를 받는 Consumer를 의미합니다.(Receive)
  - **Producer**: 메시지를 보내는 Producer를 의미합니다.(Send)
  - **Browser**: Queue에 저장된 메시지 목록 Browse를 의미합니다.
- **Persistent Mode**: MQ 서비스 Non-Persistent 또는 Persistent를 선택합니다.
- **Durable Mode**: Durable Mode의 on 또는 off를 선택합니다.
- **Transacted Mode**: Transacted Mode의 on 또는 off를 선택합니다.
- **Ack Mode**: AUTO_ACKKONWLEDGE, CLIENT_ACKKONWLEDGE, DUPS_OK_ACKKONWLEDGE 중 Acknowledge Mode를 선택합니다.
- **Header Properties**: 메시지 헤더에 별도의 설정이 필요한 경우 설정값을 입력합니다.

4. 서비스 관리를 위해 역할을 설정하려면 ⊕을 클릭한 후, "서비스 역할 선택" 창에서 역할을 선택하고 **확인**을 클릭하세요. 역할은 다중 선택이 가능합니다.
5. **저장**을 클릭하세요.

> **Note:** 이미 등록된 MQ 서비스의 커넥터 정보를 복사하여 추가로 등록하는 경우, 동일한 서비스 ID로는 등록이 불가능합니다.

MQ 서비스 테스트하기

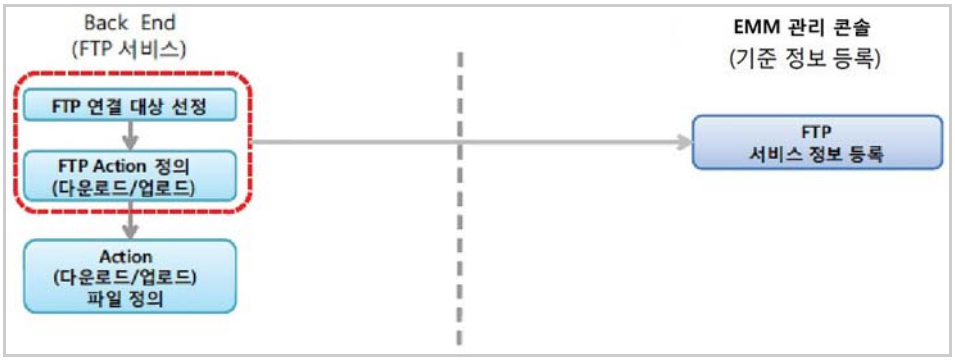
MQ 서비스가 정상적으로 연결 및 동작하는지 서비스 테스트를 통해 확인할 수 있습니다 . **설정 > 커넥터 > MQ** 내의 ▶을 클릭하여 각 서비스를 테스트할 수 있으며, 자세한 내용은 270 페이지의 " SAP ERP 서비스 테스트하기 " 를 참고하세요 .

MQ 서비스 운영하기

설정 > 커넥터 > MQ 의 커넥터 서비스에서는 커넥터 서비스 운영 시간을 설정하고 서비스 비운영시간을 안내하는 메시지를 단말에 보내거나 서비스에 대한 로그 기록을 설정할 수 있습니다 . 커넥터 서비스에 대한 자세한 내용은 266 페이지의 " 커넥터 서비스 운영하기 " 를 참고하세요 .

FTP 커넥터

FTP 커넥터는 파일의 다운로드 및 업로드 서비스를 제공합니다 . 다음은 FTP 커넥터를 설정 및 관리하는 방법에 대해 설명합니다 .



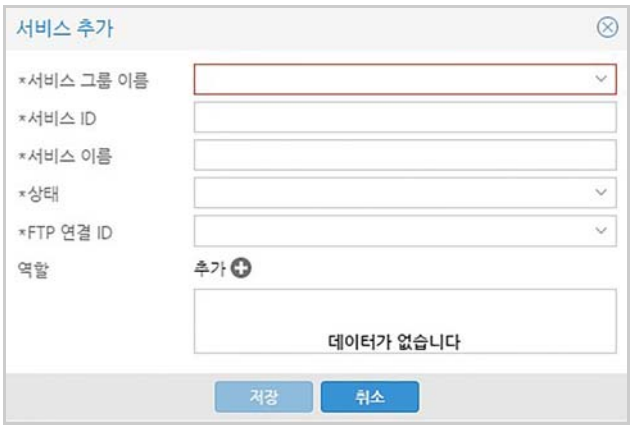
FTP 서비스 관리하기

연동시스템에서 설정한 FTP 서비스와의 설정을 이용하여 커넥터를 설정합니다. 커넥터 설정은 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다

FTP 서비스를 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > FTP**로 이동하세요.

2. FTP 서비스를 추가하려면 ＋을 클릭하세요.



3. “서비스 추가” 창에 서비스 정보를 입력하세요.
   - **서비스 그룹 이름**: **설정 > 커넥터 > 서비스 그룹**에 등록된 서비스 그룹 중 FTP 서비스를 추가할 서비스 그룹을 선택합니다.
   - **서비스 ID**: FTP 서비스 관리를 위한 ID입니다.
   - **서비스 이름**: FTP 서비스 이름입니다.
   - **상태**: 활성, 비활성, 시뮬레이션 중 서비스 상태를 선택합니다.
   - **FTP 연결 ID**: FTP 연결 정보에 등록된 FTP ID입니다.
4. 서비스 관리를 위해 역할을 설정하려면 ⊕을 클릭한 후, “서비스 역할 선택” 창에서 역할을 선택하고 **확인**을 클릭하세요. 역할은 다중 선택이 가능합니다.
5. **저장**을 클릭하세요.

> **Note:** 이미 등록된 FTP 서버의 커넥터 정보를 복사하여 추가로 등록하는 경우, 동일한 서비스 ID로는 등록이 불가능합니다.

FTP 서비스 테스트하기

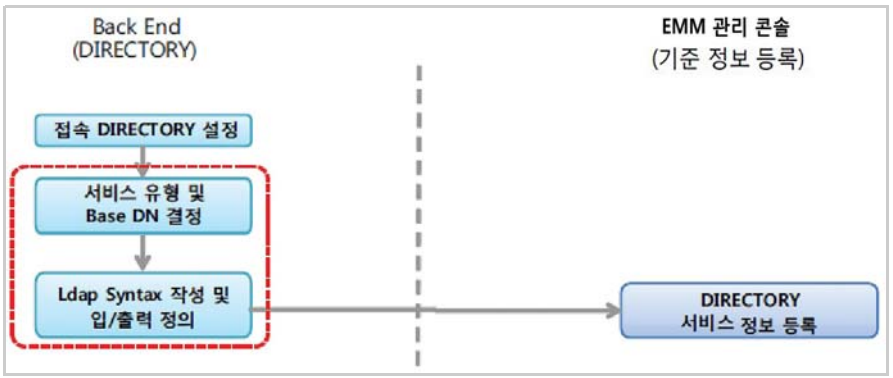
FTP 서비스가 정상적으로 연결 및 동작하는지 서비스 테스트를 통해 확인할 수 있습니다 . **설정 > 커넥터 > FTP** 내의 ▶을 클릭하여 각 서비스를 테스트할 수 있으며 , 자세한 내용은 270 페이지의 " SAP ERP 서비스 테스트하기 " 를 참고하세요 .

FTP 서비스 운영하기

설정 > 커넥터 > FTP 의 커넥터 서비스에서는 커넥터 서비스 운영 시간을 설정하고 서비스 비운영시간을 안내하는 메시지를 단말에 보내거나 서비스에 대한 로그 기록을 설정할 수 있습니다 . 커넥터 서비스에 대한 자세한 내용은 266 페이지의 " 커넥터 서비스 운영하기 " 를 참고하세요 .

Directory 커넥터

연동 시스템에 등록된 Directory 서버에서 데이터 조회나 사용자 인증 서비스 등을 제공하기 위해 Directory 커넥터를 설정합니다 . 다음은 Directory 커넥터를 설정 및 관리하는 방법에 대해 설명합니다 .



Directory 서비스를 통해 제공받은 정보로 동기화 서비스를 설정하는 방법은 다음과 같습니다 .

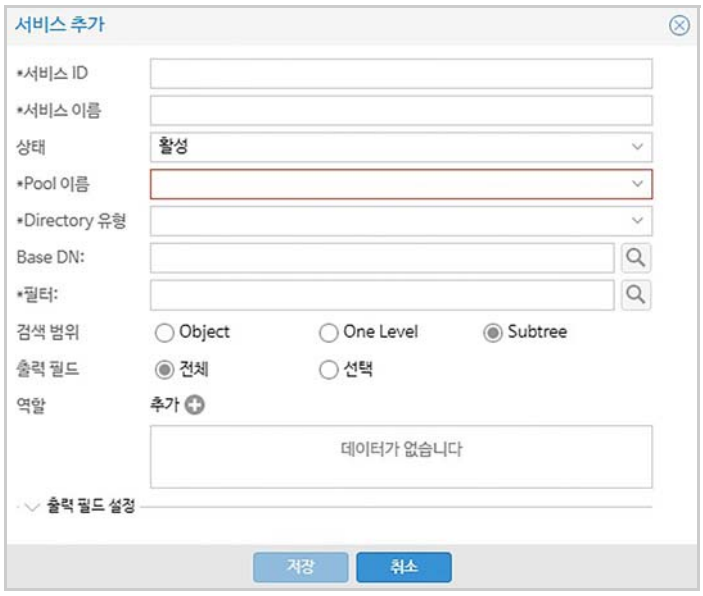
Directory 서비스 유형	서비스 설명 및 사용방법
인증	Directory 서버에서 제공하는 정해진 필터 정보로 인증하는 방식입니다. **설정 > 서비스 > 환경 설정**의 **인증 설정**에서 **Authenticator**를 **globalLdapServiceAuthenticator**으로 선택시 단말에서 사용자 확인을 위해 사용됩니다. 자세한 내용은 31페이지 2장의 "사용자 인증 설정 하기"를 참고하세요.
사용자 정의 인증 서비스	Directory 서비스의 **필터** 항목에서 제공하는 필터 정보로 인증하는 방식입니다. **설정 > 서비스 > 환경 설정**의 **인증 설정**에서 **Authenticator**를 **globalLdapServiceAuthenticator**으로 선택시 단말에서 사용자 확인을 위해 사용됩니다. 자세한 내용은 31페이지 2장의 "사용자 인증 설정 하기"를 참고하세요.
사용자 정의 검색	Directory 서비스의 **필터** 항목에 운영자가 직접 필터 정보를 입력하여 검색하는 방식입니다. 연결된 Directory 서버에서 다양한 정보를 검색할 수 있으며, 단말에 해당 정보를 전달할 수 있습니다.
프로파일 설정 검색 (사용자 정보)	**프로파일 > 단말 관리 프로파일 > Andriod 또는 iOS > 설정**의 "설정 등록" 창에서 **사용자 정보 입력 방법**으로 **커넥터 연동** 을 선택시 해당 Directory 정보가 사용됩니다.
프로파일 설정 검색 (인증서 정보)	**프로파일 > 단말 관리 프로파일 > Andriod 또는 iOS > 설정**의 "설정 등록" 창에서 **사용자 인증서 입력 방법**으로 **커넥터 연동**을 선택시 해당 Directory 정보가 사용됩니다.

Directory 서비스 관리하기

연동시스템에서 설정한 Directory 서비스와의 설정을 이용하여 커넥터를 설정합니다 . 커넥터 설정은 필요에 따라 추가 , 수정 , 복사 및 삭제가 가능합니다 .

Directory 서비스를 추가하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > Directory**로 이동하세요.
2. Directory 서비스를 추가하려면 ➕을 클릭하세요.
3. "서비스 추가" 창에 서비스 정보를 입력하세요.



- **Directory 유형:** Directory 서비스를 통해 제공받는 정보로 위의 Directory 서비스 유형 표를 참고하여 선택합니다.
- **Base DN**: 서비스 유형을 인증 또는 사용자 검색을 선택한 경우, Directory 서버의 탐색 시작 위치를 선택합니다. Base DN을 설정하지 않는 경우, Directory 서버 전체를 탐색할 수 있으므로 검색하는데 시간이 많이 걸릴 수 있습니다. Base DN에 대한 자세한 내용은 287페이지의 "Base DN 설정하기"를 참고하세요.
- **필터**: LDAP Syntax 문자열로 필터를 위한 Object Class와 변수명을 입력합니다. 필터에 대한 자세한 내용은 288페이지의 "필터 설정하기"을 참고하세요.
- **검색 범위**: Object, One Level, Subtree 중 Directory 서버의 검색 범위를 선택하세요.
  - **Object**: Base DN 위치의 동일 레벨 정보만 검색됩니다.
  - **One Level**: Base DN 위치부터 하위 1 레벨 정보까지만 검색됩니다.
  - **Subtree**: Base DN 위치부터 종속된 모든 하위 정보까지 검색됩니다.
- **출력 필드**: 전체, 선택 중 필터와 일치하는 엔트리의 정보를 반환하는 방법을 선택하세요. 출력 필드에 대한 자세한 내용은 289페이지의 "출력 필드 설정하기"을 참고하세요.
  - **전체**: 검색된 엔트리의 모든 정보가 반환됩니다.
  - **선택**: 정의한 엔트리의 속성만 반환됩니다.

4. 서비스 관리를 위해 역할 추가 ⊕을 클릭한 후, "서비스 역할 선택" 창에서 역할을 선택하고 **확인**을 클릭하세요.
5. **저장**을 클릭하세요.

Base DN 설정하기

Directory 서비스의 검색 위치를 설정하는 부분으로 Base DN 값을 직접 입력하거나 선택하여 설정할 수 있습니다 .

Base DN 값을 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > Directory**로 이동하세요.
2. 목록에서 수정하려는 **서비스 이름**을 선택한 후, 을 클릭하거나 **서비스 이름**을 클릭한 후, “서비스 보기” 창의 **수정**을 클릭하세요.

3. “서비스 수정” 창에서 **Base DN**의 을 클릭하세요.

4. “Base DN 선택” 창에서 Directory 서버의 탐색 시작 위치를 설정하려면 Directory 트리에서 엔트리를 선택하세요.
   - **선택 DN**: 선택한 엔트리 이름(Distinguish Name)이 표시됩니다.
5. “서비스 수정” 창에서 **저장**을 클릭하세요.

필터 설정하기

Directory 서비스에서 검색을 위해 필터를 설정하는 부분으로 필터값은 Directory 서버에서 검색하려는 구문 (LDAP Syntax) 을 사용하며 서버에 따라 구문이 다를 수 있습니다 .

Directory 서비스에서 검색을 위한 필터의 변수명은 다음 변수명을 참고하여 입력합니다 . 커넥터 서비스에 따라 제공되는 변수명이 다를 수 있습니다 .

- {userId}: Knox Manage 사용자 ID
- {userName}: Knox Manage 사용자 이름
- {email}: Knox Manage 사용자 이메일
- {contact}: Knox Manage 사용자 전화번호
- {empNo}: Knox Manage 사용자 사원번호

설정 > 커넥터 > Directory 의 “ 서비스 수정 ” 창에서 필터를 선택하여 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > Directory**로 이동하세요.

2. 목록에서 수정하려는 **서비스 이름**을 선택한 후, 을 클릭하거나 **서비스 이름**을 클릭한 후, "서비스 보기" 창의 **수정**을 클릭하세요.
3. "서비스 수정" 창의 **필터** 우측 을 클릭하면 "Object Class 선택" 창에 전체 Object Class 정보가 표시됩니다.

   - **반환 정보**: 선택한 Object Class 및 속성을 조합한 LDAP Syntax가 표시됩니다.
   - **기본 정의**: LDAP에서 정의한 기본적인 Object Class 및 속성입니다.
   - **연결 서버 정의**: 연결된 디렉터리 서버에서 정의한 Object Class 및 속성입니다.
4. "Object Class 선택" 창에서 Object Class를 선택하세요.
   - Object Class를 검색하려면 검색란에 **Object Class 이름**을 입력한 후, 을 클릭하세요.
5. **반환 정보** 영역에는 **Object Class 정보**에서 클릭한 LDAP Syntax가 표시됩니다.
6. **저장**을 클릭하세요.

출력 필드 설정하기

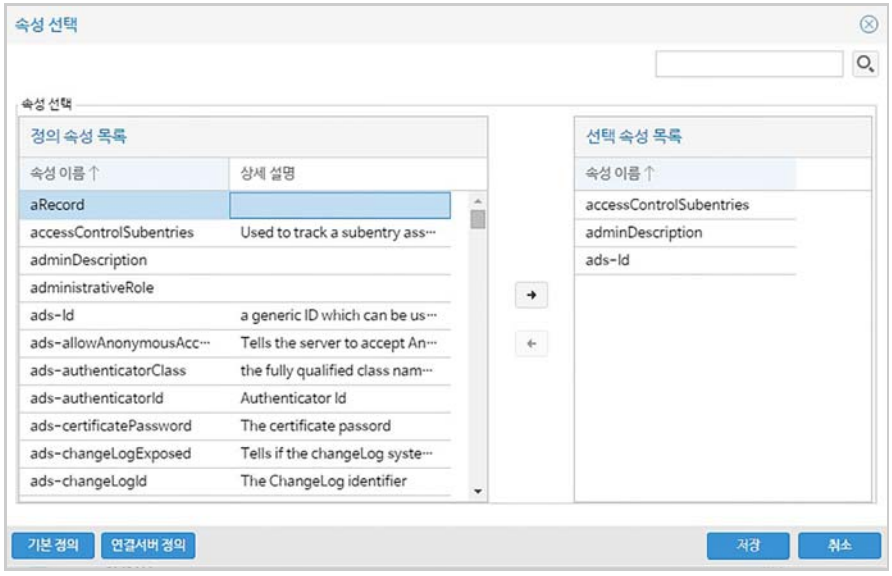
Directory 서비스의 검색을 위해 출력 필드를 설정하는 부분으로 " 서비스 추가 " 혹은 " 서비스 수정 " 창에서 **출력 필드**의 **선택**을 클릭한 경우 , 반환할 속성을 지정할 수 있습니다 .

설정 > 커넥터 > Directory 의 " 서비스 수정 " 창에서 반환하려는 속성을 선택하여 출력 필드를 설정하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > Directory**로 이동하세요.

2. 목록에서 수정하려는 **서비스 이름**을 선택한 후, 을 클릭하거나 **서비스 이름**을 클릭한 후, "서비스 보기" 창의 **수정**을 클릭하세요.

3. "서비스 수정" 창에 **출력 필드**의 **선택**을 클릭한 후, **출력 필드 설정** 영역의 **속성 선택**을 클릭하세요.



- **정의 속성 목록**: Directory 서버에 정의된 속성 이름입니다.
- **선택 속성 목록**: 서비스 호출시 반환될 속성 이름 목록 입니다.
- **기본 정의**: LDAP에서 정의한 기본 속성입니다.
- **연결 서버 정의**: Directory 서버에서 정의한 속성입니다.

4. 정의 속성을 검색하려면 검색란에 **속성이름**을 입력한 후, 을 클릭하세요.
5. "속성 선택" 창의 **정의 속성 목록** 영역에서 **속성 이름**을 선택한 후, 을 클릭하세요. 속성을 잘못 선택한 경우 을 클릭하세요.

6. "속성 선택" 창 하단의 **저장**을 클릭하세요.
7. **출력 필드 설정**의 "속성 선택" 창에서 선택한 속성들이 표시됨을 확인한 후, 하단의 **확인**을 클릭하세요.
   - 단말에 반환되는 속성명을 변경하려면 **반환 속성 명** 항목을 더블 클릭하여 직접 입력하세요.
   - **요청 속성 명**은 Directory 서버에 요청하는 속성명으로 임의적으로 수정 시 정상적으로 데이터를 가져오지 못할 수 있습니다.

Directory 서비스 테스트하기

Directory 서비스가 정상적으로 연결 및 동작하는지 서비스 테스트를 통해 확인할 수 있습니다 . **설정 > 커넥터 > Directory** 내의 ▶을 클릭하여 각 서비스를 테스트할 수 있으며 , 자세한 내용은 270 페이지의 " SAP ERP 서비스 테스트하기 " 를 참고하세요 .

Directory 서비스 운영하기

설정 > 커넥터 > Directory 의 커넥터 서비스에서는 커넥터 서비스 운영 시간을 설정하고 서비스 비운영시간을 안내하는 메시지를 단말에 보내거나 서비스에 대한 로그 기록을 설정할 수 있습니다 . 커넥터 서비스에 대한 자세한 내용은 266 페이지의 " 커넥터 서비스 운영하기 " 를 참고하세요 .

커넥터 로그 보기

EMM 은 커넥터 서비스 운영 중 발생되는 커넥터의 사용 이력을 로그 정보로 관리합니다 . 운영자는 커넥터 로그 정보를 통해 커넥터 서비스를 사용하는 사용자 정보 , 단말 정보 , 커넥터 서비스의 유형 , 서비스 요청 시간 및 응답 시간 등의 정보 확인이 가능합니다 . 커넥터 서비스의 운영 방법은 다음과 같이 두가지의 방법이 있으며 , 운영 방법 설정에 따라 커넥터가 서비스 운영 및 커넥터 로그가 발생됩니다 .

- 전체 커넥터 서비스 운영은 **설정 > 서비스 > 환경 설정**의 상단 **관리**를 클릭한 후, 설정합니다.
- 커넥터 별 서비스 운영은 **설정 > 서비스 > 커넥터**에서 커넥터 별로 상단의 **커넥터 서비스**를 클릭한 후, 설정합니다.

커넥터 서비스의 로그를 확인하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 로그 > 커넥터 로그**로 이동하세요.

2. 커넥터 로그 정보를 조회하려면 화면 상단의 을 클릭하여 날짜를 선택하거나 검색 영역에서 **사용자 ID** 또는 **서비스 ID**를 입력한 후, Enter 키를 누르거나 을 클릭하세요.
   - **사용자 ID** 또는 **서비스 ID**를 클릭하면 커넥터 로그 항목의 상세 정보가 화면 하단에 나타납니다.

커넥터 서비스를 사용하는 트랜잭션 추적하기

커넥터 운영 방법의 설정에 따라 커넥터 서비스를 사용하는 트랜잭션에 대한 추적이 가능합니다 .

다음은 커넥터 서비스의 트랜잭션 추적을 위한 트랜잭션 로그 설정 방법입니다 .

- **설정 > 서비스 > 환경 설정** 상단의 **관리**를 클릭한 후, **로그 서비스**를 탭한 다음 **커넥터 서비스 트랜잭션 로그 기록 사용**을 선택하면 EMM의 모든 커넥터 서비스에서 트랜잭션 로그가 기록됩니다.
- **설정 > 커넥터 > 서비스 그룹** 상단의 **커넥터 서비스**를 클릭한 후, 서비스 그룹별로 설정하면 해당 서비스 그룹에 속하는 커넥터 서비스들에 대해 트랜잭션 로그가 기록됩니다.
- **설정 > 커넥터**에서 각 커넥터 서비스를 선택한 후, **커넥터 서비스**를 클릭하여 설정하면 해당 커넥터 서비스만 트랜잭션 로그가 기록됩니다.

다음은 SAP ERP 커넥터에 트랜잭션 추적이 가능하도록 활성화하는 방법으로 다른 커넥터의 경우에도 동일한 방법으로 설정합니다 .

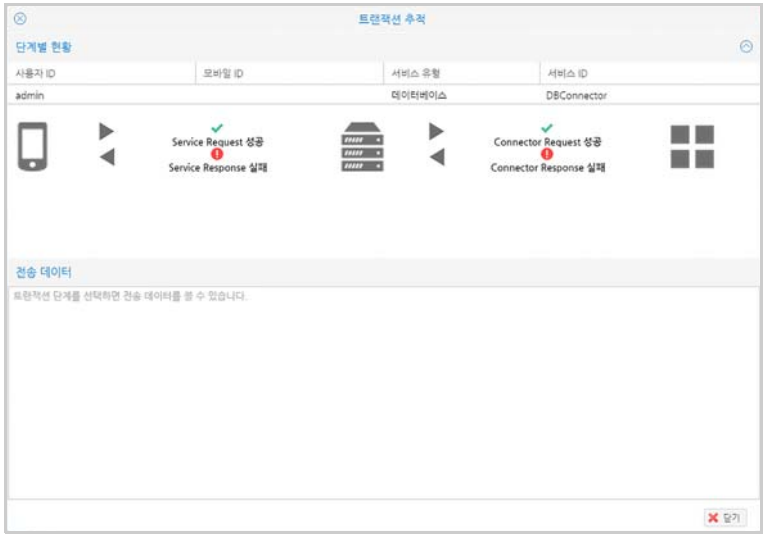
SAP ERP 커넥터의 트랜잭션을 활성화하려면 다음의 절차를 따르세요 .

1. **설정 > 커넥터 > SAP ERP**에서 활성화하려는 서비스를 선택한 후, 상단의 **관리**를 클릭하세요.
2. “커넥터 서비스 관리” 창에서 **로그 서비스** 탭을 클릭하세요.
   - **커넥터 서비스 트랜잭션 로그 기록 사용**을 선택하면 트랜잭션 추적이 가능합니다.

SAP ERP 커넥터의 트랜잭션을 활성화 한 후 , 트랜잭션을 추적하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 로그 > 커넥터 로그**로 이동하세요.
2. 화면 상단의 을 클릭하여 조회하려는 날짜를 선택하거나 검색 영역에서 **사용자 ID** 또는 **서비스 ID**를 입력한 후, Enter 키를 누르거나 을 클릭하세요.

3. 커넥터 로그 목록에서 트랜잭션을 추적하려는항목을 클릭한 후, 상단의 을 클릭하세요.



4. "트랜잭션 추적" 창의 단계별 현황에서 트랜잭션 추적을 통해 커넥터 서비스의 접속, 서비스의 요청 및 응답이 정상적인지 확인합니다.
   - 단계별 현황의 트랜잭션 구간을 클릭하면 해당 구간의 전송된 요청 및 응답데이터의 정보가 하단에 나타납니다.

커넥터 접속 통계 보기

EMM 은 커넥터 서비스 운영 중 발생되는 커넥터별 접속 통계를 관리합니다 . 운영자는 커넥터 접속 통계를 통해 커넥터를 사용한 사용자별 , 시간별 , 날짜별 커넥터 접속 정보 확인이 가능합니다 . 사용자별 , 시간별 , 날짜별로 분리된 커넥터 접속 통계는 커넥터 서비스 유형별 (SAP ERP, 데이터베이스 , 웹 클라이언트 , MBI, MQ, FTP, Directory) 로 확인이 가능하며 , 접속 통계 자료는 엑셀 파일로 내려받을 수 있습니다 .

사용자별 접속 통계 보기

커넥터 서비스에 접속한 사용자별 접속 현황을 확인하는 방법은 다음과 같습니다 .

커넥터에 접속한 사용자별 통계를 조회하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 커넥터 접속 통계 > 사용자별 통계**로 이동하세요.
2. **서비스 유형**과 을 클릭하여 조회하려는 날짜를 선택하세요.
   - 선택 가능한 커넥터 서비스 유형은 SAP ERP, 데이터베이스, 웹 클라이언트, MBI, MQ, FTP, Directory 입니다.
3. 검색란에 **사용자 이름**을 입력한 후, Enter 키를 누르거나 을 클릭하세요.

4. **사용자 이름**을 클릭한 후, "사용자별 통계 차트 보기" 창에서 접속 통계 차트를 확인하세요.

> **Note:** 차트의 세로축은 접속 건수, 가로축은 서비스 이름입니다.

사용자별 통계 엑셀 파일로 내보내기

커넥터에 접속한 사용자별 통계를 엑셀 파일로 내보내기하려면 다음의 절차를 따르세요.

1. **서비스 현황 > 커넥터 접속 통계 > 사용자별 통계**로 이동하세요.
2. **서비스 유형**을 선택하고 을 클릭하여 날짜를 선택하세요.
3. 검색란에 **사용자 이름**을 입력한 후, Enter 키를 누르거나 을 클릭하세요.
4. 엑셀 파일로 내보내기 하려는 사용자 이름을 선택한 후, 을 클릭하세요.
   - 현재 화면에 보이는 모든 정보가 엑셀 파일로 저장됩니다.

시간별 접속 통계 보기

커넥터 서비스에 접속한 시간대별 접속 현황을 확인하는 방법은 다음과 같습니다 .

커넥터에 접속한 시간별 통계 차트를 조회하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 커넥터 접속 통계 > 시간별 통계**로 이동하세요.
2. **서비스 유형**과 을 클릭하여 조회하려는 날짜를 선택하세요.
   - 선택 가능한 커넥터 서비스 유형은 SAP ERP, 데이터베이스, 웹 클라이언트, MBI, MQ, FTP, Directory 입니다.
3. 검색란에 **서비스 이름**을 입력한 후, Enter 키를 누르거나 을 클릭하세요.
4. **사용자 이름**을 클릭한 후, "시간별 통계 차트 보기" 창에서 통계 차트를 확인하세요.

> **Note:** 차트의 세로축은 접속 건수, 가로축은 시간대입니다.

시간별 통계 엑셀 파일로 내보내기

커넥터에 접속한 시간별 통계를 엑셀 파일로 내보내기하려면 다음의 절차를 따르세요.

1. **서비스 현황 > 커넥터 접속 통계 > 시간별 통계**로 이동하세요.
2. **서비스 유형**을 선택하고 을 클릭하여 날짜를 선택하세요.
3. 검색란에 **서비스 이름**을 입력한 후, Enter 키를 누르거나 을 클릭하세요.
4. 엑셀 파일로 내보내기 하려는 서비스 이름을 선택한 후, 을 클릭하세요.
   - 현재 화면에 보이는 모든 정보가 엑셀 파일로 저장됩니다.

날짜별 접속 통계 보기

커넥터 서비스에 접속한 날짜별 접속 현황을 확인하는 방법은 다음과 같습니다 .

커넥터에 접속한 날짜별 통계 차트를 조회하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 커넥터 접속 통계 > 날짜별 통계**로 이동하세요.
2. **서비스 유형**과 을 클릭하여 조회하려는 날짜를 선택하세요.
   - 선택 가능한 커넥터 서비스 유형은 SAP ERP, 데이터베이스, 웹 클라이언트, MBI, MQ, FTP, Directory 입니다.
3. **날짜**를 클릭한 후, “날짜별 통계 차트 보기” 창에서 통계 차트를 확인하세요.

> **Note:** 차트의 세로축은 접속 건수, 가로축은 서비스 이름입니다.

날짜별 통계 엑셀 파일로 내보내기

커넥터에 접속한 날짜별 통계를 엑셀 파일로 내보내기하려면 다음의 절차를 따르세요 .

1. **서비스 현황 > 커넥터 접속 통계 > 날짜별 통계**로 이동하세요.
2. **서비스 유형**을 선택하고 을 클릭하여 날짜를 선택하세요.
3. 엑셀 파일로 내보내기 하려는 날짜를 선택한 후, 을 클릭하세요.
   - 현재 화면에 보이는 모든 정보가 엑셀 파일로 저장됩니다.

17 Resources

EMM 은 다양한 서비스의 활용 및 애플리케이션 개발이 용이할 수 있도록 개발자를 위한 Open API 를 제공합니다 . 또한 Windows10 이 설치된 PC, 테블릿 기기에서 특정 기능을 제어할 수 있는 OMA-URI 의 CSP 표준 설정을 관리합니다 . 그외 EMM 에 로그인을 위한 Enrollment 및 Windows 업데이트 등의 Data 배포를 위해 프로비저닝 패키지 파일 (.ppkg) 을 관리합니다 .

EMM API

EMM API 는 EMM 서버에 대한 개발자의 제한된 접근 및 안전한 인증을 제공하기 위해 표준화된 Open Protocol 인 OAuth 인증 방식을 사용합니다 . EMM API 인증은 관리자 포털에 등록된 클라이언트 ID 로 사용자를 인증한 후 , 해당 사용자가 기간이 유효한 Token 을 발급 받아 API 를 호출합니다 . EMM API 개발 및 API 정보에 대한 자세한 내용은 "Samsung SDS EMM 개발자 매뉴얼 " 을 참고하세요 .

Note: EMM API를 사용하려면 라이선스 및 API Client 설정이 반드시 필요합니다.
- 라이선스는 TMS 관리자 포털의 **관리 > Tenant** 에서 해당 테넌트를 선택한 후, "라이선스" 창에서 **API 클라이언트** 활성화 여부를 확인합니다.
- API Client 설정은 **설정 > 서비스 > 라이선스 정보**에서 API Client 수의 설정을 확인합니다.

다음은 EMM API 사용을 위한 클라이언트 ID 등록 방법과 EMM API 로그 정보 및 API 사용 이력을 확인하는 방법에 대한 설명입니다 .

API 사용자 관리하기

EMM API 사용을 위해 클라이언트 ID(API 사용자) 를 등록하려면 다음의 절차를 따르세요 . EMM API 사용자는 필요에 따라 추가 , 수정 , 복사 , 삭제가 가능합니다 .

1. **설정 > EMM API > API 사용자**로 이동하세요.
2. 클라이언트 ID(API 사용자)를 등록하려면 ＋을 클릭하세요.

3. “API 사용자 추가” 창에 다음의 정보를 입력한 후, **저장**을 클릭합니다.
   - **클라이언트 ID**: Token 요청을 위한 클라이언트 ID입니다. API 사용자로 등록한 클라이언트 ID는 수정할 수 없습니다.
   - **비밀번호**: Token 요청을 위한 클라이언트 비밀번호입니다.
   - **Token 유효시간(초)**: 해당 클라이언트 ID로 EMM API 호출이 가능한 유효시간을 설정합니다.

> **Note:** EMM API 사용자 중 remoteuser는 Remote Support용으로 제공되는 사용자입니다.

API 사용자 상태 변경하기

클라이언트 ID(API 사용자) 를 필요에 따라 활성화하거나 비활성화 할 수 있습니다 . 클라이언트 ID 를 비활성화시키면 해당 클라이언트 ID 로 API 호출이 불가능해집니다 .

클라이언트 ID 의 상태를 활성화 또는 비활성화 하려면 다음의 절차를 따르세요 .

1. **설정 > EMM API > API 사용자**로 이동하세요.
2. 비활성화 상태로 변경하려는 항목의 을 클릭하세요.
   - 클라이언트 ID의 상태를 활성화하려면 을 클릭합니다.
3. 비활성화 확인 메시지가 나타나면 **예**를 클릭하세요.

Token Invalidate하기

Token Invalidate 는 활성화되어있는 Token 을 전부 무효화 (kill) 시킨다는 의미로 Token Invalidate 를 실행한 후 , 해당 token 값으로 API 를 호출하면 Invalid access token 에러 메시지가 발생하고 API 호출이 불가능해 집니다 . 만약 , 위와 같은 에러가 발생하는 경우에는 인증을 통해 새로 Token 을 발급 받으시기 바랍니다 .

사용 중인 Token 을 무효화 시키려면 다음의 절차를 따르세요 .

1. **설정 > EMM API > API 사용자**로 이동하세요.
2. Token 유효시간을 무효화하려는 **클라이언트 ID**를 선택한 후, **Token Invalidate**를 클릭하세요.
3. 토큰 삭제 확인 메시지가 나타나면 **예**를 클릭하세요.

API 로그 및 사용 이력 보기

EMM API 의 로그 정보 및 사용 이력은 **설정 > EMM API > API 로그와 API 사용이력**에서 확인합니다 . API 로그 정보에는 해당 클라이언트 ID 의 응답 유형에 따른 결과 코드와 오류 메시지 및 로그 일시를 보여줍니다 . 또한 API 사용 이력에서는 클라이언트 ID 의

접속 IP 정보 , Token 값 , 호출한 API 정보가 나타나며 , API 호출 중 실패 시 에러 확인은 해당 항목을 선택한 후 , 화면 하단에서 확인합니다 .

Windows10

EMM 은 Windows10 이 설치된 PC, 테블릿에서 Wi-Fi, 블루투스 , NFC 및 USB 사용에 대한 단말 제어와 단말 분실 시 대응을 위해 비밀 번호 , 공장 초기화와 같은 보안 정책을 프로파일에 설정하여 관리합니다 . 또한 카메라 , 화면 캡쳐 등의 기능 제어을 통해 데이터 유출을 차단함으로써 회사내 정보 유출을 방지할 수 있습니다 . 그외 프로파일을 통해 사용자의 단말에 Wi-Fi, VPN 과 같은 네트워크 설정 , 사내용 메일 사용을 위해 Exchange 설정 , 사용자의 인증 설정을 통해 회사 내 네트워크 사용이 가능합니다 . Windows 단말에 대한 정책 및 설정에 대한 자세한 내용은 382 페이지 18 장의 “Windows 단말 관리 정책 " 을 참고하세요 .

설정 > Windows 10 > CSP 설정관리에서는 OMA-URI (Open Mobile Alliance Uniform Resource Identifier) 설정을 통해 Windows10 이 설치된 기기의 기능 제어가 가능합니다 . OMA-URI 는 장비 제조 업체에서 PC, 테블릿과 같은 기기의 기능을 제어하는데 사용되는 표준 설정입니다 . Configuration Service Provider(이하 CSP) 설정에 대한 자세한 내용은 MS 사이트의 “Windows10 장치에 대한 사용자 지정 URI 설정 ” 을 참고하세요 .

설정 > Windows 10 > PPKG 파일관리에서는 Windows10 이 설치된 단말에서 EMM 에 로그인을 위한 Enrollment 및 Windows 업데이트 등의 Data 배포를 위해 프로비저닝 패키지 파일을 등록합니다 . 프로비저닝 패키지는 MS 사이트에서 제공하는 Windows10 용 Windows ADK 를 설치한 후 , Windows ICD 를 통해 만들 수 있습니다 . 자세한 내용은 MS 사이트의 “ 프로비저닝 패키지와 Windows ICD 시작하기 ” 를 참고하세요 .

CSP 설정하기

CSP 설정의 항목들은 EMM 설치 시 기본적으로 제공되는 항목들입니다 . 기본 CSP 는 운영자에 의해 수정 , 복사 , 삭제 시 제한 사항이 있을 수 있으며 , 추가적인 CSP 등록은 대상 유형이 Device Command 인 경우에만 등록이 가능합니다 .

CSP 설정을 관리하는 방법은 다음과 같습니다 .

- CSP 설정을 추가, 수정, 복사, 삭제하려면 299페이지의 "CSP 설정 관리하기"를 참고하세요.
- 블랙 또는 화이트 리스트를 통해 애플리케이션을 제어하려면 300페이지의 "애플리케이션 제어를 위한 CSP 설정하기"와 301페이지의 "블랙 또는 화이트리스트로 애플리케이션 제어를 위한 시나리오"를 참고하세요.

- CSP를 단말에 전송하려면 301페이지의 "CSP 설정을 단말에 배포하기"를 참고하세요.

CSP 설정 관리하기

CSP 설정은 필요에 따라 추가 , 수정 , 복사 , 삭제가 가능합니다 .

CSP 설정을 추가하려면 다음의 절차를 따르세요 .

1. **설정 > Windows 10 > CSP 설정관리**로 이동하세요.
2. CSP 설정을 추가하려면 ＋을 클릭하세요.

3. “Configuration Service Provider 추가” 창에 다음의 정보를 입력한 후, **저장**을 클릭하세요.
   - **이름**: 기기의 기능을 제어하기위한 CSP의 이름을 입력합니다.
   - **대상 유형**: Device Command가 기본 값으로 선택됩니다.
     - CSP 추가는 대상 유형이 Device Command인 것만 추가 등록이 가능합니다.
   - **실행 유형:** Read, Add, Replace, Delete, Exec 중 CSP의 실행 유형을 선택합니다.
   - **값 유형**: 문자열, 문자열(XML), 날짜 및 시간, 정수, 부동 소수점, 부울 등의 값 유형을 선택합니다.
   - **대상 기기**: 기능을 제어하려는 대상 기기를 선택합니다.
   - **OMA_URI**: OMA-URI를 입력합니다. 초기화하려면 **초기화**를 클릭합니다.
   - **기본 값**: 기본 값 입력이 필요한 경우, 값을 입력합니다.

- **설명**: 간단한 설명과 도움이 되는 관련 정보를 입력합니다.

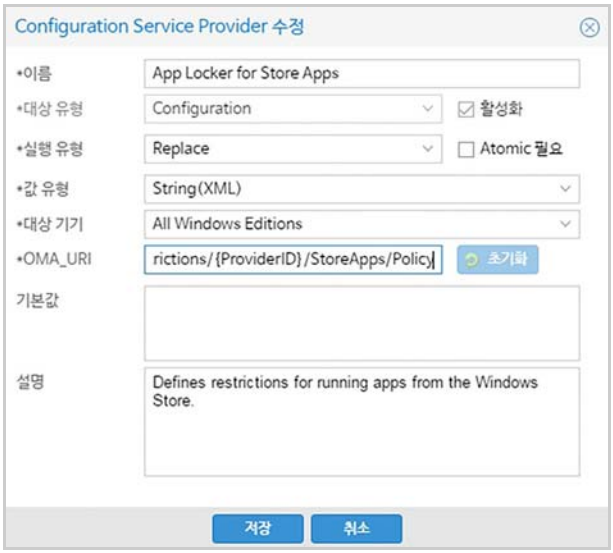
Note:
- CSP 설정을 수정하는 경우, 기본적으로 제공하는 CSP의 설정 항목들은 임의로 수정할 수 없으며, 표준 설정인 OMA_URI가 변경된 경우에만 수정이 가능합니다. 또한 임으로 OMA_URI를 수정한 경우, 기존 기능이 동작하지 않을 수 있으므로 주의가 필요합니다.
- CSP 설정을 삭제하는 경우, 기본적으로 제공하는 CSP 설정은 임의로 삭제할 수 없으며, 운영자에 의해 생성된 CSP 설정만 삭제가 가능합니다.
- 이미 등록된 CSP 설정을 복사하여 추가로 등록하려면 CSP의 설정 항목 중 대상 유형이 Device Command인 경우에만 복사가 가능합니다.

애플리케이션 제어를 위한 CSP 설정하기

PC 에서 블랙 또는 화이트리스트로 Windows AppStore 의 애플리케이션을 제어하려면 CSP 설정에 AppLocker 가 등록되어있어야 합니다 .

다음은 애플리케이션 제어를 위한 CSP 설정에 대한 설명으로 , 애플리케이션을 제어하는 자세한 방법은 301 페이지의 " 블랙 또는 화이트리스트로 애플리케이션 제어를 위한 시나리오 " 를 참고하세요 .

1. **설정 > Windows 10 > CSP 설정관리**로 이동하세요.
2. 검색란의 **이름**에 **AppLocker**를 입력한 후, 을 클릭하세요.
3. 검색된 항목 중 **AppLocker**를 클릭한 후, “Configuration Service Provider 수정” 창에 OMA_URI를 확인하고 **저장**을 클릭하세요.
   - OMA_URI 설정 값은 MS 사이트의 “Windows 10 장치에 대한 사용자 지정 URI 설정”을 참고하세요.



- AppLocker 설정을 위한 자세한 내용은 다음의 MS 사이트를 참고하세요.
  - https://msdn.microsoft.com/en-us/library/windows/hardware/dn920019(v=vs.85).aspx

Note:
- MS Intune에서 AppLocker CSP 활용 예: 제어하려는 애플리케이션이 EXE, MSI, Script, StoreApps, DLL 형태의 파일인 경우 Windows10 PC의 Group Policy를 통해 제어 설정 값(XML)을 생성한 후, 단말에 배포합니다. 자세한 내용은 다음 URL을 참고하세요. https://www.petervanderwoude.nl/post/managing-applocker-on-windows-10-via-oma-dm/

CSP 설정을 단말에 배포하기

Windows 플랫폼의 단말 제어를 위해 CSP 설정을 단말에 배포하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 단말**로 이동하세요.
2. 목록에서 CSP 설정을 전송하려는 단말을 선택한 후, ⚙을 클릭하세요.
3. "단말 제어" 창에서 **사용자 정의 제어** 메뉴를 클릭한 후, **선택**을 클릭하세요.
4. "단말 제어 - 사용자 정의 제어 선택" 창에서 CSP를 선택한 후, **실행**을 클릭하면 해당 CSP 설정이 단말에 전송됩니다.
   - 단말 제어 명령을 전송하는 자세한 방법은 128페이지 9장의 "단말 제어하기"와 438페이지 18장의 "사용자 정의 제어"를 참고하세요.

블랙 또는 화이트리스트로 애플리케이션 제어를 위한 시나리오

1. 제어하려는 Windows AppStore의 애플리케이션을 **애플리케이션 > 제어 애플리케이션**에 등록하세요.
   - 자세한 내용은 228페이지 14장의 "제어 애플리케이션 등록하기"을 참고하세요.
2. **프로파일 > 단말 관리 프로파일**에서 적용하려는 프로파일을 선택한 후, **Windows** 메뉴의 **정책** ✎을 클릭하세요. "Windows 정책 수정" 창에서 **앱**을 선택하고 **앱 블랙/화이트리스트 설정**에 애플리케이션을 추가한 후, **저장**을 클릭하세요.
3. **단말 & 사용자 > 단말**로 이동하여 단말의 ⚙을 클릭한 후, 단말 제어 명령으로 정책을 적용하면, 정책에 따라 애플리케이션이 제어됩니다.
4. **단말 & 사용자 > 단말**에서 **모바일 ID**를 클릭한 후, "단말 상세" 창의 **제어 앱** 탭을 클릭하여 제어되는 애플리케이션을 확인하세요.

PPKG 파일 설정하기

PPKG 파일관리에서는 MS 사이트에서 Windows ICD 를 이용하여 프로비저닝 패키지를 만든 후 , PPKG 파일을 등록하는 방법에 대해 설명합니다 .

PPKG 파일을 관리하는 방법은 다음과 같습니다 .

- PPKG 파일을 추가, 수정, 삭제하려면 302페이지의 "PPKG 파일 관리하기"를 참고하세요.
- PPKG 파일을 단말에 전송하려면 303페이지의 "PPKG 파일을 단말에 배포하기"를 참고하세요.

PPKG 파일 관리하기

PPKG 파일 설정은 필요에 따라 추가 , 수정 , 삭제가 가능합니다 .

PPKG 파일을 추가하려면 다음의 절차를 따르세요 .

1. **설정 > Windows 10 > PPKG 파일관리**로 이동하세요.
2. PPKG 파일을 추가하려면 ＋을 클릭하세요.

3. “PPKG 파일 추가” 창에 다음의 정보를 입력한 후, **저장**을 클릭하세요.
   - **이름**: 프로비저닝 패키지 이름을 입력합니다.
   - **PPKG 파일**: **Browse**를 클릭한 후, .ppkg 파일을 선택합니다.
   - **사용대상유형:** Enrollment, Data 배포 중 사용대상유형을 선택합니다.
   - Windows 10이 설치된 단말에서 EMM에 로그인을 하려면, Enrollment를 위한 PPKG 파일이 EMM 서버에 먼저 등록되어 있어야 합니다.
     Enrollment를 위한 PPKG 파일 등록한 후에는 Windows 업데이트 등을 위한 Data 배포 유형만 등록이 가능합니다.
   - 대상 기기: 프로비저닝 패키지를 적용하려는 대상 기기를 선택합니다.

> **Note:** Windows10의 버전 1607 단말의 경우, 프로비저닝 패키지가 외장 SD 카드에 저장됩니다. 프로비저닝 패키지를 추가하여 단말에 전송하려면 반드시 단말에 외장 SD 카드가 있어야 합니다. 자세한 내용은 다음 URL을 참고하세요.
> https://technet.microsoft.com/ko-kr/itpro/windows/deploy/provisioning-packages

PPKG 파일을 단말에 배포하기

프로비저닝 패키지 파일을 Windows 플랫폼의 단말에 배포하려면 다음의 절차를 따르세요 .

1. **프로파일 > 앱 관리 프로파일**로 이동하세요.
2. 목록에서 프로비저닝 패키지 파일을 배포하려는 **프로파일명**을 클릭하세요.
3. "앱 관리 프로파일" 창에서 **EMM Client** 메뉴를 클릭한 후, 을 클릭하세요.
4. "EMM Client 정책 수정" 창에서 **Windows 10 Desktop Data 배포** 또는 **Windows 10 Mobile Data 배포** 항목을 선택한 후, 하단에 PPKG 파일을 선택하세요.
5. **저장**을 클릭하고, 해당 프로파일을 단말에 배포하세요.

18 방문자 관리하기

EMM 사용 사이트를 방문하는 방문자의 단말에서도 EMM 을 관리합니다 . 방문자 단말 관리를 위한 조직과 사용자는 EMM 라이선스의 방문자 관리 선택 시 자동으로 생성됩니다 . 방문자가 단말 로그인 시 활성화 상태의 단말이 목록에 보여지며 , 운영자는 방문자 단말에 대해 비활성화 및 정책 할당이 가능합니다 . 또한 단말 상태 변경 이력을 조회할 수 있고 , 방문자 단말 목록을 CSV 파일로 다운로드 받을 수 있습니다 . 모두 동일한 정책을 적용받으며 단말 프로파일에 아래의 제어 기능을 설정하여 할당할 수 있습니다 . 방문자 단말 제어 명령은 다음과 같으며 단말 제어 전송 정보별 자세한 설명은 431 페이지의 " 단말 제어 전송 방법 " 을 참고하세요 . 방문자 단말에 대해 플랫폼별로 다음의 기능들을 제어할 수 있습니다 .

방문자 단말 제어 기능

단말 OS	제어 기능
Android	• 카메라 • 마이크 • 화면 캡처 • Wi-Fi • Wi-Fi 핫스팟 • Wi-Fi SSID 화이트리스트 설정 • 블루투스 • PC 연결 • USB 테더링 활성화 • 앱 실행 블랙리스트 • 앱 실행 화이트리스트
iOS	• 카메라 • 마이크 • 화면 캡처 • 앱 실행 블랙리스트 • 앱 실행 화이트리스트

방문자 단말 제어 명령

분류/OS	Android	iOS
Compliance	• 보안 정책 적용	• 보안 정책 적용 • 탈옥 여부 점검
단말 관리	• 단말 잠금/해제(단말 화면 잠금) • 단말 잠금 비밀번호 초기화 • 전원 종료 • 재부팅	• 단말 잠금/해제 • 단말 잠금 비밀번호 초기화
EMM	• 서비스 비활성화 • Audit로그 수집 • 로그 수집	• 서비스 비활성화 • Audit 로그 수집 • 로그 수집
단말 확인	• H/W상태 • 설치된 앱리스트 • 위치	• H/W상태 • 설치된 앱리스트 • 위치 • 상태보고

방문자 단말에 보안 카메라 정책을 설정하려면 185 페이지 10 장의 “Secure Browser 정책 설정하기 " 를 참고하세요 . 운영자의 권한에 따라 다음의 기능들을 이용하여 방문자 단말을관리합니다 .

구분	콘솔 제공 기능
수퍼 운영자	• 방문자 단말 프로파일 할당 및 조회 • 방문자 단말 제어 • 방문자 단말 상태 변경 • 방문자 단말 삭제 • 방문자 단말 목록 다운로드 • 방문자 단말 정보 조회 - OS버전, 플랫폼, 상태, 위변조, 단말 이력 • 방문자 단말 이력 조회 - 단말제어, Audit 로그, 보안 위반 등 • 방문자 단말 상태 변경 이력 조회
방문자 관리자	• 방문자 단말 프로파일 할당 및 조회 • 방문자 단말 상태 변경 • 방문자 단말 목록 다운로드 • 방문자 단말 정보 조회 - OS버전, 플랫폼, 상태

Note:
- 방문자 관리는 EMM 라이선스의 방문자 메뉴 사용이 **사용**인 경우에만 제공됩니다. 라이선스 정보 확인은 47페이지 2장의 “라이선스 확인하기" 를 참고하세요.
- 방문자 단말 관리를 위한 조직과 사용자는 EMM이 제공하는 단일 조직, 사용자만 사용 가능하며 운영자가 추가 등록할 수 없습니다.

방문자 단말 관리하기

방문자 단말의 상태를 변경할 수 있으며 프로파일 할당이 가능합니다 . 단말 비활성화 방법은 단말 제어 명령 전송 방법과 오프라인 인증의 두가지 방법이 있습니다 . 오프라인 인증 방식은 방문자 운영자가 관리 콘솔에서 제공되는 비활성화 코드를 방문자에게 알려주면

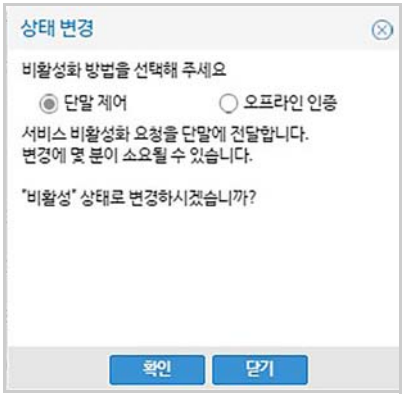
방문자가 직접 단말에 입력하여 비활성화하는 방법입니다 . 비활성화된 방문자 단말은 삭제 가능합니다 . 방문자 단말 프로파일 할당은 활성 상태의 단말에만 가능합니다 .

방문자 단말 상태 변경하기

방문자 단말을 활성화 , 비활성화 , 활성화 금지 상태로 변경할 수 있습니다 . 비활성화 방법은 단말 제어 명령 전송 방법과 사용자가 직접 비활성화 시키는 오프라인 인증 방법이 가능합니다 . 오프라인 인증 비활성화를 위한 코드 전송은 방문자 단말 상태 이력 조회 시에도 가능합니다 . 방문자 단말 상태 이력 조회는 307 페이지의 " 방문자 단말 상태 변경 이력 조회하기 " 를 참고하세요 . 단말 비활성화 시도 시 " 보안 위반 리스트 확인 " 창이 나타납니다 .

방문자 단말 상태를 변경하려면다음의 절차를 따르세요 .

1. **단말 & 사용자 > 방문자**로 이동하세요.
2. **모바일ID**나 **모델명**을 입력하여 검색한 후 상태 변경할 단말의 체크박스를 클릭하세요.
3. 상단의 ●을 클릭하세요.
   - 비활성 상태로 변경 시



4. "상태 변경" 창에서 비활성화 방법을 선택한 후 **확인**을 클릭하세요.
5. 팝업 메시지가 나타나면 **확인**을 클릭하세요.

방문자 단말 보안 정책 적용하기

방문자 단말 보안 정책 관리를 위해 프로파일을 할당할 수 있습니다 . 활성 상태의 방문자 단말에만 프로파일을 할당할 수 있습니다 .

단말 정책을 적용하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 방문자**로 이동하세요.

2. **모바일ID**나 **모델명**을 입력하여 단말을 검색한 후, 해당 단말의 체크박스를 클릭하세요.
3. [redacted]을 클릭한 후 "보안 정책 적용" 창에서 **예**를 클릭하세요.

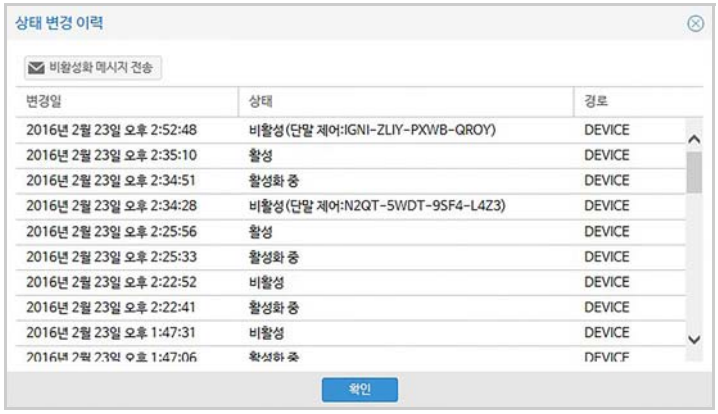
4. 확인 팝업 메시지가 나타나면 **확인**을 클릭하세요.

방문자 단말 상태 변경 이력 조회하기

방문자 단말의 상태 변경 내역을 조회할 수 있습니다 . 방문자 단말의 EMM 비활성화를 위한 메시지 전송도 가능합니다 .

방문자 단말의 상태 변경 이력을 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 방문자**로 이동하세요.
2. **모바일 ID**, **모델명**을 입력 후 단말을 검색하세요:
   - **모델명** 입력 시 Android는 모델명, iOS는 기종을 입력하세요.
3. 단말의 **마지막 업데이트** 날짜를 클릭하세요.



4. 방문자 단말 비활성화 인증 코드 전송 시, "상태 변경 이력" 창에서 **비활성화 메시지 전송**을 클릭하세요.

방문자 단말 삭제하기

더 이상 사용하지 않는 비활성 또는 활성화 금지 상태의 방문자 단말을 삭제할 수 있습니다 . 삭제하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 방문자**로 이동하세요.
2. **모바일ID**나 **모델명**을 입력하여 단말을 검색한 후 해당 단말을 클릭하세요.

3. 단말별로 을 클릭하거나, 체크박스를 선택한 후 목록 위의 을 클릭하세요.
   - 비활성, 활성화 금지 상태의 단말만 삭제 가능
4. 삭제 확인 팝업 메시지가 나타나면 **예**를 클릭하세요.

방문자 단말 조회하기

방문자 단말 목록에서 단말 정보를 확인할 수 있습니다. 방문자 단말 목록은 항목별로 필터를 적용하여 조회할 수 있습니다. 필터 적용시 상단에 이 보여지며, 클릭 시 적용된 필터는 초기화됩니다. 수퍼 운영자의 경우 단말 상세 정보도 조회할 수 있습니다.

방문자 단말 조회 항목의 내용은 다음과 같습니다.

항목		설명
상태	활성	단말의 EMM이 활성화되어 사용 중인 상태
	활성화 금지	• 비활성 상태의 단말이 활성화될 수 없도록 운영자가 직접 차단한 상태 • 단말 제어 명령을 전송할 수 없음
	시스템 차단	• 단말이 상태보고기한(KeepAlive)을 초과하거나 공장초기화되어 SYSTEM이 단말의 EMM 활성화를 차단한 상태 • 단말 제어 명령을 전송할 수 있음
	비활성	EMM을 통한 단말 제어가 불가능한 비활성 상태
	활성화 중	단말 등록이 정상적으로 이루어진 후 EMM 활성화 되기 전의 상태
	관리자 차단	• 사용자의 단말 분실이나 교체 시, 활성화 상태의 단말을 운영자가 관리 콘솔에서 차단한 상태 • 단말 제어 명령을 전송할 수 있음
플랫폼		단말의 플랫폼(Android, iOS) 표시
OS 버전		단말의 OS버전이 표시되며 단말 상태가 활성 또는 시스템 차단 상태가 아닌 경우 -로 표시
보안 준수	보안 준수	단말이 보안을 준수한 상태
	보안 위반	단말이 보안을 위반한 상태이며 클릭 시 “위반 내역 리스트” 창이 나타남

항목		설명
위변조	위변조 없음	수퍼운영자에게만 제공되는 기능으로 단말 OS 및 EMM 애플리케이션의 위변조 상태 표시
	위변조 있음	
단말 이력		수퍼운영자에게만 제공되는 기능으로 단말의 단말 제어 내역, Audit 로그, 보안 위반 이력이 나타남.
마지막 업데이트		날짜 클릭 시 단말 상태 변경 이력이 나타남

방문자 단말 관리 프로파일 조회하기

단말관리 프로파일을 조회하여 방문자 단말 적용 정책의 내용을 확인합니다 . 모든 방문자 단말에는 동일한 프로파일이 적용됩니다 .

방문자 프로파일에 적용되는 정책을 조회하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 방문자**로 이동하세요.
2. 을 클릭하세요.

방문자 단말 이력 조회하기

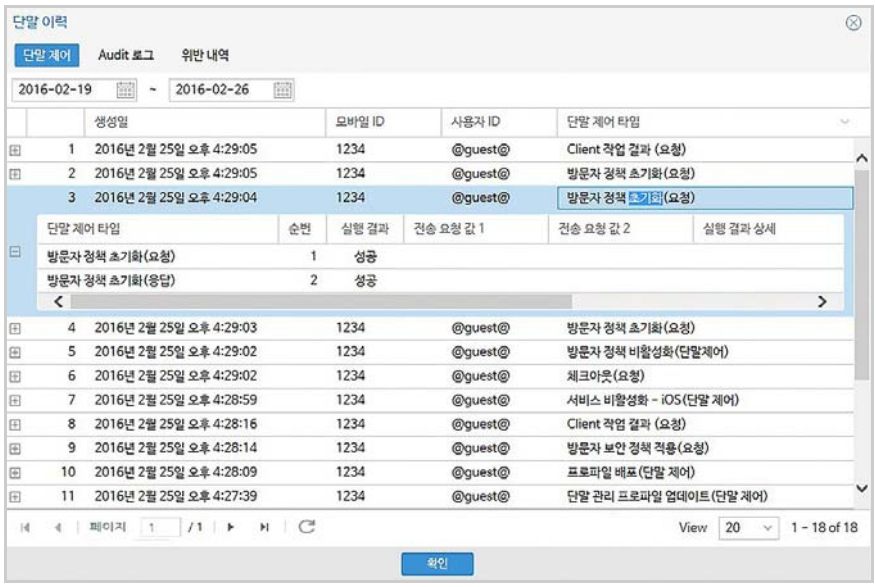
방문자 단말 목록에서 단말 제어 , Audit 로그 , 보안 위반 사항 등의 단말 정보 이력을 기간별로 조회할 수 있습니다 . 조회하려면 다음의 절차를 따르세요 .

Note: 수퍼 운영자에게만 제공되는 기능으로, 방문자 관리자는 조회할 수 없습니다.

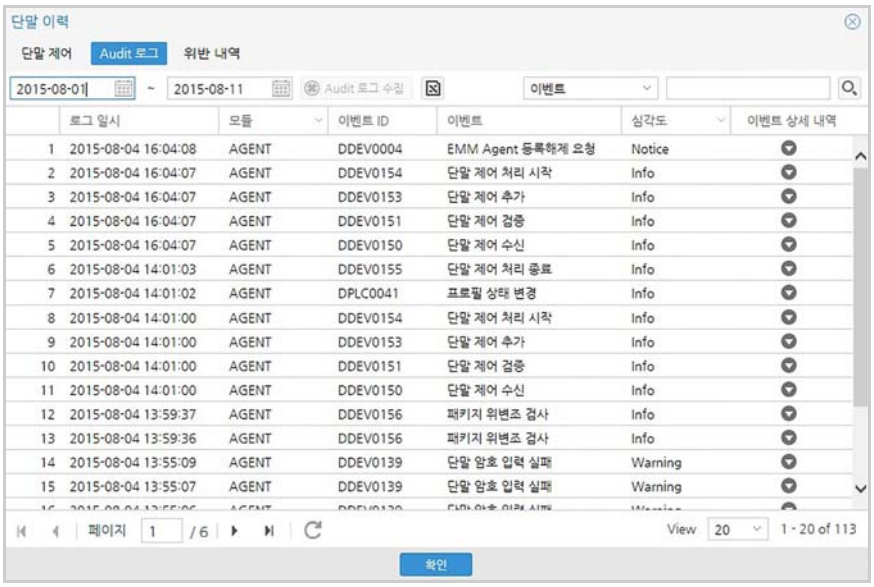
1. **단말 & 사용자 > 방문자**로 이동하세요.
2. **모바일 ID**, **모델명**을 입력 후 단말을 검색하세요.
   - 모델명 입력 시 Android는 모델명, iOS는 기종을 입력하세요.
3. **단말이력**을 클릭하세요.

4. "단말 이력"창에서 조회하고자 하는 탭을 클릭하세요.

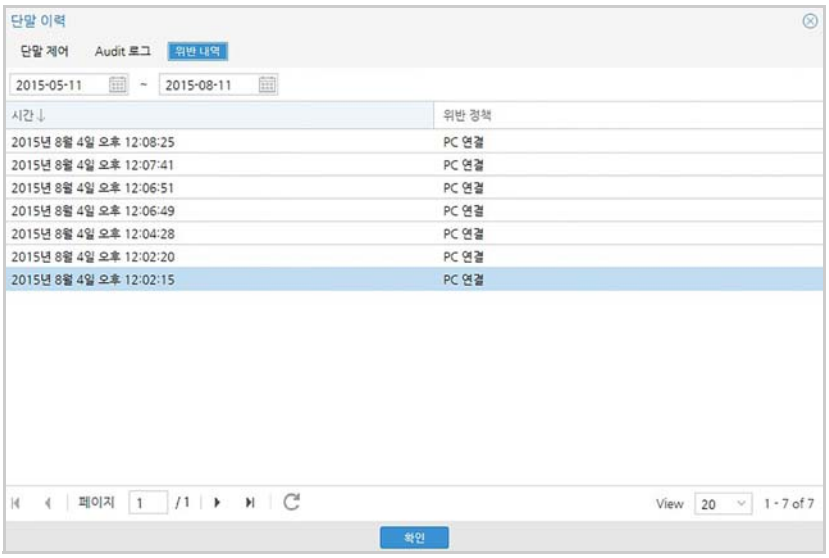
- **단말 제어** 탭



- **Audit 로그** 탭



- 위반 내역 탭



방문자 단말 제어하기

수퍼 운영자는 방문자 단말에 단말 제어 명령을 보낼 수 있습니다 . 방문자 단말제어 중에서 많이 사용하는 주요 단말 제어 명령은 플랫폼별로 다음과 같으며 , 단말 제어 시 별도로 분리되어 있어 빠르게 선택 가능합니다 . 단말 제어 방법에 대한 자세한 내용은 128 페이지 9 장의 " 단말 제어 명령 보내기 ", 431 페이지의 " 단말 제어 전송 방법 " 을 참고하세요 .

방문자 단말을 제어하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 방문자**로 이동하세요.
2. 제어할 단말을 선택 후, ⚙ 을 클릭하세요.
3. 단말 제어 명령을 선택 후 **확인**을 클릭하세요.
   - "단말 제어" 창의 Compliance 그룹에서 보안 정책 적용을 클릭하면, 프로파일과 앱 정보가 단말에 배포되며 방문자 단말이 제어됩니다.
   - 방문자 단말 제어 명령의 종류는 305페이지의 "방문자 단말 제어 명령"을 참고하세요.
4. **확인**을 클릭하세요.
5. 확인 팝업 메시지가 나타나면 **확인**을 클릭하세요.

방문자 단말 목록 다운로드하기

방문자 단말 목록을 CSV 형태의 파일로 다운로드할 수 있습니다 . 다운로드하려면 다음의 절차를 따르세요 .

1. **단말 & 사용자 > 방문자**로 이동하세요.
2. **모바일 ID**나 **모델명**을 입력하여 검색한 다음 화면 상단의 을 클릭하세요.
3. 엑셀 파일 작성 후 저장하세요.

19 Others

EMM 관리자 포털에서 사용되는 Audit 이벤트 , 프로파일 , 단말 제어 명령 등의 자세한 내용을 제공하며 , 원격 지원 , AppWrapper 등 지원되는 기타 서비스의 사용법을 설명합니다 .

Audit 이벤트 목록

다음은 EMM 의 단말 , 서버 , 관리자 포털 및 시스템에 관련한 Audit 이벤트 목록입니다 . 해당 이벤트와 관련하여 발생하는 로그 정보는 EMM 관리자 포털의 **서비스 현황 > 로그 > Audit 로그**에서 조회할 수 있습니다 . Audit 로그 관련 자세한 내용은 54 페이지 3 장의 “Audit 이벤트 " 를 참고하세요 .

단말 Audit 이벤트

이벤트 대상이 Device 이며 , 단말에 대해 정의된 Audit 이벤트 목록은 다음과 같습니다 .

이벤트 분류	이벤트
AppTunnel	AppTunnel Start AppTunnel Stop TLS 생성 TLS 형성 TLS 종료 TLS 형성 오류 CORRUPTION 검증 성공 CORRUPTION 검증 오류 키 생성 오류 암호화 오류 복호화 오류 서명 생성 오류 서명 검증 오류 CRL 요청 실패 다이제스트 검증 실패 허가되지 않은 데이터 수신 앱터널 서버와 Handshake 시작 앱터널 서버와 Handshake 성공 앱터널 서버와 Handshake 종료 앱터널 서버와 Handshake 에러
Certificate Status	인증서 발급 실패(키 생성 오류) 인증서 발급 실패(알 수 없음) BasicConstraints 체크 오류 Path 체크 오류 유효기간 체크 오류 CRL 체크 오류 인증서 검증 실패(알 수 없음) 인증서 발급 요청 인증서 발급 성공 인증서 발급 실패(파라미터 오류) 인증서 발급 실패(객체 초기화 오류) 인증서 발급 실패(내부 오류) 인증서 폐기 확인 연결 실패
Compliance	버전 제어 정책 위반 (단말) 녹음 방지 정책 위반 (단말) 시스템 위변조 검사

이벤트 분류	이벤트
Device	EMM 화면잠금 실패 (단말)
Device Command	KeepAlive 허용 시간 초과 KeepAlive 허용 시간 사용자 알림 단말 제어 수신 단말 제어 검증 단말 제어 추가 단말 제어 처리 시작 단말 제어 처리 종료 패키지 설치 실패 Knox 패키지 설치 실패 패키지 삭제 실패 Knox 패키지 삭제 실패 단말 진단 정보 단말 잠금/잠금해제 이력 Work Profile 패키지 설치 실패 Work Profile 패키지 삭제 실패 정책 위반 발생 정책 위반 종료 트리거 상태 변경 프로파일 변경
EMM Agent	단말 부팅 네트워크 연결 변경 Agent Context 변경 Agent 초기화
EMM Client	EMM 로그인 실패 EMM Client 화면잠금 해제 실패 EMM Client 로그인 실패 허용횟수 초과 EMM Client 화면잠금 해제 실패 허용 횟수 초과 EMM Client 화면잠금 비밀번호 변경
Enrollment	Push 등록 성공 Push 등록 해제 성공 EMM Agent 서비스 등록 시작 EMM Agent 서비스 등록 EMM Agent 서비스 해제 시작 EMM Agent 서비스 해제 Device Admin 활성화 Device Admin 비활성화 UMC Agent에 의한 서비스 등록 요청 ELM 라이선스 상태 변경 KLMS 라이선스 상태 변경
Kiosk Launcher	앱 설치 요청(Kiosk) 앱 목록 요청(Kiosk)
Logs	Audit 로그 기록 시작 서버로 Audit 로그 전송 EMM Agent 로그 전송
Profile	SIM 카드 PIN 코드 변경

이벤트 분류	이벤트
Profiles	단말 잠금 비밀번호 입력 허용 횟수 초과 스케줄러 작업 수행 KioskMode 적용 결과
User	지문 잠금 해제 사용 동의 (단말)

EMM 서버 Audit 이벤트

이벤트 대상이 Server 이며 , EMM 서버와 단말 같은 외부 요청 및 스케줄 작업에 대해 정의된 Audit 이벤트 목록은 다음과 같습니다 .

이벤트 분류	이벤트
AD/LDAP Sync	외부 동기화 작업 시작 외부 동기화 작업 종료 동기화 작업으로 사용자 추가 동기화 작업으로 사용자 수정 동기화 작업으로 사용자 삭제 동기화 대상 사용자 이지만 무시 동기화 대상 사용자 처리 중 오류 발생 동기화 작업으로 조직 추가 동기화 작업으로 조직 수정 동기화 작업으로 조직 삭제 동기화 대상 조직 이지만 무시 동기화 대상 조직 처리 중 오류 발생 동기화 작업 시작 동기화 작업 종료
Applications	앱 서비스 기간 만료에 따른 앱 상태 변경
Compliance	정책 위반 보고 KeepAlive Check 시작 KeepAlive Check 종료 KeepAlive Check 위반 건 처리 Check Point MTP 악성앱 진단 정보 단말상태 갱신 (System Block)
Device Command	최신 단말 관리 프로파일/앱 정보 배포 (단말제어 전송) 최신 단말 관리 프로파일 배포 (단말제어 전송) 사내 애플리케이션 최신 정보 배포 (단말제어 전송) 사용자 정의 이벤트 실행-설정 (단말제어 전송) 사용자 정의 이벤트 실행-해제 (단말제어 전송) 입출문 이벤트 실행-설정 (단말제어 전송) 입출문 이벤트 실행-해제 (단말제어 전송) Exchange 차단 해제-설정 (단말제어 전송)

이벤트 분류	이벤트
Device Command	Exchange 차단 해제-해제 (단말제어 전송) 앱 설치 (단말제어 전송) 앱 실행 (단말제어 전송) 앱 종료 (단말제어 전송) 앱 데이터 삭제 (단말제어 전송) 앱 삭제 (단말제어 전송) 앱 실행 허용/금지-허용 (단말제어 전송) 앱 실행 허용/금지-금지 (단말제어 전송) 단말 잠금/해제-잠금 (단말제어 전송) 단말 잠금/해제-해제 (단말제어 전송) 단말 잠금 비밀번호 초기화 (단말제어 전송) 공장 초기화 (단말제어 전송) 단말 전원 종료 (단말제어 전송) 단말 재부팅 (단말제어 전송) 외장 SD 카드 초기화 (단말제어 전송) CC모드 설정/해제-설정 (단말제어 전송) CC모드 설정/해제-해제 (단말제어 전송) 차단 정보 초기화 (단말제어 전송) 서비스 비활성화 (단말제어 전송) Audit 로그 수집-Agent (단말제어 전송) 로그 수집-Agent (단말제어 전송) 진단 정보 수집 (단말제어 전송) 라이선스 업데이트 (단말제어 전송) 시스템 앱 업데이트 (단말제어 전송) H/W 상태 (단말제어 전송) 설치된 앱 리스트 (단말제어 전송) 위치 (단말제어 전송) SIM 인증 (단말제어 전송) 상태 보고 (단말제어 전송) 컨테이너 잠금/해제-잠금 (단말제어 전송) 컨테이너 잠금/해제-해제 (단말제어 전송) 컨테이너 잠금 비밀번호 초기화 (단말제어 전송) 컨테이너 삭제 (단말제어 전송) 컨테이너 앱 설치 (단말제어 전송) 컨테이너 앱 실행 (단말제어 전송) 컨테이너 앱 종료 (단말제어 전송) 컨테이너 앱 데이터 삭제 (단말제어 전송) 컨테이너 앱 삭제 (단말제어 전송) 보안 정책 적용 (단말제어 전송) 최신 앱 관리 프로파일 배포 (단말제어 전송) 탈옥 여부 점검 (단말제어 전송) EMM Client 잠금 해제 (단말제어 전송) 메시지 전송 (단말제어 전송) 계정 삭제 (단말제어 전송) 화면 잠금 (단말제어 전송) Audit 로그 수집-Client (단말제어 전송) 로그 수집-Client (단말제어 전송) 진단 정보 수집 (단말제어 전송) 사용자 정보 업데이트 (단말제어 전송) 시스템 앱 업데이트 (단말제어 전송) 위치 (단말제어 전송) 보안 정책 적용 (단말제어 전송)

이벤트 분류	이벤트
Device Command	보안 정책 적용 비활성화 (단말제어 전송) 이벤트 정보 전송 (단말제어 전송) AndroidForWork 앱 설치 (단말제어 전송) AndroidForWork 앱 삭제 (단말제어 전송) 서비스 비활성화 (단말제어 전송) 프로그램 초대 (단말제어 전송) 앱 설치 여부 체크 (단말제어 전송) 시간 이벤트 실행-해제 (단말제어 전송) 시간 이벤트 실행-설정 (단말제어 전송) 서비스 활성화 실패 공지 (단말제어 전송) 방문자 정책 요청 활성화 요청 (단말제어 전송) 방문자 정책 요청 비활성화 (단말제어 전송) Agent 유효하지 않은 프로토콜 Agent 유효하지 않은 요청 Agent 단말 관리 프로파일 배포 요청 (단말->서버) Agent 단말 관리 프로파일 배포 응답 (서버->단말) Agent 이벤트 실행/해제 요청 (단말->서버) Agent 이벤트 실행/해제 응답 (서버->단말) Agent Exchange 차단 요청 (단말->서버) Agent Exchange 차단 응답 (서버->단말) Agent Exchange 차단 해제 요청 (단말->서버) Agent Exchange 차단 해제 응답 (서버->단말) Agent 앱 설치 요청 (단말->서버) Agent 앱 설치 응답 (서버->단말) Agent 앱 실행 요청 (단말->서버) Agent 앱 실행 응답 (서버->단말) Agent 앱 종료 요청 (단말->서버) Agent 앱 종료 응답 (서버->단말) Agent 앱 데이터 삭제 요청 (단말->서버) Agent 앱 데이터 삭제 응답 (서버->단말) Agent 앱 삭제 요청 (단말->서버) Agent 앱 삭제 응답 (서버->단말) Agent 앱 실행 허용 요청 (단말->서버) Agent 앱 실행 허용 응답 (서버->단말) Agent 앱 실행 금지 요청 (단말->서버) Agent 앱 실행 금지 응답 (서버->단말) Agent 단말 잠금 요청 (단말->서버) Agent 단말 잠금 응답 (서버->단말) Agent 단말 잠금 해제 요청 (단말->서버) Agent 단말 잠금 해제 응답 (서버->단말) Agent 단말 잠금 비밀번호 초기화 요청 (단말->서버) Agent 단말 잠금 비밀번호 초기화 응답 (서버->단말) Agent 공장 초기화 요청 (단말->서버) Agent 공장 초기화 응답 (서버->단말) Agent 단말 전원 종료 요청 (단말->서버) Agent 단말 전원 종료 응답 (서버->단말) Agent 단말 재부팅 요청 (단말->서버) Agent 단말 재부팅 응답 (서버->단말) Agent 외장 SD 카드 초기화 요청 (단말->서버) Agent 외장 SD 카드 초기화 응답 (서버->단말) Agent CC모드 설정 요청 (단말->서버) Agent CC모드 설정 응답 (서버->단말)

이벤트 분류	이벤트
Device Command	Agent CC모드 해제 요청 (단말->서버) Agent CC모드 해제 응답 (서버->단말) Agent 단말 정보 수집 요청 (단말->서버) Agent 단말 정보 수집 응답 (서버->단말) Agent 라이선스 업데이트 요청 (단말->서버) Agent 라이선스 업데이트 응답 (서버->단말) Agent 시스템 앱 업데이트 요청 (단말->서버) Agent 시스템 앱 업데이트 응답 (서버->단말) Agent SIM 인증 요청 (단말->서버) Agent SIM 인증 응답 (서버->단말) Agent 컨테이너 잠금 요청 (단말->서버) Agent 컨테이너 잠금 응답 (서버->단말) Agent 컨테이너 잠금 해제 요청 (단말->서버) Agent 컨테이너 잠금 해제 응답 (서버->단말) Agent 컨테이너 잠금 비밀번호 초기화 요청 (단말->서버) Agent 컨테이너 잠금 비밀번호 초기화 응답 (서버->단말) Agent 컨테이너 삭제 요청 (단말->서버) Agent 컨테이너 삭제 응답 (서버->단말) Agent 컨테이너 앱 설치 요청 (단말->서버) Agent 컨테이너 앱 설치 응답 (서버->단말) Agent 컨테이너 앱 실행 요청 (단말->서버) Agent 컨테이너 앱 실행 응답 (서버->단말) Agent 컨테이너 앱 종료 요청 (단말->서버) Agent 컨테이너 앱 종료 응답 (서버->단말) Agent 컨테이너 앱 데이터 삭제 요청 (단말->서버) Agent 컨테이너 앱 데이터 삭제 응답 (서버->단말) Agent 컨테이너 앱 삭제 요청 (단말->서버) Agent 컨테이너 앱 삭제 응답 (서버->단말) Agent 정책 위반 보고 요청 (단말->서버) Agent 정책 위반 보고 응답 (서버->단말) Agent 서비스 비활성화 코드 재발급 요청 (단말->서버) Agent 서비스 비활성화 코드 재발급 응답 (서버->단말) Agent Attestation Nonce 요청 (단말->서버) Agent Attestation Nonce 응답 (서버->단말) Agent Attestation 검증 요청 (단말->서버) Agent Attestation 검증 응답 (서버->단말) Agent 앱 정보 요청 (단말->서버) Agent 앱 정보 응답 (서버->단말) Agent Afw 앱 설치 요청 (단말->서버) Agent Afw 앱 설치 응답 (서버->단말) Agent Afw 앱 삭제 요청 (단말->서버) Agent Afw 앱 삭제 응답 (서버->단말) Agent 진단정보 수집 요청 (단말->서버) Agent 진단정보 수집 응답 (서버->단말) Agent 작업보고 요청 (단말->서버) Agent 작업보고 응답 (서버->단말) Agent 커맨드 요청 (단말->서버) Agent 프로파일 설치 (서버->단말) Agent 프로파일 삭제 (서버->단말) Agent 설치된 앱 정보 조회 (서버->단말) Agent 단말정보 조회 (서버->단말)

이벤트 분류	이벤트
Device Command	Agent 보안정보 조회 (서버->단말) Agent 단말잠금 (서버->단말) Agent 패스워드 초기화 (서버->단말) Agent 공장 초기화 (서버->단말) Agent 앱설치 (서버->단말) Agent MDM 설치 앱 정보 (서버->단말) Agent 앱삭제 (서버->단말) Agent 앱 속성정보 설정 (서버->단말) Agent 앱 설정정보 설정 (서버->단말) Agent MDM 설치 앱 설정 정보 (서버->단말) Agent MDM 설치 앱 속성 정보 (서버->단말) Agent MDM 설치 앱 설정 피드백 정보 (서버->단말) Agent 차단 정보 초기화 (서버->단말) Agent 상태 보고 (서버->단말) Agent 커맨드 응답 (서버->단말) Client Server Init 로직 수행 (단말->서버) Client 최신 앱 관리 프로파일 배포 요청 (단말->서버) Client 최신 앱 관리 프로파일 배포 응답 (서버->단말) Client 작업보고 요청 (단말->서버) Client 작업보고 응답 (서버->단말) Client 보안 정책 적용 활성화 요청 (단말->서버) Client 보안 정책 적용 활성화 응답 (서버->단말) Client 보안 정책 적용 비활성화 요청 (단말->서버) Client 보안 정책 적용 비활성화 응답 (서버->단말) Client 보안 정책 프로파일 삭제 요청 (단말->서버) Client 보안 정책 프로파일 삭제 응답 (서버->단말) Client 북마크 백업 요청 (단말->서버) Client 북마크 백업 응답 (서버->단말) Client 홈페이지 백업 요청 (단말->서버) Client 홈페이지 백업 응답 (서버->단말) Client 단말제어(EMM Agent) 전송 요청 요청 (단말->서버) Client 단말제어(EMM Agent) 전송 요청 응답 (서버->단말) 다중 단말 단말 제어 전송으로 처리 커맨드큐 삽입 커맨드큐 조회 커맨드큐 삭제 커맨드큐 업데이트 비활성화 커맨드로 인해 남은 커맨드 삭제 중복 커맨드 정책 위반 이력 삭제 (단말->서버) 정책 위반 이력 삭제 (서버->단말) Agent 커맨드 요청 (단말->서버) Agent 커맨드 요청 (서버->단말) Client 커맨드 요청 (단말->서버) Client 커맨드 요청 (서버->단말) 커스텀 단말제어 (단말제어 전송) 커맨드 요청 (단말->서버) 단말 관리 프로파일 배포 (서버->단말) 단말 정보 수집 (서버->단말) 단말 잠금 (서버->단말) 공장 초기화 (서버->단말)

이벤트 분류	이벤트
Device Command	커스텀 단말제어 (서버->단말) 커맨드 처리 응답 (단말->서버) SyncML Session 시작 (단말->서버) SyncML Session 종료 (서버->단말) Push(WNS PFN) 등록 (서버->단말) 단말/앱 정보 수집 (단말제어 전송) 단말 정보 수집 (단말제어 전송) 앱 정보 수집 (단말제어 전송) 위치 정보 수집 (단말제어 전송) Audit 정보 수집 (단말제어 전송) Log 정보 수집 (단말제어 전송) 다운로드 컨텐츠 (단말제어 전송) Fota 펌웨어 버전 업데이트 (단말제어 전송) Agent 단말/앱 정보 수집 요청 (단말->서버) Agent 단말/앱 정보 수집 응답 (서버->단말) Agent 단말 정보 수집 요청 (단말->서버) Agent 단말정보 수집 응답 (서버->단말) Agent 앱 정보 수집 요청 (단말->서버) Agent 앱 정보 수집 응답 (서버->단말) Agent 위치 정보 수집 요청 (단말->서버) Agent 위치 정보 수집 응답 (서버->단말) Agent Audit 정보 수집 요청 (단말->서버) Agent Audit 정보 수집 응답 (서버->단말) Agent 로그 정보 수집 요청 (단말->서버) Agent 로그 정보 수집 응답 (서버->단말) Agent 다운로드 컨텐츠 요청 (단말->서버) Agent 다운로드 컨텐츠 응답 (서버->단말) Agent Fota 펌웨어 버전 업데이트 요청 (단말->서버) Agent Fota 펌웨어 버전 업데이트 응답 (서버->단말) Agent 비활성화 상태 동기화 (서버->단말) MDM Agent 비활성화 (서버 -> 단말 동기화) Command Queue 소진(단말 제어 전송) 비활성화시 앱 자동 삭제 속성 동기화 요청 (단말->서버) 비활성화시 앱 자동 삭제 속성 동기화 응답 (서버->단말) 프로파일 삭제 요청 (단말->서버) 프로파일 삭제 응답 (서버->단말) 비활성화시 앱 자동 삭제 속성 동기화 (단말제어 전송) 사용자 정의 제어 요청 (단말->서버) 사용자 정의 제어 응답 (서버->단말) Agent 커맨드 응답 (서버->단말) 외장 SD 카드 인증 요청 (단말->서버) 외장 SD 카드 인증 응답 (서버->단말) 외장 SD 카드 인증 (단말제어 전송) 앱 삭제(MTP) 요청 (단말->서버) 앱 삭제(MTP) 응답 (서버->단말) 앱 삭제(MTP) (단말제어 전송) 사용자별 예외 정책-적용 사용자별 예외 정책-해제 시간 이벤트 수정 (단말제어 전송) 하나의 단말에 각 영역 별 단말 제어 전송

이벤트 분류	이벤트
Device Command	멀티 단말에 각 영역 별 단말 제어 전송 Smartkey 토큰 만료 갱신 요청 (단말->서버) Smartkey 토큰 만료 갱신 응답 (서버->단말) Smartkey 예약 정보 요청 (단말->서버) Smartkey 예약 정보 응답 (서버->단말) Smartkey 차량 정보 요청 (단말->서버) Smartkey 차량 정보 응답 (서버->단말) Smartkey 예약 가능 차량 정보 요청 (단말->서버) Smartkey 예약 가능 차량 정보 응답 (서버->단말) 차량 도어 잠금 요청 (단말 -> 서버) 차량 도어 잠금 응답 (서버 -> 단말) 차량 도어 잠금 해제 요청(단말->서버) 차량 도어 잠금 해제 응답(서버->단말) Smartkey 리포트 요청 (단말->서버) Smartkey 리포트 응답 (서버->단말) Smartkey 토큰 만료로 갱신 요청 (단말->서버) Smartkey 토큰 만료로 갱신 응답 (서버->단말) Smartkey 커맨드 요청 (단말->서버) Smartkey 커맨드 응답 (서버->단말) Smartkey 서비스 비활성화 요청 (단말->서버) Smartkey 서비스 비활성화 응답 (서버->단말) 서비스 비활성화(단말제어 전송) 서비스 비활성화 요청(서버->단말) 서비스 비활성화 응답(단말->서버) SmartKey 토큰 갱신 요청(서버->단말) SmartKey 토큰 갱신 응답(단말->서버) SmartKey 토큰 삭제 요청(서버->단말) SmartKey 토큰 삭제 응답(단말->서버) 차량 정보 수집(단말제어 전송) 차량 정보 수집 요청(서버->단말) 차량 정보 수집 응답(단말->서버) 차량 도어 잠금(단말제어 전송) 차량 도어 잠금 요청(서버->단말) 차량 도어 잠금 응답(단말->서버) 차량 도어 잠금 해제(단말제어 전송) 차량 도어 잠금 해제 요청(서버->단말) 차량 도어 잠금 해제 응답(단말->서버) Client 정책 요약 요청 (단말->서버) Client 정책 요약 응답 (서버->단말) EMM Client 정보 수집(서버 → 단말) Agent 사용자 정보 갱신(서버 → 단말) Agent 단말 제어 수행 실패 클라이언트 단말 제어 수행 실패 Agent 단말 제어 수행 성공 클라이언트 단말 제어 수행 성공

이벤트 분류	이벤트
E-FOTA	E-FOTA API - Token 얻기 E-FOTA API - CorpID 등록 E-FOTA API - 펌웨어 리스트 조회 E-FOTA API - 펌웨어 제한 E-FOTA API- 그룹버전 현황 조회 E-FOTA API- 제품, 모델 및 통신사 조회 E-FOTA API- 네트워크 오류 E-FOTA API - License 정보 얻기
Email	사용자 메일 전송 단말 메일 전송 관리자 메일 전송 관리자 SMS 전송
	재활성화 방지 (단말->서버) 재활성화 방지 (서버->단말) EMM Enrollment Spec(단말->서버) EMM Enrollment Spec(서버->단말) 활성화 중 KLM/ELM 라이선스 업데이트(단말->서버) 활성화 중 KLM/ELM 라이선스 업데이트(서버->단말) EMM Enrollment(단말->서버) EMM Enrollment(서버->단말) 서비스 비활성화 - Android(단말->서버) 서비스 비활성화 - Android(서버->단말) Enrollment(Knox) 확인 (단말->서버) Enrollment(Knox) 확인 (서버->단말) Agent MDM 활성화 요청 (단말->서버) Agent MDM 활성화 요청 (서버->단말) Agent SCEP 프로파일 요청 (단말->서버) Agent SCEP 프로파일 요청 (서버->단말) Agent MDM 프로파일 요청 (단말->서버) Agent MDM 프로파일 요청 (서버->단말) Agent 체크인 요청 (단말->서버) Agent 체크인 요청 (서버->단말) Agent 토큰 업데이트 요청 (단말->서버) Agent 토큰 업데이트 요청 (서버->단말) Agent 체크아웃 요청 (단말->서버) Agent 체크아웃 요청 (서버->단말) 서비스 비활성화 (단말->서버) 서비스 비활성화 (서버->단말) 요청 SOAP 메시지 (단말->서버) 응답 SOAP 메시지 (서버->단말) Discovery URL 요청 (단말->서버) Discovery URL 응답 (서버->단말) 인증서 발급 스펙 요청 (단말->서버) 인증서 발급 스펙 응답 (서버->단말) On-premis 기기 인증 요청 (단말->서버) On-premis 기기 인증 응답 (서버->단말) Federated 기기 인증 요청 (단말->서버) Federated 기기 인증 응답 (서버->단말)

이벤트 분류	이벤트
Enrollment	Security Token 검증 인증서 발급 요청 (단말->서버) 인증서 발급 응답 (서버->단말) DM Client 설정 응답 OTP Code 발급
Enrollment	서비스 비활성화 - Tizen(단말->서버) 서비스 비활성화 - Tizen(서버->단말) UMC 사용자 검색 요청 UMC 사용자 검색 응답 UMC Enrollment 요청 UMC Enrollment 응답 UMC Enrollment 정보 갱신 요청 UMC Enrollment 정보 갱신 응답 UMC Unenrollment 요청 UMC Unenrollment 응답
Exception Profile per User	사용자별 예외 정책 스케줄러 시작 사용자별 예외 정책 스케줄러 종료
InventoryScheduler	iOS Inventory 수집 스케줄러 시작 iOS Inventory 수집 스케줄러 종료
License Management	Knox License 추가 Knox License 수정 Knox License 삭제 Knox License 동기화 Knox License SLM 인터페이스
Logs	Audit 로그 외부 전송 Audit 원격로그서버 접속 오류
Profiles	Agent 단말 정책 적용 결과 Agent 단말 정책 적용 성공 Agent 단말 정책 적용 실패 프로파일 업데이트 시작 프로파일 업데이트 종료
Provision	공개키 요청 프로비저닝 활성화 프로비저닝 비활성화 Knox 프로비저닝 활성화 단말 상태를 Provisioned 상태로 변경 요청 단말 상태를 Inactivated 상태로 변경 요청 사용자당 단말 수 초과
SEG Profile	SEG 프로파일 자동 생성 SEG 프로파일 자동 삭제 SEG 프로파일 자동 갱신 SEG Rest API 요청 SEG Rest API 응답
Service Profiles	사용자 동의서 다운로드 서비스 프로파일 다운로드

이벤트 분류	이벤트
SmartKey	SmartKey 예약 정보 생성 SmartKey 예약 정보 수정 SmartKey 예약 정보 삭제
SMS	사용자 SMS 전송 단말 SMS 전송
Time Trigger	서버 기동 시 Time Trigger 등록 시작 서버 기동 시 Time Trigger 등록 종료 Time Trigger 동기화 시작 Time Trigger 동기화 종료
TxHistory	전송 이력 순번 에러
User Login	사용자 인증 실패 사용자 계정 로그인 사용자 계정 로그아웃

관리자 포털 Audit 이벤트

이벤트 대상이 Console 이며 , 관리자 포털에 대해 정의된 Audit 이벤트 목록은 다음과 같습니다 .

이벤트 분류	이벤트
AD/LDAP Sync	기 생성된 동기화 서비스 설정 삭제 새로운 동기화 서비스 설정 추가 기 생성된 동기화 서비스 설정 갱신 동기화된 대상(사용자/조직) 동기화 정보 삭제 동기화된 대상(사용자/조직) 동기화 정보 추가 동기화된 대상(사용자/조직) 동기화 정보 갱신 동기화 예외 대상(사용자/조직) 삭제 동기화 예외 대상(사용자/조직) 추가 동기화 예외 대상(사용자/조직) 복원 동기화 서비스 예약 상태 변경 기 생성된 동기화 서비스 다중 삭제 기 생성된 동기화 서비스 삭제 기 생성된 동기화 서비스 맵핑 정보 삭제 새로운 동기화 서비스 추가 새로운 동기화 서비스 맵핑 정보 추가 동기화 서비스 바로 실행 동기화 서비스 수정 단일 아이템(사용자/조직) 동기화 수행 동기화 테스트 수행 기 생성된 동기화 서비스 삭제 새로운 동기화 서비스 추가 동기화 서비스 수정 동기화된 객체 정보 기록 진행된 동기화 서비스 정보 기록 동기화 대상 개수 확인 외부 동기화 서비스 생성 외부 동기화 서비스 수정 외부 동기화 서비스 삭제 외부 동기화 서비스 상태 변경 외부 동기화 서비스 검색 외부 동기화 서비스 목록 검색 OAuth 토큰 발급 요청 외부 동기화 맵핑 설정 검색 외부 동기화 객체 속성 검색
Admin Login	관리자 계정 로그인 관리자 계정 로그아웃 관리자 계정 세션 시간초과로 인해 로그아웃 계정 잠금 계정 삭제 10분간 계정 차단

이벤트 분류	이벤트
Administrators	운영자 정보 수정 운영자 삭제 운영자 상태(활성/비활성) 변경 운영자 계정 생성 계정 생성 직후 또는 비밀번호를 재설정 한 후 비밀번호 수정 혹은 로그인 폼에서 자신의 비밀번호 수정 운영자 관리 화면에서 운영자의 비밀번호 수정 운영자 계정 생성 시, 운영자 환경 설정 정보가 시스템 초기값으로 자동 생성 운영자 환경설정 값 수정 운영자 환경설정 값 삭제 로그인 시에만 이벤트 발생. 운영자 환경설정 값 수정 해당 운영자의 super 유형 여부 확인 운영자 조직 추가 운영자 조직 추가(through organization) Public Push 수정 로그레벨 수정 구글계정 수정 기술 지원 활성화 및 기간 설정
Alerts	관리자별 알림 설정 삭제 관리자별 알림 설정 추가 관리자별 알림 설정 수정 알림 대상 Audit 이벤트 일괄 수정 알림 대상 Audit 이벤트 초기화 임의의 알림 생성(테스트 목적) 알림 대상 Audit 삭제 알림 대상 Audit 추가 알림 대상 Audit 수정

이벤트 분류	이벤트
Applications	구글 계정 추가/수정 앱 추가 시 다국어 정보 입력 앱 수정 시 다국어 정보 수정 사내 앱 상태 변경 사내 앱 삭제 사내 앱 삭제 사내 앱 추가 사내/외부 앱의 카테고리 변경 사내 앱 수정 사내 앱 물리 파일 등록 사내 앱 아이콘 등록 사내 앱 스크린샷 등록 시스템 앱 삭제 시스템 앱 추가 시스템 앱 수정 시스템 앱 물리 파일 등록 카테고리 다국어 정보 추가 카테고리 다국어 정보 업데이트 카테고리 삭제 카테고리 추가 카테고리 수정 카테고리 순서변경 외부 앱 삭제 외부 앱 추가

이벤트 분류	이벤트
Applications	외부 앱 수정 시스템 앱 물리 파일 삭제 사내 앱 물리 파일 삭제 제어 앱 생성 Kiosk 앱 삭제 Kiosk 앱 추가 Kiosk 앱 물리파일 등록 제어 앱 삭제 제어 앱 추가 제어 앱 수정 외부 앱 Sync 카테고리 임시 ID 생성 앱 후기 삭제 앱 다운로드 목록 생성(엑셀) 키오스크 앱 파일 삭제 키오스크 앱 임시 파일 삭제 키오스크 앱 임시 ID 생성 키오스크 앱 수정 앱 임시 파일 삭제 앱 임시 ID 생성 컨트롤 앱 업로드 외부 앱 임시 ID 생성 구글 계정 유효성 확인 타 테넌트의 EMM 앱을 등록 시스템 앱 임시 파일 삭제 시스템 앱 임시 ID 생성 앱 버전 수정 앱 버전 이력 수정 키오스크 위저드 앱 임시 ID 생성 키오스크 위저드 앱 추가 키오스크 위저드 앱 수정 컨텐츠파일 삭제 이벤트 컨텐츠파일 등록 이벤트 Kiosk 이미지 파일 삭제 이벤트 컨텐츠파일수정
Certificates	인증서 프로파일 템플릿 등록 인증서 프로파일 템플릿 수정 인증서 프로파일 템플릿 삭제 인증서 폐기 인증서 발행 CA 등록 이벤트 CA 수정 이벤트 CA 삭제 이벤트 ExternalCert 등록 이벤트 ExternalCert 수정 이벤트 ExternalCert 삭제 이벤트 APNS 수정 이벤트 ExternalCert 수정 이벤트(파일)

이벤트 분류	이벤트
Certificates	인증서 발급 이벤트 인증서 재발급 이벤트 인증서 갱신 이벤트 키 생성 오류 인증서 발급 요청 이벤트 인증서 재발급 요청 이벤트 인증서 갱신 요청 이벤트 CA 등록 이벤트 (insertCa) CA 수정 이벤트 (updateCa) CA 삭제 이벤트 (deleteCa) 인증서 프로파일 템플릿 등록 인증서 프로파일 템플릿 수정 인증서 프로파일 템플릿 삭제 iOS 인증서 삭제 상태로 변경 CA 등록 이벤트 (insertCaSCEP) CA 수정 이벤트 (updateCaSCEP) CA 등록 이벤트 (insertCaCertAgent) CA 수정 이벤트 (updateCaCertAgent) CA 등록 이벤트 (insertCaEST) CA 수정 이벤트 (updateCaEST)
Connectors	SAP 커넥터 수정 SAP 커넥터 추가 SAP 커넥터 서비스 메타데이터 추가 SAP 커넥터 서비스 필드 추가 SAP 커넥터 삭제 DB 커넥터 수정 DB 커넥터 삭제 DB 커넥터 추가 DB 커넥터 서비스 필드 추가 DB 커넥터 서비스 메타데이터 추가 DB 커넥터 XML 형식으로 출력 추가 REST 커넥터 추가 REST 커넥터 수정 REST 커넥터 삭제 WS 커넥터 추가 WS 커넥터 수정 WS 커넥터 삭제 MQ 커넥터 추가 MQ 커넥터 수정 MQ 커넥터 삭제 MQ 커넥터 목록 삭제 FTP 커넥터 수정 FTP 커넥터 삭제 FTP 커넥터 추가 FTP 커넥터 목록 삭제 서비스 관리 추가 서비스 관리 수정 서비스 관리 삭제 서비스 로그 설정 값 수정

이벤트 분류	이벤트
Connectors	서비스 관리 시간 추가 서비스 관리 시간 수정 서비스 관리 시간 삭제 서비스 그룹 삭제 서비스 그룹 추가 서비스 그룹 수정 서비스 Role Map 추가 서비스 Role Map 삭제 서비스 권한 수정 Role 추가 Role 수정 Role 삭제 디렉토리 서비스 삭제 디렉토리 서비스에서 설정한 리턴데이터 맵핑 정보 삭제 새로운 디렉토리 서비스 저장 디렉토리 서비스에서 설정한 리턴데이터 맵핑 정보 추가 기 생성된 디렉토리 서비스 갱신
Dashboard	보고서 조건 추가 보고서 조건 수정 보고서 조건 삭제 보고서 쿼리 필드 추가 보고서 쿼리 필드 삭제 보고서 쿼리 추가 보고서 쿼리 수정 보고서 쿼리 삭제 보고서 조건 추가 보고서 조건 수정 보고서 조건 삭제 보고서 상태 변경 보고서 결과값 다운로드 보고서 차트 다운로드 보고서 조건 추가 보고서 삭제 보고서 추가 보고서 수정 대시보드 추가 대시보드 수정 대시보드 삭제 대시보드 상태 변경 대시보드 메인 페이지 변경 대시보드 메인 페이지 초기화
Device Command	사용자&조직, 그룹 메뉴에서 단말 제어를 여러 단말에 전송 시도 단말 상세 메뉴에서 단말 제어를 하나의 단말에 전송 시도 방문자 프로파일 업데이트 단말제어 전송 시도 단말 제어 팝업에서 단말 제어를 여러 단말에 전송 시도 단말 제어 팝업에서 단말 제어를 하나의 단말에 전송 시도 사용자 포탈에서 자신의 단말에 단말 제어를 전송 시도

이벤트 분류	이벤트
Devices	단말 삭제 단말 등록 단말상태 갱신 단말 목록 다운로드 단말 상태 초기화 단말 목록 수정 단말 비활성화 방문자 리스트 다운로드 방문자 비활성화코드 SMS 전송 단말 로그 다운로드 단말 로그 파일 삭제 단말 로그 파일 다운로드 단말 로그 파일 제거 단말 로그 파일 수정 앱 목록 다운로드 KEM 단말 목록 다운로드 단말 위치 조회 사용자&그룹의 단말 위치 조회 단말 라이선스 업데이트 단말 라이선스 조회 대시보드에서 단말 위치 조회
E-FOTA	E-FOTA 그룹 생성 E-FOTA 그룹 삭제 E-FOTA CorpID 등록 E-FOTA 펌웨어 제한 E-FOTA 그룹 수정 E-FOTA 그룹 존재 여부 확인 E-FOTA 라이선스 정보 얻기 E-FOTA 라이선스 정보 얻기 (환경설정) E-FOTA 설정 저장 E-FOTA 유효 라이선스 확인 E-FOTA 라이선스 업데이트
Email	사용자 메일 전송 SMTP 설정 메일 템플릿 추가 메일 템플릿 삭제 메일 템플릿 수정 Tizen 설치정보 전송 사용자 SMS 전송

이벤트 분류	이벤트
Groups	그룹 내 구성요소(단말/사용자) 삭제 그룹 내 구성요소(단말/사용자) 추가 그룹 내 강제 추가/제외 요소(단말/사용자) 삭제 그룹 내 강제 추가/제외 요소(단말/사용자) 추가 그룹 내 선택한 필터 정보 삭제 그룹 내 선택한 필터 정보 추가 그룹 내 선택한 필터 정보 삭제 그룹 내 선택한 필터 정보 추가 기 생성된 그룹 삭제 새로운 그룹 추가 기 생성된 그룹 정보 업데이트 단말 그룹 구성요소(단말/사용자) 삭제 단말 그룹 구성요소(단말/사용자) 추가 동기화 실행
Integrations	JCO Pool 재 시작 JCO Pool 추가 JCO Pool 수정 JCO Pool 삭제 DB 연결 추가 DB 연결 수정 DB 연결 삭제 DB 연결 목록 삭제 DB 상태 테스트 모든 DB 상태 테스트 MQ 연결 추가 MQ 연결 수정 MQ 연결 삭제 MQ 연결 목록 삭제 FTP 연결 수정 FTP 연결 삭제 FTP 연결 추가 FTP 연결 목록 삭제 디렉토리 연결 정보 삭제 새로운 디렉토리 연결 정보 저장 기 생성된 디렉토리 연결 정보 갱신
Logs	Audit 이벤트 다운로드 단말 Audit 로그 다운로드 Audit 로그 다운로드 Audit 설정 변경 Audit 대상 유무 수정 단말진단정보 다운로드 Audit 저장소 추가 Audit 저장소 수정 Audit 저장소 삭제
Notices	공지사항 삭제 공지사항 추가 공지사항 수정 공지사항 다국어 정보 추가 공지사항 다국어 정보 수정

이벤트 분류	이벤트
Organization	기 생성된 조직 삭제 새로운 조직을 조직도에 추가 기 생성된 조직 정보를 업데이트 조직 내 그룹원의 소속 조직 정보를 갱신
Profiles	General 설정 값 저장 Knox 설정 값 저장 General 설정 값 삭제 Knox 설정 값 삭제 Knox 생성 Knox 삭제 클라이언트 앱 제어 정책 저장 클라이언트 브라우저 정책 저장 클라이언트 정책 저장 General 정책 저장 Knox 정책 저장 Trigger General 정책 저장 Trigger Knox 정책 저장 클라이언트 앱 제어 정책 삭제 EMM 프로파일을 그룹에 할당 EMM 프로파일을 조직에 할당 EMM Agent의 프로파일 생성 EMM Agent의 프로파일 삭제 Trigger 생성 Trigger 삭제 앱관리 프로파일 생성 앱관리 프로파일 삭제 앱관리 프로파일 내보내기 앱관리 프로파일 불러오기 앱관리 프로파일 수정 Knox 기본정보 수정 M메일 정책 저장 내방객 정책 저장 프로파일의 그룹 할당 정보 저장 프로파일의 조직 할당 정보 저장 단말 관리 프로파일 내보내기 단말 관리 프로파일 불러오기 단말 관리 프로파일 수정 이벤트 정책 우선순위 수정 이벤트 정책 기본 정보 수정 이벤트 정책 우선순위 변경 Pool에서 프로파일 설정 선택 Pool에서 Knox 설정 선택 파일 Upload Knox 컨테이너 Pool 생성 Knox 컨테이너 Pool 삭제 Android for Work 정책 생성 Android for Work App 정책 생성 Android for Work App 정책 복수 생성 Secu카메라 정책 생성 Knox portal 정책 생성 Winodws 일반 정책 생성

이벤트 분류	이벤트
Profiles	Pool에서 정책 선택 Winodws 이벤트 정책 생성 Android for Work App 정책 삭제 사용자별 예외 정책 우선순위 수정 사용자별 예외 정책 삭제 사용자별 예외 정책 추가 사용자별 예외 정책 수정 Pool 삭제 Pool에서 이벤트 정책 선택 단말 전송 미처리 Queue 재전송 요청 단말 전송 미처리 건 삭제 정책 저장 단말관리 프로파일 생성(빠른시작) 앱관리 프로파일 생성(빠른시작) 프로파일 사용자 그룹 할당(빠른시작) SmartKey MQTT 서버 전체 시작 SmartKey MQTT 서버 전체 종료 SmartKey MQTT 서버 개별 시작 SmartKey MQTT 서버 개별 종료 SmartKey 차량 예약 정보 삭제 SmartKey 차량 예약 정보 상세 삭제 프로파일 정책 조회 프로파일 정책 저장 프로파일 업데이트 스케줄 저장 프로파일 업데이트 단말제어 전송 요청
SEG Profile	SEG 프로파일 추가 SEG 프로파일 추가 SEG 프로파일 목록 조회 SEG 프로파일 상세 정보 조회 SEG 서버프로파일 상세 정보 조회 SEG 프로파일 대상 Tenant 정보 조회 SEG Domain 정보 조회
Service Profiles	서비스 프로파일 기본 수정 서비스 프로파일 수정

이벤트 분류	이벤트
Settings	API 사용자 활성화 API 사용자 비활성화 API 사용자 삭제 API 사용자 추가 API 사용자 토큰 무효화 API 사용자 수정 태블릿 모델 삭제 태블릿 모델 추가 태블릿 모델 수정 Cloud Connector 생성 요청 Cloud Connector 확정 요청 Cloud Connector 삭제 요청 APNs 인증서 발급요청(CSR) 다운로드 APNs 인증서 업로드 APNs 인증서 다운로드 APNs 인증서 가져오기 마스터 데이터 추가 마스터 데이터 수정 마스터 데이터 삭제
SMS	SMS 환경 설정 변경
System Configuration	인증 설정 변경 서버 설정 수정 로그인/헤더 이미지 변경 로고/알림메시지 변경 서버 설정 수정 사용자 동의서 수정

이벤트 분류	이벤트
User Management	사용자 권한을 수정 사용자 권한을 삭제 사용자 권한을 생성 사용자 단말 브라우저의 북마크 정보 삭제 사용자 단말 브라우저의 북마크 정보 삽입 사용자 단말 브라우저의 북마크 정보 삽입 사용자 단말 브라우저의 북마크 정보 수정 사용자 단말 브라우저의 북마크 정보 수정 사용자 비활성화 사용자 삭제 사용자 생성 사용자 정보 수정 사용자가 자신의 비밀번호를 초기화 운영자가 사용자 비밀번호를 업데이트 사용자 비밀번호 확인 사용자 활성화 사용자와 단말 정보 엑셀 업로드 모바일 메일 상태값 수정 보안 카메라 상태값 수정 다중 사용자 등록패스워드 초기화 동기화 사용자 등록
Windows	Configuration Service Provider 삭제 Configuration Service Provider 추가 Configuration Service Provider 수정 PPKG File 삭제 PPKG File 추가 PPKG File 수정

시스템 Audit 이벤트

이벤트 대상이 System 이며 , 시스템에 대해 정의된 Audit 이벤트 목록은 다음과 같습니다 .

이벤트 분류	이벤트
Cryptographic Support	암호화 지원 실패 Key zeroization process 실패 Key generation activity 실패 암호화 서명 실패 비 데이터 무결성을 위한 해싱 암호화 실패 암호화 또는 암호 해독 실패 Hashing function 실패 Randomization process 실패
EMM System	EMM Server 시작 EMM Server 정지 EMM Server Update 파일 목록 Server 인증서 만료 Server 인증서 폐기 새로운 파일 생성 기존 파일 삭제 기존 파일 수정 기존 파일 이름 재정의 무결성 오류 인증되지 않은 패키지 패키지 무결성 성공 암호화 모듈 자체 테스트 MDM 스케줄러 모니터 시작 MDM 스케줄러 모니터 종료
InventoryScheduler	InventoryScheduler 모니터링 시작 InventoryScheduler 모니터링 종료
Logs	Audit 로그 기록 시작 Audit 로그 기록 종료
Push	PUSH SA 등록 요청(EMM Server->Push SA) PUSH SA 등록 응답(Push SA -> EMM Server) PUSH Device 인증 요청(Push SA -> EMM Server)

Audit 이벤트 조회 항목

단말 및 EMM 서버에서 발생되는 Audit 이벤트는 관리자 포털에서 조회할 수 있으며 , 조회된 결과를 엑셀로 저장할 수 있습니다 . Audit 이벤트 항목의 설명은 다음과 같습니다 .

항목	설명
로그 일시	Audit 로그가 발생한 일시입니다.
대상	이벤트 발생 대상을 선택합니다. • Console: 관리자 포털에 대한 Audit 이벤트 • Server: EMM 서버와 단말 같은 외부 요청 및 스케줄 작업에 대한 Audit 이벤트 • Device: 사용자 단말에 대한 Audit 이벤트 • System : EMM 서버 이벤트 중 EMM 서버 기동,단말 정보 수집등 시스템에 대한 Audit 이벤트
사용자 ID	이벤트 작업 대상에 따른 관리자 ID입니다. • Console 인 경우: admin 또는 사용자 ID • Server 인 경우 : 단말에서 EMM 서버로 이벤트 요청 시 단말 사용자이고 , 스케줄 작업인 경우 System 또는 Batch user ID • Device 인 경우 : 단말 사용자 ID
단말 ID	단말 제어에 관한 Audit 이벤트경우, 이벤트 작업 대상에 따른 모바일 ID 입니다. • Console 인 경우: 단말 제어 Audit 로그 수집 할 모바일 ID • Server 인 경우 : 단말에서 EMM 서버로 이벤트 요청 시 단말의 모바일 ID 이고, 단말에 대한 스케줄 작업인 경우 해당 단말의 모바일 ID 또는 Batch user • Device 인 경우 : 단말 모바일 ID
접속 IP	관리자 포털을 접속한 IP 주소입니다.
이벤트 ID	이벤트 ID
이벤트 분류	이벤트 분류 목록은 314페이지 18장의 “Audit 이벤트 목록"를 참고하세요.
이벤트	발생된 이벤트 정보입니다
결과	발생된 이벤트의 실행 결과 정보입니다.
레벨	발생된 이벤트의 심각도를 표시합니다. • Critical: 시스템 중단 등의 심각한 오류 발생에 대한 이벤트 • Error: 일반적인 오류 이벤트 • Warning: 오류는 아니지만 주의가 필요한 이벤트 • Notice: 알림이 필요한 이벤트 • Info: 관리자에게 필요한 일반적인 이벤트 • Debug: 개발자에게 필요한 상세하게 정의된 이벤트
요청내역	Audit 이벤트를 요청한 상세 내역 정보입니다. 예를 들면 "Save General Policy" 이벤트의 경우 프로파일에 변경이 발생하여 반영되어야하는 전체 정책이 조회됩니다.
결과 코드	성공 또는 실패로 표시되며 이벤트의 결과를 조회합니다.

항목	설명
결과 내역	Audit 이벤트별 결과 내역 정보입니다. 예를 들면 "패키지 삭제 실패" 이벤트의 경우 삭제 실패된 packagename과 원인이 조회됩니다.
작업 Data	이벤트 대상 및 이벤트 항목이 다음과 같은 경우 작업 Data 정보를 확인할 수 있습니다. • 이벤트 대상 Console인 경우 : 단말에서 EMM서버로 4000byte이상의 데이터를 보낼시 • 이벤트 대상 Server인 경우: - 이벤트 분류: Device command - 이벤트: Agent 단말 잠금 요청 (단말->서버) 또는 Agent 단말 잠금 해제 요청 (단말->서버) 또는 Agent 작업보고 요청 (단말->서버) • 이벤드 대상 Device 인 경우: - 이벤트 분류: Device command - 이벤트: 단말 진단 정보 또는 단말 잠금/잠금해제 이력

Push의 Audit 로그

Push 서버에서 발생되는 Audit 이벤트는 각 서버에 로그 파일로 기록됩니다 . 기록된 Audit 로그는 EMM 관리자 포털 또는 시스템 로그를 통해 내보낼 수 없습니다 . Push 서버의 Windows 플랫폼에 RDP 로 접속하여 Audit 파일을 내보내기합니다 . 해당 서버에 원격 접속을 하여 아래 폴더에 생성된 Audit 로그 파일을 확인합니다 . Audit 로그를 확인하려면 해당 서버에 원격 접속을 하여 아래 폴더에 생성된 파일을 확인합니다 .

- `Push Proxy: {Proxy_HOME}/LOGS/audit/*`
- `Push CM: {Push_HOME}/LOGS/audit/*`
- `Push SA: {EMM_HOME}/log/push/audit/*`
- `Push SA: {EMM_HOME}/log/push/audit/*`

Push와 AppTunnel Audit 이벤트

Push 서버의 Audit 이벤트 로그는 다음과 같습니다 . 로그 타입별 항목은 342 페이지의 " 상세 로깅 항목 " 참고하세요 .

서버	로그 타입
Push	STARTUP SHUTDOWN TLS_HANDSHAKE_START TLS_HANDSHAKE_COMPLETED TLS-TERMINATED TLS_HANDSHAKE_ERROR CORRUPTION_CHECK_FAIL KEY_GENERATION_FAIL ENCRYPT_FAIL DECRYPT_FAIL MAKE_SIGNATURE_FAIL VERIFY_SIGNATURE_FAIL DIGEST_FAIL CERT_EXCEPTION RANDOM_FAIL CRYPTOJ_SELFTEST_START CRYPTOJ_SELFTEST_FINISHED CRYPTOJ_SELFTEST_PASSED CRYPTOJ_SELFTEST_FAILED CRYPTOJ_SELFTEST_FORCED_TO_FAIL

Audit 이벤트 로그 항목

Push 서버의 Audit 로깅 상세 내용은 다음과 같습니다 .

항목	설명
로그 일시	Audit 이벤트가 발생한 일시입니다.
클래스	Audit 이벤트 로그의 클래스 정보입니다. 기본값은 'INFO [c.s.p.l.a.i.ServerAuditLogger:60]' 입니다.
이벤트	Push서버에서 발생한 Audit 로그 이벤트입니다. 자세한 사항은 341페이지의 "Push와 AppTunnel Audit 이벤트"참고하세요.
소스 타입	Push서버 로그 대상 정보입니다. • PUSH-DA, PUSH-SERVER, PUSH-SA.
초기 설정값	Push서버의 InstanceID 값과 PkiMode 사용 여부를 설정합니다 . • instanceId=인스턴스ID • N/A • PkiMode=true or PkiMode=false (PkiMode가 false이 경우 상세 로깅의 마지막에 표기됩니다 .)

항목	설명
레벨	발생된 이벤트의 심각도를 표시합니다. • Critical: 시스템 중단 등의 심각한 오류 발생에 대한 이벤트 • Error: 일반적인 오류 이벤트 • Warning: 오류는 아니지만 주의가 필요한 이벤트 • Notice: 알림이 필요한 이벤트 • Info: 관리자에게 필요한 일반적인 이벤트 • Debug: 개발자에게 필요한 상세하게 정의된 이벤트
상세 로깅 항목	Audit 이벤트 상세 로깅 항목입니다. 자세한 사항은 342페이지의 "상세 로깅 항목"을 참고하세요.
로그 생성일	Audit 이벤트가 발생한 일시입니다.

상세 로깅 항목

Push 서버 Audit 상세 로깅 이벤트명은 “,” 로 구분하여 표기됩니다 . 로그 시간 , 클래스 명등 이벤트내의 세부 항목의 “&” 로 구분하여 표기합니다 .

이벤트	항목
STARTUP	• tcpPort=TCP 리스닝 포트 • eTcpPort= 외부 TCP 리스닝 포트 &iTcpPort=내부 TCP 리스닝 포트 • tcpPort=TCP 리스닝 포트&UdpPort=UDP 리스닝 포트 • UdpPort=UDP 리스닝 포트 • SAIID=SA Instance ID &SAGID=SA 그룹 ID
SHUTDOWN	• CAUSE=접속 종료 이유 • N/A
TLS_HANDSHAKE_START	• remote-host= 접속 Host&remote-port=접속 Port • remote-host= 접속 Host • remote-host=접속 Host&remote-port=접속 Port &CHID=채널 ID
TLS_HANDSHAKE_COMPLETED	• remote-host=접속 Port &protocol=TLS 프로토콜 &ciphersuite=TLS에 설정된 CipherSuite명 • remote-host=Connection host&protocol=TLS 프로토콜 &ciphersuite=TLS에 설정된 CipherSuite 명 &CHID=채널 ID
TLS_TERMINATED	• remote-host= 접속 Host 정보 • CHANNELID=채널 ID&EXCEPTION OCCURRED=에러 내용 • CHANNELID=채널 ID&Cause=에러 내용 • remote-host=접속 host&remote-port=접속 Port &CHID=채널 ID
TLS_HANDSHAKE_ERROR	• remote-host=접속 host&remote-port=접속 Port &cause=에러 클래스&ERR=에러 메시지 • remote-host=접속 Host 정보&cause=에러 클래스&ERR=에러 메시지 • remote-host=접속 Host 정보&cause=에러 클래스와 메시지 • ERR=에러 메시지 • remote-host=접속 Host 정보&remote-port=접속 Port&CHID=채널 ID&cause=에러 클래스와 메시지

이벤트	항목
CORRUPTION_CHECK_FAIL	• jar 파일 경로=Not Signed • jar 파일 경로=is Corrupted • jar 파일 경로=is not signed By Push
KEY_GENERATION_FAIL	• cert=에러 코드 및 메시지 • EX=Error class&MSG=에러 메시지
ENCRYPT_FAIL	• EX=에러 클래스&MSG=에러 메시지
DECRYPT_FAIL	• EX=에러 클래스&MSG=에러 메시지
MAKE_SIGNATURE_FAIL	• EX=에러 클래스&MSG=에러 메시지
VERIFY_SIGNATURE_FAIL	• cert=에러 코드 및 메시지 • EX=에러 클래스&MSG=에러 메시지
DIGEST_FAIL	• EX=에러 클래스&MSG=에러 메시지
CERT_EXCEPTION	• ERRCODE=에러 코드&MSG=에러 메시지
RANDOM_FAIL	• EX=에러 클래스&MSG=에러 메시지
CRYPTOJ_SELFTEST_START	- 암호화 모듈 자체 테스트시 서버의 암호화 모듈(Crypto-J)의 암호화 무결성 체크 대상로 지정된 테스트 대상이름및 ID를 표기합니다. 테스트 대상 이름은 다음과 같습니다. - JarVerify, SHA512, AES, TripleDES, KDFTLS10, HMACDRBG, ECDRBG, FIPS186Random, DSA, ECDSA,CTRDRBG • testName=테스트대상이름 &testId=테스트대상 ID
CRYPTOJ_SELFTEST_FINISHED	• testName=테스트대상이름&testId=테스트대상 ID
CRYPTOJ_SELFTEST_PASSED	• testName=테스트대상이름&testId=테스트대상 ID
CRYPTOJ_SELFTEST_FAILED	• testName=테스트대상이름&testId=테스트대상 ID
CRYPTOJ_SELFTEST_FORCED_TO_FAIL	• testName=테스트대상이름&testId=테스트대상 ID

정책 목록

Android 단말 관리 정책

Android 단말의 정책 목록은 다음과 같습니다 . 삼성 단말에만 적용된는 정책명 옆에는 이 표시됩니다 .(버전명 뒤에 + 는 버전이상 , - 는 버전이하를 의미합니다 . MDM 2.0 은 삼성그룹향 라이선스를 사용하는 경우 적용되는 정책을 의미합니다 .)

보안 그룹

정책	설명
비밀번호 정책	화면 잠금 비밀번호를 강제로 설정하거나 미설정하여 제어하지 않도록 선택합니다. • 설정: 화면 잠금 비밀번호를 제어합니다.
	Note: 화면 잠금 상태에서는 카메라 사용이 금지됩니다.
비밀번호 최소강도	[Android 2.2(SDK8)+] 단말 화면 잠금 비밀번호의 최소강도를 설정합니다. 비밀번호의 강도는 패턴 < 숫자 < 영숫자 < 특수문자포함 순으로 강해집니다. • 패턴: 패턴 이상(패턴, 숫자, 영숫자포함, 특수문자포함)의 비밀번호를 설정해야 합니다. • 숫자: 숫자 이상(숫자, 영숫자포함, 특수문자포함)의 비밀번호를 설정해야 합니다. • 영숫자포함: 영숫자-이상(영숫자포함, 특수문자포함)의 비밀번호를 설정해야 합니다. • 특수문자포함: 특수문자를 반드시 포함하여 영숫자포함, 특수문자포함의 비밀번호를 설정해야 합니다.
비밀번호 입력 실패 허용 횟수	[Android 2.2(SDK8)+] 입력 실패 허용 횟수 이상으로 비밀번호를 잘못 입력하면 통제 동작을 수행합니다. • 설정값: 0~10 회
비밀번호 입력 허용 횟수 이상 실패 시 조치	[Android 2.2(SDK8)+] 실패 허용 횟수 이상으로 비밀번호를 잘못 입력하는 경우 실행할 통제 동작을 지정합니다. • 단말 잠금: 단말 잠금을 합니다. • 공장 초기화 + SD Card 초기화: 사용자 단말을 공장 초기화시키며 SD 카드를 동시에 초기화시킵니다. • 공장 초기화 (Only): 사용자 단말을 공장 초기화시키며, SD 카드는 초기화되지 않습니다.
	Note: 2.0 버전 이하의 단말 Agent에서는 공장 초기화 (Only)가 적용되지 않기 때문에 공장 초기화를 하려면 공장 초기화 + SD Card 초기화를 선택해야 합니다.

정책	설명
비밀번호 최소 길이 (자)	[Android 2.2(SDK8)+] 비밀번호의 최소 길이를 지정합니다. 패턴의 경우에는 지정되는 점의 개수가 최소 길이 보다 하나 더 필요합니다. • 설정값: 4~16 자
	Note: 패턴 비밀번호의 최소 길이는 각 점을 잇는 선의 개수를 의미합니다. 따라서 정책이 4자이면 5개의 점을 잇는 4개의 선이 입력되어야 정책을 만족합니다.
비밀번호 최대 사용 기간 (일)	[Android 3.0(SDK11)+, Samsung(SAFE2+)] 비밀번호를 사용할 수 있는 최대 기간이 지나면 비밀번호를 재설정하도록 합니다. • 설정값: 0~365 일
비밀번호 내역 관리 (회)	[Android 3.0(SDK11)+, Samsung(SAFE2+)] 이전 입력 비밀번호를 최근 몇 회 이전까지 재사용할 수 없는지 설정합니다. **비밀번호 최소 강도**가 **숫자**, **영숫자포함**, **특수문자포함** 선택 시에만 값을 설정할 수 있습니다. • 설정값: 0~10 회
단말 잠금 유예 시간 최대값 (분)	[Android OS, Samsung Only(SAFE2+)] 사용자가 특정 시간 이상 비밀번호를 설정하지 않을 경우 단말 잠금을 합니다. • 설정값: 0~60 분
비밀번호 최대 순차적 숫자 사용 길이 (자)	[Android OS, Samsung Only(SAFE2.2+)] 순차적으로 입력할 수 있는 숫자의 최대 개수를 설정합니다. • 설정값: 1~10 자
비밀번호 최대 순차적 문자 사용 길이 (자)	[Android OS, Samsung Only(SAFE4+)] 순차적으로 입력할 수 있는 문자의 최대 개수를 설정합니다. • 설정값: 1~10 자
화면 잠금 상태의 기능 차단	잠금화면 시 기능 제어를 설정합니다. • 설정: 잠금 화면에서 설정한 기능을 차단합니다.
차단 기능 선택	[Android 5.0(SDK21)+, Samsung (SAFE5.4+)] 사용자의 단말에 비밀번호 정책이 설정되는 경우, 잠금화면에서 차단할 기능을 선택합니다. 잠금 화면에서 보이는 알림의 가시성은 앱에서 설정한 옵션에 따라 달라집니다. • 카메라: 잠금 화면에서 카메라 직접 실행 • Trust Agent: 특정 조건(신체 활동, 장소, 기기 추가 등)에서 자동으로 화면 잠금이 해제되는 기능인 Smart Lock • 지문: 지문으로 화면 잠금 해제 기능 • 알림내용 숨김: 알림은 표시되지만 앱에서 설정한 Private 한 컨텐츠는 숨김 • 알림 숨김: 모든 알림이 잠금 화면에서 사라짐
	Note: • 해당 정책은 비밀번호가 패턴 이상으로 설정된 경우 동작합니다. • EMM 1.6 버전 이전에 활성화된 단말의 경우, Android 권한 동의를 추가로 해야합니다.

정책	설명
화면 잠금 시간	[Android 2.2(SDK8)+, Samsung(SAFE5+)] 지정된 시간 동안 사용자 입력이 없으면 단말 화면을 잠급니다. • 15초 • 30초 • 1분 • 2분 • 5분 • 10분
EMM Guardian	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] EMM 활성화 상태에서 관리자의 서비스 해제 조치 없이 공장 초기화한 단말의 외부 장치 연결 허용 여부를 지정합니다. EMM Guardian 사용을 금지 시, 단말 사용자는 카메라, SD 카드, MTP, 블루투스, Wi-Fi 테더링, USB 디버깅, 화면 캡처를 사용할 수 없습니다. • 허용: 외부 장치에 연결할 수 있습니다. • 금지: 외부 장치에 연결할 수 없습니다.
단말 서버간 통신 제어	단말과 EMM 서버간의 통신이 불가한 경우 지정된 재시도 주기에 따라 통신을 수행 합니다. • 허용: 통신 재시도를 허용합니다. • 금지: 통신 재시도를 금지합니다.
통신 재시도 횟수 (회)	[Android 1.0(SDK1)+] [MDM 2.0] 단말의 통신이 불가한 경우 1분 간격으로 지정된 횟수만큼 통신을 재시도 합니다. 지정된 횟수 동안 통신이 계속 불가한 경우, 통신 재시도 주기만큼 대기한 후 다시 통신을 시도합니다. • 설정값: 0~60 회
통신 재시도 주기 (분)	[Android 1.0(SDK1)+] [MDM 2.0] 단말의 통신이 원활하지 않은 경우 다음 통신 시도까지의 대기시간을 설정합니다. 대기 중 상태에서 단말의 통신 상태 변경 시 바로 통신을 다시 시도합니다. • 설정값: 1~60 분
스마트카드 브라우저 인증	[Android OS, Samsung Only(Knox1+)] 인터넷 브라우저에서 스마트카드 인증을 허용할지 여부를 설정합니다. 블루투스 스마트카드 관련 앱이 단말에 설치 되어야 하며, 사용하는 스마트카드를 **설정 > 보안** 에서 등록하여야 사용이 가능한 정책입니다. 사용 시 블루투스 보안 모드가 적용되어 타 블루투스 기기와 연결이 제한됩니다. • 허용: 스마트카드 브라우저 인증을 허용합니다. • 금지: 스마트카드 브라우저 인증을 금지합니다.
인증서 삭제	[Android OS, Samsung Only(Knox2+)] 사용자가 단말에서 환경 설정에 있는 인증서 삭제를 사용하지 못하도록 제어합니다. • 허용: 인증서 삭제를 허용합니다. • 금지: 인증서 삭제를 금지합니다.

정책	설명
인증서 설치 시 검증 여부	[Android OS, Samsung Only(Knox1+)] 인증서 설치 시점에 유효성을 검사하는 기능을 설정합니다. 유효성에 실패하면 설치 되지 않습니다. • 검증: 인증서 설치 시 유효성 검증을 합니다. • 미검증: 인증서 설치 시 유효성 검증을 하지 않습니다.
Attestation (단말 펌웨어 위변조 탐지)	[Android OS, Samsung Only(Knox1.0.1+)] 펌웨어 변조를 감시하는 정책으로 단말의 정상 여부를 판단하기 위해 Attestation 서버와의 통신을 사용할지 여부를 설정합니다. 미설정으로 지정하였을 경우에는 미사용과 동일하게 동작합니다. • 사용: Attestation 서버와의 통신을 사용합니다. • 미사용: Attestation 서버와의 통신을 사용하지 않습니다.
검증 실패 시 조치	[Android OS, Samsung Only(Knox1.0.1+)] Knox Attestation을 위반한 경우 조취 방법을 설정합니다. Knox Attestation 위반 시 Knox 컨테이너 신규 생성 금지 및 기생성된 Knox 컨테이너 사용이 금지됩니다. • Knox 잠금: Knox 컨테이너를 잠금 처리합니다. • Knox 삭제: Knox 컨테이너를 삭제합니다. • 단말 잠금: 단말을 잠금 처리합니다. • 공장 초기화: 단말을 공장 초기화합니다.
구글 Android 보안 정책 업데이트	[Android OS, Samsung Only(SAFE5.6+)] 단말의 보안을 향상시키기 위하여 구글 Android에서 보안 정책을 업데이트 해주는 서비스입니다. 자동 업데이트 여부를 설정합니다. • 허용: 보안 자동 업데이트 여부를 사용자가 단말에서 설정할 수 있습니다. • 금지: 보안 자동 업데이트 여부를 사용자가 단말에서 설정할 수 없습니다. • 강제 사용: 강제로 보안 자동 업데이트를 설정합니다.

인터페이스 그룹

정책	설명
Wi-Fi	[Android 1.0(SDK1)+, Samsung(SAFE2+)] [MDM 2.0] Wi-Fi 사용 여부를 설정합니다. 1.5.1 버전부터 신규 단말 등록 시, Wi-Fi 정책은 **프로파일 > 앱 관리 프로파일 > 애플리케이션**에서 필수로 지정한 애플리케이션이 설치된 이후 적용됩니다. Wi-Fi 정책 적용이 정상적으로 되지 않은 경우, EMM이 활성화 된 이후 30분이 지나면 Wi-Fi 정책이 다시 적용됩니다. • 허용: Wi-Fi를 사용할 수 있습니다. • On 금지: Wi-Fi를 켤 수 없습니다. • Off 금지: Wi-Fi를 항상 켜야 합니다.
Wi-Fi Direct	[Android OS, Samsung Only(SAFE4+)] Wi-Fi P2P (Wi-Fi Direct)의 사용 여부를 설정합니다. • 허용: Wi-Fi P2P (Wi-Fi Direct) 사용을 허용합니다. • 금지: Wi-Fi P2P (Wi-Fi Direct) 사용을 금지합니다. **Note:** • Wi-Fi 정책을 **허용** 또는 **Off 금지**로 설정해야, Wi-Fi Direct 정책을 설정할 수 있습니다. • Wi-Fi P2P 허용 정책은 Android 아이스크림 샌드위치(4.0 이상)이후 버전에서 사용할 수 있습니다. • 단말에 따라서 2개의 단말을 직접 연결해야 통제가 되거나 메뉴 자체가 통제되기도 합니다.
Wi-Fi 핫스팟	[Android 2.3(SDK9)+, Samsung(SAFE2+)][MDM 2.0] Wi-Fi 핫스팟 사용 여부를 설정합니다. • 허용: Wi-Fi 핫스팟 사용을 허용합니다. • 금지: Wi-Fi 핫스팟 사용을 금지합니다.
Wi-Fi SSID 화이트리스트 설정	Wi-Fi SSID 화이트리스트를 설정하여, 등록한 Wi-Fi SSID에만 접속이 가능하도록 합니다. • 설정: Wi-Fi SSID 화이트리스트를 설정합니다.
Wi-Fi SSID 화이트리스트	[Android 1.0(SDK1)+, Samsung(SAFE2.2+)] Wi-Fi SSID 화이트리스트를 설정합니다. 해당 화이트리스트에 추가한 Wi-Fi AP에만 연결되고, 그 외의 AP에는 연결이 허용되지 않습니다. Wi-Fi 설정 프로파일 추가, 삭제와는 무관하며, 연결 허용 여부만 관여합니다. • 추가: Wi-Fi SSID 입력 후 ⊕ 클릭 • 전체 추가: ⊕를 클릭하면 Wi-Fi 전체 리스트에 연결이 가능합니다. • 삭제: Wi-Fi SSID 선택 후 X 클릭
Wi-Fi SSID 블랙리스트 설정	Wi-Fi SSID 블랙리스트를 설정하여, 등록한 Wi-Fi SSID에 접속이 불가능하도록 합니다. • 설정: Wi-Fi SSID 블랙리스트를 설정합니다.

정책	설명
Wi-Fi SSID 블랙리스트	[Android 1.0(SDK1)+, Samsung(SAFE2.2+)] Wi-Fi SSID 블랙리스트를 설정합니다. 해당 블랙리스트에 추가한 Wi-Fi AP에는 연결되지 않고, 그 외의 AP에는 연결이 허용됩니다. Wi-Fi 설정 프로파일 추가, 삭제와는 무관하며, 연결 허용 여부만 관여합니다. • 추가: Wi-Fi SSID 입력 후 ⊕ 클릭 • 전체 추가: ⊕를 클릭하면 Wi-Fi 전체 리스트에 연결이 가능합니다. • 삭제: Wi-Fi SSID 선택 후 X 클릭
Wi-Fi 네트워크 자동 접속	[Samsung Only(SAFE4+)] 이미 단말에 저장된 Wi-Fi AP에 자동으로 접속되는 것을 제어합니다. • 허용: Wi-Fi AP 자동 접속을 허용합니다. • 금지: Wi-Fi AP 자동 접속을 금지합니다.
Wi-Fi 최소 보안 수준 설정	[Android OS, Samsung (SAFE2+)] Wi-Fi 최소 보안 레벨을 지정합니다. 보안 레벨에 따라 그룹 단위로 보안 레벨이 지정되며, 최소 보안 레벨 이상만 설정 가능합니다. 보안 수준은 WEP(낮음) < WPA < LEAP, PWD < FAST, PEAP < TSL, TTLS, SIM, AKA, AKA'(높음)입니다. • OPEN: 보안에 상관없이 모든 Wi-Fi를 허용합니다. • WEP • WPA • LEAP, PWD • FAST, PEAP • TSL, TTLS, SIM, AKA, AKA'
블루투스	[Android 1.0(SDK1)+, Samsung(SAFE2+)] [MDM 2.0] 블루투스 사용 허용 여부를 설정합니다. • 허용: 블루투스 사용을 허용합니다. • On 금지: 블루투스를 켤 수 없습니다. • Off 금지: 블루투스를 항상 켜야 합니다.
데스크탑 연결	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] 기기를 블루투스로 데스크탑, 노트북 등과 연결 허용 여부를 지정합니다. • 허용: 연결을 허용합니다. • 금지: 연결을 금지합니다.
데이터 교환	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] 사용자의 기기를 다른 기기와 블루투스 방식으로 연결하여 파일 등 데이터 교환 허용 여부를 설정합니다. • 허용: 데이터 교환을 허용합니다. • 금지: 데이터 교환을 금지합니다.
탐색 모드	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] 블루투스 탐색 모드 설정 허용 여부를 설정합니다. • 허용: 블루투스 탐색 모드 설정을 허용합니다. • 금지: 블루투스 탐색 모드 설정을 금지합니다.

정책	설명
블루투스 테더링	[Android 4.2(SDK17)+, Samsung(SAFE2+),LG(GATE 2+)] [MDM 2.0] 블루투스 테더링 연결 허용 여부를 설정합니다. • 허용: 블루투스 테더링 사용을 허용합니다 • 금지: 블루투스 테더링 사용을 금지합니다
블루투스 UUID 블랙/화이트리스트 설정	블루투스 UUID (Universal Unique Identifier)기준으로 블루투스 장비의 연결 허용 여부를 설정합니다. • 블랙리스트 설정: 블루투스 연결을 차단할 기기를 설정합니다. • 화이트리스트 설정: 블루투스 연결을 허용할 기기 를 설정합니다. **Note:** 해당 정책 업데이트시 기존 연결되어있던 블루투스 연결이 끊기게 되어, 단말 사용자가 다시 연결해주어야 합니다.
블루투스 UUID 블랙리스트	[Android OS, Samsung Only(SAFE2.2+)] 블루투스 연결을 차단할 기기를 설정합니다. • 오디오, 파일 전송, 연락처, 헤드셋, 핸즈프리
블루투스 UUID 화이트리스트	[Android OS, Samsung Only(SAFE2.2+)] 블루투스 연결을 허용할 기기를 설정합니다. • 오디오, 파일 전송, 연락처, 헤드셋, 핸즈프리
NFC 제어	[Android OS, Samsung(SAFE2+)] NFC 제어를 허용할지 여부를 설정합니다. • 허용: NFC 사용을 허용합니다. • 금지: NFC 사용을 금지합니다.
PC 연결	[Android OS, Samsung(SAFE2+)] [MDM 2.0] PC와의 이동식 디스크 또는 MTP 연결 허용 여부를 설정합니다. • 허용: 이동식 디스크로 사용을 허용합니다. • 금지: 이동식 디스크로 사용을 금지합니다.
USB 테더링 활성화	[Android OS, Samsung(SAFE2+)] [MDM 2.0] USB 테더링 연결 허용 여부를 설정합니다. • 허용: USB 테더링 연결을 허용합니다. • 금지: USB 테더링 연결을 금지합니다.
USB Host Storage (OTG)	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] OTG(On the Go) 기기 연결 허용 여부를 설정합니다. OTG를 통한 메모리 연결만 제어가 되며 키보드, 마우스 등은 사용이 가능합니다. • 허용: OTG 기기 사용을 허용합니다. • 금지: OTG 기기 사용을 금지합니다.
USB 디버깅 활성화	[Android OS, Samsung(SAFE2+)] [MDM 2.0] USB 디버깅 기능 허용 여부를 설정합니다. • 허용: USB 디버깅을 허용합니다. • 금지: USB 디버깅을 금지합니다.

정책	설명
마이크	[Android 1.0(SDK1)+, Samsung(SAFE2+)] [MDM 2.0] 마이크 사용 허용 여부를 설정합니다. • 허용: 마이크 사용을 허용합니다. • 금지: 마이크 사용을 금지합니다.
녹음	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] 마이크를 사용한 녹음 기능의 허용 여부를 설정합니다. • 허용: 마이크 녹음을 허용합니다. • 금지: 마이크 녹음을 금지합니다.
S Voice	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] 마이크를 이용한 S Voice 사용 여부를 설정합니다. • 허용: S Voice를 사용을 허용합니다. • 금지: S Voice를 사용을 금지합니다.
GPS	[Android OS, Samsung(SAFE3+)] GPS상태를 제어합니다. • 허용: GPS 사용을 허용합니다. 사용자가 GPS를 On/Off 합니다. • On 금지: GPS 기능이 항상 Off 되어 있으며 기능이 비활성화 되어 사용자가 제어할 수 없습니다. • Off 금지: GPS 기능이 항상 On 되어 있으며 기능이 비활성화 되어 사용자가 제어할 수 없습니다. **Note:** 정책을 적용하기 전에 높은 정확도/절전모드/GPS만 3가지 기능 중에 사용자가 설정한 상태로 GPS를 On 시킵니다.
Wearable 기기 정책 승계	[Android OS, Samsung Only(SAFE5.6+)] Phone 정책을 승계하여 Gear에 정책 적용 여부를 설정합니다. • 사용: Wearable 기기에 정책 승계를 허용합니다. • 미사용: Wearable 기기에 정책 승계를 금지합니다.

앱 그룹

정책	설명
알 수 없는 출처의 앱 설치	[Android OS, Samsung(SAFE2+)] **알 수 없는 출처** 옵션을 설정하여 마켓 이외에서 다운로드된 앱에 대한 설치 허용 여부를 설정합니다. • 허용: 설치할 수 있습니다. • 금지: 설치할 수 없습니다.
Play 스토어	[Android OS, Samsung Only(SAFE1+)] [MDM 2.0] 사용자의 단말에서 구글 Play 스토어 사용 여부를 설정합니다. Amazon Store, T-Store, 올레마켓 등의 사설 앱 스토어는 제어 대상이 아닙니다. • 허용: Play 스토어 사용을 허용합니다. • 금지: Play 스토어 사용을 금지합니다.
YouTube	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] 사용자가 단말에서 YouTube 앱을 사용할 수 있는지 허용 여부를 설정합니다. • 허용: YouTube 사용을 허용합니다. • 금지: YouTube 사용을 금지합니다.
앱 블랙/화이트 리스트 설정	앱 제어 정책을 블랙리스트 또는 화이트리스트 기준으로 설정할 것인지 지정합니다. • 앱 블랙리스트 설정: 블랙리스트는 실행하거나 설치하면 안 되는 앱 목록입니다. 앱 설치 블랙리스트와 앱 실행 블랙리스트를 설정할 수 있습니다. • 앱 화이트리스트 설정: 화이트리스트로 등록된 앱만 실행하거나 설치할 수 있습니다. 앱 설치 화이트리스트와 앱 실행 화이트리스트를 설정할 수 있습니다. • 앱 블랙/화이트 리스트 설정: 블랙리스트/화이트리스트 정책을 동시에 적용할 수 있습니다. 동일한 앱이 블랙/화이트 리스트에 등록된 경우, 화이트 리스트의 우선 순위가 높습니다. **Note:** 앱 블랙/화이트리스트 설정 후 앱을 추가하지 않으면 시스템 앱(Samsung SDS EMM Client)과 필수 앱(Secure Browser, mMail)을 제외한 모든 앱의 실행 및 설치가 금지됩니다.
앱 설치 블랙리스트	[Android OS, Samsung(SAFE2.1+)] 지정된 앱 설치를 차단하는 정책입니다. 정책 설정 시 이미 설치된 앱은 자동으로 삭제 처리 되며, 신규로 설치되는 앱도 설치 후 자동 삭제 됩니다. 패키지명에 와일드카드(*)를 사용하여 등록된 제어 앱을 앱 설치 블랙리스트 정책에 추가하면 등록된 특정 패키지는 설치되지 않습니다. 예) com.*.emm / com.sds.* / com.*.emm.* 앱 설치 화이트리스트, 앱 실행 화이트리스트, 앱 삭제 방지 리스트에 이미 추가된 앱은 앱 설치 블랙리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 전체 앱 추가: ⊕ 클릭하면 목록에 * 추가되며 전체 앱이 설치 블랙리스트에 추가 • 삭제: 목록에서 앱 선택 후 **X** 클릭

정책	설명
앱 실행 블랙리스트	[Android 2.2(SDK8)+, Samsung(SAFE2+)] [MDM 2.0] 지정된 앱 실행을 차단하는 정책입니다. 정책 설정 시 정의된 앱의 아이콘이 사라져 사용자가 임의로 앱을 실행할 수 없게 됩니다. 앱이 삭제되는 것은 아니기 때문에 정책 변경 또는 EMM 서비스 해제 시 다시 앱이 표시됩니다. 앱 실행 화이트리스트에 이미 추가된 앱은 앱 실행 블랙리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 앱 선택 후 X 클릭
앱 실행 방지 리스트	[Android OS, Samsung(SAFE5+)] [MDM 2.0] 지정된 앱에 대해서 앱 실행을 차단하는 정책입니다. 정책 설정 시 사용자가 임의로 앱을 실행할 수 없게 됩니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
앱 설치 화이트리스트	[Android OS, Samsung(SAFE2.1+)] 목록에 등록된 앱만 설치를 허용하는 정책입니다. EMM Client, EMM Agent, Push Agent 등과 같은 시스템 앱은 자동으로 대상 목록으로 등록됩니다. 단말에 사전에 설치된 앱 이외에도 사용자가 추가 설치하는 앱에 대해서 동작을 하게 됩니다. 정책 적용 시 이미 설치되었으나 허용되지 않은 앱은 자동으로 삭제 처리됩니다. 패키지명에 와일드카드(*)를 사용하여 등록된 제어 앱을 앱 설치 화이트리스트 정책에 추가하면 등록된 특정 패키지는 설치가 허용됩니다. 예) com.*.emm / com.sds.* / com.*.emm.* 이미 앱 설치 블랙리스트에 추가된 앱은 앱 설치 화이트리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 전체 앱 추가: ⊕ 클릭하면 목록에 * 추가되며 전체 앱이 설치 화이트리스트에 추가 • 삭제: 목록에서 앱 선택 후 X 클릭
앱 실행 화이트리스트	[Android 2.2(SDK8)+ ,Samsung(SAFE2+)] 앱 실행 화이트리스트에 등록된 앱만 실행을 허용하는 정책입니다. EMM Client, EMM Agent, Samsung SDS Push Agent 등과 같은 시스템 앱과 단말에 사전 설치된 Preload 앱은 앱 실행 화이트리스트에 자동으로 등록됩니다. 해당 정책을 적용하면 앱 실행 화이트리스트에 없는 앱의 아이콘이 사용자 단말에서 사라지게 되며, 사용자가 임의로 실행할 수 없게 됩니다. 앱이 삭제되는 것은 아니기 때문에 정책이 변경되거나 EMM Agent Unenrollment 시, 숨겨진 앱의 아이콘은 사용자 단말에 다시 나타납니다. 이미 앱 설치 블랙리스트 또는 앱 실행 블랙리스트에 추가된 앱은 앱 실행 화이트리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 앱 선택 후 X 클릭

정책	설명
앱 삭제 방지리스트	[Android OS, Samsung(SAFE1+)] 단말에서 사용자가 임의로 삭제할 수 없는 앱을 설정합니다. 이미 앱 설치 블랙리스트에 추가된 앱은 앱 삭제 방지 리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 앱 선택 후 **X** 클릭
앱 위변조 시 조치	[Android OS(SDK3), Samsung(SAFE2+)] 사내 또는 Kisok 앱 및 EMM 애플리케이션에 등록된 앱이 단말에서 사용 중인 앱과 다르면 앱 위변조로 판단하여 단말에 적용할 조치 방법을 다음과 같이 설정합니다. • 실행 금지: 사용자 단말에서 해당 앱 실행을 금지합니다. • 삭제: 사용자 단말의 해당 앱을 삭제합니다. • 단말 잠금: 사용자의 단말을 잠급니다. 단말 잠금 해제는 관리자에 의해서만 가능합니다. • 컴플라이언스 보고: 콘솔의 **서비스 현황 > 대시보드**를 통해 관리자에게 해당 단말의 위변조 여부를 알립니다. 위 메뉴에서 **앱 위변조** 건수를 클릭하여, 해당 단말에 적용할 단말 제어 명령을 전송합니다. 자세한 내용은 5장 단말&사용자의 128페이지 9장의 "단말 제어 명령 보내기"를 참고하세요. • 공장 초기화 + SD Card 초기화: 사용자 단말을 공장 초기화시키며 SD 카드를 동시에 초기화시킵니다. • 공장 초기화 (Only): 사용자 단말을 공장 초기화시키며, SD 카드는 초기화되지 않습니다. **Note:** • Samsung 전자, LG 전자 단말이 아닌 일반 Android 단말의 경우 단말 잠금, 공장초기화, 컴플라이언스 보고 정책만 적용됩니다. • 2.0 버전 이하의 단말 Agent에서는 공장 초기화 (Only)가 적용되지 않기 때문에 공장 초기화를 하려면 공장 초기화 + SD Card 초기화를 선택해야 합니다.
앱 설치 시 ProgressBar 표시	[Android 1.0(SDK1.5)+] 사용자가 Knox Manage의 앱 스토어에서 애플리케이션을 다운로드 받는 경우 다운로드 진행 현황을 표시합니다. • 사용: 사용자의 단말에 앱 다운로드 진행 현황이 표시됩니다. • 미사용: 사용자의 단말에 앱 다운로드 진행 현황이 표시되지 않습니다.

정책	설명
배터리 최적화 예외 앱 설정	배터리 최적화 예외 앱을 설정하는 정책입니다. 등록된 앱은 배터리 소모를 유발할 수 있기 때문에 예외 처리가 필요한 경우에만 설정합니다. Android N (Nougat) OS 이상에서 설정 가능하며, EMM 애플리케이션에 등록된 System 앱은 배터리 최적화 작업 대상에서 자동으로 제외됩니다. • 배터리 최적화 예외 앱 설정: 배터리 사용량을 최적화하기 위한 CPU 및 네트워크 제한 대상에서 등록된 앱을 예외시킵니다.
배터리 최적화 예외 앱	[Android OS, Samsung Only(SAFE5.7+)] 지정된 앱에 대하여 배터리 수명 연장을 위해 OS에서 수행하는 절전기능인 Doze 모드(Doze mode), 앱 대기모드(App Standby mode), 절전모드(power saving mode) 작업에 대한 예외 처리를 수행합니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭

Kiosk Wizard 그룹

정책	설명
Kiosk 앱 설정	[Android OS, Samsung Only(SAFE3+)] Kiosk 앱 (전용 런처)를 등록하여 해당 화면 내에서만 동작하는 Kiosk 모드를 설정합니다. 해당 정책을 사용하려면 Kiosk 전용 앱이 서버에 등록되고, 단말에 배포되어 설치되어 있어야 합니다. • 싱글 앱: 등록되어 있는 싱글 앱 Kiosk 를 선택합니다. • 멀티 앱: 등록되어 있는 멀티 앱 Kiosk 를 선택하거나 Wizard에서 직접 Kiosk 앱을 생성하여 선택합니다. • Kiosk Browser: EMM 앱으로 등록된 Kiosk Browser로 자동 선택되며, 기본 페이지 URL만 실행하도록 합니다. **Note:** Kiosk Browser 설정을 하려면 **애플리케이션 > EMM 애플리케이션**에서 Kiosk Browser 앱이 등록되어 있어야합니다.
Kiosk 앱	[Android OS, Samsung Only(SAFE3+)] Kiosk 모드에서 사용할 앱을 설정합니다. • 싱글 앱: 🔍 를 클릭하여 등록되어 있는 싱글 앱 Kiosk를 선택합니다. • 멀티 앱: 🔍 를 클릭하여 등록되어 있는 멀티 앱 Kiosk를 선택하거나 **Customize**를 실행하여 직접 Kiosk 앱을 생성하여 선택합니다. • **Customize**를 클릭하면 Kiosk Wizard가 나타납니다. Kiosk Wizard에 대한 자세한 사용법은 240페이지 14장의 "쿠키 정책 설정: 웹 페이지의 쿠키 관련 설정을 변경할 수 있습니다."를 참고합니다.
Kiosk Browser 설정	[Android] Kiosk Browser 설정 시, EMM 애플리케이션의 Kiosk Browser로 등록된 앱의 패키지명으로 자동 선택됩니다.
기본 페이지 URL	[Android] Kiosk Browser에서 호출할 기본 페이지 URL을 설정합니다.
화면보호기 설정	[Android] 멀티 애플리케이션, Kiosk Browser의 화면 보호기 설정 여부를 지정합니다. 단말에서 설정한 화면 자동 꺼짐 시간 또는 세션 타임아웃에서 설정한 시간 동안 사용자의 작동이 없는 경우 등록한 이미지 또는 비디오 파일을 실행합니다. GIF 애니메이션 파일은 지원하지 않습니다. 기본값은 금지이며 허용으로 지정한 경우에는 세션 타임아웃 설정이 필수입니다. • 허용: 화면 보호기 설정을 허용합니다. • 금지: 화면 보호기 설정을 금지합니다.
화면보호기 타입 설정	[Android] 멀티 애플리케이션, Kiosk Browser의 화면 보호기 타입을 이미지 또는 비디오로 설정합니다. • 이미지: PNG, JPG, JPEG, GIF (애니메이션 파일 적용 불가) 형식의 이미지 파일을 10개까지 추가 가능합니다. • 비디오: MP4, MKV 형식의 비디오를 1개만 추가 가능합니다.

정책	설명
이미지	[Android] 화면 보호기 타입을 이미지로 설정합니다. 단말에 이미지 파일을 적용하기 위해서는 단말 제어 명령을 전송해야합니다. • 업로드: **Browser**를 클릭하여 이미지를 업로드 할 수 있습니다. 이미지는 10개까지 등록 가능하며 1개의 용량 제한은 5MB입니다. • 삭제: **X**를 클릭하여 업로드한 이미지를 삭제합니다.
비디오	[Android] 화면 보호기 타입을 비디오로 설정합니다. 단말에 비디오 파일을 적용하기 위해서는 단말 제어 명령을 전송해야합니다. • 업로드: **Browser**를 클릭하여 비디오를 업로드 할 수 있습니다. 비디오는 1개만 등록 가능하며 용량 제한은 50MB입니다. • 삭제: **X**를 클릭하여 업로드한 비디오를 삭제합니다.
세션 타임아웃	[Android] Kiosk Browser의 세션타임아웃 설정여부를 지정합니다. 설정된 시간 동안 사용자의 작동이 없는 경우 단말의 Kiosk Browser가 가진 Cache, Cookie 등 사용자 정보를 삭제하고 기본 페이지 URL로 이동합니다. • 설정: 세션타임아웃을 설정하여 Browser의 세션을 해제합니다.
시간(초)	[Android] Kiosk Browser의 세션타임아웃을 초단위로 입력합니다. • 설정값: 10~3600 초(기본값: 1800)
문자열 복사	[Android] 앱 내에서 문자열 복사를 허용 여부를 설정합니다. 기본 값은 금지입니다. • 허용: 문자열 복사를 허용합니다.
Javascript	[Android] 웹 페이지 내에 포함된 Java Script 실행 여부를 설정합니다. • 허용: 사용자가 자바스크립트 사용 여부를 변경할 수 있습니다.
Http Proxy	[Android] Kiosk Browse가 통신할 때 Http Proxy의 사용을 허용할 지를 설정합니다. • 허용: Http Proxy 사용을 허용합니다. PORT를 설정할 수 있습니다. • 금지: Http Proxy 사용을 금지합니다.
IP/DOMAIN : PORT	[Android] Http Proxy 서버 IP 또는 도메인 주소와 PORT를 설정합니다. PORT 미 입력시, PORT 번호가 80으로 자동 설정됩니다.
User Agent 설정 키 값	[Android] User Agent에 추가할 키값을 설정합니다. Http 헤더내에 존재하는 User Agent에 해당 키 값을 포함하여 Kiosk Browser가 웹 서버에 접근하게 합니다. **Note:** User Agent 설정키 값은 웹 서버에서 Kiosk Browser가 아닌 타 브라우저의 접근인지를 구분하는 키 값으로 사용할 수 있습니다.

정책	설명
작업관리자	[Android OS, Samsung Only(SAFE3~5.4)] Kiosk 모드에서 작업관리자 실행 허용 여부를 설정합니다. • 허용: 작업관리자 실행을 허용합니다. • 금지: 작업관리자 실행을 금지합니다.
시스템바	[Android OS, Samsung Only(SAFE3+)] Kiosk 모드에서 시스템바 실행 허용 여부를 설정합니다. • 허용: 시스템바 사용을 허용합니다. • 금지: 시스템바 사용을 금지합니다.
하드웨어 키 금지 설정	[Android OS, Samsung Only(SAFE3+)] Kiosk 모드에서 하드웨어 키 제어를 설정합니다. • 설정: 금지할 하드웨어 키를 설정합니다.
하드웨어 키 금지	[Android OS, Samsung Only(SAFE3+)] Kiosk 모드의 금지할 하드웨어 키를 설정합니다. 기기에 따라 하드웨어 키의 종류가 다를 수 있습니다. • 홈 • 뒤로 가기 • 음량 올리기 • 음량 내리기 • 전원 • 카메라 • 메뉴 • 검색
멀티 윈도우	[Android OS, Samsung Only(SAFE4+)] Kiosk 모드의 멀티 윈도우 동작 여부를 설정합니다. 멀티 윈도우 기능이 제공되는 단말에 한해서 동작합니다. • 허용: 멀티 윈도우 동작을 사용할 수 있습니다. • 금지: 멀티 윈도우 동작을 사용할 수 없습니다.
에어 커맨드	[Android OS, Samsung Only(SAFE5.2+)] Kiosk 모드의 에어 커맨드 사용 여부를 설정합니다. 에어 커맨드는 삼성전자 단말의 기능 중 하나로, S펜을 단말기 화면에 가까이 대면 나타나는 메뉴를 말합니다. • 허용: 에어 커맨드를 허용합니다. • 금지: 에어 커맨드를 금지합니다.
에어 뷰	[Android OS, Samsung Only(SAFE5.2+)] Kiosk 모드의 에어 뷰 사용 여부를 설정합니다. 에어 뷰는 삼성전자 단말의 기능 중 하나로, 이메일이나 사진 등에 S펜 또는 손가락을 가까이하면 정보를 미리 보거나 텍스트 또는 이미지를 확대해서 볼 수 있는 기능입니다. • 허용: 에어 뷰를 허용합니다. • 금지: 에어 뷰를 금지합니다.
엣지 스크린 허용	[Android OS, Samsung Only(SAFE5.5+)] Kiosk 모드의 엣지 스크린 사용 여부를 설정합니다. 엣지 스크린은 삼성전자 단말의 기능 중 하나로, 화면의 곡면 엣지 패널에 자주 사용하는 애플리케이션과 연락처, 카메라 등을 설정하여 편리하게 사용하는 기능입니다. • 허용: 엣지 스크린을 허용합니다. • 금지: 엣지 스크린을 금지합니다.

전화그룹

정책	설명
비행모드	[Android OS, Samsung(SAFE5+)] 비행 모드 진입 가능 여부를 설정합니다. • 허용: 비행 모드 사용을 허용합니다. • 금지: 비행 모드 사용을 금지합니다.
Cellular 데이터 연결	[Android OS, Samsung (SAFE2+)] [MDM 2.0] Cellular 데이터 접속 허용 여부를 설정합니다. 1.5.1 버전부터 신규 단말 등록 시, Cellular 데이터 연결 정책은 **프로파일 > 앱 관리 프로파일 > 애플리케이션**에서 필수로 지정한 애플리케이션이 설치된 이후 적용됩니다. Cellular 데이터 연결 정책 적용이 정상적으로 되지 않은 경우, EMM이 활성화 된 이후 30분이 지나면 Cellular 데이터 연결 정책이 다시 적용됩니다. • 허용: 데이터 접속을 허용합니다. • 금지: 데이터 접속을 금지합니다.
음성 통화	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] 음성 통화 사용 여부를 설정합니다. • 모두 허용: 음성 통화를 사용할 수 있습니다. • 수신만 허용: 음성 통화를 수신만 할 수 있습니다. • 발신만 허용: 음성 통화를 발신만 할 수 있습니다. • 긴급 전화만 허용: 긴급 전화 번호(예: 119, 112)만 사용할 수 있고 일반 전화번호는 사용할 수 없습니다.
데이터 사용량 설정	[Android OS, Samsung Only(SAFE4+)] 단말 사용자가 데이터 사용량을 제한 할 수 있는지 여부를 설정합니다. • 허용: 데이터 사용량을 제한 할 수 있습니다. • 금지: 데이터 사용량을 제한 할 수 없습니다.
최대 데이터 사용량 설정	[Android OS, Samsung Only(SAFE4+)] 최대 데이터 사용량을 제한할지 여부를 설정합니다. 정해진 사용량을 초과할 경우 단말의 데이터 사용을 제한합니다. 정확한 사용량 확인을 위해 시스템 그룹의 날짜, 시간 변경 정책은 금지로 설정되어야 합니다. • 설정: 최대 데이터 사용량을 설정합니다.
최대사용량	[Android OS, Samsung Only(SAFE2+)] 데이터 사용량 제한을 1일, 1주일, 1개월 단위로 설정합니다. 1일 기준 매일 0시, 1주 기준 매주 일요일, 1달 기준 매월 1일 이후 사용량을 확인합니다 • 단말이 최대 사용량을 초과한 경우 데이터 네트워크 접속을 차단합니다. 데이터 네트워크 접속이 차단된 후, 사용자가 데이터 네트워크 접속을 허용하면 사용한 데이터양은 초기화됩니다.
로밍 시 데이터 통신	[Android OS, Samsung(SAFE1+)] 해외 로밍 상태에서 데이터 통신 허용 여부를 설정합니다. • 허용: 데이터 통신을 할 수 있습니다. • 금지: 데이터 통신을 할 수 없습니다.

정책	설명
로밍 시 WAP 푸시	[Android OS, Samsung Only(SAFE1+)] [MDM 2.0] 해외 로밍 상태에서 WAP 푸시 통신 허용 여부를 설정합니다. • 허용: WAP 푸시 통신을 할 수 있습니다. • 금지: WAP 푸시 통신을 할 수 없습니다.
로밍 시 데이터 동기화	[Android OS, Samsung Only(SAFE1+)] [MDM 2.0] 해외 로밍 상태에서 데이터 동기화 허용 여부를 설정합니다. • 허용: 데이터 동기화를 허용합니다. • 금지: 데이터 동기화를 금지합니다.
로밍 시 음성 통화	[Android OS, Samsung Only(SAFE3+)] 해외 로밍 상태에서 음성 통화 허용 여부를 설정합니다. • 허용: 음성 통화를 허용합니다. • 금지: 음성 통화를 금지합니다.
SMS/MMS 수.발신 금지 설정	[Android OS, Samsung Only(SAFE3+)] SMS/MMS의 수신 및 발신 기능의 사용 금지 여부를 설정합니다. • 설정: SMS/MMS의 수신 및 발신 금지 설정을 허용합니다.
SMS/MMS 수.발신 금지	[Android OS, Samsung Only(SAFE3+)] 금지할 SMS/MMS의 수신 및 발신 기능을 선택합니다. • SMS 수신, SMS 발신, MMS 수신, MMS 발신
SIM카드 잠금 사용	[Android OS, Samsung Only(SAFE4+)] 단말에서 사용하는 SIM카드를 다른 단말에서 사용하지 못하도록 잠금 여부를 설정합니다. SIM 카드의 PIN 번호는 랜덤 생성되어 설정되며, SIM 카드가 잠긴 상태에서 다른 단말에 SIM카드를 사용하게되면 단말이 잠기고 PIN 번호를 입력해야 사용가능 합니다. 해당 SIM 카드의 PIN 번호는 단말 상세 화면에서 조회 가능합니다. • 사용: SIM카드 잠금을 허용합니다.
기본 SIM PIN	SIM 카드 상단에 표시된 기본 PIN 번호를 입력합니다. • 설정값: 4자리 숫자를 입력합니다. **Note:** 기업 소유의 단말인 COPE 단말 기준으로 사용되는 것이 목적이며, SIM 카드 상단에 표시된 기본 PIN 번호가 동일할 경우에만 해당 정책이 적용됩니다.

브라우저 그룹

정책	설명
Android 브라우저	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] Android에서 제공하는 브라우저의 사용 유무를 설정합니다. • 허용: 브라우저 사용을 허용합니다. • 금지: 브라우저 사용을 금지합니다.
쿠키	[Android OS, Samsung Only(SAFE2+)] Android 브라우저의 쿠키 사용 여부를 설정합니다. • 허용: 사용자가 쿠키 사용 메뉴를 변경할 수 있습니다. • 금지: 쿠키 사용을 할 수 없고 사용자가 쿠키 사용 메뉴를 변경할 수 없습니다.
자바스크립트	[Android OS, Samsung Only(SAFE2+)] Android 브라우저의 자바 스크립트 사용 여부를 설정합니다. • 허용: 사용자가 자바스크립트 사용 메뉴를 변경할 수 있습니다. • 금지: 자바스크립트 사용을 할 수 없고 사용자가 자바스크립트 사용 메뉴를 변경할 수 없습니다.
양식 데이터 저장	[Android OS, Samsung Only(SAFE2+)] Android 브라우저의 양식 데이터 저장 사용 여부를 설정합니다. • 허용: 사용자가 양식 데이터 저장 사용 메뉴를 변경할 수 있습니다. • 금지: 양식 데이터 저장을 할 수 없고 사용자가 양식 데이터 저장 사용 메뉴를 변경할 수 없습니다.
팝업 차단	[Android OS, Samsung Only(SAFE2+)] Android 브라우저의 팝업 차단 사용 여부를 설정합니다. • 허용: 사용자가 팝업 차단 사용 메뉴를 변경할 수 있습니다. • 금지: 팝업 차단을 할 수 없고 사용자가 팝업 차단 사용 메뉴를 변경할 수 없습니다.
브라우저 Proxy 주소	[Android OS, Samsung Only(Knox4.0.1+)] 일반 영역 내 Android 브라우저의 Proxy 주소를 설정합니다. 설정값은 IP 또는 도메인:Port 형식으로 입력합니다. **Note:** 적용 브라우저는 크롬과 삼성 기본 S 브라우저이며, 크롬 지원 버전은 Knox Standard SDK 4.0.1~5.6입니다.

Note: 브라우저 설정이 변경되는 경우 브라우저 전체 종료 후 재실행 시 적용됩니다.

시스템 그룹

정책	설명
공장 초기화	[Android OS, Samsung(SAFE2+)] [MDM 2.0] 사용자가 환경 설정 메뉴에서 공장 초기화를 수행할 수 있는지 허용 여부를 설정합니다. 하드웨어 키를 이용한 공장 초기화 모드도 제어가 되며, 다운로드 모드 진입 후 펌웨어 업데이트 유틸리티를 이용한 초기화는 제어할 수 없습니다. • 허용: 사용자가 공장 초기화를 수행할 수 있습니다. • 금지: 사용자가 공장 초기화를 수행할 수 없습니다.
전원 종료	[Android OS, Samsung Only(SAFE3+)] 사용자가 전원 종료하는 것을 허용할지 여부를 설정합니다. 전원 종료를 금지하면 단말 공장초기화가 진행되지 않습니다. 따라서 운영자가 공장초기화 명령을 보내도 진행이 되지 않으므로 주의해서 사용해야 합니다. • 허용: 전원 종료를 허용합니다. • 금지: 전원 종료를 금지합니다.
백업	[Android OS, Samsung Only(SAFE2+)] 사용자가 데이터 백업하는 것을 허용할지 여부를 설정합니다. • 허용: 백업을 허용합니다. • 금지: 백업을 금지합니다.
OTA 업그레이드	[Android OS, Samsung Only(SAFE3+)] OTA 업그레이드 허용 여부를 설정합니다. • 허용: OTA 업그레이드를 허용합니다. • 금지: OTA 업그레이드를 금지합니다.
환경 설정	[Android OS, Samsung Only(SAFE2+)] 환경 설정 변경 허용 여부를 설정합니다. • 허용: 환경 설정 변경을 허용합니다. • 금지: 환경 설정 변경을 금지합니다.
시스템 앱 종료	[Android OS, Samsung Only(SAFE4+)] 사용자가 시스템 앱을 강제로 종료하는 것을 허용할지 여부를 설정합니다. • 허용: 사용자가 시스템 앱을 종료할 수 있습니다. • 금지: 사용자가 시스템 앱을 종료할 수 없습니다.
앱 오류 발생 시 구글 보고	[Android OS, Samsung Only(SAFE3+)] 앱 오류 발생 시 사용자가 구글에 오류 정보를 보고할 수 있는지 여부를 설정합니다. • 허용: 구글에 오류 내용을 보고할 수 있습니다. • 금지: 구글에 오류 내용을 보고할 수 없습니다.
다중 사용자	[Android OS, Samsung Only(SAFE4+)] 단말에 추가 사용자 등록을 허용할지 여부를 설정합니다. • 허용: 단말에 추가 사용자를 등록할 수 있습니다. • 금지: 단말에 추가 사용자를 등록할 수 없습니다.
상태바 확장	[Android OS, Samsung Only(SAFE3+)] 상태바 확장 여부를 설정합니다. • 허용: 상태바 확장을 허용합니다. • 금지: 상태바 확장을 금지합니다.

정책	설명
배경화면 변경	[Android OS, Samsung Only(SAFE3+)] 사용자가 배경화면 및 잠금 화면 등을 변경할 수 있는지 여부를 설정합니다. • 허용: 변경을 허용합니다. • 금지: 변경을 금지합니다.
날짜, 시간 변경	[Android OS, Samsung Only(SAFE3+)] 사용자가 날짜, 시간 변경하는 것을 허용할지 여부를 설정합니다. • 허용: 변경을 허용합니다. • 금지: 변경을 금지합니다.
카메라	[Android 4.0(SDK14)+, Samsung(SAFE2+)] [MDM 2.0] 카메라 사용 허용 여부를 설정합니다. 일반 영역의 카메라를 제한하는 경우 Knox컨테이너의 카메라 기능은 사용할 수 없습니다. • 허용: 카메라 사용을 허용합니다. • 모두 금지: 카메라를 사용할 수 없습니다. • 녹화만 금지: 사진 촬영은 가능하나 동영상 녹화는 금지합니다. 삼성전자 단말에서만 사용이 가능합니다.
화면 캡처	[Android OS, Samsung(SAFE2+)] [MDM 2.0] 화면 캡처 허용 여부를 설정합니다. 화면 캡쳐의 기본 값은 허용이며, 관리자가 금지로 변경 시 캡쳐가 불가능합니다. • 허용: 화면 캡처를 허용합니다. • 금지: 화면 캡처를 금지합니다.
클립보드	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] 클립보드 사용 여부를 설정합니다. • 허용: 클립보드를 허용합니다. • 금지: 클립보드를 금지합니다. • 동일 앱 내 허용: 동일 앱 내에서만 클립보드를 사용할 수 있습니다.
공유 목록	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] 공유 목록 허용 여부를 설정합니다. • 허용: 공유 목록을 사용할 수 있습니다. • 금지: 공유 목록을 사용할 수 없습니다.
안드로이드 빔(S 빔)	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] 안드로이드 빔 기능 사용을 허용할 것인지 지정합니다. • 허용: Android 빔(S 빔)을 사용할 수 있습니다. • 금지: Android 빔(S 빔)을 사용할 수 없습니다.
저장소 암호화 설정	단말의 시스템 저장소 또는 외장SD 카드를 암호화할지 여부를 설정합니다. • 설정: 시스템 저장소 또는 외장 SD카드의 암호화를 설정할 수 있습니다.

정책	설명
저장소 암호화	[Android 4.1(SDK16)+, Samsung(SAFE2+)] 암호화할 저장소를 선택합니다. 내장 메모리는 전체 제조사를 지원하나 외장 SD 카드는 삼성전자만 가능합니다. • 시스템 저장소: 내장 메모리를 암호화합니다. • 외장 SD 카드: 외장 SD 카드 메모리를 암호화합니다.
외장 SD 카드	[Android OS, Samsung Only(SAFE2+)] 외장 SD 카드 사용을 허용할 것인지 설정합니다. • 허용: 외장 SD카드 사용을 허용합니다. • 금지: 외장 SD카드 사용을 금지합니다.
외장 SD 카드 쓰기	[Samsung Only(SAFE3+)] 외장 SD 카드 쓰기를 허용할 것인지 지정합니다. 외장 SD 카드 정책을 **허용**한 후, 쓰기 제어를 **금지**하면 외장 SD 카드의 읽기만 허용됩니다. • 허용: 외장 SD카드 쓰기를 허용합니다. • 금지: 외장 SD카드 쓰기를 금지합니다.
미인가 SD카드	[Android 1.0(SDK1)+] [MDM 2.0] 허가되지 않은 SD 카드를 사용하는지 탐지 여부를 설정합니다. • 미인가 SD 카드 사용 탐지: 미인가 SD 카드 사용을 탐지합니다. • 미인가 SD카드 사용 미탐지: 미인가 SD 카드 사용을 탐지하지 않습니다.
OS 위변조 시 조치	[Android 2.2(SDK8)+, Samsung(SAFE2+)] 단말의 OS 위변조를 감지하면 단말 잠금, 공장초기화 등 정책에 따라 동작합니다. • 단말 잠금: 단말의 OS 위변조를 감지하면 단말 잠금을 수행합니다. 이메일 잠금: 단말의 OS 위변조를 감지하면 이메일 잠금을 수행합니다. • 공장 초기화 + SD Card 초기화: 단말의 OS 위변조를 감지하면 사용자 단말을 공장 초기화시키며 SD 카드를 동시에 초기화 시킵니다. • 공장 초기화 (Only): 단말의 OS 위변조를 감지하면 사용자 단말을 공장 초기화시키며, SD 카드는 초기화되지 않습니다. **Note:** 2.0 버전 이하의 단말 Agent에서는 공장 초기화 (Only)가 적용되지 않기 때문에 공장 초기화를 하려면 공장 초기화 + SD Card 초기화를 선택해야 합니다.
스마트 클립	[Android OS, Samsung Only(SAFE5.2+)] 스마트 클립 허용 여부를 설정합니다. 삼성전자 단말의 기능 중 하나로, S 펜으로 원형을 그리면 일부만 캡처되어 다른 노트 등에서 활용할 수 있는 기능입니다. • 허용: 스마트 클립 사용을 허용합니다. • 금지: 스마트 클립 사용을 금지합니다.

정책	설명
기기관리자 앱 설치 및 활성화	[Android OS, Samsung Only(SAFE5+)] 기기관리자가 EMM 외의 다른 것(예. Airwatch MDM등 기기관리자가 사용하는 것)을 활성화하거나 설치되지 않도록 제어하는 기능입니다. 해당 정책을 설정하기 전에 미리 단말의 기기관리자에 다른 앱이 활성화 되어 있으면 제어할 수 없습니다. • 허용: 기기 관리자 앱 설치 및 활성화를 허용합니다. • 설치 금지: 기기 관리자 앱 설치를 금지합니다. • 기기 관리자 활성화 금지: 기기 관리자 앱의 활성화를 금지합니다.
디바이스관리자 설정의 예외적 앱 화이트리스트	[Android OS, Samsung Only(SAFE5+)] 기기관리자 앱 설치 및 활성화 허용 정책에서 설치 금지 또는 기기관리자 활성화 금지를 선택한 경우에만 화이트리스트 앱을 설정할 수 있는 정책입니다. 설치 금지를 선택한 경우, 목록에 등록된 앱만 설치를 허용하며, 활성화 금지를 선택한 경우, 목록에 등록된 앱만 기기관리자를 활성화시킵니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 앱 선택 후 **X** 클릭
개발자 모드 허용	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 개발자 모드 허용 여부를 설정합니다. • 허용: 개발자 모드를 허용합니다. • 금지: 개발자 모드를 금지합니다.
백그라운드 프로세스 제한 설정	[Android OS, Samsung Only(SAFE4+)] 백그라운드 프로세스 제한 설정 허용 여부를 설정합니다. • 허용: 백그라운드 프로세스 제한 설정을 허용합니다. • 금지: 백그라운드 프로세스 제한 설정을 금지합니다.
액티비티 종료 시 앱 종료	[Android OS, Samsung Only(SAFE4+)] 액티비티 종료 시 앱 종료 설정 허용 여부를 지정합니다. • 허용: 액티비티 종료 시 앱 종료 설정을 허용합니다. • 금지: 액티비티 종료 시 앱 종료 설정을 금지합니다.
모의 위치	[Android OS, Samsung(SAFE2+)] [MDM 2.0] 모의 위치 사용을 허용할지 여부를 지정합니다. 모의 위치는 일반적으로 개발이나 테스트 용도로 현재 위치를 임의로 지정하는 것을 의미합니다. **모의 위치 사용 허용**은 단말 제어 명령(단말 정보 업데이트)에 대하여 잘못된 위치를 얻어올 수 있는 우려가 있을 때 사용합니다. • 허용: 모의 위치 사용을 허용합니다. • 금지: 모의 위치 사용을 금지합니다.
안전 모드	[Android OS, Samsung Only(SAFE4+)] 부팅 시 하드웨어 키에 의해서 진입되는 안전 모드 허용 여부를 지정합니다. 안전 모드에서 카메라 제어 등의 단말 제어 기능은 유지되지만 EMM 앱 및 Preload된 앱은 실행할 수 없습니다. • 허용: 안전 모드를 허용합니다. • 금지: 안전 모드를 금지합니다

정책	설명
재부팅 배너	[Android OS, Samsung Only(SAFE4+)] 사용자의 단말이 부팅시 보여질 재부팅 배너의 사용 여부를 설정합니다. 재부팅 배너를 설정하면 단말의 부팅 혹은 재부팅 시 Android 4.4 (SAFE 4.0) 단말은 제조업체가 등록한 문구만 배너로 보여집니다. Android 5.0 (SAFE 5.2 이상) 단말에서는 특정 문구의 설정과 배너 노출이 가능합니다. • 사용: 재부팅 배너를 사용합니다. • 미사용: 재부팅 배너를 사용하지 않습니다.
재부팅 배너 문구	[Android OS, Samsung Only(SAFE5.2+)] 사용자의 단말이 부팅시 보여질 재부팅 배너의 문구를 입력합니다. 1000 Byte까지 입력 가능합니다.
도메인 블랙 리스트 설정	도메인 블랙 리스트 설정 여부를 지정합니다. • 도메인 블랙 리스트: 사용자가 단말에 Exchange 와 Email 계정을 등록할 경우, 사용하면 안되는 도메인 리스트를 설정할 수 있습니다.
도메인 블랙 리스트	[Android OS, Samsung Only(SAFE4+)] 지정된 도메인 리스트를 차단하는 정책입니다. Exchange와 Email에 계정 등록시 사용하면 안되는 도메인 리스트를 입력합니다. • 추가: 도메인 입력 후 ⊕ 클릭 • 삭제: 목록에서 도메인 선택 후 **X** 클릭
NTP 설정	NTP (Network Time Protocol) 서버 사용 여부를 설정합니다. NTP서버를 등록하여 단말의 시간에 NTP 서버의 시간 정보를 반영하는 정책입니다. • 허용: NTP 사용을 허용합니다. • 금지: NTP 사용을 금지합니다.
서버 주소	[Android OS, Samsung Only(SAFE5.5+)] NTP 서버 주소를 입력합니다.
최대 시도 횟수 (회)	[Android OS, Samsung Only(SAFE5.5+)] 시간 정보를 조회하기 위하여 NTP 서버에 접속을 시도하는 최대 시도 횟수를 설정합니다. • 설정값: 0~100 회
폴링 주기 (시간)	[Android OS, Samsung Only(SAFE5.5+)] NTP 서버에 재 연결을 시도하는 주기를 설정합니다. • 설정값: 0~8760 시간(1년)
짧은 폴링 주기 (초)	[Android OS, Samsung Only(SAFE5.5+)] 타임 아웃 발생 후 NTP 서버에 재 연결을 시도하는 주기를 설정합니다. • 설정값: 0~1000 초
타임아웃 (초)	[Android OS, Samsung Only(SAFE5.5+)] NTP 서버에 연결 제한시간을 설정합니다. • 설정값: 0~1000 초

정책	설명
이벤트 On 알림	[Android 1.0(SDK1.4)+] [MDM 2.0] 설정한 이벤트가 적용되는 시점에 단말 알림을 표시를 설정합니다. • 사용자 지정: 사용자가 단말에서 이벤트 알림 설정을 지정합니다. EMM Client의 **서비스** 메뉴에서 설정합니다. • 알림 표시: 이벤트 적용되는 시점에 알림을 표시합니다. • 알림 숨김: 이벤트 적용되는 시점에 알림을 숨깁니다.
이벤트 Off알림	[Android 1.0(SDK1.4)+] [MDM 2.0] 설정한 이벤트가 해제되는 시점에 단말 알림을 표시를 설정합니다. • 사용자 지정: 사용자가 단말에서 이벤트 알림 설정을 지정합니다. EMM Client의 **서비스** 메뉴에서 설정합니다. • 알림 표시: 이벤트 적용되는 시점에 알림을 표시합니다. • 알림 숨김: 이벤트 적용되는 시점에 알림을 숨깁니다.
이벤트 알림 고정	[Android 1.0(SDK1.5)+] [MDM 2.0] 단말의 퀵 패널에 EMM 아이콘을 삭제 또는 삭제 불가능하도록 고정시키는 정책입니다. • 사용자 지정: 사용자가 단말에서 이벤트 고정 여부를 설정합니다. EMM Client의 **서비스** 메뉴에서 설정합니다. • 알림 제거 불가: 사용자의 단말에 EMM 아이콘이 고정됩니다. • 알림 제거 가능: 사용자의 단말의 퀵 패널에서 Swipe하여 아이콘을 제거 가능 합니다.
E-FOTA	[Android OS, Samsung Only(SAFE5.5+)] 단말의 펌웨어를 무선으로 업그레이드하는 FOTA 서비스를 통하여 특정 펌웨어 버전으로 업데이트를 허용할지 여부를 설정합니다. • 사용: 설정된 펌웨어로 업데이트를 진행합니다. 설정한 범위 외의 펌웨어로 업데이트 할 수 없습니다. • 미사용: 사용자가 단말 OS별로 제공되는 펌웨어 버전을 선택하여 업데이트를 진행합니다.
절전 모드 제어	[Android OS, Samsung Only(SAFE5.8+)] 단말에서 배터리 절전 모드 제어를 허용할지 여부를 설정합니다. • 허용: 사용자가 단말에서 절전 모드 제어를 직접 할 수 있습니다. • 금지: 절전 모드는 사용안함으로 설정되며, 단말의 설정 메뉴에서 절전 모드가 사라져 사용자가 변경할 수 없습니다.

스케줄러 그룹

정책	설명
정책 업데이트 스케줄	[MDM 2.0] 사용자의 단말에 정책 업데이트를 수행할 스케줄러를 설정합니다. • 요일: 일/월/화/수/목/금/토 중 선택합니다. • 시간대: 나라/도시별 시간대를 선택합니다. • 시작시간: 시각과 분을 24시간 단위로 입력합니다. 예) 오후 2시 30분이면 1430로 입력 - 설정값: 0000~2359 (HH24MM) • Random Seed: **시작시간**에 지정한 시각 이후 업데이트를 진행할 시간을 지정합니다. - 설정값: 1~60 분
EMM 앱 업데이트 스케줄	사용자의 단말에 EMM Agent 업데이트를 수행할 스케줄러를 설정합니다. • 요일: 일/월/화/수/목/금/토 중 선택합니다. • 시작 시간: 시각과 분을 24시간 단위로 입력합니다. 예) 오후 2시 30분이면 1430로 입력 - 설정값: 0000~2359 (HH24MM) • Random Seed: **시작 시간**에 지정한 시각 이후 업데이트를 진행할 시간을 지정합니다. - 설정값: 1~60 분 **Note:** 스케줄 시간은 단말 시간을 기준으로 하기 때문에 단말의 시간, 시간대 등의 요인에 의해 정책이 변동될 수 있습니다.

로깅 그룹

정책	설명
로그 기록	[Android 1.0(SDK1)+] [MDM 2.0] 단말의 로그 기록 여부를 설정합니다. 미 설정 시 기본값은 로깅 사용입니다. • 사용: 로깅 관련 정책을 설정하여 로깅을 사용합니다. • 미사용: 로깅을 수행하지 않습니다.
로그 기록 수준	[Android 1.0(SDK1)+] [MDM 2.0] 기록할 로그의 수준을 설정합니다. 로그 기록 수준의 미 설정 시(—) 기본값은 DEBUG 입니다. • DEBUG: 개발자에게 필요한 상세한 정보 기록 • INFO: 운영자에게 필요한 정보 기록 • WARNING: 에러는 아니지만 주의할 정보기록 • ERROR: 일반적인 오류 발생에 대한 정보 기록 • FATAL: 시스템 중단 등의 심각한 오류 발생에 대한 정보 기록

정책	설명
로그 최대 수집 용량 (MB)	[Android 1.0(SDK1)+] [MDM 2.0] 로그 파일로 저장되는 최대 로그 용량을 설정합니다. • 설정값: 0~20 MB
로그 최대 보관 기간 (일)	[Android 1.0(SDK1)+] [MDM 2.0] 로그에 대한 최대 보관 기간을 설정합니다. • 설정값: 0~30 일

방화벽 그룹

방화벽 설정은 SDK 2.6 이상인 경우 IPv6 를 지원하며 , IPv4 와 IPv6 주소가 물리적으로 동일한 주소를 의미하더라도 별도로 설정을 해야합니다 .

앱별로 IP 또는 도메인 방화벽 정책을 설정할 수 있으며 , 전체 앱에 대하여 특정 방화벽을 허용 또는 금지하려면 패키지명에 와일드카드 (*) 를 입력합니다 .

여러개의 방화벽이 설정되어 있는 경우 제약적인 제어의 우선순위가 높습니다 .

- 전체 앱과 특정 앱에 방화벽 설정이 되어 있는 경우 앱별 정책의 우선순위가 높습니다.
- 허용 정책에 와일드 카드(*)를 사용하여 전체를 설정하면, 금지 정책에 특정 IP 또는 도메인을 입력하더라도 모든 IP 또는 모든 도메인 접근이 가능합니다.

정책	설명
방화벽	[Android OS, Samsung Only(SAFE2+)] 방화벽 사용 여부를 설정합니다. 허용 정책이 금지 정책보다 우선합니다. 정책이 적용되지 않으면 기본적으로 허용 상태이므로 허용 정책은 금지 정책에 예외 되는 대상 IP 및 포트를 설정할 때 사용합니다. • 사용: 방화벽을 사용합니다. • 미사용: 방화벽을 사용하지 않습니다.
허용 정책(앱별)	[Android OS, Samsung Only(SAFE5.5+)] 허용할 대상 IP 및 포트를 설정합니다. 특정 IP 및 포트만을 허용하기 위해서는 **금지 정책**의 **IP 주소(범위)**와 **포트(범위)**를 ***로 설정하여, 전체 차단 후 동작하도록 설정해야 합니다. 1. IP 주소(범위), 포트(범위) 입력 2. 적용 포트 범위 설정값 선택: • 모두 • 로컬: 단말에서 해당 포트 사용이 허용됩니다. • 원격: 대상 서버의 포트로 접속이 허용됩니다. 3. 허용하려는 애플리케이션의 패키지명을 입력하거나 을 클릭하여 선택한 후, 을 클릭하여 추가

정책	설명
금지 정책(앱별)	[Android OS, Samsung Only(SAFE5.5+)] 금지할 대상 IP 및 포트를 설정합니다. IP 주소 입력 시 와일드 카드(*)를 사용하여 대역 범위를 금지할 수 있습니다. 로컬 IP 주소로 설정할 경우 단말에서 해당 포트 사용이 금지되며, 원격으로 설정할 경우 대상 IP 및 Port로 접근이 차단됩니다. 1. IP 주소(범위), 포트(범위) 입력 2. 적용 포트 범위 설정값 선택: • 모두 • 로컬: 단말에서 해당 포트 사용이 금지됩니다. • 원격: 대상 서버의 포트로 접속이 차단됩니다. 3. 금지하려는 애플리케이션의 패키지명을 입력하거나 을 클릭하여 선택한 후, 을 클릭하여 추가
허용 정책(도메인)	[Android OS, Samsung Only(SAFE5.6+)] 허용할 도메인 주소를 설정합니다. 도메인 주소 입력 시 와일드 카드(*)를 사용하여 특정 도메인을 허용할 수 있으며, 와일드 카드(*)는 도메인의 앞 또는 뒤에 위치해야하며 중간에 입력은 불가합니다. 예) *android.com 또는 www.samsung* 특정 도메인만을 허용하기 위해서는 금지 정책을 *로 설정하여 전체 도메인을 차단한 후 동작하도록 설정해야합니다. 1. 허용하려는 애플리케이션의 패키지명을 입력하거나 을 클릭하여 선택 2. 도메인 주소(범위)를 입력한 후 을 클릭하여 추가
금지 정책(도메인)	[Android OS, Samsung Only(SAFE5.6+)] 금지할 도메인 주소를 설정합니다. 도메인 주소 입력 시 와일드 카드(*)를 사용하여 특정 도메인을 금지할 수 있습니다. 로컬로 설정할 경우 단말에서 해당 도메인 사용이 금지되며, 원격으로 설정할 경우 대상 도메인으로 접근이 차단됩니다. 1. 금지하려는 애플리케이션의 패키지명을 입력하거나 을 클릭하여 선택 2. 도메인 주소(범위)를 입력한 후 을 클릭하여 추가
DNS 설정	[Android OS, Samsung Only(SAFE5.7+)] 전체앱 또는 등록한 앱의 도메인 서버 주소를 설정합니다. 앱당 하나의 DNS만 설정이 가능하며, 앱에 할당된 VPN이나 Proxy 정책이 없을 때만 적용됩니다. 1. 애플리케이션의 패키지명을 입력하거나 을 클릭하여 선택 2. Primary DNS를 **DNS1**에, Secondary DNS를 **DNS2**에 IP 주소 형식으로 입력한 후 을 클릭하여 추가

Android for Work 단말 관리 정책

Android for Work 정책 목록은 다음과 같습니다 .

시스템 그룹

정책	설명
Android for Work 사용	Android for Work 사용의 허용 여부를 설정합니다. • 허용: Android for Work 사용을 허용합니다. • 금지: Android for Work 사용을 금지합니다. **Note:** • Android for Work은 Android LOLLIPOP(5.0) 이상 버전에서 지원됩니다. • 단말에 Android for Work이 설치되면 앱 아이콘에 뱃지가 표시되어 일반앱과 구분되며, 단말의 **설정 > 계정/업무용 프로필 삭제**에서 확인 및 삭제가 가능합니다. 또한 미 설치 시 단말의 **설정 > 미설치**에서 Android for Work을 추가 설치할 수 있습니다.
화면 캡처	[Android 5.0(SDK21+)] Android for Work 앱의 화면 캡처 허용 여부를 설정합니다. • 허용: 화면 캡처를 허용합니다. • 금지: 화면 캡처를 금지합니다.
클립보드	[Android 5.0(SDK21+)] Android for Work 앱의 문자열 복사 사용 여부를 설정합니다. • 허용: 클립보드를 허용합니다. • 금지: 클립보드를 금지합니다.

iOS 단말 관리 정책

iOS 단말의 정책 목록은 다음과 같습니다 .

보안 그룹

정책	설명
비밀번호 정책	단말 화면 잠금 비밀번호 제어 여부를 설정합니다. • 설정: 단말 화면 잠금 비밀번호 제어합니다.
비밀번호 강도	[iOS 4.0+] 단말 화면 잠금 비밀번호의 강도를 설정합니다. • 없음: 1자리 이상의 숫자로 이루어진 비밀번호를 설정해야합니다. • 4자리숫자: 4자리의 숫자로 이루어진 비밀번호를 사용할 수 있도록 설정합니다. • 영숫자포함: 영어, 숫자를 반드시 포함하여 비밀번호를 설정해야 합니다. • 특수문자포함: 특수 문자를 반드시 포함하여 비밀번호를 설정해야 합니다.
비밀번호 입력 실패 허용 횟수 (회)	[iOS 4.0+] 입력 실패 허용 횟수 이상으로비밀번호를 잘못 입력하면 단말을 초기화합니다. 단, 잘못된 비밀번호를 동일하게 여러번 입력하면 한번의 실패로 처리됩니다. • 설정값: 1~10 회
비밀번호 최소 길이 (자)	[iOS 4.0+] 비밀번호의 최소 길이를 설정합니다. • 설정값: 1~16 자
비밀번호 최대 사용 기간 (일)	[iOS 4.0+] 비밀번호를 사용할 수 있는 최대 기간이 지나면 비밀번호를 재설정하도록 합니다. • 설정값: 0~730 일 • 0 : 최대 사용 기간이 무기한입니다.
비밀번호 내역 관리 (회)	[iOS 4.0+] 사용자가 비밀번호를 변경할 때 지정된 수 만큼의 최근 비밀번호 내역 중에서 유일한 비밀번호를 사용하도록 합니다. • 설정값: 1~50 회
화면 잠금 시간 (분)	[iOS 4.0+] 사용자가 선택할 수 있는 자동 화면 잠금 시간의 최대값을 설정하여 제한합니다. • 0 분: 안함 • 1 분: iPhone만 설정 가능합니다. • 2 분 • 3 분: iPhone만 설정 가능합니다. • 4 분: iPhone만 설정 가능합니다. • 5 분 • 10 분: iPad만 설정 가능합니다. • 15 분: iPad만 설정 가능합니다.

정책	설명
화면 잠금 유예 시간 (분)	[iOS 4.0+] 사용자가 단말 화면을 끈 후 비밀번호를 입력하지 않고 단말의 잠금을 해제할 수 있는 유예시간의 최대값을 지정합니다. • 0분: 즉시 단말 잠금을 합니다. • 1분 • 5분 • 15분 • 60분 • 240분
지문(Touch ID)으로 화면 잠금 해제	[iOS 7.0+] 사용자가 지문인식을 통해 화면 잠금 해제하는 것을 허용할지 여부를 설정합니다. • 허용: 지문으로 화면 잠금 해제하는 것을 허용합니다. • 금지: 지문으로 화면 잠금 해제하는 것을 금지합니다.

앱 그룹

정책	설명
앱 설치	[iOS 4.0+] 단말에서 EMM서비스를 통하지 않고 앱 설치하는 것을 허용할지 여부를 설정합니다. 앱 설치는 MDM을 통해 가능하며, itunes을 통한 앱 설치는 불가능합니다. • 허용: 앱을 설치할 수 있습니다. • 금지: AppStore 앱이 사라지고 단말에 앱을 설치할 수 없습니다. **Note:** 앱 설치 정책을 **금지**로 설정한 경우 iOS 버전별 앱 설치 제약은 다음과 같습니다. • iOS 9 이상 버전에서는 Knox Manage 앱 스토어에서 사내 또는 사외 앱은 설치 가능합니다. • iOS 8 이하 버전에서는 Knox Manage 앱 스토어에서 사내 앱만 설치 가능합니다.
App Store를 사용하여 App 설치 허용	[iOS 9.0+, Supervised] App Store를 통해 App 설치 허용 여부를 설정합니다. 앱 설치는 MDM과 itunes을 통해 가능합니다. • 허용: App Store를 통해 App 설치를 허용합니다. • 금지: App Store를 통해 App 설치를 금지합니다.
앱 삭제	[iOS 6.0+, Supervised] 단말에서 EMM서비스를 통하지 않고 앱 삭제하는 것을 허용할지 여부를 설정합니다. • 허용: 사용자가 앱 삭제하는 것을 허용합니다. • 금지: 사용자가 앱 삭제하는 것을 금지합니다.
iTunes Store	[iOS 4.0+] 단말에서 iTunes Store 사용 허용 여부를 설정합니다. • 허용: iTunes Store 사용을 허용합니다. • 금지: iTunes Store 사용을 금지합니다.
유해한 음악 및 Podcast	[iOS 4.0+] 사용자가 iTunes Store에서 구입한 무삭제판 음악이나 동영상 콘텐츠를 허용할지 여부를 설정합니다. • 허용: 콘텐츠를 허용합니다. • 금지: 콘텐츠를 금지합니다.

정책	설명
구입할 때마다 iTunes Store, 비밀번호 요구	[iOS 5.0+] 사용자가 iTunes Store에서 콘텐츠를 구입할 때 마다 iTunes Store 비밀번호를 입력하도록 강제할지 여부를 설정합니다. • 사용: 구입할 때마다 비밀번호를 입력하도록 합니다. • 미사용: 구입할 때마다 비밀번호를 입력하지 않아도 됩니다.
게임 센터	[iOS 6.0+, Supervised] 단말에서 게임 센터 사용 허용 여부를 설정합니다. • 허용: 게임 센터 사용을 허용합니다. • 금지: 게임 센터 사용을 금지합니다.
게임 센터에서 친구 추가	[iOS 4.0+] 게임 센터 허용 시 친구 추가 허용 여부를 설정합니다. • 허용: 친구 추가를 허용합니다. • 금지: 친구 추가를 금지합니다.
멀티플레이어 게임	[iOS 4.0+] 게임 센터 허용 시 멀티 플레이어 게임 허용 여부를 설정합니다. • 허용: 멀티 플레이어 게임을 허용합니다. • 금지: 멀티 플레이어 게임을 금지합니다.
iBookstore	[iOS 7.0+, Supervised] 단말에서 iBookstore 사용 허용 여부를 설정합니다. • 허용: iBookstore 사용을 허용합니다. • 금지: iBookstore 사용을 금지합니다.
iBookestore에서 선정성 미디어 다운로드	[iOS 6.0+, Supervised] iBookstore 허용 시 선정성 미디어 다운로드 허용 여부를 설정합니다. • 허용: 다운로드를 허용합니다. • 금지: 다운로드를 금지합니다.
메시지 앱	[iOS 6.0+, Supervised] 단말에서 메시지 앱 사용 허용 여부를 설정합니다. • 허용: 메시지 앱 사용을 허용합니다. • 금지: 메시지 앱 사용을 금지합니다.
YouTube	[iOS 5.1 below] 단말에서 YouTube 사용 허용 여부를 설정합니다. • 허용: YouTube 사용을 허용합니다. • 금지: YouTube 사용을 금지합니다.
나의 친구 찾기	[iOS 7.0+, Supervised] 단말에서 **나의 친구 찾기** 사용 허용 여부를 설정합니다. • 허용: 사용을 허용합니다. • 금지: 사용을 금지합니다.
앱내 구매	[iOS 4.0+] 앱 내 구매 허용 여부를 설정합니다. 앱 내 구매 유형으로 소모품(추가 경험치), 비 소모품(도시 안내 지도), 비 갱신 구독(한달 구독), 자동 갱신 가능 구독(주간 신문) 등이 존재합니다. • 허용: 앱 내 구매를 허용합니다. • 금지: 앱 내 구매를 금지합니다.

정책	설명
앱 블랙/화이트 리스트 설정	[iOS 4.0+] 앱 제어 정책을 블랙리스트 또는 화이트리스트 기준으로 설정할 것인지 지정합니다. • 앱 블랙리스트 설정: 블랙리스트는설치하면 안되는 앱을 설정합니다. • 앱 화이트리스트 설정: 화이트리스트는설치 가능한 앱을 설정합니다. • 앱 블랙/화이트 리스트 설정: 블랙리스트/화이트리스트 정책을 동시에 적용할 수 있습니다. **앱 > 앱 설치** 정책은 금지로 설정됩니다. **Note:** 앱 블랙/화이트리스트 설정 후 앱을 추가하지 않으면 시스템 앱(EMM Client)과 필수앱(Secure Browser, mMail)을 제외한 모든 앱의 설치가 금지됩니다.
앱 설치 블랙리스트	[iOS 4.0+] 지정된 앱 설치를 차단하는 정책입니다. 이미 앱 설치 화이트리스트에 추가된 앱은 앱 설치 블랙리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 선택 • 삭제: 목록에서 앱 선택 후 **X** 클릭
앱 설치 화이트리스트	[iOS 4.0+] 목록에 등록된 앱만 설치를 허용하는 정책입니다. 이미 앱 설치 블랙리스트에 추가된 앱은 앱 설치 화이트리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 선택 • 삭제: 목록에서 앱 선택 후 **X** 클릭
자동 Single 앱 모드 허용 앱 설정	[iOS 7.0+, Supervised] 자동 Single 앱 모드 허용 여부를 설정합니다. App. Lock 기능을 수행할 수 있는 권한을 부여하는 기능입니다. • 설정: 자동 Single 앱 모드를 사용할 앱을 설정합니다.
자동 Single 앱 모드 허용 앱	[iOS 7.0+, Supervised] 자동 Single 앱 모드를 사용할 수 있는 앱 목록을 지정합니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 선택 • 삭제: 목록에서 삭제할 앱 선택 후 **X** 클릭
기업용 App 신뢰하기	[iOS 9.0+] 기업용 App 신뢰하기 허용 여부를 설정합니다. 기업용 App 신뢰하기를 금지로 설정하고 정책이 적용되면 이후, 설치된 기업용 앱들은 실행되지않습니다. 금지 정책을 내리기 전에 사용자가 신뢰하기를 허용한 기업용 앱들은 실행이 가능합니다. • 허용: 기업용 App 실행을 허용합니다. • 금지: 기업용 App 실행을 금지합니다.

전화 그룹

정책	설명
앱별 셀룰러 데이터 사용 여부 변경	[iOS 7.0+, Supervised] 앱별 통신사 데이터 사용량의 변경 허용 여부를 설정합니다. • 허용: 변경을 허용합니다. • 금지: 변경을 금지합니다.
화상 통화	[iOS 4.0+] 화상 통화 허용 여부를 설정합니다. • 허용: 화상 통화를 허용합니다. • 금지: 화상 통화를 금지합니다.
음성 다이얼	[iOS 4.0+] 음성 다이얼 허용 여부를 설정합니다. • 허용: 음성 다이얼을 허용합니다. • 금지: 음성 다이얼을 금지합니다.
로밍상태에서 백그라운드 작업	[iOS 4.0+] 로밍 상태에서 백그라운드 작업 허용 여부를 설정합니다. • 허용: 백그라운드 작업을 허용합니다. • 금지: 백그라운드 작업을 금지합니다.

공유 그룹

정책	설명
Managed 앱에서 Unmanaged 앱으로의 데이터 공유	[iOS 7.0+] Samsung SDS EMM 서버로부터 설치된 Managed 앱에서 사용자가 임의로 설치한 Unmanaged 앱으로 데이터 전송을 허용할지 여부를 설정합니다. • 허용: 데이터 전송을 허용합니다. • 금지: 데이터 전송을 금지합니다.
Unmanaged 앱에서 Managed 앱으로의 데이터 공유	[iOS 7.0+] 사용자가 임의로 설치한 Unmanaged 앱에서 EMM 서버로부터 설치된 Managed 앱으로 데이터 전송을 허용할지 여부를 설정합니다. • 허용: 데이터 전송을 허용합니다. • 금지: 데이터 전송을 금지합니다.
AirDrop	[iOS 7.0+, Supervised] 단말에서 AirDrop 사용 허용 여부를 설정합니다. • 허용: AirDrop 사용을 허용합니다. • 금지: AirDrop 사용을 금지합니다.
AirDrop을 관리되지 않는 대상으로 취급	[iOS 9.0+, Supervised] 단말에서 AirDrop을 사용 시 관리되는 문서의 공유 허용 여부를 설정합니다. • 허용: 문서 공유를 허용합니다. • 금지: 문서 공유를 금지합니다.

iCloud 그룹

정책	설명
백업	[iOS 5.0+] 단말의 데이터를 iCloud에 백업하는 것을 허용할지 여부를 설정합니다. • 허용: iCloud에 백업하는 것을 허용합니다. • 금지: iCloud에 백업하는 것을 금지합니다.
도큐멘트 동기화	[iOS 5.0+] 단말의 문서를 iCloud에 동기화 하는 것을 허용할지 여부를 설정합니다. • 허용: iCloud에 동기화하는 것을 허용합니다. • 금지: iCloud에 동기화하는 것을 금지합니다.
사진 보관함	[iOS 9.0+] iCloud의 사진 보관함을 허용할지 여부를 설정합니다. • 허용: iCloud의 사진 보관함 사용을 허용합니다. • 금지: iCloud의 사진 보관함 사용을 금지합니다.
나의 사진 스트림	[iOS 5.0+] 단말의 사진을 iCloud에 저장하는 것을 허용할지 여부를 설정합니다. • 허용: iCloud에 사진 저장하는 것을 허용합니다. • 금지: iCloud에 사진 저장하는 것을 금지합니다.
사진 공유	[iOS 6.0+] iCloud를 통해 사진을 다른 사람과 공유하는 것을 허용할지 여부를 설정합니다. • 허용: iCloud를 통해 사진 공유하는 것을 허용합니다. • 금지: iCloud를 통해 사진 공유하는 것을 금지합니다.
키체인 동기화	[iOS 7.0+] 사용자의 모든 장비에서 사용자의 계정, 이름, 비밀번호, 신용 카드 번호, 이메일, 연락처, 일정 등을 iCloud와 동기화하는 것을 허용할지 여부를 설정합니다. • 허용: 키체인 동기화를 허용합니다. • 금지: 키체인 동기화를 금지합니다.
Managed 앱 동기화	[iOS 8.0+] EMM 서버로부터 설치된 Managed 앱을 iCoud 와 동기화하는것을 허용할지 여부를 설정합니다. Managed 앱 동기화를 금지하면 Managed 앱의 데이터가 iCloud에 저장되지 않습니다. • 허용: Managed 앱 동기화를 허용합니다. • 금지: Managed 앱 동기화를 금지합니다.
핸드오프	[iOS 8.0+] 핸드 오프 기능 허용 여부를 설정합니다. 핸드오프를 금지하면 iCloud를 통한 단말 간의 업무 연속성 기능을 사용할 수 없게 됩니다. • 허용: 핸드 오프 사용을 허용합니다. • 금지: 핸드 오프 사용을 금지합니다.

브라우저 그룹

정책	설명
Safari	[iOS 4.0+] iOS 기본 브라우저인 Safari 사용 허용 여부를 설정합니다. • 허용: Safari 사용을 허용합니다. • 금지: Safari 사용을 금지합니다.
쿠키	[iOS 6.0 and below] Safari 사용 시 쿠키 사용 허용 여부를 설정합니다. • 허용안함: 쿠키 사용을 금지합니다. • 방문한 사이트만 허용: 방문한 사이트에 한하여 쿠키 사용을 허용합니다. • 항상: 쿠키 사용을 허용합니다.
자바스크립트	[iOS 6.0 and below] 브라우저의 자바 스크립트의 실행 허용 여부를 설정합니다. • 허용: 사용자가 자바스크립트 실행여부를 선택할 수 있습니다. • 금지: 자바스크립트 사용을 할 수 없고 사용자가 자바스크립트 사용 메뉴를 변경할 수 없습니다.
양식 데이터 저장	[iOS 4.0+] Safari에서 웹 페이지상에 입력하는 내용들의 자동완성 기능을 허용할지 여부를 설정합니다. • 허용: 양식 데이터 저장을 허용합니다. • 금지: 양식 데이터 저장을 금지합니다.
팝업 차단	[iOS 4.0+] 브라우저의 팝업 강제 차단 사용 여부를 설정합니다. • 허용: 팝업을 강제로 차단합니다. • 금지: 팝업 차단 여부를 사용자가 설정합니다.
신뢰할 수 없는 TLS 인증서	[iOS 5.0+] HTTPS(TLS)로 접근 시 공인 인증이 아닌 사설 인증서일 때 접근 동의 팝업 창이 보일지 여부를 설정합니다. • 허용: 접근 동의 팝업창을 허용합니다. • 금지: 접근 동의 팝업창을 금지합니다.
위조된 웹사이트 경고	[iOS 4.0+] 위조된 웹사이트 방문 시 경고 여부를 설정합니다. • 강제 사용: 항상 경고합니다. • 사용자 선택: 경고 여부를 사용자가 설정합니다.

시스템 그룹

정책	설명
카메라	[iOS 4.0+] 단말에서 카메라 사용 허용 여부를 설정합니다. • 허용: 카메라 사용을 허용합니다. • 금지: 카메라 사용을 금지합니다.
화면 캡처	[iOS 4.0+] 단말에서 화면 캡처 허용 여부를 설정합니다. 화면 캡쳐의 기본 값은 허용이며, 관리자가 금지로 변경 시 캡쳐가 불가능합니다. • 허용: 화면 캡처를 허용합니다. • 금지: 화면 캡처를 금지합니다.

정책	설명
Siri	[iOS 5.0 (iPhone 4S), iOS 6.0 (iPad 3)] 단말에서 Siri 사용 여부를 설정합니다. • 허용: Siri 제어를 허용합니다. • 금지: Siri 제어를 금지합니다.
잠금화면에서 Siri	[iOS 5.1 (iPhone 4S), iOS 6.0 (iPad 3)] Siri 제어 허용 시 잠금 화면에서도 Siri 사용을 허용할지 여부를 설정합니다. • 허용: 잠금 화면에서도 Siri 사용을 허용합니다. • 금지: 잠금 화면에서 Siri 사용을 금지합니다.
Siri에서 웹검색 결과	[iOS 7.0+, Supervised] Siri에서 웹 검색 결과를 표시할지 여부를 설정합니다. • 허용: Siri 검색 결과 보기를 허용합니다. • 금지: Siri 검색 결과 보기를 금지합니다.
Siri 비속어 필터	[iOS 5.0 (iPhone 4S), iOS 6.0 (iPad 3) +Supervised] Siri에서 비속어 필터를 사용하도록 할 것인지 설정합니다. • 강제 사용: 욕설 필터를 사용하도록 합니다. • 사용자 선택: 욕설 필터 사용 여부를 사용자가 설정합니다.
진단 및 사용내용 보내기	[iOS 6.0+] 단말의 진단 및 사용 내용을 Apple로 보내도록 허용할지 여부를 설정합니다. • 허용: Apple로 보내는 것을 허용합니다. • 금지: Apple로 보내는 것을 금지합니다.
잠금화면에서 Passbook	[iOS 6.0+] 잠금 화면에서도 Passbook 사용 여부를 설정합니다. • 허용: 잠금 화면에서 Passbook 사용을 허용합니다. • 금지: 잠금 화면에서 Passbook 사용을 금지합니다.
잠금화면에서 제어 센터	[iOS 7.0+] 잠금 화면에서도 제어 센터 사용을 허용할지 여부를 설정합니다. • 허용: 제어 센터 사용을 허용합니다. • 금지: 제어 센터 사용을 금지합니다.
잠금화면에서 알림보기	[iOS 7.0+] 잠금 화면에서도 알림 보기 사용을 허용할지 여부를 설정합니다. • 허용: 알림 보기 사용을 허용합니다. • 금지: 알림 보기 사용을 금지합니다.
잠금화면에서 오늘보기	[iOS 7.0+] 잠금 화면에서도 오늘 보기 사용을 허용할지 여부를 설정합니다. • 허용: 오늘 보기 사용을 허용합니다. • 금지: 오늘 보기 사용을 금지합니다.
프로파일 수동 설치	[iOS 6.0+, Supervised] Apple Configuration Profile을 사용자가 수동으로 설치하는 것을 허용할지 여부를 설정합니다. • 허용: 수동 설치하는 것을 허용합니다. • 금지: 수동 설치하는 것을 금지합니다.
계정 정보 수정 제어	[iOS 7.0+, Supervised] 사용자 계정 정보 수정을 허용할지 여부를 설정합니다. • 허용: 수정을 허용합니다. • 금지: 수정을 금지합니다.

정책	설명
인증서 신뢰 설정 자동 업데이트	[iOS 7.0+] 신뢰할 수 있는 인증서의 자동 업데이트 허용 여부를 설정합니다. • 허용: 인증서 자동 업데이트를 허용합니다. • 금지: 인증서 자동 업데이트를 금지합니다.
iTunes 백업시 암호화	[iOS 7.1+] 단말에서 iTunes 백업 시 암호화를 강제 사용 할 것인지 설정합니다. • 강제 사용: 암호화를 사용하도록 합니다. • 사용자 선택: 사용자가 암호화 사용 여부를 설정합니다.
iTunes 페어링	[iOS 7.0+, Supervised] 감독PC로 설정되지 않은 PC로의 iTunes 연결 허용 여부를 설정합니다. • 허용: iTunes 페어링을 허용합니다. • 금지: iTunes 페어링을 금지합니다.
광고 추적 제한	[iOS 7.0+] 단말에서 광고 추적 제한 기능 사용을 허용할지 여부를 설정합니다. • 강제 사용: 광고 추적 제한 기능을 사용하도록 합니다. • 사용자 선택: 사용자가 사용 여부를 설정합니다.
공장 초기화	[iOS 8.0+, Supervised] 단말의 모든 콘텐츠 및 설정을 지우는 공장초기화 허용 여부를 설정합니다. • 허용: 공장초기화를 허용합니다. • 금지: 공장초기화를 금지합니다. **Note:** 공장 초기화 금지 정책을 설정할 경우, 단말 이상 증상 발생 시 공장 초기화가 불가능하니 사용에 주의해야 합니다.
Spotlight에서 웹 검색 결과	[iOS 8.0+, Supervised] Spotlight 검색에서 웹 검색 결과 보기를 허용할지 여부를 설정합니다. • 허용: 검색 결과 보기를 허용합니다. • 금지: 검색 결과 보기를 금지합니다.
차단 구성	[iOS 8.0+, Supervised] 차단 메뉴를 활성화하여 사용자가 임의의 제한사항을 구성하도록 허용할지 여부를 지정합니다. **차단 구성**을 금지하면 사용자가 차단 메뉴를 통해 단말 기능을 차단할 수 없게 됩니다. • 허용: 차단 메뉴 사용을 허용합니다. • 금지: 차단 메뉴 사용을 금지합니다.
단말 이름 변경	[iOS 8.0+, Supervised] 프로파일을 업데이트 할 때마다 단말 이름을 자동으로 모바일 ID로 변경할지 여부를 지정합니다. 단말 이름 변경을 사용하게 되면, 관리자가 단말 이름을 모바일 ID로 설정하는 단말 제어를 전송할 수 있습니다. • 사용: 단말 이름 변경을 사용합니다. • 미사용: 단말 이름 변경을 사용하지 않습니다.
블루투스 설정 변경	[iOS 10.0+, Supervised] 단말에서 블루투스 설정 수정을 허용할지 여부를 설정합니다. • 허용: 설정 변경을 허용합니다. • 금지: 설정 변경을 금지합니다.

미디어 그룹

정책	설명
국가별 등급	[iOS 4.0+] 미디어 콘텐츠(동영상, TV 프로그램, 앱)의 등급을 선택할 국가를 지정합니다. • 미국 / 영국 / 뉴질랜드 / 일본 / 아일랜드 / 독일 / 프랑스 / 캐나다 / 호주 중 선택
동영상	[iOS 4.0+] 동영상의 최대 허용 등급을 지정합니다. • 미국: 모든 동영상 허용 안 함 / G / PG / PG-13 / R / NC-17 / 동영상 모두 허용 중 선택 • 영국: 모든 동영상 허용 안 함 / U /Uc / PG / 12 / 12A / 15 / 18 / 동영상 모두 허용 중 선택 • 뉴질랜드: 모든 동영상 허용 안 함 / G / PG / M / R13/ R15 / R16 / R18 / R / RP16 / 동영상 모두 허용 중 선택 • 일본: 모든 동영상 허용 안 함 / G / PG-12 / R-15 / R-18 / 동영상 모두 허용 중 선택 • 아일랜드: 모든 동영상 허용 안 함 / G / PG / 12 / 15 / 16 / 18 / 동영상 모두 허용 중 선택 • 독일: 모든 동영상 허용 안 함 / ab 0 jahren / ab 6 jahren / ab 12 jahren / ab 16 jahren / ab 18 jahren / 동영상 모두 허용 중 선택 • 프랑스: 모든 동영상 허용 안 함 / -10 / -12 / -16 / -18 / 동영상 모두 허용 중 선택 • 캐나다: 모든 동영상 허용 안 함 / G / PG / 14A / 18A / R / 동영상 모두 허용 중 선택 • 호주: 모든 동영상 허용 안 함 / G / PG / M / MA15+ / R18+ / 동영상 모두 허용 중 선택
TV 프로그램	[iOS 4.0+] TV 프로그램의 최대 허용 등급을 지정합니다. • 미국: 모든 TV 프로그램 허용 안함 / TV-Y / TV-Y7 / TV-G / TV-PG / TV-14 / TV-MA / TV 프로그램 모두 허용 중 선택 • 영국: 모든 TV 프로그램 허용 안함 / 주의 / TV 프로그램 모두 허용 중 선택 • 뉴질랜드: 모든 TV 프로그램 허용 안함 / G / PGR / A0 / TV 프로그램 모두 허용 중 선택 • 일본: 모든 TV 프로그램 허용 안함 / 무삭제판 허용 / TV 프로그램 모두 허용 중 선택 • 아일랜드: 모든 TV 프로그램 허용 안함 / GA / Ch / YA / PS / MA / TV 프로그램 모두 허용 중 선택 • 독일: 모든 TV 프로그램 허용 안함 / ab 0 jahren / ab 6 jahren / ab 12 jahren / ab 16 jahren / ab 18 jahren / TV 프로그램 모두 허용 중 선택 • 프랑스: 모든 TV 프로그램 허용 안 함 / -10 / -12 / -16 / -18 / TV 프로그램 모두 허용 중 선택 • 캐나다: 모든 TV 프로그램 허용 안 함 / C / C8 / G / PG / 14+ / 18+ / TV 프로그램 모두 허용 중 선택 • 호주: 모든 TV 프로그램 허용 안 함 / P / C / G / PG / M / MA15+ / AV15+ / TV 프로그램 모두 허용 중 선택
앱	[iOS 4.0+] 단말에서 광고 추적 제한 기능을 사용할 지 여부를 지정합니다. • 모든 앱 허용 안함 / 4 + / 9+ / 12+ / 17+ / 앱 모두 허용 중 선택

Windows 단말 관리 정책

Windows 단말의 정책 목록은 다음과 같습니다 . (버전명 뒤에 + 는 버전이상 , - 는 버전 이하를 의미)

보안 그룹

정책	설명
비밀번호 정책	[Windows 10(Mobile)+] 화면 잠금 비밀번호를 강제로 설정하거나 미설정하여 제어하지 않도록 선택합니다. 화면 잠금 상태에서는 카메라 사용이 금지됩니다. • 설정: 화면 잠금 비밀번호를 제어합니다. **Note:** 비밀번호를 설정하지 않은 단말에서 Samsung SDS EMM 을 활성화 한 경우 단말에 등록된 인증서는 삭제됩니다.
비밀번호 입력 실패 허용 횟수 (회)	[Windows 10(Mobile)+] 실패 허용 횟수 이상으로 비밀번호를 잘못 입력하면 Challenge Phrase를 표시한 후, 공장초기화 동작을 수행합니다. Challenge Phrase는 정보 보호를 위해 자동 입력 방지를 위하여 제공되는 특정 문구입니다. 대소문자 구분하여 동일하게 입력합니다. • 설정값: 3– 998
비밀번호 최소 길이 (자)	[Windows 10(Mobile)+] 비밀번호의 최소 길이를 지정합니다. • 설정값: 4~16 자(기본값 4)
화면잠금 유예 시간 최대값 (분)	[Windows 10(Mobile)+] 화면 잠금 시간의 최대값을 설정합니다. 사용자는 해당 설정값 내의 시간에서 화면 잠금시간을 설정할 수 있습니다. • 설정값: 0~999 분
비밀번호 최대 사용 기간 (일)	[Windows 10(Mobile)+] 비밀번호를 사용할 수 있는 최대 기간이 지나면 비밀번호를 재설정하도록 합니다. • 설정값: 0~730 일 • 0 : 최대 사용 기간이 무기한입니다.
비밀번호 내역 관리 (회)	[Windows 10(Mobile)+] 현재 비밀번호를 포함하여 최대 몇 번의 이전 입력 비밀번호를 재사용할 수 없는지 횟수를 지정합니다. • 설정값: 2~50 회

인터페이스 그룹

정책	설명
Wi-Fi	[Windows 10(Mobile/Desktop)+] Wi-Fi 사용 여부를 설정합니다. • 허용: Wi-Fi를 사용을 허용합니다. • 금지: Wi-Fi를 사용을 금지합니다.
Wi-Fi 테더링	[Windows 10(Mobile/Desktop)+] Wi-Fi 테더링의 사용 여부를 설정합니다. • 허용: Wi-Fi 테더링의 사용을 허용합니다. • 금지: Wi-Fi 테더링의 사용을 금지합니다.
블루투스	[Windows 10(Mobile/Desktop)+] 블루투스 사용 허용 여부를 설정합니다. • 허용: 블루투스 사용을 허용합니다. • 금지: 블루투스 사용을 금지합니다.
탐색 모드	[Windows 10(Mobile/Desktop)+] 블루투스 탐색 모드 설정 허용 여부를 설정합니다. • 허용: 블루투스 탐색 모드 설정을 허용합니다. • 금지: 블루투스 탐색 모드 설정을 금지합니다.
NFC 제어	[Windows 10(Mobile)+] NFC 제어를 허용할지 여부를 설정합니다. • 허용: NFC 사용을 허용합니다. • 금지: NFC 사용을 금지합니다.
USB 제어	[Windows 10(Mobile)+] USB 테더링 연결 허용 여부를 설정합니다. • 허용: USB 테더링 연결을 허용합니다. • 금지: USB 테더링 연결을 금지합니다.

앱그룹

정책	설명
Windows App Store 접근 제어	[Windows 10(Mobile)+] Windows App Store 접근 가능 여부를 설정합니다. • 허용: App Store 접근이 허용됩니다. • 금지: App Store 접근이 금지됩니다.
앱 블랙/화이트리스트 설정	[Windows 10(Mobile/Desktop)+] Windows 내에 앱 제어 정책을 블랙리스트 또는 화이트리스트 기준으로 설정할 것인지 지정합니다. • 앱 블랙리스트 설정: 블랙 리스트르에 등록된 앱을 실행하거나 설치하면 안 되는 앱 목록입니다. 앱 설치 블랙리스트와 앱 실행 블랙리스트를 설정할 수 있습니다. • 앱 설치/실행 화이트리스트: 화이트리스트에 등록된 앱만 실행하거나 설치할 수 있습니다. 앱 설치 화이트리스트와 앱 실행 화이트리스트를 설정할 수 있습니다.
앱 설치/실행 블랙 리스트	[Windows 10(Mobile/Desktop)+] 지정된 앱에 대한 설치 및 실행을 차단하는 정책입니다. 정책 설정 시 이미 설치된 앱은 자동으로 삭제되며, 신규로 설치되는 앱도 설치 후 자동 삭제 됩니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭

정책	설명
Preload 앱 자동 추가	[Windows 10(Mobile/Desktop)+] 단말에 이미 설치되어 있는 Preload 앱을 화이트리스트에 자동 추가합니다. 확인란을 선택하면 Preload 앱이 자동 추가됩니다.
앱 설치/실행 화이트리스트	[Windows 10(Mobile/Desktop)+] 등록된 앱만 설치 및 실행을 허용하는 정책입니다. EMM Agent, EMM Client, Samsung SDS Push Agent는 자동으로 대상 목록으로 등록됩니다. 단말에 사전에 설치된 앱 이외에도 사용자가 추가 설치하는 앱에 대해서 동작을 하게 됩니다. 정책 적용 시 이미 설치되었으나 허용되지 않은 앱은 자동으로 삭제됩니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭

전화그룹

정책	설명
로밍 시 데이터 통신	[Windows 10(Mobile/Desktop)+] 해외 로밍 상태에서 데이터 사용 허용 여부를 설정합니다. • 허용: 데이터 사용을 허용합니다. • 금지: 데이터 사용을 금지합니다.

시스템그룹

정책	설명
공장초기화	[Windows 10(Mobile/Desktop)+] 사용자가 공장초기화를 수행할 수 있는지 여부를 설정합니다. • 허용: 공장초기화를 허용합니다. • 금지: 공장초기화를 금지합니다.
카메라	[Windows 10(Mobile/Desktop)+] 카메라 사용 허용 여부를 설정합니다. • 허용: 카메라 사용을 허용합니다. • 금지: 카메라를 사용할 수 없습니다.
화면 캡처	[Windows 10(Mobile)+] 화면 캡처 허용 여부를 설정합니다. • 허용: 화면 캡처를 허용합니다. • 금지: 화면 캡처를 금지합니다.
VPN	[Windows 10(Mobile)+] 사용자가 VPN 설정의 변경 여부를 설정합니다. • 허용: VPN 설정 변경을 허용합니다. • 금지: VPN 설정 변경을 금지합니다.

기타그룹

정책	설명
PPKG 삭제	[Windows 10(Mobile/Desktop)+] 사용자가 PPKG (Provisioning Package) 파일을 사용하는 중에 파일을 삭제 허용 여부를 설정합니다. • 허용: PPKG 파일 삭제를 허용합니다. • 금지: PPKG 파일 삭제를 금지합니다.
MDM Client Unenrollment	[Windows 10(Mobile/Desktop)+] Windows 10의 단말에서 MDM 기능을 사용하는 중에 삭제 허용 여부를 설정합니다. • 허용: MDM 삭제를 허용합니다. • 금지: MDM 삭제를 금지합니다.

Tizen Wearable 단말 관리 정책

Tizen Wearable 단말의 정책 목록은 다음과 같습니다 . (버전명 뒤에 + 는 버전이상 , - 는 버전이하를 의미)

보안 그룹

정책	설명
비밀번호 정책	화면 잠금 비밀번호를 강제로 설정하거나 미설정하여 제어하지 않도록 선택합니다. 화면 잠금 상태에서는 카메라 사용이 금지됩니다. • 설정: 화면 잠금 비밀번호를 제어합니다. **Note:** 비밀번호를 설정하지 않은 단말에서 Samsung SDS EMM을 활성화한 경우 단말에 등록된 인증서는 삭제됩니다.
비밀번호 최소강도	[Samsung(SAFE5+)] 단말 화면 잠금 비밀번호의 최소강도를 설정합니다. • 숫자: 숫자 이상(숫자, 영숫자포함)의 비밀번호를 설정해야 합니다. • 영숫자포함: 영숫자 이상의 비밀번호를 설정해야 합니다.
비밀번호 입력 실패 허용 횟수	[Samsung(SAFE5+)] 입력 실패 허용 횟수 이상으로 비밀번호를 잘못 입력하면 공장 초기화를 수행합니다. • 설정값: 0~10 회
비밀번호 최소 길이 (자)	[Samsung(SAFE5+)] 비밀번호의 최소 길이를 지정합니다. 패턴의 경우에는 지정되는 점의 개수가 최소 길이 보다 하나 더 필요합니다. • 설정값: 0~20 자 **Note:** 패턴 비밀번호의 최소 길이는 각 점을 잇는 선의 개수를 의미합니다. 따라서 정책이 4자이면 5개의 점을 잇는 4개의 선이 입력되어야 정책을 만족합니다.

인터페이스 그룹

정책	설명
Wi-Fi	[Samsung(SAFE1+)] Wi-Fi 사용 여부를 설정합니다. Wi-Fi 정책은 **프로파일 > 앱 관리 프로파일 > 애플리케이션**에서 필수로 지정한 애플리케이션이 설치된 이후 적용됩니다. Wi-Fi 정책 적용이 정상적으로 되지 않은 경우, EMM이 활성화 된 이후 30분이 지나면 Wi-Fi 정책이 다시 적용됩니다. • 허용: Wi-Fi를 사용을 허용합니다. • 금지: Wi-Fi를 사용을 금지합니다.
블루투스	[Samsung(SAFE1+)] 블루투스 사용 허용 여부를 설정합니다. • 허용: 블루투스 사용을 허용합니다. • 금지: 블루투스 사용을 금지합니다.
NFC 제어	[Samsung(SAFE2+)] NFC 제어를 허용할지 여부를 설정합니다. • 허용: NFC 사용을 허용합니다. • 금지: NFC 사용을 금지합니다.
GPS	[Samsung(SAFE3+)] GPS상태를 제어합니다. • 허용: GPS 사용을 허용합니다. 사용자가 GPS를 On/Off 합니다. • On 금지: GPS 기능이 항상 Off 되어 있으며 기능이 비활성화 되어 사용자가 제어할 수 없습니다. • Off 금지: GPS 기능이 항상 On 되어 있으며 기능이 비활성화 되어 사용자가 제어할 수 없습니다. **Note:** 정책을 적용하기 전에 높은 정확도/절전모드/GPS만 3가지 기능 중에 사용자가 설정한 상태로 GPS를 On 시킵니다.

앱그룹

정책	설명
앱 블랙/화이트 리스트 설정	앱 제어 정책을 블랙리스트 또는 화이트리스트 기준으로 설정할 것인지 지정합니다. • 앱 블랙리스트 설정: 블랙리스트는 실행하거나 설치하면 안 되는 앱 목록입니다. 앱 설치 블랙리스트와 앱 실행 블랙리스트를 설정할 수 있습니다. • 앱 화이트리스트 설정: 화이트리스트로 등록된 앱만 실행하거나 설치할 수 있습니다. 앱 설치 화이트리스트와 앱 실행 화이트리스트를 설정할 수 있습니다. • 앱 블랙/화이트 리스트 설정: 블랙리스트/화이트리스트 정책을 동시에 적용할 수 있습니다. **Note:** 앱 블랙/화이트리스트 설정 후 앱을 추가하지 않으면 시스템 앱(Samsung SDS EMM Client)과 필수 앱(Secure Browser, mMail)을 제외한 모든 앱의 실행 및 설치가 금지됩니다.
앱 설치 블랙리스트	[Samsung(SAFE1+)] 지정된 앱 설치를 차단하는 정책입니다. 정책 설정 시 이미 설치된 앱은 자동으로 삭제 처리 되며, 신규로 설치되는 앱도 설치 후 자동 삭제 됩니다. 앱 설치 화이트리스트, 앱 실행 화이트리스트, 앱 삭제 방지 리스트에 이미 추가된 앱은 앱 설치 블랙리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 전체 앱 추가: ⊕ 클릭하면 목록에 * 추가되며 전체 앱이 설치 블랙리스트에 추가 • 삭제: 목록에서 앱 선택 후 X 클릭
앱 실행 블랙리스트	[Samsung(SAFE1+)] 지정된 앱 실행을 차단하는 정책입니다. 정책 설정 시 정의된 앱의 아이콘이 사라져 사용자가 임의로 앱을 실행할 수 없게 됩니다. 앱이 삭제되는 것은 아니기 때문에 정책 변경 또는 EMM 서비스 해제 시 다시 앱이 표시됩니다. 앱 실행 화이트리스트에 이미 추가된 앱은 앱 실행 블랙리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 앱 선택 후 X 클릭
앱 설치 화이트리스트	[Samsung(SAFE1+)] 목록에 등록된 앱만 설치를 허용하는 정책입니다. EMM Client 등과 같은 시스템 앱, 앱 관리 프로파일에 할당받은 사내 애플리케이션은 자동으로 대상 목록으로 등록됩니다. 단말에 사전에 설치된 앱 이외에도 사용자가 추가 설치하는 앱에 대해서 동작을 하게 됩니다. 정책 적용 시 이미 설치되었으나 허용되지 않은 앱은 자동으로 삭제 처리됩니다. 이미 앱 설치 블랙리스트에 추가된 앱은 앱 설치 화이트리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 전체 앱 추가: ⊕ 클릭하면 목록에 * 추가되며 전체 앱이 설치 화이트리스트에 추가 • 삭제: 목록에서 앱 선택 후 X 클릭

정책	설명
앱 실행 화이트리스트	[Samsung(SAFE1+)] 앱 실행 화이트리스트에 등록된 앱만 실행을 허용하는 정책입니다. EMM Client 등과 같은 시스템 앱, 앱 관리 프로파일에 할당받은 사내 애플리케이션, 단말에 사전 설치된 Preload 앱은 앱 실행 화이트리스트에 자동으로 등록됩니다. 해당 정책을 적용하면 앱 실행 화이트리스트에 없는 앱의 아이콘이 사용자 단말에서 사라지게 되며, 사용자가 임의로 실행할 수 없게 됩니다. 앱이 삭제되는 것은 아니기 때문에 정책이 변경되거나 EMM 서비스 해제 시, 숨겨진 앱의 아이콘은 사용자 단말에 다시 나타납니다. 이미 앱 설치 블랙리스트 또는 앱 실행 블랙리스트에 추가된 앱은 앱 실행 화이트리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 앱 선택 후 **X** 클릭
앱 삭제 방지리스트	[Samsung(SAFE1+)] 단말에서 사용자가 임의로 삭제할 수 없는 앱을 설정합니다. 이미 앱 설치 블랙리스트에 추가된 앱은 앱 삭제 방지 리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 앱 선택 후 **X** 클릭

전화그룹

정책	설명
Cellular 데이터 연결	[Samsung (SAFE2+)] Cellular 데이터 접속 허용 여부를 설정합니다. Cellular 데이터 연결 정책은 **프로파일 > 앱 관리 프로파일 > 애플리케이션**에서 필수로 지정한 애플리케이션이 설치된 이후 적용됩니다. Cellular 데이터 연결 정책 적용이 정상적으로 되지 않은 경우, EMM이 활성화된 이후 30분이 지나면 Cellular 데이터 연결 정책이 다시 적용됩니다. • 허용: 데이터 접속을 허용합니다. • 금지: 데이터 접속을 금지합니다.

시스템그룹

정책	설명
공장초기화	[Samsung (SAFE2+)] 사용자가 공장초기화를 수행할 수 있는지 여부를 설정합니다. • 허용: 공장초기화를 허용합니다. • 금지: 공장초기화를 금지합니다.
환경 설정	[Samsung (SAFE2+)] 환경 설정 변경 허용 여부를 설정합니다. • 허용: 환경 설정 변경을 허용합니다. • 금지: 환경 설정 변경을 금지합니다.
펌웨어 복구 허용	[Samsung (SAFE2+)] 사용자가 펌웨어를 변경하지 못하도록 펌웨어 복구 허용 여부를 설정합니다. • 허용: 사용자의 웨어러블 기기의 펌웨어 복구를 허용합니다. • 금지: 사용자의 웨어러블 기기의 펌웨어 복구를 금지합니다.

로깅 그룹

정책	설명
로그 기록	[Samsung (SAFE1+)] 단말의 로그 기록 여부를 설정합니다. 미설정 시 기본값은 로깅 사용입니다. • 사용: 로깅 관련 정책을 설정하여 로깅을 사용합니다. • 미사용: 로깅을 수행하지 않습니다.
로그 기록 수준	[Samsung (SAFE1+)] 기록할 로그의 수준을 설정합니다. 로그 기록 수준의 미설정 시 기본값은 DEBUG입니다. • DEBUG: 개발자에게 필요한 상세한 정보 기록 • INFO: 운영자에게 필요한 정보 기록 • WARNING: 에러는 아니지만 주의할 정보기록 • ERROR: 일반적인 오류 발생에 대한 정보 기록
로그 최대 수집 용량 (MB)	[Samsung (SAFE1+)] 로그 파일로 저장되는 최대 로그 용량을 설정합니다. • 설정값: 0~20 MB
로그 최대 보관 기간 (일)	[Samsung (SAFE1+)] 로그에 대한 최대 보관 기간을 설정합니다. • 설정값: 0~30 일

Knox 영역 단말 관리 정책

Knox 영역의 정책 목록은 다음과 같습니다 .

Knox 시스템 그룹

정책	설명
화면 캡처	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] Knox 컨테이너 내에서 화면 캡처의 허용 여부를 설정합니다. 기본 값은 허용입니다. • 허용: 화면 캡처를 허용합니다. • 금지: 화면 캡처를 금지합니다.
클립보드	[Android OS, Samsung Only(SAFE2+)] Knox 컨테이너 내에서 클립보드 사용 여부를 설정합니다. • 허용: 클립보드 사용을 허용합니다. • On 금지: 클립보드 사용을 금지합니다. • 동일 앱 내 허용: 동일 앱 내에서만 클립보드를 사용할 수 있습니다.
공유 목록	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] Knox 컨테이너 내에서 공유 목록 허용 여부를 설정합니다. • 허용: 공유 목록을 사용할 수 있습니다. • 금지: 공유 목록을 사용할 수 없습니다.
구글 계정 동기화	[Android OS, Samsung Only(SAFE5+)] Knox 컨테이너 내에서 구글 계정 동기화 허용 여부를 설정합니다. • 허용: 구글 계정 동기화를 허용합니다. • 금지: 구글 계정 동기화를 금지합니다.
앱 오류 발생 시 구글 보고	[Android OS, Samsung Only(SAFE3+)] Knox 컨테이너 내에서 앱 오류 발생 시, 구글에 오류 정보 보고를 허용할지 여부를 설정합니다. • 허용: 오류 정보 보고를 허용합니다. • 금지: 오류 정보 보고를 금지합니다.
시스템 앱 종료	[Android OS, Samsung Only(SAFE4+)] Knox 컨테이너 내에서 사용자가 시스템 앱을 강제로 종료 할 수 있는지 여부를 설정합니다. • 허용: 시스템 앱 종료를 허용합니다. • 금지: 시스템 앱 종료를 금지합니다.
Trusted Boot 검증	[Android OS, Samsung Only(Knox2+)] Trust boot 검증 기능 허용 여부를 설정합니다. • 허용: Trusted Boot 검증을 허용합니다. • 금지: Trusted Boot 검증을 금지합니다.
외부 키보드	[Android OS, Samsung Only(Knox2+)] [MDM 2.0] Knox 컨테이너 내에서 추가로 설치되는 3rd Party 키보드 앱 허용 여부를 지정합니다. • 허용: 키보드 앱을 허용합니다. • 금지: 키보드 앱을 금지합니다.

정책	설명
도메인 화이트리스트 설정	[MDM 2.0] Exchange와 Email에 계정 등록 시 허용되는 도메인 설정 여부를 지정합니다. • 도메인 화이트 리스트 설정
도메인 화이트리스트	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] Exchange와 Email에 계정 등록 시 허용되는 도메인을 지정합니다. • 추가: 도메인 입력 후 ⊕ 클릭 • 삭제: 삭제할 도메인 선택 후 X 클릭

Knox 인터페이스 그룹

정책	설명
Wi-Fi 네트워크 추가	[Android OS, Samsung Only(SAFE2+)] Knox 컨테이너 내에서 Wi-Fi 추가 설정을 허용할 것인지 설정합니다. • 허용: Wi-Fi 추가 설정을 허용합니다. • 금지: Wi-Fi추가 설정을 금지합니다.
마이크	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] Knox 컨테이너 내에서 마이크 사용 허용 여부를 설정합니다. • 허용: 마이크 사용을 허용합니다. • 금지: 마이크 사용을 금지합니다.
녹음	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] Knox 컨테이너 내에서 마이크를 사용한 녹음 기능의 허용 여부를 설정합니다. • 허용: 마이크 녹음을 허용합니다. • 금지: 마이크 녹음을 금지합니다.
카메라	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] Knox 컨테이너 내에서 카메라 사용 허용 여부를 설정합니다. 일반 영역의 카메라를 제한하는 경우 Knox 컨테이너의 카메라 기능은 사용할 수 없습니다. • 허용: 카메라 사용을 허용합니다. • 모두 금지: 카메라를 사용할 수 없습니다. • 녹화만 금지: 사진 촬영은 가능하나 동영상 녹화는 금지합니다. 삼성전자 단말에서만 사용이 가능합니다.
USB 접근 허용	[Android OS, Samsung Only(Knox 2.5+)] Knox에서 OTG를 통한 프린터, 스캐너 등의 USB 장치의 허용 여부를 설정합니다. 저장 장치 외에 악세서리 모드인 USB 장치만 설정 가능하며, 미국 Verizon 통신사의 단말은 지원하지 않습니다. 미설정 시 기본값은 미사용입니다. • 사용: USB 접근을 허용합니다. • 미사용: USB Accessory Mode를 사용하지 않습니다.

정책	설명
USB장치 기본 접근 허용	[Android OS , Samsung Only(SAFE5.1+)] Knox 컨테이너 내 특정앱에서 사용 가능한 USB 제품을 설정합니다. 1. 앱의 패키지명 입력 2. USB 벤더 아이디 선택 3. 제품 아이디 입력: 4자리의 16진수 문자만 입력가능, 다중 입력 시 , (콤마)로 구분하여 입력 • ABCD(벤더 아이디)+1234(제품 아이디)를 입력할 경우, ABCD 제조사의 1234 제품만 허용 • ABCD(벤더 아이디)+1234,0909(제품 아이디)를 입력할 경우, ABCD 제조사의 1234와 0909제품만 허용 4. ⊕을 클릭하여 추가, 삭제하려면 X를 클릭
저전력 블루투스	[Android OS, Samsung Only(Knox2.4+)] Knox 컨테이너 내에서 블루투스 사용 시 저전력 블루투스(Bluetooth Low Energy) 사용 여부를 설정합니다. 일반 영역에서 블루투스의 사용이 허용되는 경우에만 제어 가능합니다. • 허용: 저전력 모드를 허용합니다. • 금지: 저전력 모드를 금지합니다.
NFC 제어	[Samsung(SAFE2+)] NFC 제어를 허용할지 여부를 설정합니다. • 허용: NFC 사용을 허용합니다. • 금지: NFC 사용을 금지합니다.

Knox 브라우저 그룹

정책	설명
Android 브라우저	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] Knox 컨테이너 내 Android에서 제공하는 브라우저의 사용 허용 여부를 설정합니다. • 허용: 브라우저 사용을 허용합니다. • 금지: 브라우저 사용을 금지합니다.
쿠키	[Android OS, Samsung Only(SAFE2+)] Knox 컨테이너 내 Android 브라우저의 쿠키 사용 여부를 설정합니다. • 허용: 사용자가 쿠키 사용 메뉴를 변경할 수 있습니다. • 금지: 쿠키 사용을 할 수 없고 사용자가 쿠키 사용 메뉴를 변경할 수 없습니다.
자바스크립트	[Android OS, Samsung Only(SAFE2+)] Knox 컨테이너 내 Android 브라우저의 자바 스크립트 사용 여부를 설정합니다. • 허용: 사용자가 자바스크립트 사용 메뉴를 변경할 수 있습니다. • 금지: 자바스크립트 사용을 할 수 없고 사용자가 자바스크립트 사용 메뉴를 변경할 수 없습니다.
양식 데이터 저장	[Android OS, Samsung Only(SAFE2+)] Knox 컨테이너 내 Android 브라우저의 양식 데이터 저장 사용 여부를 설정합니다. • 허용: 사용자가 양식 데이터 저장 사용 메뉴를 변경할 수 있습니다. • 금지: 양식 데이터 저장을 할 수 없고 사용자가 양식 데이터 저장 사용 메뉴를 변경할 수 없습니다.
팝업 차단	[Android OS, Samsung Only(SAFE2+)] Knox 컨테이너 내 Android 브라우저의 팝업 차단 사용 여부를 설정합니다. • 허용: 사용자가 팝업 차단 사용 메뉴를 변경할 수 있습니다. • 금지: 팝업 차단을 할 수 없고 사용자가 팝업 차단 사용 메뉴를 변경할 수 없습니다.
브라우저 Proxy 주소	[Android OS, Samsung Only(Knox4.0.1+)] [MDM 2.0] Knox 컨테이너 내 Android 브라우저의 Proxy설정 주소를 설정합니다. 설정값은 IP 또는 도메인:Port 형식으로 입력합니다. **Note:** • 방화벽 정책 설정과 동시에 적용되지 않습니다. • 적용 브라우저는 크롬과 삼성 기본 S 브라우저이며, 크롬 지원 버전은 Knox Standard SDK 4.0.1~5.6입니다.

Note: 브라우저 설정이 변경되는 경우 브라우저 전체 종료 후 재실행 시 적용됩니다.

Knox 컨테이너 데이터 그룹

정책	설명
App 이동	[Android OS, Samsung Only(Knox2+)] 일반 영역의 앱을 Knox 컨테이너로 설치하는 것을 허용할지 여부를 설정합니다. • 허용: 앱 이동을 허용합니다. • 금지: 앱 이동을 금지합니다.
Knox영역으로 File 이동	[Android OS, Samsung Only(Knox2+)] 일반영역에서 생성한 파일을 Knox 컨테이너로의 이동을 허용할지 여부를 설정합니다. 단말의 기본 상태는 일반 영역의 파일을 Knox 컨테이너로 이동하는 것을 허용합니다. • 허용: 파일 이동을 허용합니다. • 금지: 파일 이동을 금지합니다.
일반영역으로 File 이동	[Android OS, Samsung Only(Knox2+)] Knox 컨테이너 내에서 생성한 파일을 일반 영역으로 이동을 허용할지 여부를 설정합니다. • 허용: 파일 이동을 허용합니다. • 금지: 파일 이동을 금지합니다.
달력 데이터 동기화 설정	일반 영역과 Knox 컨테이너와의 달력 데이터 동기화 여부를 설정합니다. • 달력 데이터 동기화 설정
달력 데이터 동기화	[Android OS, Samsung Only(Knox2+)] 일반 영역과 Knox 컨테이너와의 달력 데이터 동기화를 설정합니다. • Import 허용: 일반 영역의 정보를 Knox 컨테이너 안으로 전달하는 것을 허용합니다. • Export 허용: Knox 컨테이너의 데이터를 일반 영역으로 전달하는 것을 허용합니다.
연락처 데이터 동기화 설정	일반 영역과 Knox 컨테이너와의 연락처 데이터 동기화 여부를 설정합니다. • 연락처 데이터 동기화 설정
연락처 데이터 동기화	[Android OS, Samsung Only(Knox2+)] 일반 영역과 Knox 컨테이너와의 연락처 데이터 동기화를 설정합니다. • Import 허용: 일반 영역의 정보를 Knox 컨테이너 안으로 전달하는 것을 허용합니다. • Export 허용: Knox 컨테이너의 데이터를 일반영역으로 전달하는 것을 허용합니다.
DLP 사용 설정	[Android OS, Samsung Only(Knox2.6+)] Data Loss Protection (DLP) 활성화 사용 여부를 설정합니다. • DLP 활성화 화이트리스트 설정: 파일 다운로드 및 읽기 권한을 앱별로 부여합니다.
DLP 활성화 허용	[Android OS, Samsung Only(Knox2.6+)] DLP 활성화 허용 여부를 설정합니다. • 활성화: DLP 활성화를 허용합니다. • 비활성화: DLP 활성화를 금지합니다.

정책	설명
DLP LOCK 설정	[Android OS, Samsung Only(Knox2.6+)] DLP LOCK 설정 여부를 설정합니다. • 잠금: DLP 파일 다운로드 및 열람을 금지합니다. • 해제: DLP 파일 다운로드 및 열람을 허용합니다.
DLP 유효기간(분)	[Android OS, Samsung Only(Knox2.6+)] Knox 컨테이너 내의 DLP 활성화 앱에서 다운로드한 첨부파일의 유효기간을 설정합니다. • 설정값: 1~10080 분
DLP 생산자 앱 화이트 리스트	[Android OS, Samsung Only(Knox2.6+)] Knox 컨테이너 내에서 DLP 파일을 다운로드할 수있는 앱을 패키지 명으로 지정합니다. • 추가: ⊕ 클릭하여 **앱** 목록에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
DLP 사용자 앱 화이트 리스트	[Android OS, Samsung Only(Knox2.6+)] Knox 컨테이너 내의 DLP 생산자 앱에서 다운로드한 DLP 파일을 열람할 수 있는 앱을 설정해주는 정책이며, 패키지 명으로 지정합니다. • 추가: ⊕ 클릭하여 **앱** 목록에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭

Knox 앱 그룹

정책	설명
앱 블랙/화이트 리스트 설정	Knox 컨테이너 내에 앱 제어 정책을 블랙리스트 또는 화이트리스트 기준으로 설정할 것인지 지정합니다. • 앱 블랙 리스트 설정: 블랙리스트는 실행하거나 설치하면 안 되는 앱 목록입니다. 앱 설치 블랙리스트와 앱 실행 블랙리스트를 설정할 수 있습니다. • 앱 화이트 리스트 설정: 화이트리스트에 등록된 앱만 실행하거나 설치할 수 있습니다. 앱 설치 화이트리스트와 앱 실행 화이트리스트를 설정할 수 있습니다. • 앱 블랙/화이트 리스트 설정: 블랙리스트/화이트리스트 정책을 동시에 적용할 수 있습니다. **Note:** 앱 블랙/화이트리스트 설정 후 앱을 추가하지 않으면 시스템 앱(EMM Agent, EMM Client, Samsung SDS Push Agent)과 필수 앱(Secure Browser, mMail)을 제외한 모든 앱이 실행 및 설치가 금지됩니다.
앱 설치 블랙 리스트	[Android OS, Samsung Only(SAFE2.1+)] Knox 컨테이너 내에서 지정된 앱에 대한 설치를 차단하는 정책입니다. 정책 설정 시 이미 설치된 앱은 자동으로 삭제되며, 신규로 설치되는 앱도 설치 후 자동 삭제 됩니다. 패키지명에 와일드카드(*)를 사용하여 등록된 제어 앱을 앱 설치 블랙리스트 정책에 추가하면 등록된 특정 패키지는 설치되지 않습니다. 예) com.*.emm / com.sds.* / com.*.emm.* 이미 앱 설치 화이트리스트 또는 앱 삭제 방지리스트에 추가된 앱은 앱 설치 블랙리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 앱 선택 • 전체 앱 추가: ⊕ 클릭하면 목록에 * 추가되며 전체 앱이 설치 블랙리스트에 추가 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
앱 실행 블랙 리스트	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] Knox 컨테이너 내에서 지정된 앱 실행을 차단하는 정책입니다. 정책 설정 시 정의된 앱의 아이콘이 사라져 사용자가 임의로 앱을 실행할 수 없게 됩니다. 앱이 삭제되는 것은 아니기 때문에 정책 변경 시 다시 앱이 표시됩니다. 이미 앱 설치 화이트리스트 또는 앱 삭제 방지리스트에 추가된 앱은 앱 실행 블랙리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
앱 실행 방지 리스트	[Android OS, Samsung(SAFE5+)] Knox 컨테이너 내에서 지정된 앱에 대해서 앱 실행을 차단하는 정책입니다. 정책 설정 시 사용자가 임의로 앱을 실행할 수 없게 됩니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭

정책	설명
앱 설치 화이트리스트	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] Knox 컨테이너에 등록된 앱만 설치를 허용하는 정책입니다. EMM Agent, EMM Client, Samsung SDS Push Agent는 자동으로 대상 목록으로 등록됩니다. 단말에 사전에 설치된 앱 이외에도 사용자가 추가 설치하는 앱에 대해서 동작을 하게 됩니다. 정책 적용 시 이미 설치되었으나 허용되지 않은 앱은 자동으로 삭제됩니다. 패키지명에 와일드카드(*)를 사용하여 등록된 제어 앱을 앱 설치 화이트리스트 정책에 추가하면 등록된 특정 패키지는 설치가 허용됩니다. 예) com.*.emm / com.sds.* / com.*.emm.* 이미 앱 설치 블랙리스트에 추가된 앱은 앱 설치 화이트 리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 앱 선택 • 전체 앱 추가: ⊕ 클릭하면 목록에 * 추가되며 전체 앱이 설치 화이트리스트에 추가 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
앱 삭제 방지리스트	[Android OS, Samsung Only(SAFE2+)] Knox 컨테이너 내에서 사용자가 임의로 삭제할 수 없는 앱을 설정합니다. 이미 앱 설치 블랙리스트에 추가된 앱은 앱 삭제 방지 리스트에 추가할 수 없습니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 **X** 클릭
앱 설치 권한 화이트리스트 설정	Knox 컨테이너 내에서 앱을 설치할 수 있는 권한을 가진 패키지(앱)를 설정하는 정책입니다. 앱 설치 권한 화이트리스트 설정 여부를 설정합니다. • 앱 설치 권한 화이트리스트 설정
앱 설치 권한 화이트리스트	[Android OS, Samsung Only(SAFE2.1+)] Knox 컨테이너 내에서 앱 설치 권한을 가진 패키지(앱)를 설정합니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 **X** 클릭
GMS 앱	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] Knox 컨테이너 내에서, 구글에서 기본 제공하는 앱 설치를 허용할지 여부를 설정합니다. • 허용: 구글 제공 앱 설치를 허용합니다. • 금지: 구글 제공 앱 설치를 금지합니다.
TIMA CCM 프로파일 앱 화이트리스트 설정	[Android OS, Samsung Only(Knox2.1+)] Knox 컨테이너 내 TIMA Client Certificate Management (CCM) 프로파일의 사용 권한을 특정 앱 또는 전체 앱에 부여할지 설정합니다. • 전체 앱: Knox 컨테이너 내 모든 앱이 TIMA CCM에 접근할 수 있습니다. • 화이트리스트 앱: 화이트리스트로 설정한 앱만 Knox 컨테이너 내 TIMA CCM에 접근할 수 있습니다.

정책	설명
TIMA CCM 프로파일 앱 화이트리스트	[Android OS, Samsung Only(Knox2.1+)] Knox 컨테이너 내 TIMA Client Certificate Management (CCM) 프로파일의 사용 권한을 부여받을 앱을 설정합니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
TIMA CCM 프로파일 앱 접근제한 예외 리스트 설정	Knox 컨테이너가 잠긴 상태에서도 설정한 앱이 TIMA CMM 프로파일에 접근하도록 허용할지를 설정합니다. • TIMA CCM 프로파일 앱 접근제한 예외 리스트 설정: 설정한 앱만 Knox 컨테이너가 잠긴 상태에서 Knox 컨테이너 내 TIMA CCM에 접근할 수 있습니다.
TIMA CCM 프로파일 앱 접근제한 예외 리스트	[Android OS, Samsung Only(Knox2.1+)] Knox 컨테이너가 잠긴 상태에서도 TIMA CCM 프로파일에 접근을 허용하려는 앱을 설정합니다. **TIMA CCM 프로파일 앱 화이트리스트 설정** 정책에서 화이트리스트 앱을 설정한 경우에는 설정된 앱에 한하여 접근이 허용됩니다. (단, **TIMA CCM 프로파일 앱 화이트리스트 설정**이 **미설정** 또는 **전체앱**으로 설정되는 경우에는 적용 앱의 제한이 제외됩니다.) • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
외장 SD카드 사용 허용 앱 화이트리스트 설정	Knox 컨테이너 내에서는 기본적으로 외장 SD 카드를 사용할 수 없지만, 허용 앱을 지정하여 SD 카드를 사용할 수 있도록 설정합니다. • 설정: 외장 SD카드를 허용할 앱 화이트리스트를 설정합니다.
외장 SD카드 사용 허용 앱 화이트리스트 설정	[Android OS, Samsung Only(Knox2.2+)] Knox 컨테이너 내에서 외장 SD 카드를 허용할 앱을 설정합니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
배터리 최적화 예외 앱 설정	배터리 최적화 예외 앱을 설정하는 정책입니다. 등록된 앱은 배터리 소모를 유발할 수 있기 때문에 예외 처리가 필요한 경우에만 설정합니다. Android N (Nougat) OS 이상에서 설정 가능하며, EMM 애플리케이션에 등록된 System 앱은 배터리 최적화 작업 대상에서 자동으로 제외됩니다. • 배터리 최적화 예외 앱 설정: 배터리 사용량을 최적화하기 위한 CPU 및 네트워크 제한 대상에서 등록된 앱을 예외 시킵니다.
배터리 최적화 예외 앱	[Android OS, Samsung Only(SAFE5.7+)] 지정된 앱에 대하여 배터리 수명 연장을 위해 OS에서 수행하는 절전기능인 Doze 모드(Doze mode), 앱 대기모드(App Standby mode), 절전모드(power saving mode) 작업에 대한 예외 처리를 수행합니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
일반영역 앱 설치 리스트 설정	일반영역에 설치된 앱을 Knox 영역 안에 설치할 수 있도록 설정합니다. • 일반영역 앱 설치 리스트 설정: 일반 영역의 앱을 등록하여 Knox 영역에 설치합니다.

정책	설명
일반영역 앱 설치 리스트	[Samsung Only(SAFE5.1+)] 일반영역에 설치된 앱 중에서 Knox Container 영역에 설치할 앱을 선택합니다. **애플리케이션 > 제어 애플리케이션**에 Android 플랫폼으로 등록된 앱 목록이 조회됩니다. • 추가: ⊕ 클릭하여 "앱 목록" 창에서 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
앱 데이터 삭제 제어 설정	사용자가 Knox 컨테이너 내부에서 앱 내부 데이터 삭제를 허용할지 여부를 설정합니다. • 앱데이터 삭제 방지 리스트: 앱 데이터를 보호하기 위하여 삭제 방지 없도록 앱을 설정합니다.
앱 데이터 삭제 방지리스트	[Samsung Only(SAFE5.1+)] 지정된 앱에 대하여 앱 내부 데이터 삭제가 불가능합니다. 앱 내부 데이터 삭제버튼을 사용 할 수 없기 때문에 사용자가 임의로 앱 데이터를 삭제할 수 없으며, 앱 데이터를 보호할 수 있습니다. • 추가: ⊕ 클릭하여 **"앱 목록" 창**에서 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
앱 데이터 삭제 방지 예외리스트	[Samsung Only(SAFE5.1+)] 지정된 앱에 대하여 앱 내부 데이터 삭제가 가능합니다. 사용자가 앱 내부 데이터 삭제버튼을 사용하여 데이터를 삭제할 수 있습니다. • 추가: ⊕ 클릭하여 **"앱 목록" 창**에서 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
앱 설치 시 ProgressBar 표시(Onprem 정책에 없음)	사용자가 Knox Manage의 앱 스토어에서 애플리케이션을 다운로드 받는 경우 다운로드 진행 현황을 표시합니다. • 사용: 사용자의 단말에 앱 다운로드 진행 현황이 표시됩니다. • 미사용: 사용자의 단말에 앱 다운로드 진행 현황이 표시되지 않습니다.

Knox 보안 그룹

정책	설명
비밀번호 정책	Knox 컨테이너 잠금 비밀번호 제어 여부를 설정합니다. **Note:** 화면 잠금 상태에서는 카메라 사용이 금지됩니다.
기업 ID 연동	[Android OS, Samsung Only(SAFE5.4+)] [MDM 2.0] Knox 컨테이너 잠금 해제를 기업 ID 연동을 통해 제어합니다. • 사용: Knox 컨테이너 로그인시 단말 사용자가 기업 ID 사용하는것을 허용합니다. • 강제 사용: Knox 컨테이너 로그인시 기업 ID를 통해서만 로그인이 가능합니다.
도메인주소	[Android OS, Samsung Only(SAFE5.4+)] [MDM 2.0] 기업 ID 연동을 위해 기업 ID 연동 서버의 도메인 주소를 입력합니다. http(s)는 생략합니다.
설치 파일	[Android OS, Samsung Only(SAFE5.4+)] [MDM 2.0] 기업 ID 연동을 위해 Knox 내 설치해야 하는 파일을 선택합니다. Samusng SSO Authenticator (com.sec.android.service.singlesignon)와 같은 애플리케이션을 사용합니다. **애플리케이션 > 사내 애플리케이션** 또는 **애플리케이션 > 외부 애플리케이션**에 먼저 등록해야, 앱목록에서 선택할 수 있습니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭
FIDO 연동	[Android OS, Samsung Only(Knox2.7+)] 기업 ID 연동을 사용하는 경우 Knox 컨테이너 내 FIDO 연동 기능 사용 여부를 지정합니다. • 사용: Knox 컨테이너 로그인시 단말 사용자가 기업 ID로 FIDO를 사용하는것을 허용합니다.
Request URL	[Android OS, Samsung Only(Knox2.7+)] FIDO 연동을 위한 요청 URL을 설정합니다.
Response URL	[Android OS, Samsung Only(Knox2.7+)] FIDO 연동을 위한 응답 URL을 설정합니다.
FIDO 앱 설치리스트	[Android OS, Samsung Only(Knox2.7+)] FIDO 연동을 위하여 Knox 영역에 설치할 일반 영역의 FIDO 애플리케이션을 지정합니다. FIDO 인증을 위한 기본 앱이 목록에 자동으로 추가되며 추가 설치할 앱을 등록합니다. • 추가: ⊕ 클릭하여 “앱 목록” 창에서 앱 선택 • 삭제: 목록에서 삭제하려는 앱 선택 후 X 클릭

정책	설명
비밀번호 최소강도	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 단말 화면 잠금 비밀번호의 최소 강도를 설정합니다. • 패턴: 패턴 이상(패턴, PIN, 영숫자포함, 특수문자포함)의 비밀번호를 설정해야 합니다. • 숫자: 숫자 이상(숫자, 영숫자포함, 특수문자포함)의 비밀번호를 설정해야 합니다. • 영숫자포함: 영숫자 이상(영숫자포함, 특수문자포함)의 비밀번호를 설정해야 합니다. • 특수문자포함: 특수문자를 반드시 포함하여 강력한 비밀번호를 설정해야 합니다.
비밀번호 입력 실패 허용 횟수 (회)	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 입력 실패 허용 횟수 이상으로 비밀번호를 잘못 입력하면 통제 동작을 수행합니다. • 설정값: 0~10 회
비밀번호의 입력 허용 횟수 이상 실패 시 조치	[Android OS, Samsung Only(SAFE2+)] [MDM 2.0] 실패 허용 횟수 이상으로 비밀번호를 잘못 입력하는 경우의 통제 동작을 지정합니다. 삼성 그룹향의 경우에는 Knox 컨테이너 잠금만 가능하며 미설정인 경우에는 Knox 컨테이너가 삭제됩니다. 컨테이너 잠금 해제 단말 제어를 전송하여 잠금을 해제합니다. • Knox 컨테이너 잠금: 비밀번호의 입력 허용 횟수 이상 실패 시 Knox 컨테이너를 잠급니다. • Knox 컨테이너 삭제: 비밀번호의 입력 허용 횟수 초과 실패 시 Knox 컨테이너가 삭제됩니다.
비밀번호 최대 사용 기간 (일)	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 비밀번호를 사용할 수 있는 최대 기간이 지나면 비밀번호를 재설정 하도록 합니다. • 설정값: 0~365 일
비밀번호 히스토리 개수	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 최대 몇 번의 이전 입력 비밀번호를 재사용할 수 없는지 설정합니다. • 설정값: 0~10 개수
비밀번호 최소 길이 (자)	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 비밀번호의 최소 길이를 설정합니다. **비밀번호 최소 강도**가 **패턴**의 경우에는 지정되는 점의 개수가 최소 길이 보다 하나 더 필요합니다. **비밀번호 최소 강도**가 **특수문자포함**의 경우, **비밀번호 최소 길이**는 **비밀번호 최소 문자수**와 **비밀번호 최소 비문자수**의 정책 값을 합한 값보다 크거나 같아야 합니다. **비밀번호 최소강도**가 : • 숫자일 경우 설정값: 4~16 자 • 숫자/영숫자포함일 경우 설정값: 4~16 자 • 특수문자포함일 경우 설정값: 5~16 자

정책	설명
	Note: 패턴 비밀번호의 최소 길이는 각 점을 잇는 선의 개수를 의미합니다. 예를 들어 정책이 4자이면 5개의 점을 잇는 4개의 선이 입력되어야 정책을 만족합니다.
비밀번호 최소 문자수	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 비밀번호의 최소 문자열 길이를 지정합니다. **비밀번호 최소강도**가 **영숫자포함**의 경우에는 항상 1을 입력해야 합니다. **특수문자포함**의 경우에는 기본값 3이 설정되며, 다른 값 입력 시 **비밀번호 최소 소문자수**와 **비밀번호 최소 대문자수** 정책 값을 합한 값보다 크거나 같아야 합니다. • 설정값: 1~10 자 • 영숫자 포함 : 항상 1 • 특수문자 포함: 기본값 3
비밀번호 최소 소문자수	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 비밀번호에 설정 시 최소 소문자수를 설정합니다. • 설정값: 1~10 자
비밀번호 최소 대문자수	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 비밀번호에 설정 시 최소 대문자수를 설정합니다. • 설정값: 1~10 자
비밀번호 최소 비문자수	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 비밀번호에 설정 시 최소 비문자(숫자, 특수문자)수를 설정합니다. **비밀번호 최소강도**가 **특수문자포함**인 경우에는 기본값 2가 설정되며, 다른 값 입력 시 **비밀번호 최소 숫자수**와 **비밀번호 최소 특수문자수**를 합한 값보다 크거나 같아야 합니다. • 설정값: 1~10 자 • 특수문자 포함: 기본값 2
비밀번호 최소 숫자수	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 비밀번호에 설정 시 최소 숫자수를 설정합니다. **비밀번호 최소강도**가 **특수문자포함**인 경우에는 기본값 1이 설정됩니다. • 설정값: 1~10 자
비밀번호 최소 특수문자수	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 비밀번호 설정 시 특수문자의 최소 길이를 설정합니다. 특수문자는 숫자와 기호문자를 포함합니다. **비밀번호 최소강도**가 **특수문자포함**의 경우에는 기본값 1이 설정됩니다. • 설정값: 1~10 자
비밀번호 최대 중복 문자 포함 길이 (자)	[Android OS, Samsung Only(SAFE2.2+)] [MDM 2.0] 중복으로 입력할 수 있는 문자의 최대 개수를 설정합니다. • 설정값: 1~10 자
비밀번호 최대 순차적 숫자 사용 길이 (자)	[Android OS, Samsung Only(SAFE2.2+)] [MDM 2.0] 순차적으로 입력할 수 있는 숫자의 최대 개수를 설정합니다. • 설정값: 1~10 자

정책	설명
비밀번호 최대 순차적 문자 사용 길이 (자)	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] 순차적으로 입력할 수 있는 문자의 최대 개수를 설정합니다. • 설정값: 1~10 자
비밀번호 최소 문자 변경 길이 (자)	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] 이전 비밀번호에서 변경되어야 할 최소한의 문자의 길이를 설정합니다. **비밀번호 최소강도**가 **숫자**, **영숫자포함**, **특수문자포함**의 경우에는 **비밀번호 최소 길이** 정책 값보다 작은 값이어야 합니다. • 설정값: 1~10 자
금지어 설정	비밀번호 금지어 설정 여부를 설정합니다. [MDM 2.0] • 금지어: 비밀번호에 설정할 수 없는 문자, 문자열을 설정합니다.
금지어	[Android OS, Samsung Only(SAFE2.2+)] [MDM 2.0] 비밀번호에 설정할 수 없는 문자, 문자열을 설정합니다. • 추가: 금지어 입력 후 ⊕ 클릭 • 삭제: 목록에서 삭제할 금지어 선택 후 **X** 클릭
화면 잠금 시간	[Android OS, Samsung Only(SAFE5+)] [MDM 2.0] 지정된 시간 동안 사용자 입력이 없으면 화면을 잠급니다. • 15초 • 30초 • 1분 • 2분 • 5분 • 10분
비밀번호 보임/감춤 설정	[Android OS, Samsung Only(SAFE4+)] [MDM 2.0] 비밀번호 입력 시 방금 입력한 비밀번호를 표시할 것인지 설정합니다. • 허용: 입력한 비밀번호 표시를 허용합니다. • 금지: 입력한 비밀번호 표시를 금지합니다.
화면잠금 패턴 보임/감춤 설정	[Android OS, Samsung Only(SAFE3+)] [MDM 2.0] 화면 잠금 패턴 입력 시 입력한 패턴을 표시할 것인지 설정합니다. • 허용: 입력한 패턴 표시를 허용합니다. • 금지: 입력한 패턴 표시를 금지합니다.
스마트카드 브라우저 인증	[Android OS, Samsung Only(Knox1+)] 인터넷 브라우저에서 스마트카드 브라우저 인증 허용 여부를 설정합니다. 블루투스 스마트카드 관련 앱이 Knox내 설치 되어야 하며, 사용하는 스마트카드를 Knox내 **설정 > 보안**에서 등록하여야 사용이 가능한 정책입니다. 사용 시 블루투스 보안 모드가 적용되어 타 블루투스 기기와 연결이 제한됩니다. • 허용: 스마트카드 브라우저 인증을 허용합니다. • 금지: 스마트카드 브라우저 인증을 금지합니다.

정책	설명
지문 잠금해제 제어	[Android OS, Samsung Only(SAFE5.1+)] [MDM 2.0] 사용자가 지문인식을 통해 화면 잠금 해제하는 것을 허용할지 여부를 설정합니다. • 허용: 지문으로 화면 잠금 해제하는 것을 허용합니다. • 금지: 지문으로 화면 잠금 해제하는 것을 금지합니다.
홍채 잠금해제 제어	[Android OS, Samsung Only(SAFE5.2+)] [MDM 2.0] 사용자가 홍채인식을 통해 화면 잠금 해제하는 것을 허용할지 여부를 설정합니다. • 허용: 홍채 인식을 통해 화면 잠금 해제하는 것을 허용합니다. • 금지: 홍채 인식을 통해 잠금 해제하는 것을 금지합니다.
2단계 인증 강제 설정	[Android OS, Samsung Only(SAFE5.2+)] Knox 컨테이너 생성 시, 비밀번호 설정 단계에서 2단계 인증만 선택하도록 설정합니다. 사용 선택 시 관리자가 '지문 잠금해제 제어' 정책이나 '홍채 잠금해제 제어' 정책을 금지로 설정하더라도 지문이나 홍채를 2단계 인증으로 사용할 수 있습니다. • 사용: 지문이나 홍채 인식을 통해 화면 잠금 해제하는 것을 강제 사용합니다. • 미사용: 지문이나 홍채 인식을 통해 2단계 인증 설정을 금지합니다.
화면 잠금 상태의 기능 차단	화면 잠금 시 기능 제어를 설정합니다. • 설정: 잠금 화면에서 설정한 기능을 차단합니다.
차단 기능 선택	[Samsung Only(SAFE5.4+)] 잠금화면에서 차단할 기능 옵션을 설정합니다. • Trust Agent: 잠금 화면에서 Knox 빠른 실행 사용 여부를 설정합니다.

Knox 방화벽 그룹

방화벽 설정은 SDK 2.6 이상인 경우 IPv6 를 지원하며 , IPv4 와 IPv6 주소가 물리적으로 동일한 주소를 의미하더라도 별도로 설정을 해야합니다 .

앱별로 IP 또는 도메인 방화벽 정책을 설정할 수 있으며 , 전체 앱에 대하여 특정 방화벽을 허용 또는 금지하려면 패키지명에 와일드카드 (*) 를 입력합니다 .

여러개의 방화벽이 설정되어 있는 경우 제약적인 제어의 우선순위가 높습니다 .

- 전체 앱과 특정 앱에 방화벽 설정이 되어 있는 경우 앱별 정책의 우선순위가 높습니다.

- 허용 정책에 와일드 카드(*)를 사용하여 전체를 설정하면, 금지 정책에 특정 IP 또는 도메인을 입력하더라도 모든 IP 또는 모든 도메인 접근이 가능합니다.

정책	설명
방화벽	[Android OS, Samsung Only(SAFE2+)] Knox 컨테이너 내에서 방화벽 기능 사용할지 여부를 설정합니다. 허용 정책이 금지 정책보다 우선합니다. 정책이 적용되지 않으면 기본적으로 허용 상태이므로 허용 정책은 금지 정책에 예외 되는 대상 IP 및 포트를 설정할 때 사용합니다. • 사용: 방화벽을 사용합니다. • 미사용: 방화벽을 사용하지 않습니다.
방화벽 타입	방화벽 정책을 전체 Container 대상으로 적용할 것인지 앱별로 적용할 것인지 선택합니다. Knox 컨테이너의 방화벽 기능을 **사용**으로 선택한 경우, 방화벽 타입을 설정합니다. • Container의 전체 패키지: 선택 시 컨테이너 전체 패키지에 대해 방화벽 기능이 설정되며, 앱 별 방화벽 설정은 불가능합니다. 하단의 허용 정책과 금지 정책을 설정합니다. • 앱별: 선택 시 컨테이너 내 앱별로 방화벽 기능이 설정됩니다. 하단의 상세 항목을 설정합니다. - 허용 정책(앱별) - 금지 정책(앱별) - 허용 정책(도메인) - 금지 정책 (도메인) - DNS 설정
허용 정책	[Android OS, Samsung Only(SAFE2+)] 허용할 대상 IP 및 포트를 지정합니다. 특정 IP 및 포트만을 허용하기 위해서는 **금지 정책**의 **호스트 패턴**과 **포트(범위)**를 ***로 설정하여, 전체 차단 후 동작하도록 설정해야 합니다. 1. 호스트 패턴, 포트 입력 2. 적용 포트 설정값: • 모두 • 로컬: 단말에서 해당 포트 사용이 허용됩니다. • 원격: 대상 서버의 포트로 접속이 허용됩니다. 3. ⊕을 클릭하여 추가
금지 정책	[Android OS, Samsung Only(SAFE2+)] 금지할 대상 IP 및 포트를 지정합니다. 로컬 IP 주소로 설정할 경우 단말에서 해당 포트 사용이 금지되며, 원격으로 설정할 경우 대상 IP 및 Port로 접근이 차단됩니다. 1. 호스트 패턴, 포트 입력 2. 적용 포트 설정값: • 모두 • 로컬: 단말에서 해당 포트 사용이 금지됩니다. • 원격: 대상 서버의 포트로 접속이 차단됩니다. 3. ⊕을 클릭하여 추가

정책	설명
허용 정책(앱별)	[Android OS, Samsung Only(SAFE5.5+)] 허용할 대상 IP 및 포트를 지정합니다. 특정 IP 및 포트만을 허용하기 위해서는 **금지 정책**의 **IP 주소(범위)**와 **포트(범위)**를 ***로 설정하여, 전체 차단 후 동작하도록 설정해야 합니다. 1. IP 주소(범위), 포트(범위) 입력 2. 적용 포트 범위 설정값: • 모두 • 로컬: 단말에서 해당 포트 사용이 허용됩니다. • 원격: 대상 서버의 포트로 접속이 허용됩니다. 3. 허용하려는 애플리케이션의 패키지명을 선택 후, ⊕을 클릭하여 추가
금지 정책(앱별)	[Android OS, Samsung Only(SAFE5.5+)] 금지할 대상 IP 및 포트를 지정합니다. 로컬 IP 주소로 설정할 경우 단말에서 해당 포트 사용이 금지되며, 원격으로 설정할 경우 대상 IP 및 Port로 접근이 차단됩니다. 1. IP 주소(범위), 포트(범위) 입력 2. 적용 포트 범위 설정값: • 모두 • 로컬: 단말에서 해당 포트 사용이 금지됩니다. • 원격: 대상 서버의 포트로 접속이 차단됩니다. 3. 금지하려는 애플리케이션의 패키지명을 입력하거나 🔍을 클릭하여 선택한 후, ⊕을 클릭하여 추가
허용 정책(도메인)	[Android OS, Samsung Only(SAFE5.5+)] 허용할 도메인 주소를 설정합니다. 도메인 주소 입력 시 와일드 카드(*)를 사용하여 특정 도메인을 허용할 수 있으며, 와일드 카드(*)는 도메인의 앞 또는 뒤에 위치해야하며 중간에 입력은 불가합니다. 예) *android.com 또는 www.samsung* 특정 도메인만을 허용하기 위해서는 금지 정책을 *로 설정하여 전체 도메인을 차단한 후 동작하도록 설정해야합니다. 1. 허용하려는 애플리케이션의 패키지명을 입력하거나 🔍을 클릭하여 선택 2. 도메인 주소(범위)를 입력한 후 ⊕을 클릭하여 추가
금지 정책(도메인)	[Android OS, Samsung Only(SAFE5.5+)] 금지할 도메인 주소를 설정합니다. 도메인 주소 입력 시 와일드 카드(*)를 사용하여 특정 도메인을 금지할 수 있습니다. 로컬로 설정할 경우 단말에서 해당 도메인 사용이 금지되며, 원격으로 설정할 경우 대상 도메인으로 접근이 차단됩니다. 1. 금지하려는 애플리케이션의 패키지명을 입력하거나 🔍을 클릭하여 선택 2. 도메인 주소(범위)를 입력한 후 ⊕을 클릭하여 추가
DNS 설정	[Android OS, Samsung Only(SAFE5.5+)] 등록한 패키지명의 앱이 실행될 때 사용되는 도메인 서버 주소를 설정합니다. 앱당 하나의 DNS만 설정이 가능하며, 앱에 할당된 VPN이나 Proxy 정책이 없을 때만 적용됩니다. 1. 애플리케이션의 패키지명을 입력하거나 🔍을 클릭하여 선택 2. Primary DNS를 **DNS1**에, Secondary DNS를 **DNS2**에 IP 주소 형식으로 입력한 후 ⊕을 클릭하여 추가

EMM Client 애플리케이션 정책

정책	설명
로그인 실패 허용 횟수	[Android / iOS / Windows 10] 로그인 시도 시 최대 실패 허용 횟수를 설정합니다. • 설정값: 0~10 회(기본값 5)
로그인 실패 허용 횟수 이상 입력 시 조치	[Android / iOS / Windows 10] 로그인 실패 허용 횟수 이상 입력 시에 수행할 조치 항목을 선택합니다. • 없음: 통제하지 않습니다. • 공장 초기화: 공장 초기화를 합니다. • 단말 잠금: 단말 잠금을 합니다. • EMM 잠금: EMM 잠금을 합니다.
화면 잠금 유효 시간 최대값 (초)	[Android / iOS / Windows 10] 앱 사용을 일정시간 사용하지 않을 경우 자동으로 일반 영역 화면을 잠금 시킬 시간을 설정합니다. 0으로 설정시 화면 잠금이 실행되지 않습니다. • 설정값: 0, 300~3600 초(기본값 1800)
Knox 화면 잠금 유효 시간 최대값 (초)	[Android] 앱 사용을 일정시간 사용하지 않을 경우 자동으로 Knox 영역 화면을 잠금 시킬 시간을 설정합니다. 0으로 설정시 화면 잠금이 실행되지 않습니다. • 설정값: 0, 300~3600 초(기본값 1800)
지문 잠금 해제	[Android / iOS] 지문 잠금 해제 옵션을 설정합니다. • 사용: 지문 잠금 해제 옵션을 사용합니다. • 미사용: 지문 잠금 해제 옵션을 사용하지 않습니다.
비밀번호 입력 실패 허용 횟수 (회)	[Android / iOS] 화면 잠금 비밀번호 최대 실패 허용 횟수를 설정합니다. • 설정값: 0~10 회(기본값 5)
비밀번호 입력 허용 횟수 이상 실패 시 조치	[Android / iOS] 화면 잠금 비밀번호 최대 실패 허용 횟수 이상 실패 시 조치할 수행 목록을 설정합니다. • 없음: 통제하지 않습니다. • 공장 초기화: 공장 초기화를 합니다. • 단말 잠금: 단말 잠금을 실행합니다. • EMM 잠금: EMM 잠금을 실행합니다.
비밀번호 최소 길이 (자)	[Android / iOS / Windows 10] 화면 잠금 비밀번호의 최소 길이를 설정합니다. 패턴의 경우 지정되는 점의 개수가 최소 길이 보다 하나 더 필요합니다. • 설정값: 6~20 자(기본값 6) **Note:** 패턴 비밀번호의 최소 길이는 각 점을 잇는 선의 개수를 의미합니다. 따라서 정책이 4자이면 5개의 점을 잇는 4개의 선이 입력되어야 정책을 만족합니다.
화면 잠금 비밀번호 구성조건	[Android / iOS / Windows 10] 비밀번호에 포함시켜야 할 문자 종류를 설정합니다. • 대문자 1개 이상: 대문자 1개 이상 포함시킬지 여부를 설정합니다. • 숫자 1개 이상: 숫자 1개 이상 포함할지 여부를 설정합니다. • 특수문자 1개 이상: 대문자 1개 이상 포함시킬지 여부를 설정합니다.

정책	설명
화면 잠금 비밀번호 구성 시 연속된 3개 문자	[Android / iOS / Windows 10] 비밀번호에 연속된 3개 문자 허용 여부를 설정합니다. • 허용: 연속된 3개 문자를 허용합니다.
비활성화 요청 허용	[Android / iOS] 비활성화 요청이 가능하도록 단말의 비활성화 버튼을 활성화합니다. • 허용: 단말에서 비활성화 요청을 허용합니다.
Android 버전 제어	[Android] Android 기기의 버전을 선택하여 조건 위배 시 단말을 잠그거나 preload 된 이메일 애플리케이션을 숨겨 사용할 수 없게 합니다. • 사용: Android 기기의 버전 조건을 설정합니다.
권장 버전	[Android] Android 기기의 권장 버전을 선택합니다. • ICE_CREAM_SANDWICH(4.0) • ICE_CREAM_SANDWICH_MR1(4.03) • JELLY_BEAN(4.1) • JELLY_BEAN _MR1(4.2) • JELLY_BEAN _MR2(4.3) • KITKAT(4.4) • LOLLIPOP(5.0) • MARSHMALLOW(6.0) • NOUGAT(7.0) **Note:** LOLLIPOP의 경우 기기 버전의 확인을 보장할 수 없습니다.
버전 관리 정책	[Android] Android 기기의 버전 선택 후 적용할 조건을 선택합니다. • 권장 버전만 허용: 기기의 버전이 **권장 버전**에서 선택한 버전과 동일해야 합니다. • 권장 버전 이하만 허용: 기기의 버전이 **권장 버전**에서 선택한 버전과 동일하거나 낮아야 합니다. • 권장 버전 상만 허용:기기의 버전이 **권장 버전**에서 선택한 버전과 동일하거나 높아야 합니다.
위배 시 조치	[Android] OS 버전 선택 조건에 위배시 단말에 취할 동작을 선택합니다. • 단말 잠금: 위배시 사용자의 단말을 잠금 처리합니다. • EAS 잠금: 위배시 preload 된 이메일 애플리케이션을 숨겨 사용할 수 없게 합니다.
iOS 버전 제어	[iOS] iOS 기기의 버전을 체크하여 조건 위배 시 단말을 잠그도록 설정합니다. • 사용
권장 버전	[iOS] iOS 기기의 권장 버전을 선택합니다. • iOS 7.0, iOS 7.1 • iOS 8.0, iOS 8.1, iOS 8.2, iOS 8.3, iOS 8.4 • iOS 9.0, iOS 9.1, iOS 9.2, iOS 9.3 • iOS 10.0, iOS 10.1, iOS 10.2, iOS 10.3 • iOS 11.0, iOS 11.1, iOS 11.2

정책	설명
버전 관리 정책	[iOS] Android 기기의 버전 선택 시 적용할 조건을 선택합니다. • 권장 버전만 허용: 기기의 버전이 **권장 버전**에서선택한 버전과 동일해야 합니다. • 권장 버전 이하만 허용: 기기의 버전이 **권장 버전**에서 선택한 버전과 동일하거나 낮아야 합니다. • 권장 버전 상만 허용:기기의 버전이 **권장 버전**에서 선택한 버전과 동일하거나 높아야 합니다.
위배 시 조치	[iOS] OS 버전 선택 조건에 위배시 단말에 취할 동작을 선택합니다. • 단말 잠금: 위배 시 사용자의 단말을 잠금 처리합니다.
외부 애플리케이션 다운로드 화면 표시 제한	[Android/iOS] EMM Client에서 외부 애플리케이션의 다운로드 화면 표시를 제한합니다. **프로파일 > 앱 관리 프로파일> 애플리케이션**에 등록된 외부 애플리케이션만 다운로드 화면에 표시됩니다.
Windows 10 Desktop Data 배포	[Windows 10] Windows 10 데스크탑에 프로비저닝 패키지 파일의 배포 여부를 설정합니다. • PPKG 파일 선택: 배포하려는 프로비저닝 패키지 파일을 선택합니다.
PPKG 파일 선택	**설정 > Windows 10 > PPKG 파일관리**에 등록되어 있는 프로비저닝 패키지 파일을 선택합니다.
Windows 10 Mobile Data 배포	[Windows 10] Windows 10 모바일에 프로비저닝 패키지 파일의 배포 여부를 설정합니다. • PPKG 파일 선택: 배포하려는 프로비저닝 패키지 파일을 선택합니다.
PPKG 파일 선택	**설정 > Windows 10 > PPKG 파일관리**에 등록되어 있는프로비저닝 패키지 파일을 선택합니다.

Secure Browser 애플리케이션 관리 정책

정책	설명
Secure Browser 앱 사용 여부	[Android / iOS] Secure Browser 앱의 사용 여부를 설정합니다. • 사용: Secure Browser 앱을 사용합니다.
Tiny Mode 사용	[Android] Secure Browser의 주소창이 삭제되는 모드이며, Secure Browser 아이콘을 탭하여 설정된 홈페이지 URL을 호출합니다. 해당 정책을 사용하려면 반드시 **홈페이지 URL**이 설정되어야하며, 파일 다운로드 정책은 자동적으로 **금지**됩니다. • 사용: Tiny Mode를 사용합니다.
홈페이지 URL	[Android / iOS] Secure Browser를 처음 시작하거나 홈버튼 클릭시 표시될 기본 홈페이지를 설정합니다.
홈페이지 URL 강제 적용	[Android / iOS] **홈페이지 URL**에 입력한 주소를 기본 홈페이지로 강제 사용할지 여부를 설정합니다. • 강제: Secure Browser의 기본 홈페이지 URL을 강제 설정합니다.

정책	설명
	Note: 강제 적용 하게 될 경우 사용자가 변경할 수 없습니다.
URL 블랙/화이트리스트 설정	[Android / iOS] URL의 제어 유형을 설정합니다. • 화이트리스트: 지정된 URL만 접속을 허용하며, 그 외 URL은 모두 차단합니다. • 블랙리스트: 지정된 URL만 차단하고, 그 외 모든 URL을 허용합니다.
대상 URL	[Android / iOS] 제어할 URL을 추가/삭제 합니다. • 추가: 대상 URL 입력 후 ⊕ 클릭 • 삭제: 삭제할 URL 선택 후 X 클릭
캐쉬	[Android / iOS] 브라우저의 캐쉬 사용 여부를 설정합니다. • 허용: 캐쉬 사용을 허용합니다.
User Agent 설정 키 값	[Android / iOS] User Agent 에 추가할 키 값을 설정합니다. Http 헤더내에 존재하는 User Agent에 해당 키 값을 포함하여 Kiosk Browser가 웹 서버에 접근하게 합니다. **Note:** User Agent 설정키 값은 웹 서버에서 Kiosk Browser가 아닌 타 브라우저의 접근인지를 구분하는 키 값으로 사용할 수 있습니다.
쿠키	[Android / iOS] 브라우저의 쿠키 사용 여부를 설정합니다. • 허용: 사용자가 쿠키 사용 메뉴를 변경할 수 있습니다. • 금지: 쿠키 사용을 할 수 없고 사용자가 쿠키 사용 메뉴를 변경할 수 없습니다.
파일 다운로드	[Android / iOS] 파일 다운로드 허용 여부를 설정합니다. Tiny Mode를 사용하는 경우 **파일 다운로드** 정책은 금지로 자동 설정됩니다. • 허용: 다운로드를 허용합니다.
문자열 복사	[Android / iOS] 앱 내에서 문자열 복사를 허용할지 여부를 설정합니다. • 허용: 문자열 복사를 허용합니다.
화면 캡처	[Android] 앱 내에서 화면 캡처를 허용할지 여부를 설정합니다. • 허용: 화면 캡처를 허용합니다.
Javascript	[Android] Javascript를 허용할 지 여부를 설정합니다. • 허용: 사용자가 자바스크립트 사용 메뉴를 변경할 수 있습니다.
Browser 양식 자동입력	[Android] 양식 자동 입력 기능의 사용 여부를 설정합니다. • 허용: 사용자가 양식 데이터 저장 사용 메뉴를 변경할 수 있습니다.
보안경고 보기 표시	[Android / iOS] HTTPS 주소 접속 시 브라우저의 보안경고 보기 표시를 허용할지 여부를 설정합니다. • 허용: 보안경고 보기를 허용합니다.

정책	설명
Http Proxy	[Android] Android 브라우저의 Http Proxy 사용을 허용할지 설정합니다. • 허용: Http Proxy 사용을 허용합니다. PORT를 설정할 수 있습니다. • 금지: Http Proxy 사용을 금지합니다.
IP/DOMAIN : PORT	[Android] Http Proxy 서버 IP 또는 도메인 주소와 PORT를 설정합니다.

mMail 애플리케이션 관리 정책

정책	설명
mMail 앱 사용 여부	[Android / iOS] mMail 앱의 사용 여부를 설정합니다. • 사용: mMail 앱을 사용합니다.
사용자 정보 입력방법	[Android, iOS] mMail 로그인 시 필요한 사용자 정보 입력 방법을 선택합니다. 직접 입력하거나 커넥터 연동 서비스를 통해 사용자 정보를 설정할 수 있습니다. • 직접입력: 사용자의 E-mail 주소 입력합니다. ex) user@example.com • 커넥터 연동: 연동된 사용자 정보 커넥터에 등록되어 있는 서비스 ID를 선택합니다.
E-mail	[Android, iOS] 사용자의 E-mail 주소를 입력합니다.
Http Proxy	[Android, iOS] Http Proxy 허용 여부를 설정합니다. • 허용: Http Proxy를 허용합니다.
IP/Domain : PORT	[Android, iOS] Http Proxy 허용 시 Proxy 서버 IP 또는 도메인 주소과 포트를 설정합니다.
SSL	[Android, iOS] 접속하고자 하는 서버가 Secure Socket Layer를 사용하는지 여부를 설정합니다.
수신메일 동기화기간설정	[Android, iOS] 사용자의 회사 메일을 mMail에 동기화할 기간을 설정합니다. • 없음: 수동으로 메일을 가져옵니다. • 1일: 1일간 받은 메일을 가져옵니다. • 3일: 3일간 받은 메일을 가져옵니다. • 1주일: 일주일간 받은 메일을 가져옵니다. • 2주일: 2주일간 받은 메일을 가져옵니다. • 전체: 회사 메일함에 있는 전체 메일을 가져옵니다. 사용자의 단말 성능에 영향을 끼칠 수 있으니 주의합니다.
일정 동기화 단위	[Android, iOS] 사용자의 회사 일정을 mMail에 동기화할 기간을 설정합니다. • 없음: 수동으로 회사 일정을 가져옵니다. • 2주일: 2주일간의 회사 일정을 가져옵니다. • 1개월: 1개월간의 회사 일정을 가져옵니다. • 3개월: 3개월간의 회사 일정을 가져옵니다. • 6개월: 6개월간의 회사 일정을 가져옵니다. • 전체: 회사 등록한 전체 일정을 가져옵니다. 사용자의 단말 성능에 영향을 끼칠 수 있으니 주의합니다.

정책	설명
연락처 동기화	[Android, iOS] 사용자의 회사 연락처를 mMail과 동기화할지 여부를 설정합니다. • 사용: 회사 연락처를 동기화합니다.
사용자 인증서 입력방법	[Android, iOS] mMail 서비스 사용을 위해 사용자를 인증할 인증서 입력 방법을 설정합니다. • EMM 관리 인증서: EMM 서버에서 관리되고 있는 사용자 인증서를 선택합니다. • 커넥터 연동: 커넥터 서비스에 연동되어있는 사용자 인증서를 선택합니다. **Note:** **인증서 > 외부인증서** 메뉴에서 인증서를, **설정 > 연동 시스템 > Directory** 메뉴에서 Directory 서비스를 사전에 등록하여 이용합니다.
화면 잠금 유효 시간 최대값 (초)	[Android, iOS] 앱 사용을 일정시간 사용하지 않을 경우 자동으로 화면 잠금시킬 시간을 설정합니다. • 설정값: 300~3600 초 • 기본값 1800
첨부조회	[Android, iOS] 메일에 첨부된 문서 보기를 허용할지 여부와 조회 방식을 선택합니다. • 다운로드: 첨부 문서를 단말의 보안 저장소에 다운로드하여 조회되도록 합니다. • 스트리밍: 첨부 문서가 스트리밍 방식으로 조회됩니다. 단말에 저장되지 않습니다. • 금지: 첨부 문서 조회를 금지합니다.
스트리밍 서버 주소 (IP/Domain: PORT)	[Android, iOS] 첨부조회에서 스트리밍을 선택한 경우, 사용할 스트리밍 서버의 IP 주소 또는 도메인 주소와 포트를 설정합니다.
AD 도메인	[Android, iOS] 이메일 서버의 도메인 이름을 입력합니다.
AD 사용자 ID 입력방법	[Android, iOS] 이메일 계정의 사용자 ID 입력 방법을선택합니다. 직접 입력하거나 커넥터 연동 서비스를 통해 사용자 정보를 설정할 수 있습니다. • 직접입력: **AD 사용자 ID**에 사용자의 E-mail 주소 입력합니다. ex) user@example.com • 커넥터 연동: 사용자 정보 커넥터에 등록되어 있는 서비스 ID를 **AD 사용자 ID** 커넥터에서 선택합니다.
해외 로밍시 사용	[Android, iOS] 해외 로밍 시 데이터 싱크 허용할지 여부를 설정합니다.
문자열 복사	[Android, iOS] 앱 내 텍스트 복사 허용 여부를 설정합니다.
화면 캡처	[Android, iOS] 화면 캡처 허용 여부를 설정합니다.

SecuCamera 애플리케이션 관리 정책

정책	설명
SecuCamera 앱 사용 여부	단말에 SecuCamera 사용을 허용할지 여부를 설정합니다. • 사용: SecuCamera 사용을 허용합니다.

Knox Portal 애플리케이션 관리 정책

정책	설명
Knox Portal 앱 사용 여부	[Android / iOS] Knox Portal 앱의 사용 여부를 설정합니다. • 사용: Knox Portal 앱을 사용합니다.
수신메일 첨부 보기	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 수신된 메일의 첨부파일 조회 권한과 방식을 설정합니다. • 스트리밍: 첨부파일의 내용을 스트리밍으로 조회합니다. • 다운로드: 첨부파일을 다운로드 합니다. • 금지: 첨부파일을 조회할 수 없습니다.
발신메일 첨부 보기	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 발신한 메일의 첨부파일 조회 권한과 방식을 설정합니다. • 스트리밍: 첨부파일의 내용을 스트리밍으로 조회합니다. • 다운로드: 첨부파일을 다운로드 합니다. • 금지: 첨부파일을 조회할 수 없습니다.
발신메일 조회	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 발신한 메일의 조회 권한을 설정합니다. • 허용: 발신 메일의 내용 조회를 허용합니다.
나에게발신메일 조회	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 나에게 발신한 메일의 조회 권한을 설정합니다. • 허용: 나에게 발신한 메일의 내용 조회를 허용합니다.
기결함/상신함 첨부 보기	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 결재의 기결함과 상신함의 첨부 파일 조회 권한과 방식을 설정합니다. • 스트리밍: 첨부파일의 내용을 스트리밍으로 조회합니다. • 다운로드: 첨부파일을 다운로드 합니다. • 금지: 첨부파일을 조회할 수 없습니다.
기결함/상신함 본문 보기	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 결재의 기결함과 상신함의 결재 본문 내용 조회 권한을 설정합니다. • 허용: 기결함과 상신함의 결재 본문 내용 조회를 허용합니다.
수신메일 동기화기간 설정	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 수신된 메일의 동기화 기간을 설정합니다. • 2: 삼성 전자 • 3: 삼성 그룹사
임직원 조회	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 임직원 정보 조회 권한을 설정합니다. • 허용: 임직원 정보 조회를 허용합니다.
일정 동기화	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 일정 동기화 활성화 권한을 설정합니다. • 허용: 일정 사용을 허용합니다.
연락처 동기화	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 연락처 동기화 활성화 권한을 설정합니다. • 허용: 연락처 사용을 허용합니다.

정책	설명
화면잠금 로그아웃 사용여부	[Android OS, Samsung Only(SAFE1+)] Knox Portal에서 화면 잠금이 되었을 경우, 로그 아웃 실행 여부를 설정합니다. 허용 시 잠금화면에서 로그아웃 버튼이 활성화됩니다. • 허용: 화면 잠금 시, 로그아웃 버튼을 클릭하여 로그아웃을 실행합니다.
화면잠금 주기	[Android OS, Samsung Only(SAFE1+)] Knox Portal의 화면 잠금 주기를 설정합니다. • 설정값: 0~1800 초 • 기본값 1800

방문자 정책

정책	설명
카메라	[Android 4.0(SDK14)+, Samsung(SAFE2+), iOS 4.0] Android 단말에 카메라 사용을 허용할지 여부를 설정합니다. • 허용: 카메라 사용을 허용합니다. • 금지: 카메라를 사용할 수 없습니다.
마이크	[Android 1.0(SDK1)+, Samsung(SAFE2+), iOS] 마이크 앱 사용을 통한 녹음을 허용할지 여부를 설정합니다. 써드 파티 앱에서 사용하는 마이크 기능은 제어되지 않습니다. • 허용: 마이크 사용을 허용합니다. • 금지: 마이크 사용을 금지합니다. **Note:** iOS 단말의 경우 마이크 금지 정책이 설정되었으나, 방문자가 마이크 기능을 사용하면 이를 기록합니다. 방문자에게는 마이크 금지 정책 위반 사실을 알리고, 관리자는 방문자의 컴플라이언스 위반 여부를 확인할 수 있습니다.
화면 캡처	[Android OS, Samsung Only(SAFE2+)] 삼성, 엘지 단말의 화면 캡처 허용 여부를 설정합니다. [iOS 4.0] 단말에서 화면 캡처 기능 사용 여부를 지정합니다. • 허용: 화면 캡처를 허용합니다. • 금지: 화면 캡처를 금지합니다.
Wi-Fi	[Android 1.0(SDK1)+, Samsung(SAFE2+)] Wi-Fi 사용을 허용할지 여부를 설정합니다. • 허용: Wi-Fi를 사용할 수 있습니다. • On 금지: Wi-Fi를 켤 수 없습니다. • Off 금지: Wi-Fi를 항상 켜야 합니다.
Wi-Fi 핫스팟	[Android 2.3(SDK9)+, Samsung(SAFE2+)] Wi-Fi 핫스팟 사용 여부를 설정합니다. • 허용: Wi-Fi 핫스팟 사용을 허용합니다. • 금지: Wi-Fi 핫스팟 사용을 금지합니다.
Wi-Fi SSID 화이트리스트 설정	Wi-Fi SSID 화이트리스트를 설정하여, 등록한 Wi-Fi SSID에만 접속이 가능하도록 합니다. • 설정: Wi-Fi SSID 화이트리스트를 설정합니다.

정책	설명
Wi-Fi SSID 화이트리스트	[Android 1.0(SDK1)+, Samsung(SAFE2.2+)] Wi-Fi SSID 화이트리스트를 설정합니다. 해당 화이트리스트에 추가한 Wi-Fi AP에만 연결되고, 그 외의 AP에는 연결이 허용되지 않습니다. Wi-Fi 설정 프로파일 추가, 삭제와는 무관하며, 연결 허용 여부만 관여합니다. • 추가: Wi-Fi SSID 입력 후 ⊕ 클릭 • 삭제: Wi-Fi SSID 선택 후 X 클릭
블루투스	[Android 1.0(SDK1)+, Samsung(SAFE2+)] 블루투스 사용을 허용할지 여부를 설정합니다. • 허용: 블루투스 사용을 허용합니다. • 금지: 블루투스 사용을 금지합니다
블루투스 테더링	[Android 4.2(SDK17)+, Samsung(SAFE2+)] 블루투스 테더링 연결을 허용할지 여부를 설정합니다. • 허용: 블루투스 테더링 사용을 허용합니다. • 금지: 블루투스 테더링 사용을 금지합니다.
PC 연결	[Android OS, Samsung Only(SAFE2+)] PC와의 이동식 디스크 또는 MTP 연결 허용 여부를 설정합니다. • 허용: 이동식 디스크로 사용을 허용합니다. • 금지: 이동식 디스크로 사용을 금지합니다.
USB 테터링 활성화	[Android OS, Samsung Only(SAFE2+)] USB 테더링 연결 허용 여부를 설정합니다. • 허용: USB 테더링 연결을 허용합니다. • 금지: USB 테더링 연결을 금지합니다.
앱 실행 블랙리스트	지정된 앱 실행을 차단하는 정책입니다. • 설정 (Android only): Android 단말을 위한 앱 실행 블랙리스트를 설정합니다. **Note:** 해당 정책은 사용자 단말의 배터리 소모를 많이 발생시킵니다.
블랙리스트(Android)	[Android 2.2(SDK8)+,Samsung(SAFE2+),LG(GATE1+)] Android 단말을 위한 앱 실행 블랙리스트를 지정합니다. 정책 설정 시 정의된 앱의 아이콘이 사라져 사용자가 임의로 앱을 실행할 수 없게 됩니다. 앱이 삭제되는 것이 아니기 때문에 정책 변경 혹은 EMM Agent unenrollment 시 다시 앱이 표시되게 됩니다. • 추가: ⊕클릭하여 “앱 목록” 창에서 선택 • 삭제: 목록에서 앱 선택 후 X 클릭

정책	설명
앱 실행 화이트리스트	지정된 앱만 실행을 허용하는 정책입니다. • 설정 (Android only): Android 단말을 위한 앱 실행 화이트리스트를 설정합니다.
화이트리스트(Android)	[Android 2.2(SDK8)+,Samsung(SAFE2+),LG(GATE1+)] Android 단말을 위한 앱 실행 화이트리스트를 지정합니다. EMM Client, Agent, Push 등은 자동으로 대상 목록으로 등록되며 단말에 Preload 된 앱 이외에 사용자가 추가로 설치한 앱의 아이콘이 사라져 사용자가 임의로 앱을 실행할 수 없게 됩니다. 앱이 삭제되는 것은 아니기 때문에 정책 혹은 EMM Agent unenrollemnt 시 다시 앱이 표시되게 됩니다. • 추가: ⊕클릭하여 “앱 목록” 창에서 선택 • 삭제: 목록에서 앱 선택 후 X 클릭

단말 적용 프로파일 코드

단말 & 사용자 > 단말 메뉴에서 단말에 적용한 프로파일의 상세 정보를 엑셀로 다운로드하여 확인합니다. 엑셀의 **단말 관리 프로파일 정책** 항목에 단말 플랫폼에 따라 Android의 경우에는 json, iOS의 경우에는 xml 코드 형식으로 표기됩니다. 키값에 대한 프로파일 정보는 아래의 표를 참고합니다.

Android 정책

정책명	코드
Wi-Fi	Wi-Fi
Wi-Fi 제어	AllowWiFi
Wi-Fi Direct 허용	AllowWiFiDirect
Wi-Fi 핫스팟 허용	AllowWiFiHotSpot
Wi-Fi SSID 화이트리스트 설정	WifiSsidWhiteList
Wi-Fi 네트워크 자동 접속	AllowAutomaticConnectionToWifi
Wi-Fi 최소 보안 수준 설정	WifiMinimumRequiredSecurity
블루투스	Bluetooth
블루투스 제어	AllowBluetooth
데스크탑 연결 허용	AllowDesktopConnectivity
데이터 교환 허용	AllowDataTransfer
탐색 모드 허용	AllowDiscoverableMode
블루투스 테더링 허용	AllowBluetoothTethering
블루투스 UUID 블랙리스트	BluetoothUuidBlackList
블루투스 UUID 화이트리스트	BluetoothUuidWhiteList
USB	Usb
PC 연결 허용	AllowPcConnectivity
USB 테더링 활성화 허용	AllowUsbTethering
USB Host Storage (OTG) 허용	AllowUsbHostStorage
USB 디버깅 활성화 허용	AllowUsbDebugging
앱	App
알 수 없는 출처 앱 설치 허용	AllowNonTrustApps
Android 마켓 사용 여부	AllowMarket
Android 유튜브 허용	AllowYouTube
앱 설치 블랙리스트	AppInstallationBlackList
앱 설치 화이트리스트	AppInstallationWhiteList
앱 삭제 블랙리스트	AppDeletionBlackList

정책명	코드
앱 실행 블랙리스트	AppRunningBlackList
앱 실행 화이트리스트	AppRunningWhiteList
앱 위변조 시 조치	AppModificationMeasure
앱 실행 방지리스트	AppPreventStartBlackList
배터리 최적화 예외 앱 설정	AppBatteryOptimizationWhiteList
전화	Phone
비행모드 사용 허용	AllowAirplaneMode
데이터 접속 허용	AllowCellularData
통화 허용	AllowCall
데이터 사용량 설정 허용	AllowUserMobileDataLimit
데이터 사용량 제한 (일) (단위: KB)	MobileDataLimitPerDay
데이터 사용량 제한 (주) (단위: KB)	MobileDataLimitPerWeek
데이터 사용량 제한 (월) (단위: KB)	MobileDataLimitPerMonth
SMS 수신 허용	AllowIncomingSms
SMS 발신 허용	AllowOutgoingSms
MMS 수신 허용	AllowIncomingMms
MMS 발신 허용	AllowOutgoingMms
로밍	Roaming
로밍 시 데이터 통신 허용	AllowRoamingData
로밍 시 WAP 푸시 허용	AllowRoamingPush
로밍 시 데이터 동기화 허용	AllowRoamingSync
로밍 시 보이스 콜 허용	AllowRoamingVoiceCalls
위치	Location
모의 위치 허용	AllowMockLocation
GPS 제어	AllowGps
브라우저	Browser
Android 브라우저 허용	AllowBrowser
쿠키 사용 허용	AllowUseOfCookies
자바스크립트 사용 허용	AllowUseOfJavaScript
양식 데이터 저장 사용 허용	AllowUseOfAutoFill
팝업 차단 사용 허용	AllowUseOfPopups
시스템	System
공장 초기화 허용	AllowWipeDevice

정책명	코드
전원 종료 허용	AllowPowerOff
백업 허용	AllowBackup
OTA 업그레이드 허용	AllowOtaUpgrade
환경 설정 변경 허용	AllowSettingsChanges
백그라운드 프로세스 개수 제어 설정 허용	AllowBackgroundProcessLimit
액티비티 종료 시 앱 종료 설정 허용	AllowKillingActivitiesOnLeave
시스템 앱 종료 허용	AllowStopSystemApp
앱 오류 발생 시 구글 보고 허용	AllowGoogleCrashReport
다중 사용자 허용	AllowMultiUsers
상태바 확장 허용	AllowStatusBarExpansion
배경화면 변경 허용	AllowWallpaperChange
날짜, 시간 변경 허용	AllowChangeDateTime
화면 캡쳐 허용	AllowScreenCapture
클립보드 제어	AllowClipboard
공유 목록 허용	AllowShareList
안드로이드 빔(S 빔) 허용	AllowBeam
OS 위변조 시 조치	OsModificationMeasure
스마트 클립 허용	AllowSmartClip
NFC 제어	AllowNfc
기기관리자 앱 설치 및 활성화 허용	AllowAdministrationApp
기기관리자 활성화 화이트리스트	AdmistrationAppWhiteList
개발자 모드 허용	AllowDeveloperMode
안전 모드 허용	AllowSafeMode
재부팅 배너 사용	EnableRebootBanner
재부팅 배너 문구	RebootBannerText
Android 보안 정책 업데이트 제어	AllowSecurityPolicyUpdate
웨어러블 장비 정책 활성화	EnableWearablePolicy
카메라	Camera
카메라 제어	AllowCamera
외장 SD 카드	SdCard
외장 SD 카드 제어	AllowExternalSdCard
외장 SD 카드 쓰기	AllowSDCardWrite

정책명	코드
미인가 SD카드 사용 탐지	EnableDetectUnauthorizedSdCard
마이크	Microphone
마이크 허용	AllowMicrophone
녹음 허용	AllowAudioRecord
S Voice 허용	AllowSVoice
Enrollment	Enrollment
EMM Guardian	AllowDmMonitor
Kiosk	Kiosk
Kiosk 앱 설정	KioskAppPackageName
작업관리자	AllowTaskManager
시스템바	AllowSystemBar
하드웨어 키 제어	AllowHardwareKeys
멀티 윈도우	AllowMultiWindow
에어 커맨드	AllowAirCommand
에어 뷰	AllowAirView
엣지 스크린 허용	AllowEdgeScreen
Kiosk Browser	KioskSingleWeb
키오스크 화면 보호기 컨텐츠	KioskScreenSaverContents
컨텐트 유형	Type
컨텐트 ID	Ids
통신	Retry
통신 재시도 횟수	NumRetries
통신 재시도 주기 (분)	RetryInterval
비밀번호	Password
비밀번호 최소강도	Quality
비밀번호 입력 실패 허용 횟수 (회)	MaximumFailedAttempts
비밀번호의 입력 실패 허용 횟수 초과 시 조치	MaximumFailedAttemptsViolationMeasure
비밀번호 최소 길이 (자)	MinimumLength
비밀번호 최대 사용 기간 (일)	MaximumAgeInDays
비밀번호 내역 관리 (회)	History
단말 잠금 유효 시간 최대값 (분)	MaximumGracePeriod
비밀번호 최대 순차적 숫자 사용 길이 (자)	MaximumNumericSequenceLength

정책명	코드
비밀번호 최대 순차적 문자 사용 길이 (자)	MaximumCharacterSequenceLength
잠금 화면시 기능 차단	KeyguardDisabledFeatures
단말 잠금 유효 시간 최대값	TimeToLock
스케줄러	Scheduler
정책 업데이트 스케줄	UpdateProfileScheduler
EMM Agent 업데이트 스케줄	UpdateAgentScheduler
저장소	Storage
저장소 암호화	StorageEncryption
로깅	Logging
로그 기록 여부	AllowLog
로그 기록 수준	LogLevel
로그 최대 수집 용량 (MB)	MaximumLogSize
로그 최대 보관 기간 (일)	MaximumLogDuration
스마트카드	SmartCard
스마트카드 브라우저 인증 허용	AllowSmartCardBrowserAuthentication
인증서	Certificate
인증서 삭제	AllowUserRemoveCertificates
인증서 설치 시 검증 여부	EnableCertificateValidationAtInstall
Attestation	Attestation
Attestation	EnableAttestation
검증 실패 시 조치	AttestationViolationMeasure
이메일	Mail
도메인 블랙리스트	DomainBlacklist
NTP	Ntp
서버 주소	NtpServerAddress
최대 시도 횟수 (회)	NtpMaxAttempts
폴링 주기 (시간)	NtpPollingInterval
짧은 폴링 주기 (초)	NtpPollingIntervalShorter
타임아웃 (초)	NtpTimeout
알림	Notification
이벤트 On 알림	ShowEventOnNotification
이벤트 Off 알림	ShowEventOffNotification
이벤트 알림 고정	ShowEventOffNotification
Enterprise FOTA	EnterpriseFota
Enterprise FOTA 사용	EnableEnterpriseFota

Android for Work 정책

Policy	Code
시스템	System
Android For Work 사용	UseAndroidForWork
화면 캡처	AllowScreenCapture
클립보드 제어	AllowClipboard

Knox 정책

Policy	Code
시스템	System
화면 캡처	AllowScreenCapture
클립보드	AllowClipboard
공유 목록	AllowShareList
구글 계정 동기화	AllowGoogleAccountSync
앱 오류 발생 시 구글 보고	AllowGoogleCrashReport
시스템 앱 종료	AllowStopSystemApp
외부 키보드	AllowThirdPartyKeyboard
USB장치 기본 접근 허용	UsbDeviceDefaultAccessList
패키지명	PackageName
벤더 아이디	VendorId
장비 아이디	ProductId
마이크	Microphone
마이크	AllowMicrophone
녹음	AllowAudioRecord
카메라	Camera
카메라	AllowCamera
외장 SD 카드	SdCard
외장 SD 카드	AllowExternalSdCard
외장 SD카드 사용 허용 앱 화이트리스트	AllowExternalSdCardAppWhiteList
시스템 (고급)	AdvancedSystem
Trusted Boot 검증	AllowTrustedBoot
Wi-Fi	WiFi
Wi-Fi 네트워크 추가	AllowAddUserProfiles
브라우저	Browser
Android 브라우저	AllowBrowser

Policy	Code
쿠키	AllowUseOfCookies
자바스크립트	AllowUseOfJavaScript
양식 데이터 저장	AllowUseOfAutoFill
팝업 차단	AllowUseOfPopups
브라우저 Proxy 주소	ProxyUrl
컨테이너 데이터 교환	ContainerDataExchange
App 이동	AllowMoveAppToContainer
Knox영역으로 File 이동	AllowMoveFileToContainer
일반영역으로 File 이동	AllowMoveFileToOwner
달력 데이터 동기화	AllowCalendarSyncData
연락처 데이터 동기화	AllowContactsSyncData
앱	App
앱 설치 블랙리스트	AppInstallationBlackList
앱 설치 화이트리스트	AppInstallationWhiteList
앱 삭제 방지리스트	AppDeletionBlackList
앱 실행 블랙리스트	AppRunningBlackList
앱 설치 화이트리스트	AppInstallationPermissionWhiteList
GMS 앱	AllowGms
앱 실행 방지리스트	AppPreventStartBlackList
배터리 최적화 예외 앱 설정	AppBatteryOptimizationWhiteList
일반영역 앱 설치 리스트	InstallAppListFromGeneralArea
비밀번호	Password
기업 ID 연동	EnableEnterpriseIdentityAuthentication
도메인주소	EnterpriseIdentifyAuthenticationAddress
설치 파일	EnterpriseIdentifyAuthenticationPackageName
FIDO 연동	EnableFido
Request URL	FidoRequestUrl
Response URL	FidoResponseUrl
FIDO 패키지명	FidoPackageList
비밀번호 강도	Quality
비밀번호 입력 실패 허용 횟수 (회)	MaximumFailedAttempts
비밀번호 입력 실패 허용 횟수 초과 시 조치	MaximumFailedAttemptsMeasure
비밀번호 최대 사용 기간 (일)	MaximumAgeInDays
비밀번호 히스토리 개수	MaximumHistoryLength

Policy	Code
비밀번호 최소 길이 (자)	MinimumLength
비밀번호 최소 문자수	MinimumLetter
비밀번호 최소 소문자수	MinimumLowerCase
비밀번호 최소 대문자수	MinimumUpperCase
비밀번호 최소 비문자수	MinimumNonLetter
비밀번호 최소 숫자수	MinimumNumeric
비밀번호 최소 특수문자수	MinimumSymbol
비밀번호 최대 중복 문자 포함 길이 (자)	MaximumDupliationCharacter
비밀번호 최대 순차적 문자 사용 길이 (자)	MaximumSequentialCharacterLength
비밀번호 최소 문자 변경 길이 (자)	MinimumChangeLength
금지어 설정	ForbiddenStrings
비밀번호 최대 순차적 숫자 사용 길이 (자)	MaximumSequentialNumericLength
화면 잠금 시간	TimeToLock
비밀번호 보임/감춤 설정	PasswordVisibility
화면잠금 패턴 보임/감춤 설정	PasswordPatternVisibility
지문 잠금해제 제어	AllowFingerprintBiometricAuthentication
홍채 잠금해제 제어	AllowIrisBiometricAuthentication
2단계 인증 강제 설정	EnforceMultifactorAuthentication
잠금화면 시 기능 차단	KeyguardDisabledFeatures
방화벽	Firewall
방화벽	EnableFirewall
허용 정책	AllowRuleList
허용 정책(앱별)	AllowAppRuleList
아이피 주소	IpAddress
포트 넘버	PortNumber
포트 위치	PortLocation
패키지 이름	PackageName
금지 정책	DenyRuleList
금지 정책(앱별)	DenyAppRuleList
아이피 주소	IpAddress
포트 넘버	PortNumber
포트 위치	PortLocation
패키지 이름	PackageName

Policy	Code
스마트카드	SmartCard
스마트카드 브라우저 인증	AllowSmartCardBrowserAuthentication
TIMA CCM	TimaCcm
전체앱	AllowAllPackages
TIMA CCM 프로파일 앱 화이트리스트	CcmProfileAppWhiteList
블루투스	Bluetooth
저전력 블루투스	AllowBle
DLP	Dlp
DLP 활성화	AllowDlpActivate
DLP LOCK 설정	AllowDlpFileDownload
DLP 유효기간 (분)	DlpExpiryAfter
DLP 생산자 앱 화이트 리스트	DlpCreatorAppWhiteList
DLP 소비자 앱 화이트 리스트	DlpConsumerAppWhiteList

iOS 정책

Policy	Code
비밀번호 정책	allowPasswordPolicy
비밀번호 강도	passwordQuality
비밀번호 입력 실패 허용 횟수 (회)	passwordMaxFailedAttempts
비밀번호 최소 길이 (자)	passwordMinLength
비밀번호 최대 사용 기간 (일)	passwordMaxPINAgeInDays
비밀번호 내역 관리 (회)	passwordPinHistory
자동 화면 잠금 시간 최대값 (분)	passwordMaxInactivity
화면 잠금 유예시간 최대값 (분)	passwordMaxGracePeriod
지문(Touch ID)으로 화면 잠금 해제	allowFingerprintForUnlock
앱 설치	allowAppInstallation
App Store를 사용하여 App 설치 허용	allowUIAppInstallation
앱 삭제	allowAppRemoval
YouTube	allowYouTube
iTunes Store	allowiTunes
유해한 음악 및 Podcast	allowExplicitContent
구입할 때마다 iTunes Store, 비밀번호 요구	forceITunesStorePasswordEntry
게임 센터	allowGameCenter
게임 센터에서 친구 추가	allowAddingGameCenterFriends
멀티플레이어 게임	allowMultiplayerGaming
iBookstore	allowBookStore
iBookestore에서 선정성 미디어 다운로드	allowBookstoreErotica
메시지 앱	allowChat
나의 친구 찾기	allowFindMyFriendsModification
앱내 구매	allowInAppPurchases
자동 Single 앱 모드 허용 앱 목록 설정	autonomousSingleAppModePermittedAppIDsSetting
자동 Single 앱 모드 허용 앱	autonomousSingleAppModePermittedAppIDs
기업용 App 신뢰하기	allowEnterpriseAppTrust
앱별 셀룰러 데이터 사용 여부 변경	allowAppCellularDataModification

Policy	Code
화상 통화	allowVideoConferencing
음성 다이얼	allowVoiceDialing
로밍상태에서 백그라운드 작업	allowGlobalBackgroundFetchWhenRoaming
Managed 앱에서 Unmanaged 앱으로의 데이터 공유	allowOpenFromUnmanagedToManaged
Unmanaged 앱에서 Managed 앱으로의 데이터 공유	allowOpenFromManagedToUnmanaged
AirDrop	allowAirDrop
AirDrop을 관리되지 않는 대상으로 취급	forceAirDropUnmanaged
백업	allowCloudBackup
도큐멘트 동기화	allowCloudDocumentSync
나의 사진 스트림	allowPhotoStream
사진 공유	allowSharedStream
키체인 동기화	allowCloudKeychainSync
Managed 앱 동기화	allowManagedAppsCloudSync
핸드오프	allowActivityContinuation
Safari	allowSafari
쿠키	safariAcceptCookies
자바스크립트	safariAllowJavaScript
양식 데이터 저장	safariAllowAutoFill
팝업 차단	safariAllowPopups
신뢰할 수 없는 TLS 인증서	allowUntrustedTLSPrompt
위조된 웹사이트 경고	safariForceFraudWarning
카메라	allowCamera
화면 캡처	allowScreenShot
Siri	allowAssistant
잠금화면에서 Siri	allowAssistantWhileLocked
Siri에서 웹 검색 결과	allowAssistantUserGeneratedContent
Siri 비속어 필터	forceAssistantProfanityFilter
진단 및 사용내용 보내기	allowDiagnosticSubmission
잠금화면에서 Passbook	allowPassbookWhileLocked
잠금화면에서 제어 센터	allowLockScreenControlCenter
잠금화면에서 알림보기	allowLockScreenNotificationsView
잠금화면에서 오늘보기	allowLockScreenTodayView
프로파일 수동 설치	allowUIConfigurationProfileInstallation

Policy	Code
계정 정보 수정 제어	allowAccountModification
인증서 신뢰 설정 자동 업데이트	allowOTAPKIUpdates
iTunes 백업시 암호화	forceEncryptedBackup
iTunes 페어링	allowHostPairing
광고 추적 제한	forceLimitAdTracking
공장 초기화	allowEraseContentAndSettings
Spotlight에서 웹 검색 결과	allowSpotlightInternetResults
차단 구성	allowEnablingRestrictions
단말 이름 변경	forceDeviceNameSetting
블루투스 설정 변경	allowBluetoothModification
국가별 등급	ratingRegion
동영상	ratingMovies
TV 프로그램	ratingTVShows
앱	ratingApps

단말 제어 전송 방법

Compliance

단말 제어	설명
최신 단말 관리 프로 파일/앱 정보 배포	[Android, Knox, iOS, Tizen Wearable] 최신 단말 관리 프로파일과 앱 정보를 단말에 배포하여, 변경된 정책, 설정, 앱 정보로 사용자 단말을 제어합니다.
최신 단말 관리 프로파일 배포	[Android, Knox, Windows, Tizen Wearable] 단말에 최신 단말 관리 프로파일을 배포하여, 변경된 정책으로 단말을 제어합니다.
최신 앱 관리 프로파일 배포	[Android, Knox, iOS, Windows, Tizen Wearable] 최신 앱 관리 프로파일을 단말에 배포하여, 변경된 EMM Client 앱 정책으로 사용자 단말을 제어합니다.
사내 애플리케이션 최신 정보 배포	[Android, Knox, Tizen Wearable] 단말에 사내 애플리케이션 최신 정보를 배포하여, 사내 애플리케이션의 최신 정보로 단말을 업데이트합니다.
사용자 정의 이벤트 실행	[Android, Knox, iOS] 사용자 정의 이벤트를 실행시켜, 사용자 정의 이벤트에 설정된 정책으로 단말을 제어합니다. 단말에 사용자 정의 이벤트를 실행하려면 다음의 절차를 따르세요. 1. Compliance 그룹의 **사용자 정의 이벤트** 실행을 클릭하세요. 2. "단말 제어" 창에서 실행할 이벤트 코드를 선택하세요. • 해당 단말이 할당받은 프로파일에 사용자 지정 이벤트가 등록되어 있는 경우, 이벤트 코드가 목록에 나타납니다. 3. 실행할 항목을 선택하세요. • 설정: 사용자 지정 이벤트에 설정된 정책으로 단말을 제어합니다. • 해제: 단말에 적용된 사용자 지정 이벤트를 해제하여, 프로파일에 설정된 기본 정책으로 단말을 제어합니다. 4. **확인**을 클릭하세요. 사용자 정의 이벤트에 적용된 정책을 확인하려면 다음의 절차를 따르세요. 1. **프로파일 > 단말 관리 프로파일**로 이동하세요. 2. 목록에서 **프로파일명**을 클릭하세요. 3. "단말 관리 프로파일" 창에서 이벤트 탭을 클릭하세요. 4. **이벤트 관리**를 클릭하여 이벤트 유형을 확인한 후, 이벤트 메뉴 아래의 **이벤트명**을 클릭하세요. 5. Android, iOS, Knox 컨테이너별 정책을 확인하세요.

단말 제어	설명
입출문 이벤트 실행	[Android, iOS] 입출문 이벤트를 실행시켜, 입출문 이벤트에 설정된 정책으로 단말을 제어합니다. 단말에 입출문 이벤트를 실행시키려면 다음의 절차를 따르세요. 1. Compliance 그룹의 **입출문 이벤트 실행**을 클릭하세요. 2. "단말 제어" 창에서 실행할 이벤트 코드를 선택하세요. • 해당 단말이 할당받은 프로파일에 입출문 이벤트가 등록되어 있는 경우, 입출문 코드가 목록에 나타납니다. 3. 실행할 항목을 선택하세요. • 설정: 입출문 이벤트에 설정된 정책으로 단말을 제어합니다. • 해제: 단말에 적용된 입출문 이벤트를 해제하여, 프로파일에 설정된 기본 정책으로 단말을 제어합니다. 4. **확인**을 클릭하세요. 입출문 이벤트에 적용된 정책을 확인하려 다음의 절차를 따르세요. 1. **프로파일 > 단말 관리 프로파일**로 이동하세요. 2. 목록에서 **프로파일명**을 클릭하세요. 3. "단말 관리 프로파일" 창에서 **이벤트**탭을 클릭하세요. 4. **이벤트 관리**를 클릭하여 이벤트 유형을 확인한 후, 이벤트 메뉴 아래의 **이벤트명**을 클릭하세요. 5. Android, iOS, Knox 컨테이너별 정책을 확인하세요.
Exchange 차단 해제	[Android] Exchange ActiveSync를 차단하거나 해제하세요. ● 설정: Exchange ActiveSync 차단 해제를 설정합니다. 즉, 단말에서 Exchange ActiveSync를 사용할 수 있습니다. ● 해제: Exchange ActiveSync를 차단합니다. 즉, 단말에서 Exchange ActiveSync를 사용할 수 없습니다.
탈옥 여부 점검	[iOS] 탈옥 정보 수집 기능으로, OS 위변조 상태를 확인할 수 있습니다.

애플리케이션 관리

애플리케이션 > 사내 애플리케이션 또는 애플리케이션 > Kiosk 애플리케이션에 등록된 앱이 " 단말 제어 " 창의 앱 목록에 나타납니다 .

단말 제어	설명
설치	선택한 앱을 단말에 설치 및 업데이트하려면 다음의 절차를 따르세요. 1. 애플리케이션 관리 그룹의 **설치**를 클릭하세요. • Android 단말의 경우, 사내 또는 Kiosk 앱 설치/업데이트 가능 • Knox, iOS 단말의 경우, 사내/EMM 앱 설치/업데이트 가능 • Tizen Wearable 단말의 경우, 사내 앱 설치/업데이트 가능 2. "단말 제어" 창에서 설치 유형을 선택하세요. • 설치 및 업데이트 • 삭제 후 설치 3. 애플리케이션을 선택 후, **확인**을 클릭하세요. 4. "확인" 창이 나타나면 **확인**을 클릭하세요.
실행	선택한 앱이 단말에서 실행되도록 하려면 다음의 절차를 따르세요. 1. 애플리케이션 관리 그룹의 **실행**을 클릭하세요. • Android 단말의 경우, 사내 또는 Kiosk 앱 실행 가능 • Knox, Tizen Wearable 단말의 경우, 사내 앱 실행 가능 2. "단말 제어" 창에서 실행시킬 앱을 선택한 후, **확인**을 클릭하세요. 3. "확인" 창이 나타나면 **확인**을 클릭하세요.
종료	선택한 앱을 단말에서 종료시키려면 다음의 절차를 따르세요. 1. 애플리케이션 관리 그룹의 **종료**를 클릭하세요. • Android 단말의 경우, 사내 또는 Kiosk 앱 종료 가능 • Knox, Tizen Wearable 단말의 경우, 사내 앱 종료 가능 2. "단말 제어" 창에서 종료시킬 앱을 선택 후, **확인**을 클릭하세요. 3. "확인" 창이 나타나면 **확인**을 클릭하세요.
데이터 삭제	선택한 앱의 데이터를 단말에서 삭제하려면 다음의 절차를 따르세요. 1. 애플리케이션 관리그룹의 **데이터 삭제**를 클릭하세요. • Android 단말의 경우, 사내 또는 Kiosk 앱 데이터 삭제 가능 • Knox 단말의 경우, 사내 앱 데이터 삭제 가능 2. "단말 제어" 창에서 데이터를 삭제할 앱을 선택한 후, **확인**을 클릭하세요. 3. "확인" 창이 나타나면 **확인**을 클릭하세요.

단말 제어	설명
삭제	선택한 앱을 단말에서 삭제하려면 다음의 절차를 따르세요. 1. 애플리케이션 관리 그룹의 **삭제**를 클릭하세요. • Android 단말의 경우, 사내 또는 Kiosk 앱 삭제 가능 • iOS, Knox, Tizen Wearable 단말의 경우, 사내 앱 삭제 가능 2. "단말 제어" 창에서 종료시킬 앱을 선택한 후, **확인**을 클릭하세요. 3. "확인" 창이 나타나면 **확인**을 클릭하세요.
실행 허용/금지	[Android] 선택한 사내/Kiosk 앱이 단말에서 실행되는것을 허용하거나 금지하려면 . 1. 애플리케이션 관리(사내/Kiosk) 그룹의 **실행 허용/금지**를 클릭하세요. 2. "단말 제어" 창에서 앱을 허용할지 여부를 선택하세요. • 허용: 지정한 앱이 단말에서 실행되는것을 허용합니다. • 금지: 지정한 앱이 단말에서 실행되는것을 금지합니다. 3. 허용 또는 금지할 앱을 선택 후, **확인**을 클릭하세요. 4. "확인" 창이 나타나면 **확인**을 클릭하세요.

단말 관리

단말 제어	설명
단말 잠금/해제	[Android] 단말을 잠금 또는 해제합니다. [iOS] iOS는 단말 잠금을 할 수 없으나, 단말 잠금 제어를 통해서 주요 기능들이 금지됩니다. [Windows] 단말을 잠금 처리만 가능합니다. [Tizen Wearable] 단말 잠금 처리합니다. 사용자가 단말 잠금을 해제하려며 운영자에게 문의하여 잠금 해제 코드를 부여받아 입력합니다. 운영자는 단말 잠금 해제 코드를 해당 단말 상세 화면에서 조회할 수 있습니다.
단말 잠금 비밀번호 초기화	[Android, iOS] 단말 잠금 비밀번호를 초기화합니다.
공장 초기화	[Android, iOS, Windows, Tizen Wearable] 단말을 공장초기화합니다. 내장 메모리, 외장 SD 카드의 데이터도 모두 초기화합니다.
단말 전원 종료	[Android, Tizen Wearable] 단말의 전원을 종료합니다.
단말 재부팅	[Android, Tizen Wearable] 단말을 재부팅합니다.
외장 SD 카드 초기화	[Android] 단말의 외장 SD 카드를 초기화합니다.
업데이트 FOTA 펌웨어 버전	[Android] E-FOTA 서비스로 단말의 펌웨어를 무선으로 업데이트합니다.
차단 정보 초기화	[iOS+Supervised] 단말의 차단 정보를 초기화합니다.

EMM 관리

단말 제어	설명
서비스 비활성화	[Android, iOS, Windows, Tizen Wearable] 단말 상태를 비활성화 상태로 변경합니다.
서비스 비활성화 시 앱 자동 삭제 속성 동기화	[iOS] 환경설정에서 "Unenrollment시 앱 삭제"의 값을 변경했다면 OTC를 전송하여 managed앱들에 대하여 비활성화 시 앱 자동 삭제 속성을 동기화합니다.
메시지 전송	[Android, Knox, iOS] 단말에 긴급하게 전달할메시지를 전송합니다. 메시지는 단말 상단 노티바에 표시됩니다. 메시지를 전송하려면 다음의 절차를 따르세요. 1. **EMM 관리** 그룹의 **메시지 전송**을 클릭하세요. 2. "단말 제어" 창에서 단말에 보낼 메시지 제목과 내용을 작성한 후, **확인**을 클릭하세요. 3. 메시지 전송 성공 메시지가 나타나면, **확인**을 클릭하세요.
화면 잠금	[Android, Knox, iOS, Windows] 단말의 화면 잠금을 실행합니다. 화면 잠금 상태에서는 카메라 사용이 금지됩니다. 화면 잠금을 실행하려면 다음의 절차를 따르세요. 1. **EMM 관리** 그룹의 **화면 잠금**을 클릭하세요. 2. "단말 제어" 창에서 보낼 제어 명령을 확인한 후, **확인**을 클릭하세요.
EMM Client 잠금 해제	[Android, Knox, iOS, Windows] 단말의 EMM Client 잠금 해제를 실행하려면 다음의 절차를 따르세요. 1. **EMM 관리** 그룹의 **EMM Client 잠금해제**를 클릭하세요. 2. "단말 제어" 창에서 보낼 제어 명령을 확인한 후, **확인**을 클릭하세요.
계정 삭제	[Android, Knox, iOS, Windows] 해당 단말의 Samsung SDS EMM Client에 등록된 계정을 삭제합니다.
Audit 로그 수집	[Android, Knox, iOS] EMM Client와 EMM Agent의 audit 로그를 단말로부터 수집합니다. 로그 사이즈 초과 시 자동 전송은 되지만, 로그 파일의 유실 우려가 있습니다. Audit 로그 수집에 대한 자세한 내용은 54페이지 3장의 "Audit 이벤트"를 참고하세요.
로그 수집	[Android, Knox, iOS, Tizen Wearable] 해당 단말의 Samsung SDS EMM Client 로그를 단말로부터 수집하려면 다음의 절차를 따르세요. 1. **EMM 관리** 그룹의 **로그 수집**을 클릭하세요. 2. "단말 제어" 창에서 Client 또는 Agent를 선택한 후, **확인**을 클릭하세요. 3. 메시지 전송 성공 메시지가 나타나면, **확인**을 클릭하세요.

단말 제어	설명
진단 정보 수집	[Android, iOS] 단말 잠금의 원인 진단을 위한 Samsung SDS EMM Client 로그를 단말로부터 수집하려면 다음의 절차를 따르세요. 1. **EMM 관리** 그룹의 **진단 정보 수집**을 클릭하세요. 2. "단말 제어-진단 정보 수집" 창에서 **확인**을 클릭하세요. 3. 메시지 전송 성공 메시지가 나타나면, **확인**을 클릭하세요.
사용자 정보 업데이트	[Android, Knox, iOS, Windows] 단말의 사용자 정보를 업데이트 합니다. 사용자 활성 상태/사용자명/사용자 설정(Secure Browswer 홈페이지 URL 정보, Bookmark 정보), 라이선스 정보, SecuCamera 허용유부, mMail 허용유무 정보 변경 시, 변경처리합니다.
라이선스 업데이트	[Android, Tizen Wearable] 삼성전자 단말제어에 필요한 Samsung SDS EMM 라이선스를 업데이트하여 새로 등록합니다.
시스템 앱 업데이트	[Android, iOS, Tizen Wearable] EMM Agent, Push Agent, EMM Client에 대한 패치, 버전업이 발생한 경우 단말에 설치된 Samsung SDS EMM Agent를 업데이트하기 위한 명령입니다. Samsung SDS EMM 서버에 등록된 Agent 정보가 단말로 전달되며, 단말은 자신에게 맞는 Agent를 선택하여 서버로 파일을 요청하여 설치 작업을 수행합니다.

단말 확인

단말 제어	설명
H/W 상태	[Android, iOS, Windows, Tizen Wearable] 단말의 인벤토리 정보를 업데이트합니다. 단말 제어를 보낸 후, 단말의 H/W 상태를 확인하려면 다음의 절차를 따르세요. 1. **단말 & 사용자 > 단말**에서 해당 단말의 모바일 ID를 클릭하세요. 2. "단말 상세" 창의 **기본 정보** 중 **Details**를 확인하세요.
설치된 앱 리스트	[Android, iOS, Windows, Tizen Wearable] 단말에 설치된 앱 정보를 업데이트합니다. iOS 단말의 경우 "단말 제어" 창에서 관리되는 앱 피드백 삭제 여부를 선택한 후, 단말 제어를 전송하세요. 단말 제어를 보낸 후, 단말에 설치된 앱 리스트를 확인하려면 다음의 절차를 따르세요. 1. **단말 & 사용자 > 단말**에서 해당 단말의 모바일 ID를 클릭하세요. 2. "단말 상세" 창에서 앱 탭을 클릭 후 설치된 앱 리스트를 확인하세요.
단말/앱 정보 수집	[Android, iOS, Windows] 단말에 설치된 앱 정보와 인벤토리 정보를 수집합니다. 단말 제어를 보낸 후, 해당 내용을 확인하려면 다음의 절차를 따르세요. 1. **단말 & 사용자 > 단말**에서 해당 단말의 **모바일 ID**를 클릭하세요. 2. "단말 상세" 창의 **기본 정보** 탭과 **앱** 탭을 확인하세요.
위치	[Android, iOS, Windows, Tizen Wearable] 단말의 현재 위치 정보를 가져옵니다. 단말 제어를 보낸 후, 단말의 위치를 확인하려면 다음의 절차를 따르세요. 1. **단말 & 사용자 > 단말**에서 해당 단말의 모바일 ID를 클릭하세요. 2. "단말 상세" 창의 **기본 정보** 중 **Details**의 **위치**를 확인하세요.
SIM 인증	[Android] 단말의 SIM 인증 처리를 수행합니다.
외장 SD 카드 인증	[Android] 단말의 외장 SD 카드 인증 처리를 수행합니다.
상태 보고	[iOS] 단말의 서비스 연결 상태를 확인합니다. 단말 제어를 보낸 후, 단말의 상태를 확인하려면 다음의 절차를 따르세요. 1. **단말 & 사용자 > 단말**에서 해당 단말의 모바일 ID를 클릭하세요. 2. "단말 상세" 창의 **기본 정보** 중 **Security** 그룹의 **KeepAlive**를 확인하세요. • : 단말과 EMM 서버의 연결 상태가 정상입니다. • : 단말과 EMM 서버와의 연결이 끊긴 상태입니다. • : 환경설정에서 KeepAlive를 설정하지 않은 경우입니다. • KeepAlive 설정을 위한 자세한 내용은 26페이지 2장의 "KeepAlive 설정하기"를 참고하세요.

컨테이너 관리

단말 제어	설명
컨테이너 잠금/해제	[Knox] Knox 컨테이너를 잠급니다. 사용자는 컨테이너에 진입할 수 없으며, 관리자에 의해 잠금 해제 명령을 받아야 진입이 가능합니다. ● 잠금: Knox 컨테이너를 잠급니다. ● 해제: Knox 컨테이너 잠금을 해제합니다.
컨테이너 잠금 비밀번호 초기화	[Knox] Knox 컨테이너의 비밀번호를 재설정하도록 합니다. 사용자는 자신의 기존 비밀번호 입력 후 변경이 가능합니다.
컨테이너 삭제	[Knox] 지정된 Knox 컨테이너를 삭제합니다. 컨테이너가 삭제되면 서버에 보고하여 인벤토리 정보를 갱신합니다.

사용자 정의 제어

단말 제어	설명
선택	[Windows] EMM에 등록된 CSP 설정을 선택하여 Windows 단말에 전송합니다. 선택을 클릭하면 전송 가능한 CSP 목록이 보여지며 선택 후 **실행**을 클릭합니다. ● CSP는 **설정 > Windows10 > CSP설정관리**에서 등록 및 관리가 가능합니다. ● CSP 관련 자세한 내용은 298페이지 17장의 "Windows10"를 참고하세요.

에러 코드 및 설명

Samsung SDS EMM 서버 또는 관리자 포털에서 정책 적용 시 또는 사용자의 단말을 제어하는 상황에서 발생할 수 있는 에러 코드의 리스트입니다 . 에러 발생 시 아래의 설명을 참고하며 관리자에게 해당 에러코드로 문의 가능합니다 .

로그인

코드	설명	로그 위치
session	다른 사용자가 해당 계정을 사용 중입니다	emm.log
disabled	계정이 잠겨 있습니다.	
accountDeleted	정책에 의하여 계정 접근이 허용되지 않습니다.	
accountLocked	정책에 의하여 계정 접근이 허용되지 않습니다.	
continuousFailure	계정 접근이 10분 동안 제한됩니다.	

보고서

코드	설명	로그 위치
1101	유효하지 않은 파라미터	emm.log
1102	데이터를 찾을 수 없는 경우	
1103	서비스가 비활성화 상태인 경우	
1104	내부 보고서는 수정 불가	
1120	SQL 예외	
1121	Datasource Pool을 찾을 수 없음	
1199	런타임 에러	

Open API

코드	설명	로그 위치
-102	Null 또는 Empty string	emm.log
-103	Null object	
-104	숫자(Integer)가 아닌 경우	
-105	숫자는 %d보다 커야 합니다.	
-106	숫자는 %d보다 작아야 합니다.	
-107	숫자는 %d와 %d사이의 값이어야 합니다.	
-108	문자열 길이는 %d보다 커야 합니다.	
-109	문자열 길이는 %d보다 작아야 합니다.	
-110	데이터 값은 %s 포맷이어야 합니다.	
-111	시작 일자는 종료 일자 이전이어야 합니다.	
-112	문자열은 %s와 매치되어야 합니다.	
-113	문자열의 서브시퀀스가 %s를 포함하지 않거나 매치되지 않습니다.	
-114	대소문자 구분하여 문자열과 %s이 동일하지 않습니다.	
-115	대소문자 구분없이 문자열과 %s이 동일하지 않습니다.	
-116	문자열은 공백 또는 탭으로만 구성됩니다.	
-117	문자열의 길이는 %d보다 큽니다(bytes)	
-200	라이선스 수가 초과되었습니다.	
-201	중복 데이터가 존재함	
-202	결과값이 없는 경우	
-203	관련 데이터가 오류인 경우	
-204	활성화된 단말이 존재함	
-205	Not found	
-206	선택된 그룹에 이미 등록되어 있는 경우	
-999	Unknown Error code	

인증서

코드	설명	로그 위치
3000	인증서 요청의 생성 실패	emm.log
3001	인증서 요청의 검증 실패	
3002	클라이언트 초기화 실패	
3003	인증서 등록 트랜잭션 실패	
3004	인증서 등록 요청 실패	
3005	인증서 등록의 최대 재시도 횟수 초과	
3006	인증서 등록 실패	
3007	CRL 요청 실패	
3008	CA 체인 요청 실패	
LEGO_ERR_0001	Provider Load 실패	certlog.log
LEGO_ERR_1100	잘못된 CA Type	
LEGO_ERR_1101	CA Type이 없음	
LEGO_ERR_1102	조회한 Root 인증서가 존재하지 않음	
LEGO_ERR_1103	조회한 CA 정보가 존재하지 않음	
LEGO_ERR_1104	managed CA가 존재하지 않음	
LEGO_ERR_1105	Entity 등록을 위해서는 CN과 password 가 필요함	
LEGO_ERR_1106	조회한 Ext CERT 정보가 없음	
LEGO_ERR_1107	조회한 CERT 정보가 없음	
LEGO_ERR_1108	조회한 Template 정보가 없음	
LEGO_ERR_1109	조회한 Batch 정보가 없음	
LEGO_ERR_1200	인증서 번호가 없음	
LEGO_ERR_1201	CN 정보 부재	
LEGO_ERR_1202	저장할 파일 경로가 없음	
LEGO_ERR_1203	Entity ID가 없음	
LEGO_ERR_1204	TemplateID가 없다면 CA 정보, CertProfileName, EndEntityProfile 정보 필요	
LEGO_ERR_1205	폐지하려는 인증서가 존재하지 않음.	
LEGO_ERR_1206	인증서 Revoke 정보를 저장하는 중 에러 발생	
LEGO_ERR_1207	ReIssue 중 에러 발생	
LEGO_ERR_1208	ReNew 정보를 저장하는 중에 에러 발생	
LEGO_ERR_1300	TemplateID가 없음	
LEGO_ERR_1301	Tenant ID가 없음	
LEGO_ERR_1302	DB에 업데이트된 데이터가 없음	
LEGO_ERR_1400	동일한 인증서 이름이 존재하는 경우	
LEGO_ERR_1401	이미 동일한 Tenant ID가 존재함	

코드	설명	로그 위치
LEGO_ERR_1500	CERT 검증 실패: 시작날짜가 현재날짜 이후인 경우	certlog.log
LEGO_ERR_1501	CERT 검증 실패: 만기날짜가 현재날짜 이전인 경우	
LEGO_ERR_1502	CERT 검증 에러: CA ROOT Init Verify시 에러 발생	
LEGO_ERR_1503	CERT 검증 에러: Signature 에러발생	
LEGO_ERR_1504	조회된 데이터가 없음	
LEGO_ERR_1505	PKCS12 인증서 가져오기 실패	
LEGO_ERR_1506	해당 파일에 CA Cert 가 존재하지 않습니다.	
LEGO_ERR_1900	파일 생성 시 에러	
LEGO_ERR_1901	존재하지 않는 파일	
LEGO_ERR_2001	CRL 생성 실패	
LEGO_ERR_2002	CRL request 생성 실패	
LEGO_ERR_2003	CRL 검증 실패	
LEGO_ERR_2004	마지막으로 실행한 CRL 정보가 없음	
LEGO_ERR_2005	마지막으로 실행한 CRL 요청 실패	
LEGO_ERR_2006	CRL 정보 저장 실패	
LEGO_ERR_2101	CRL BATCH SCHEDULE 추가 실폐	
LEGO_ERR_2102	CRL BATCH SCHEDULE 정보 UPDATE 실폐	
LEGO_ERR_2103	CRL BATCH SCHEDULE 제거 실폐	
LEGO_ERR_3000	Scep 메시지 생성 실패:certificate Request 생성 실패	
LEGO_ERR_3001	Scep 메시지 생성 실패:잘못된 trandsId	
LEGO_ERR_3002	Scep 메시지 생성 실패:잘못된 senderNonce	
LEGO_ERR_3003	Scep 검증 실패: signer 값이 없음.	
LEGO_ERR_3004	Scep 검증 실패: 잘못된 digest algorithm	
LEGO_ERR_3005	Scep 검증 실패: 잘못된 CA signer	
LEGO_ERR_3006	Scep 검증 실패: 잘못된 Signature	
LEGO_ERR_3007	Scep 검증 실패: ScepRequestMessage에 failInfo 포함	
LEGO_ERR_3008	Scep 검증 실패: 잘못된 message type	
LEGO_ERR_3009	Scep 검증 실패: ScepRequestMessage에 pkiStatus 가 없음	
LEGO_ERR_3010	Scep 검증 실패: success message 가 없음	
LEGO_ERR_3011	Scep 검증 실패: 잘못된 response status	
LEGO_ERR_3012	Scep 검증 실패: 잘못된 SenderNonce	
LEGO_ERR_3013	Scep 검증 실패: 잘못된 recipientNonce	
LEGO_ERR_3014	Scep 검증 실패: 잘못된 Transaction	

코드	설명	로그 위치
LEGO_ERR_3015	Scep 연결 실패: 잘못된 responseCode	certlog.log
LEGO_ERR_3016	Scep 연결 실패: 잘못된 content type	
LEGO_ERR_3017	Scep 연결 실패: Response 데이터가 없음	
LEGO_ERR_3018	Scep 연결 실패: Response byte 변환 실패	
LEGO_ERR_4000	Cmp 연결 실패: HTTP 연결 실패	
LEGO_ERR_4001	Cmp 연결 실패: 잘못된 responseCode	
LEGO_ERR_4002	Cmp 연결 실패: content type 이 없음	
LEGO_ERR_4003	Cmp 연결 실패: 잘못된 content type	
LEGO_ERR_5000	WebService 연결 시 인증 실패	
LEGO_ERR_5001	WebService 연결 실패	
LEGO_ERR_5002	FIND ENTITY 중에 에러발생	
LEGO_ERR_5003	Entity change 중에 에러발생	
LEGO_ERR_5004	Entity 등록 시 에러 발생	
LEGO_ERR_5005	이미 등록된 Entity	
LEGO_ERR_6000	Root CA 변환 실패	
LEGO_ERR_6001	Root CA 변환 실패: X509Certificate 변환 실패	
LEGO_ERR_6002	Root CA 변환 실패: 잘못된 Algorithm	
LEGO_ERR_6003	Root Cert 가 없음	
LEGO_ERR_8000	certificate 검증 실패: PKIMessage 구성 실패	
LEGO_ERR_8001	certificate 검증 실패: PKI Header 구성 실패	
LEGO_ERR_8002	certificate 검증 실패: 잘못된 Issuer sign 값, revoke 된 certificate 일 수 있음	
LEGO_ERR_8003	certificate 검증 실패: 잘못된 senderNonce	
LEGO_ERR_8004	certificate 검증 실패: 잘못된 transactionID	
LEGO_ERR_8005	certificate 검증 실패: 잘못된 algorithm	
LEGO_ERR_8006	certificate 검증 실패: 보호되지 않은 서명	
LEGO_ERR_8007	certificate 검증 실패: 보호되지 않은 password	
LEGO_ERR_8008	certificate 검증 실패: 유효하지 않은 algorithm	
LEGO_ERR_8009	certificate 검증 실패: 검증되지 않은 CA signature	
LEGO_ERR_8010	certificate 검증 실패: 잘못된 PBE hash	
LEGO_ERR_8011	certificate 검증 실패: Signature 검증 실패	
LEGO_ERR_8012	certificate 구성 실패: PKIBody 구성 실패	
LEGO_ERR_8013	certificate 구성 실패: CertRepMessage 구성 실패	

코드	설명	로그 위치
LEGO_ERR_8014	certificate 구성 실패: CertResponse 구성 실패	certlog.log
LEGO_ERR_8015	certificate 구성 실패: CertReqId 불일치	
LEGO_ERR_8016	certificate 구성 실패: PKIStatusInfo 구성 실패	
LEGO_ERR_8017	certificate 구성 실패: 잘못된 Status Value	
LEGO_ERR_8018	certificate 구성 실패: CertifiedKeyPair 구성 실패	
LEGO_ERR_8019	certificate 구성 실패: CertOrEncCert 구성 실패	
LEGO_ERR_8020	certificate 구성 실패: X509CertificateStructure 구성 실패	
LEGO_ERR_8021	certificate 구성 실패: certificate 인코딩 실패	
LEGO_ERR_8022	certificate 구성 실패: X509Certificate 구성 실패	
LEGO_ERR_8023	certificate 구성 실패: SubjectDN 불일치	
LEGO_ERR_8024	certificate 구성 실패: IssuerDN 불일치	
LEGO_ERR_8025	certificate 구성 실패: X509Certificate 검증 실패	
LEGO_ERR_9000	잘못된 URL 정보	
LEGO_ERR_9002	Http Connection 연결 실패	
LEGO_ERR_9003	CA로 부터 Reposonse 데이터가 없음	
LEGO_ERR_9004	잘못된 Host 정보	
LEGO_ERR_9005	Socket 연결 실패	
LEGO_ERR_9006	HOST 정보 없음	
LEGO_ERR_9007	ASN1 InputStream 변환 중 예외 발생	
LEGO_ERR_9008	DER OutputStream 변환 중 예외 발생	
LEGO_ERR_9009	존재하지 않은 Provider	
LEGO_ERR_9010	존재하지 않은 Algorithm	
LEGO_ERR_9011	X509Certificate 변환 실패	
LEGO_ERR_9012	X509Certificate 인코딩 실패	
LEGO_ERR_9013	KeyStore 생성 시 에러 발생	
LEGO_ERR_9014	Class 변환 시 에러 발생	
LEGO_ERR_9015	InputStream 변환 중 예외 발생	
LEGO_ERR_9016	KeyStore 패스워드가 일치 하지 않음	
LEGO_ERR_9017	SecretKey 생성 시 에러발생	
LEGO_ERR_9018	정의되지 않은 Revoke Reason	
LEGO_ERR_9019	Object를 byte[] 으로 변환 시 에러발생	
LEGO_ERR_9020	byte[] 를 Object으로 변환 시 에러발생	
LEGO_ERR_9100	alias에 해당하는 Certificate가 존재하지않음	
LEGO_ERR_9101	KeyStore PrivateKey 추출 시 에러발생	
LEGO_ERR_9102	KeyStore Certificate 추출 시 에러발생	

코드	설명	로그 위치
LEGO_ERR_9103	KeyStore Aliases 추출 시 에러발생	certlog.log
LEGO_ERR_9104	PKCS12 형태의 KeyStore 저장 시 에러발생	
LEGO_ERR_9105	KeyStore 삭제 시 예외 발생: KeyStore 에러 발생	
LEGO_ERR_9106	KeyStore 삭제 시 예외 발생: 존재하지 않는 파일	
LEGO_ERR_9107	KeyStore 삭제 시 예외 발생: 재저장 시 에러 발생	
LEGO_ERR_9108	파일 InputStream이 비어있음	
LEGO_ERR_9109	Object를 Map 으로 변환 시 에러 발생	
LEGO_ERR_9110	Map을 Object 으로 변환 시 에러 발생	
LEGO_ERR_9111	존재하지 않는 Batch Type	
LEGO_ERR_9112	존재하지 않는 Template	
LEGO_ERR_9200	필수 입력값 누락: Serial Number	
LEGO_ERR_9901	암호화 실패	
LEGO_ERR_9902	복호화 실패	
LEGO_ERR_999	예상하지 못한 에러가 발생하였습니다. 관리자에게 문의하세요.	

인증서 CA 접속 테스트

모듈	코드	설명	로그 위치
인증서 ADCS CA	ERROR_ROOT_CHAIN_TEST	Root Chain 가져오기 실패	emm.log
	ERROR_ROOT_CERT_PW	인증서 비밀번호 오류	
	ERROR_Android_ISSUE_TEST	인증서 발급 실패(Android)	
	ERROR_Android_KEY_ALG	키 알고리즘 에러(Android)	
	ERROR_Android_DOMAIN	도메인 에러(Android)	
	ERROR_Android_CES_URL	웹서비스 URL 에러(Android)	
	ERROR_Android_CA_SERVER	CA 서버 설정 에러(Android)	
	ERROR_Android_KERBEROS_REALM	Kerberos 설정 에러(Android)	
	ERROR_Android_KEY_TABEL	Keytab 설정 에러(Android)	
	ERROR_Android_CERT	인증서 에러(Android)	emm.log
	ERROR_iOS_ISSUE_TEST	인증서 발급 실패(iOS)	
	ERROR_iOS_KEY_ALG	키 알고리즘 에러(iOS)	
	ERROR_iOS_DOMAIN	도메인 에러(iOS)	
	ERROR_iOS_CES_URL	웹서비스 URL 에러(iOS)	
	ERROR_iOS_CA_SERVER	CA 서버 설정 에러(iOS)	
	ERROR_iOS_KERBEROS_REALM	Kerberos 설정 에러(iOS)	
	ERROR_iOS_KEY_TABEL	Keytab 설정 에러(iOS)	
	ERROR_iOS_CERT	인증서 에러(iOS)	
인증서 SCEP CA	ERROR_ROOT_CHAIN_TEST	Root Chain 가져오는데 실패함	emm.log
	ERROR_ISSUE_TEST	인증서 발급 실패	
	ERROR_SCEP_MSGSIGNERCERT_TEST	SCEP Message Signer Certificate 생성 실패	

모듈	코드	설명	로그 위치
인증서 NDES CA	CONNECTION_FAIL	Challenge URL 오류	emm.log
	CERTSRV_ADMIN_UNAUTHORIZED	아이디 또는 비밀번호 오류	
	CERTSRV_ADMIN_URL_INVALID	Challenge URL이 잘못 됨IDID	
	NDES_NOT_PERMISSION	도메인 오류	
	NDES_CHALLENGE_NOT_FOUND	Challenge 암호를 찾을 수 없음. NDES 서버 설정 확인 필요	
	NDES_CHALLENGE_FAIL	Challenge 암호를 찾을 수 없음	

정책

모듈	코드	설명	로그 위치
Common	0000000	성공	Console
	9999999	실패	
	9000001	동일 컴포넌트 존재	
	9000002	컴포넌트 ID 및 타입 불 일치	
	9000003	필수 파라미터 에러	
	9000004	동일 컴포넌트 값 존재	
	9000005	유효하지 않은 MDM 라이선스	
	9000006	동일 config 타입 존재	
	9000007	동일 VPN 앱 ID 존재	
	9000008	특수 문자 비 허용	
	9000009	인가되지 않은 어드민 ID	
	9000010	DB 서비스 에러	
	9000011	잘못된 URL 정보	
	2000000	유효하지 않은 OTC 코드	mdm_otc.log mdm.log
	2000001	OTC를 지원하지 않는 단말 플랫폼	
	2000002	OTC 코드 미 입력	
	2000003	전송 대상 단말 device ID 미 입력	
	2000004	iOS Agent용 device token 미 존재	
	2000005	Push AppID 정보 미 입력	
	2000006	OTC 메시지 생성 실패	
	2000008	OTC 파라미터 정보 미 입력	
	2000010	iOS 단말 Push magic 미 존재	
	2000011	유효하지 않은 UMP AppID	
	2000012	사용자에 등록된 단말 없음	
Common	2000013	사용자에 OTC 대상 단말 없음	mdm_otc.log mdm.log
	2000014	iOS Client용 device token 미 존재	
	2000015	유효하지 않은 iOS Agent용 device token	
	2000016	유효하지 않은 iOS Client용 device token	
	2000017	Screen Lock OTC 적용 불가	
	2000018	OTC 큐 입력시 예외 오류 발생	
	2000019	OTC를 전송할 단말의 TenantID가 존재하지 않음	

모듈	코드	설명	로그 위치
Push	2001000	Unknown Error	mdm_otc.log mdm.log
	2001001	전송 메시지 최대 길이 초과	
	2001002	Push-DA 접속 불가	
	2001003	Push-SA DB 서비스 오류	
	2001004	Push-DA 비활성화	
	2001005	Push-SA 미등록	
	2001006	Push-DA 미등록	
	2001007	Push-SA로부터 메시지 ID 리턴 불가	
	2001008	메시지 TTL OVER	
	2001009	메시지 최대 재전송 횟수 초과	
	2001010	Push-SA 등록 실패	
Profile	0100001	단말에 적용된 프로파일은 삭제 금지	Console
	0100002	존재하지 않는 프로파일 ID	
	0100003	내방객 프로파일 ID	
	0100004	존재하지 않는 프로파일 구성 요소	
	0100005	존재하지 않는 프로파일 관계 요소	
	0103001	해쉬값 생성 실패	
	0103002	해쉬값 일치하지 않음	
	0103003	프로파일 타입이 일치 하지 않음	
	0103004	Import시 프로파일 파일 읽기 실패	
	0103005	Export시 프로파일 파일 저장 실패	
	0103006	Import시 프로파일 파일의 확장자 불일치	
	0199001	단말에 프로파일 미할당됨	
	0199002	사용자에 프로파일이 미할당됨	
	0199003	조직에 프로파일이 미할당됨	
	0199004	그룹에 프로파일이 미할당됨	
	0199005	프로파일에 할당된 단말 없음	
	0199010	존재하지 않는 그룹	
	0199012	이미 프로파일이 할당된 그룹	
	0199020	존재하지 않는 조직	
	0199022	이미 프로파일이 할당된 조직	
Knox	0210001	Knox Container Alias 중복	Console
	0210002	Knox Container 생성시 최대치 초과	
	0210003	Knox Container 생성시 생성할 수 없는 타입	

모듈	코드	설명	로그 위치
EVENT	0301500	이벤트 정책 우선순위 범위 초과	Console
	0301501	이벤트 정책 우선순위 삭제 오류	
	0301502	이벤트 정책 우선순위 중복	
	0301503	프로파일에 존재 하지 않는 이벤트	
	0301504	이벤트 정책 우선순위가 타 사용자에 의해 변경됨	
	0301505	SIM변경 이벤트는 1개만 생성 가능	
	0301506	로밍 이벤트는 1개만 생성 가능	
	0301507	사용자 예외정책 이벤트는 1개만 생성 가능	
	0320001	구성요소로 사용되고 있는 이벤트 삭제 금지	
POLICY	0410001	Boolean 값만 허용된 정책	Console
	0410002	정수값만 허용된 정책	
	0410003	범위 값을 초과한 정책	
	0420001	정책 비교 최소값 오류	
	0420002	정책 비교 최대값 오류	
	0430001	사내앱 App 정책 최대치(플랫폼별 15개) 초과 저장	
CONFIGRATION	0510000	프로파일내에 사용하는 인증서(삭제 금지)	Console
	0510001	iOS 사용 인증서(삭제 금지)	mdm_ios_agent.log, mdm.log
	0530001	XML 포맷이 아닙니다.	Console
GCM Push	2002000	[GCM] 서버 정보 없음	mdm_otc.log, mdm.log
	2002001	[GCM] 인증 실패	
	2002002	[GCM] 서버 내부 오류	
	2002003	[GCM] 서비스 중단	
	2002004	[GCM] 한번에 너무 많은 메시지 전송(1000)	
	2002005	[GCM] 한 단말에 너무 많은 메시지 전송(100)	
	2002006	[GCM] 단말 등록 ID 분실	
	2002007	[GCM] 잘못된 단말 등록 ID	
	2002008	[GCM] 등록된 Sender ID와 단말 등록 ID 간 불일치	

모듈	코드	설명	로그 위치
GCM Push	2002009	[GCM] 단말 등록 해제 또는 알림 사용 중지	mdm_otc.log , mdm.log
	2002010	[GCM] 전송 메시지 최대 길이 초과(4KB)	
	2002011	[GCM] Sender ID 누락	
	2002012	[GCM] 메시지 전송 에러	
	2002013	[GCM] 메시지 전송 에러	
	2002014	[GCM] 유효하지 않은 메시지 TTL	
	2002015	[GCM] push key 없음	
	2002016	[GCM] 내부 Exception 발생	
	2002017	[GCM] unknown 에러	
APNS Push	2003000	[APNS] 서버 정보 없음	mdm_otc.log , mdm.log
	2003001	[APNS] 내부 처리 에러	
	2003002	[APNS] token 누락	
	2003003	[APNS] 인증서 내 topic 누락	
	2003004	[APNS] 메시지 누락	
	2003005	[APNS] token 크기 오류	
	2003006	[APNS] topic 크기 오류	
	2003007	[APNS] 전송 메시지 최대 길이 초과	
	2003008	[APNS] 유효하지않은 token	
	2003009	[APNS] 서버 다운	
	2003010	[APNS] protocol 에러	
	2003011	[APNS] 내부 Exception 발생	
	2003012	[APNS] unknown 에러	
	2003013	[APNS] payload 생성 오류	
	2003014	[APNS] agent push key 없음	
	2003015	[APNS] client push key 없음	
WNS Push	2004000	[WNS] 서버 정보 없음	mdm_otc.log , mdm.log
	2004001	[WNS] 잘못된 요청	
	2004002	[WNS] 유효하지 않은 token	
	2004003	[WNS] 요청된 channel에 전송 권한 없음	
	2004004	[WNS] 유효하지 않은 channel	
	2004005	[WNS] 유효하지 않은 http 방식	
	2004006	[WNS] 부하량 초과	
	2004007	[WNS] 종료된 channel	
	2004008	[WNS] 전송 메시지 최대 길이 초과(5KB)	
	2004009	[WNS] 서버 내부 오류	

모듈	코드	설명	로그 위치
WNS Push	2004010	[WNS] 서비스 중단	mdm_otc.log , mdm.log
	2004011	[WNS] 내부 Exception 발생	
	2004012	[WNS] unknown 에러	
	2004013	[WNS] push key 없음	
	2004014	[WNS] 단말 채널 URI 정보는 없지만 커맨드 큐에는 큐정보가 생성되고, 추후 처리됩니다.	
	2004015	[WNS] WNS 서버 정보는 없지만 커맨드 큐에는 큐정보가 생성되고, 추후 처리됩니다.	
Tizen Push	2005000	[Tizen] 환경 설정 내 서버 정보 없음	mdm_otc.log , mdm.log
	2005001	[Tizen] 전송실패	
	2005002	[Tizen] 유효기간 만료	
	2005003	[Tizen] Tizen 서버 알수없는 이유로 전송 실패	
	2005004	[Tizen] Tizen 서버 내부 오류	
	2005005	[Tizen] APPID 필드없음	
	2005006	[Tizen] 단말 인증 Token 없음	
	2005007	[Tizen] REGID 필드 없음	
	2005008	[Tizen] REQUESTID 필드 없음	
	2005009	[Tizen] MESSAGE, APPDATA 필드 둘 다 없음	
	2005010	[Tizen] 등록되지 않은 REGID	
	2005011	[Tizen] 등록되지 않은 APPID	
	2005012	[Tizen] REQUEST DATA 형식 오류	
	2005013	[Tizen] CONTENT 매핑 중 중대 오류 발생	
	2005014	[Tizen] 일부 필드 누락	
	2005015	[Tizen] ENQUEUE 불가	
	2005016	[Tizen] Queue에 없거나 이미 발송되었기에 취소 불가	
	2005017	[Tizen] IO 처리 시 문제 발생	
	2005018	[Tizen] 지원하지 않는 URI	
	2005019	[Tizen] 지원하지 않는 요청 방식	
	2005020	[Tizen] 읽을 수 없는 데이터 포함되었음을	

모듈	코드	설명	로그 위치
Tizen Push	2005021	[Tizen] 비정상 데이터 포함	mdm_otc.log , mdm.log
	2005022	[Tizen] 지원하지 Reliability 옵션 포함	
	2005023	[Tizen] Bad padding 예외	
	2005024	[Tizen] Json 파싱 오류	
	2005025	[Tizen] Json 매핑 오류	
	2005026	[Tizen] Block size 오류	
	2005027	[Tizen] REGID 디코딩 오류	
	2005028	[Tizen] SECRET KEY 필드 없음	
	2005029	[Tizen] 인증되지 않은 Application	
	2005030	[Tizen] 지원하지 않는 인코딩 타입	
	2005031	[Tizen] 파싱할 수 없는 요청 타입	
	2005032	[Tizen] 메시지 사이즈 초과 (2KB)	
	2005033	[Tizen] 지원하지 않는 접속 방식	
	2005034	[Tizen] 지원하지 않는 Body	
	2005035	[Tizen] 유효하지 않은 만료 시간	
	2005036	[Tizen] 유효하지 않은 대기 시간	
	2005037	[Tizen] 메시지 길이 초과	
	2005038	[Tizen] Empty multiple 요청	
	2005039	[Tizen] Notification Key 생성 오류	
	2005040	[Tizen] Application 생성 오류	
	2005041	[Tizen] Application 삭제 오류	
	2005042	[Tizen] Application 읽기 오류	
	2005043	[Tizen] Application 업데이트 오류	
	2005044	[Tizen] 유효하지 않은 timestamp	
	2005045	[Tizen] 유효하지 않은 타입	
	2005046	[Tizen] 등록되지 않은 Application	
	2005047	[Tizen] Application 인증 오류	
	2005048	[Tizen] Push 서버 사용이 허가되지 않음	
	2005049	[Tizen] HTTP_STATUS_CODE 에러	
	2005050	[Tizen] 응답 파싱 에러	
	2005051	[Tizen] 접근 지역 URL 에러	
	2005052	[Tizen] 알 수 없는 오류	

모듈	코드	설명	로그 위치
iOS MDM	1500000	Command에 대한 Request가 10번 이상인 경우	mdm_ios_agent.log, mdm.log
	1500001	할당된 mdm프로파일 없음	
	1500002	단말정보 테이블에 deviceId에 해당 하는 단말이 없음	
	1500003	프로파일 생성할 수 없음	
	1500004	인증서 파일 찾을 수 없음	
	1500005	인증서 파일 읽어올 수 없음	
	1500006	Check-In Authenticate 인증실패	
	1500007	iOS가 아님	
	1500008	활성화된 유저가 아님	
	1500010	단말이 활성화상태(A) 또는 Provision(P)상태가 아님	
	1500011	디바이스를 업데이트 할 수 없음 이미 UDID가 존재함	
	1500013	Tenant ID에 해당 Device ID가 없음	
	1500014	Push 발송 실패	
	1500015	활성화 실패- 재활성화 방지 (활성화된 단말이 공장초기화 등으로 다시 활성화 할 경우)	
	1500016	활성화 실패 (동일 단말에서 같은 테넌트로 다른 mobileId(DeviceID)로 활성화 시도로 인해)	
	1500017	프로파일 Signing 실패	
	1500018	활성화 실패 (다른 단말에서 같은 테넌트로 mobileId(DeviceID)로 활성화 시도로 인해)	
	1500020	파라미터 정보 오류	
	1500024	enrollment profile 생성할 수 없음	
	1500029	애플리케이션 정보 조회 실패	
	1500030	단말 활성화 실패	
	1500031	단말 비활성화 실패	
	1500032	토큰 업데이트 실패	
	1500033	앱설치 금지	
	1500034	앱설치 실패	
	1500035	블랙&화이트리스트 조회 실패	
	1500036	비활성화시 앱삭제 속성 동기화에서 앱정보를 가져오지 못함	
	1500101	지금 명령을 수행할 수 없음	
	1500102	MDM Command 형식에 어긋남	

모듈	코드	설명	로그 위치
Android MDM	1900000	프로파일을 복제할 수 없음	mdm.log
	1900001	프로파일을 JSON string 으로 변경할 수 없음	
	1900002	프로파일을 JSON string 으로 변경할 수 없음	
	1900003	프로파일을 JSON string 으로 변경할 수 없음	
	1900004	프로파일 코드가 유효하지 않음	
	1900005	프로파일 Type 이 유효하지 않음	
	1901000	일반영역의 설정 Category가 유효하지 않음	
	1901001	Knox영역의 설정 Category가 유효하지 않음	
	1901010	단말에서 요청한 정보를 확인할 수 없음	mdm_android_agent.log, mdm.log
	1901011	단말 요청 메세지 파싱 불가	
	1901012	EMM Agent 요청 메세지 확인 불가	
	1901013	정의되지 않은 Command Code	
	1901014	파일 생성 오류	
	1901015	요청된 프로토콜 버전이 유효하지 않음	
	1901016	단말 요청 메세지 확인 불가	
	1901017	ELM 라이선스, Knox 라이선스를 찾을 수 없음	
	1901018	Tenant ID를 확인할 수 없음	
	1901019	유효하지 않은 Command Parameter	
	1901020	EMM Client 또는 EMM Agent 앱 정보를 찾을 수 없음	
	1901021	프로파일 생성 불가	
	1901022	Device에 할당된 프로파일 을 찾을 수 없음	
	1901024	Device 상태를 업데이트 할 수 없음	
	1901025	Device 상태를 업데이트 할 수 없음 (UpdateDeviceInformation Command)	
	1901026	KeepAliveRequest 처리 중 오류	
	1901027	LockDeviceRequest 처리 중 오류	
	1901028	UnlockDeviceRequest 처리 중 오류	
	1901029	LockKnoxContainerRequest 처리 중 오류	
	1901030	InstallKnoxAppRequest 처리 중 오류	
	1901031	UninstallKnoxAppRequest 처리 중 오류	
	1901032	RemoveKnoxAppInternalDataRequest 처리 중 오류	
	1901033	StartKnoxAppRequest 처리 중 오류	
	1901034	StopKnoxAppRequest 처리 중 오류	
	1901035	EMM Agent 에서 전달받은 메세지 Result가 success 가 아니라 처리할 수 없음	

모듈	코드	설명	로그 위치
Android MDM	1901036	EMM Agent 에서 전달받은 메세지의 Result를 확인할 수 없음	mdm_android_agent.log, mdm.log
	1901037	EnrollmentSpecRequest의 Parameter가 적절하지 않음	
	1901038	InstallAppRequest 처리 중 오류	
	1901039	TriggerRequest 처리 중 오류	
	1901040	ReportRequest 처리 중 오류	
	1901041	ResetPasswordRequest 처리 중 오류	
	1901042	ResetExternalSdCardRequest 처리 중 오류	
	1901043	AuthorizeExternalSDCardRequest 처리 중 오류	
	1901044	WipeDeviceRequest 처리 중 오류	
	1901045	RebootDeviceRequest 처리 중 오류	
	1901046	PowerOffDeviceRequest 처리 중 오류	
	1901047	UninstallAppRequest 처리 중 오류	
	1901048	RemoveAppInternalDataRequest 처리 중 오류	
	1901049	StartAppRequest 처리 중 오류	
	1901050	StopAppRequest 처리 중 오류	
	1901051	AppInfoRequest 처리 중 오류	
	1901052	UnlockKnoxContainerRequest 처리 중 오류	
	1901053	ResetKnoxContainerPasswordRequest 처리 중 오류	
	1901054	RemoveKnoxContainerRequest 처리 중 오류	
	1901055	StartCCModeRequest 처리 중 오류	
	1901056	StopCCModeRequest 처리 중 오류	
	1901057	EMM Agent Profile이 존재하지 않음	
	1901058	요청받은 앱 정보를 찾을 수 없음	
	1901059	해당 경로에 실제 앱 파일을 찾을 수 없음	
	1901060	KeepAlive 정보를 가져올 수 없음(환경설정에 포함되어있음)	
	1901061	요청받은 Knox 앱 정보를 찾을 수 없음	
	1901062	해당 경로에 실제 Knox 앱 파일을 찾을 수 없음	
	1901063	InstallAppRequest 처리 중 오류	
	1901064	해당 Device ID로 단말 기본 정보를 검색할 수 없음	
	1901065	단말 상태가 Activated가 아님	
	1901066	단말 상태를 확인할 수 없음	
	1901067	시스템 앱 정보를 찾을 수 없음	

모듈	코드	설명	로그 위치
Android MDM	1901068	EMM Agent 앱 정보를 찾을 수 없음	mdm_android_agent.log, mdm.log
	1901069	UpdateAgentRequest 처리 중 오류	
	1901070	단말 상태가 Provisioned 또는 Activated가 아님	
	1901071	파일 경로를 가져올 수 없음	
	1901072	Command Parameter 에 APP ID가 존재하지 않음	
	1901073	Command Parameter 에 Package Name이 존재하지 않음	
	1901074	단말 상태가 Provisioned가 아님	
	1901075	단말 상태를 Unmanaged로 변경할 수 없음	
	1901076	단말 상태를 Managed로 변경할 수 없음	
	1901077	단말이 이미 Activated 되어있음	
	1901079	오프라인 비활성화 코드를 업데이트 할 수 없음	
	1901080	LockEasRequest 처리 중 오류	
	1901081	UnlockEasRequest 처리 중 오류	
	1901082	단말 상태가 Activated가 아니며 Blocked(System)도 아님	
	1901083	유효하지 않은 데이터(정책 적용 결과에 오는 InvalidCommandData)	
	1901084	GetAttestationNonceRequest 처리 중 오류	
	1901085	VerifyAttestationDataRequest 처리 중 오류	
	1901086	Attestation 서버 주소를 찾을 수 없음	
	1901087	Attestation API 키 를 찾을 수 없음	
	1901088	유효하지 않은 Attestation Parameter	
	1901090	EMM Client 앱 정보를 찾을 수 없음	
	1901091	EMM Agent 앱 정보를 찾을 수 없음	
	1901092	AuthorizeSimRequest 처리 중 오류	
	1901093	UpdateUnenrollCodeRequest 처리 중 오류	
	1901094	단말 상태가 Blocked 임	
	1901095	EnableAppRequest 처리 중 오류	
	1901096	DisableAppRequest 처리 중 오류	
	1901097	ELM 라이선스를 복호화 하는데 실패하였음	
	1901098	ReportPolicyViolationRequest 처리 중 오류	
	1901099	AndroidForWork 앱 정보를 찾을 수 없음	
	1901100	해당 경로에 실제 AndroidForWork 앱 파일을 찾을 수 없음	
	1901101	InstallAfwAppRequest 처리 중 오류	
	1901102	UninstallAfwAppRequest 처리 중 오류	

모듈	코드	설명	로그 위치
Android MDM	1901103	단말 상태를 "BS" 로 변경할 수 없음	mdm_android_agent.log, mdm.log
	1901104	중복 단말 체크 실패	
	1901105	동일한 기기로 활성화된 단말 정보가 존재함	
	1901106	UpdateDiagnosisRequest 처리 중 오류	
	1901107	비활성화시 앱 삭제 설정 정보를 찾을 수 없음	
	1901108	다음 커맨드를 가져올 수 없음	
	1901109	커맨드 메세지를 생성할 수 없음	
	1901110	커맨드를 삭제할 수 없음	
	1901111	MDM old protocol 통신 사용	
	1901112	Update Device Inventory (요청) 처리 중 오류	
	1901113	Update App Inventory (요청) 처리 중 오류	
	1901114	Update Current Location Inventory (요청) 처리 중 오류	
	1901115	Update Audit Inventory (요청) 처리 중 오류	
	1901116	Update Log Inventory (요청) 처리 중 오류	
	1901117	요청 파라미터에 ContentId 가 존재하지 않음	
	1901118	컨텐츠 정보를 찾을 수 없음	
	1901119	다운로드 컨텐츠 (요청) 처리 중 오류	
	1901120	Update Device and App Inventory (요청) 처리 중 오류	
	1901121	요청 파라미터에 Model Number 가 존재하지 않음	
	1901121	요청 파라미터에 Model Number 가 존재하지 않음	
	1901122	요청 파라미터에 Customer Code 가 존재하지 않음	
	1901123	허용된 펌웨어 버전을 조회할 수 없음	
	1901124	허용된 펌웨어 버전이 존재하지 않음	
Client	1600000	Header의 파라미터 정보 없음	mdm_ai_client.log, mdm.log
	1600001	압축실패	
	1600002	암호화 실패	
	1600003	없는 command	
	1600004	유효하지 않은 버전	
	1600005	Server에 해당 device id가 없음	
	1600006	유효하지 않은 deviceid (A,P상태가 아님)	
	1600010	Device id DB 조회 실패	
	1601001	OTC전송 실패	

모듈	코드	설명	로그 위치
Client	1601002	앱정보 DB 조회 실패	mdm_ai_client.log, mdm.log
	1601003	Knox ID DB 조회실패	
	1601004	요청 파라미터에서 사용자 ID가 없음	
	1601005	요청 파라미터에서 App ID가 없음	
	1601006	요청 파라미터에서 패키지명이 없음	
	1601007	요청 파라미터에서 Knox ID가 없음	
	1601008	파라미터 knox id와 매칭되는 knoxcontainer ID가 없음	
	1601009	파라미터 app ID에 해당하는 앱정보가 없음	
	1601010	유효하지 않은 OTC 코드	
	1601011	White/blackList 에 포함된 애플리케이션이 아님	
	1601012	AndroidForWork에 profileId를 찾을 수 없음	
	1601020	요청 파라미터에서 user ID가 없음	
	1601021	홈페이지 정보 insert실패	
	1601022	요청 파라미터에서 user ID가 없음	
	1601023	요청 파라미터에서 북마크 index가 없음	
	1601024	북마크 정보 DB insert실패	
	1601030	devicetoken DB 업데이트 실패	
	1601031	프로파일 DB 조회 실패	
	1601032	앱정보 DB 조회 실패	
	1601033	프로파일 생성 실패	
	1601034	최종프로파일 업데이트 시간 DB 업데이트 실패	
	1601035	앱정보 DB 조회 실패	
	1601036	EMM Client 패키지 정보를 업데이트 실패	
	1601040	위치정보 및 jailbreak정보등 DB 업데이트 실패	
	1601041	유효하지 않은 reportype	
	1601060	device ID가 없음	
	1601061	활성화상태(A)가 아님	
	1601062	비활성화상태(I)가 아님	
	1601063	방문자 프로파일(visitorProfile)을 만들 수 없음	
	1601064	방문자 프로파일 삭제 금지 해제 프로파일(initVisitor)을 만들 수 없음	
	1601065	방문자 프로파일 삭제 실패	
	1601066	단말 조회 실패	
	1601070	Knox CheckEnrollment 실패	
	1601080	커맨드를 fetch할 수 없음	

모듈	코드	설명	로그 위치
Client	1601081	커맨드를 삭제할 수 없음	
	1601082	더 이상 커맨드가 없음	
	1601083	커맨드 메시지를 만들 수 없음	
	1601090	INI 설정 파일을 가져올 수 없음	
Kiosk	1700001	서버 키 획득 실패	mdm.log
	1700002	복호화 실패	
	1700003	암호화 실패	
	1700004	HTTP 바디 없음	
	1700005	HTTP 헤더의 지원되지 않는 값 입력	
	1700006	EMM Message 내의 필수 인자 입력되지 않음	
	1700007	지원하지 않는 프로토콜 버전	
	1700008	단말 정보 조회 실패	
	1700009	단말이 활성화되지 않음	
	1700010	앱 정보 조회 실패	
	1700011	지원되지 않는 OTC 코드	
	1700012	OTC 전송 중 실패	
	1700013	Kiosk Launcher 정보 조회 실패	
	1700014	Kiosk Launcher가 Wizard로 만들어지지 않음	
	1700015	현재 시간 조회 실패	
	1700016	압축 실패	
	1700017	압축 해제 실패	
	1700018	EMM Message 생성 실패	
	1700019	HTTP Response 전송 실패	

모듈	코드	설명	로그 위치
Provision	1001	서버에 PublicKey가 존재하지 않을 경우	mdm_provision.log
	1002	서버 GetPublicKey Runtime 오류	
	1003	서버에 단말 정보가 없을 경우	
	1004	서버에 등록된 단말이 없을 경우	
	1005	단말이 Block상태일 때	
	1008	서버 Provision Runtime 오류	
	1009	서버에 PrivateKey 가 존재하지 않을 경우	
	1011	서버의 단말 상태가 initProvision을 못 하는 경우	
	1018	InitProvision을 하기 위해 매칭되는 단말이 없는 경우	
	1019	서버에 단말이 이미 Provision 되어있는 경우	
	1021	서버 InitProvision Runtime 오류	
	1022	사용자 ID를 찾을 수 없는 경우	
	1023	ID 또는 Password 불일치로 인증이 실패한 경우	
	1024	Network Communication 오류	
	1025	자동등록 단말 허용 개수 초과	
	1026	Device ID가 유효하지 않은 값일 경우	
	1031	라이선스 정보 읽어오기 실패	
	1032	단말상태가 block(System block)일 경우	
	1033	사용자별 등록가능 단말 개수가 초과할 경우	
	1034	단말에서 전송한 Platform 정보와 서버에 저장된 Platform 정보가 일치하지 않을 경우	
	1035	WiFi 전용 단말이 아니지만 Mac address 와 IMEI 정보가 없는 경우	
	1036	WiFi 전용 단말이면서 Serial number 정보가 없는 경우	
	1037	Windows 단말이면서 Mac address 정보가 없는 경우	
	1038	Windows 단말 ProvisionIdentifier 중복	
	1039	Knox Provisioning 시도 시 일반영역에 동일한 ProvisionIdentifier 로 활성화된 단말이 없을 경우	
	1040	Knox Provisioning 중 사용자 정보를 가져올 수 없는 경우	
	1041	KME 단말 여부가 일치하지 않는 경우	
	1042	타이젠 파라미터 정보가 없음	
	1043	타이젠 OTP Code가 유효하지 않음	
	1044	타이젠 Registration ID가 없음	
	1045	타이젠 인증 실패	

E-FOTA API

코드	설명	상태 / HTTP 상태 코드
FUD_1001	**MDM vender ID**가 없거나 제한 길이를 초과합니다(문자열 기준 최대 50 bytes).	파라미터 에러 / 400 Bad Request
FUD_1002	**E-FOTA 고객 아이디**가 없거나 제한 길이를 초과합니다(문자열 기준 최대 50 bytes).	
FUD_1003	E-FOTA 신규 등록 시 EMM 내부에서 자동 생성되는 고유의 **Group ID**가 없거나 제한 길이를 초과합니다(문자열 기준 최대 50 bytes).	
FUD_1004	**E-FOTA API Key**가 없거나 제한 길이를 초과합니다(문자열 기준 최대 100 bytes).	
FUD_1005	**모델 이름**이 없거나 제한 길이를 초과합니다(문자열 기준 최대 20 bytes).	
FUD_1006	**모델 이름**에 허용되지 않는 문자가 포함됩니다(허용 문자는 숫자, 영문 대/소문자, -, _).	
FUD_1007	**통신사 코드**가 없거나 제한 길이를 초과합니다(문자열 기준 최대 20 bytes).	
FUD_1008	**통신사 코드**값에 허용되지 않는 문자가 포함됩니다(허용 문자는 숫자, 영문 대/소문자).	
FUD_1009	**현재 펌웨어 버전**이 없거나 제한 길이를 초과합니다(문자열 기준 최대 100 bytes).	
FUD_1010	**현재 펌웨어 버전**값에 허용되지 않는 문자가 포함됩니다(허용 문자는 숫자, 영문 대/소문자, -, /, ., _).	
FUD_1011	**언어 코드**가 제한 길이를 초과합니다(최대 길이 20 bytes).	
FUD_1012	**언어 코드**값에 허용되지 않는 문자가 포함됩니다(허용 문자는 숫자, 영문 대/소문자, -).	
FUD_1013	**대상 펌웨어 버전**이 없거나 제한 길이를 초과합니다(문자열 기준 최대 100 bytes).	
FUD_1014	**시작일**이 없거나 유효하지 않은 날짜 포맷입니다((GMT)YYYYMMDD).	
FUD_1015	**종료일**이 없거나 유효하지 않은 날짜 포맷입니다((GMT)YYYYMMDD).	
FUD_1016	**시작시간**이 없거나 유효하지 않은 시간 포맷입니다((GMT)24HH).	
FUD_1017	**종료시간**이 없거나 유효하지 않은 시간 포맷입니다((GMT)24HH).	

코드	설명	상태 / HTTP 상태 코드
FUD_3001	전송 종료일이 시작일보다 빠릅니다.	프로세스 에러 / 400 Bad Request
FUD_3002	전송 시작일부터 종료일까지가 7일을 넘을 수 없습니다.	
FUD_3003	전송 종료시간이 시작시간보다 빠릅니다.	
FUD_3004	전송 시작시간 부터 종료시간 까지 12시간을 넘습니다. The delivery end time is more than 12 hours after the delivery start time.	
FUD_3005	전송 시작일시가 현재 일시보다 빠릅니다.	
FUD_3011	MDM, 고객, 그룹ID의 조합이 등록되지 않았습니다.	
FUD_3012	MDM과 고객 아이디의 조합이 등록되지 않았습니다.	
FUD_3013	알 수 없는 요청에 대해 서버 초기화 서비스가 작동하지 않습니다.	
FUD_3014	모델 이름 또는 통신사 코드가 등록되지 않았거나 이들간의 매칭이 잘못 되었습니다.	
FUD_3015	해당 모델과 통신사 코드에 대한 대상 펌웨어 버전이 유효하지 않습니다.	
FUD_3016	API Key가 등록된 것과 일치하지 않습니다.	
FUD_3017	API Key가 만료되었습니다.	
FUD_9001	데이터베이스 연결 시 알 수 없는 에러가 발생하였습니다.	Unknow 에러/ 500 Internal Service Error
FUD_9003	서버에 알 수 없는 에러가 발생하였습니다.	

원격 지원 서비스

원격지원 서비스는 모바일 사용자의 요청에 따라 단말 화면을 공유하여 원격으로 제어하는 서비스입니다 . 해당 서비스는 많은 사용자에 대하여 동시 원격제어가 가능하며 , 고객 문의 사항에 대하여 신속히 대응하여 운영자의 편의를 돕고 사용자의 만족을 높일 수 있습니다 .

Note: EMM 원격지원 릴레이 서버와 PC 뷰어 설치는 "*S*amsung SDS EMM 설치매뉴얼"을 참고하세요.

구성 컴포넌트

원격 지원 서비스를 위해 필요한 컴포넌트는 다음과 같습니다 .

- 모바일 Agent: 사용자의 단말에 설치되는 애플리케이션
- PC 뷰어: 운영자의 PC에서 사용자의 단말과 동일한 화면을 보여주는 뷰어
- 릴레이 서버: 사용자의 모바일 Agent와 PC 뷰어의 통신을 연결해주는 서버

지원 플랫폼

원격 지원 서비스는 일반 보안에서만 사용하며 , 지원 플랫폼은 다음과 같습니다 .

- 단말: Android 4.4(Kitkat) 이상의 삼성 단말
- PC 뷰어: Microsoft Windows 7 이상

방화벽 설정하기

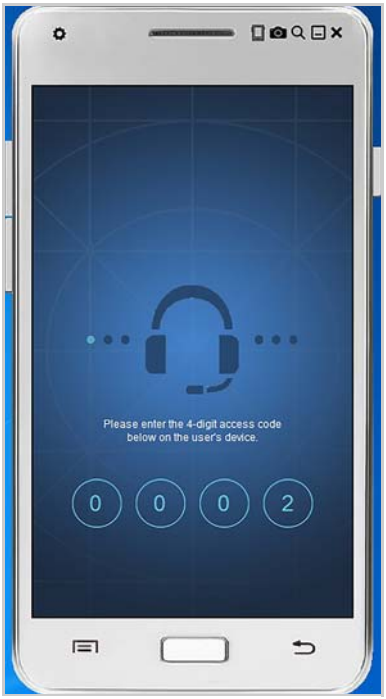
운영자의 PC 에서 사용자의 단말에 원격으로 접속하려면 운영자의 PC 에서 릴레이 서버의 IP/Port 방화벽을 해제해야합니다 .

원격 지원 서비스 연결하기

운영자의 PC 에서 원격 지원 서비스를 연결하려면 다음의 절차를 따르세요 .

1. 원격 지원 서비스가 필요한 단말 사용자에게 APK 파일을 전달하여, 설치를 요청합니다.

2. PC 뷰어를 실행한 후 **Start**를 클릭하면 4자리 접속 코드가 나타납니다. 단말 사용자에게 접속 코드를 알려주고, 단말의 원격지원 Agent에 동일한 코드를 입력하게 합니다.
   - Start 클릭 시, EMM 라이선스의 유효성을 체크하고 실행 여부를 판단합니다.



> **Note:**
> - 원격 접속 요청 후 접속 코드를 입력하지 않으면, 10분 뒤에 접속이 자동 종료됩니다.
> - 운영자는 여러 개의 PC 뷰어를 실행시켜 동시에 여러대의 단말과 연결할 수 있습니다.

3. 사용자가 접속 코드를 입력하면 사용자의 단말과 원격 지원 서비스가 연결됩니다.

원격 지원 서비스 세부 기능

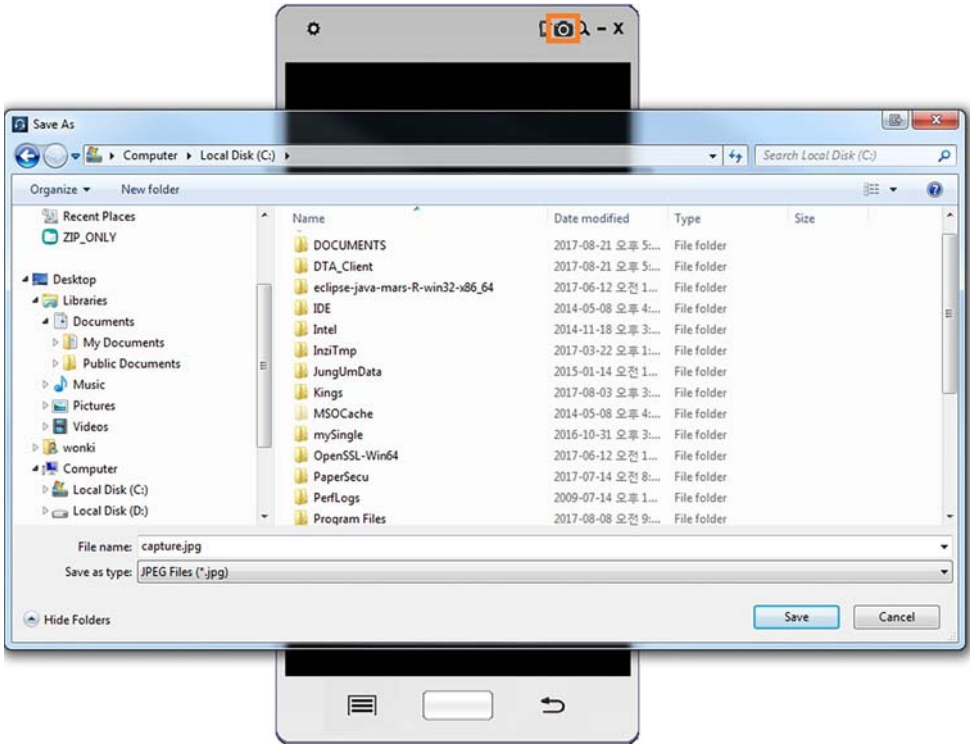
모바일 단말의 기능과 동일하게 메뉴와 이전 버튼이 동작하며 , 좌측 볼륨 조정 버튼과 우측 전원 버튼이 동작됩니다 .

화면 전환

가로 또는 세로 화면으로 전환할 수 있습니다 .

화면 캡쳐

에러 메시지 발생 등 단말 화면의 상황 파악을 위하여 화면을 캡쳐할 수 있습니다 . 파일 형식을 JEPG 로 선택하면 마지막 화면이 저장이되며 , MP4 를 선택하면 최근 1 분 간의 화면 내용이 저장됩니다 .



파일 전송

단말의 상황 파악을 위하여 로그 파일 등 단말 내부의 파일을 전송할 수 있습니다. 또한 PC Viewer 를 실행한 운영자의 PC 에서 파일을 드래그하거나 복사한 후 , 붙여넣기하여 사용자의 단말로 복사할 수 있습니다 .

원격 지원 서비스 종료하기

사용자의 단말에서 **종료** 버튼을 터치하거나 뷰어의 상단 우측 **X** 를 클릭한 후 , **Exit** 를 클릭하면 원격 지원이 종료되고 뷰어 실행 창이 닫힙니다 . **Disconnect** 를 클릭하면 원격 지원이 종료되고 뷰어 실행 창은 닫히지 않습니다 .

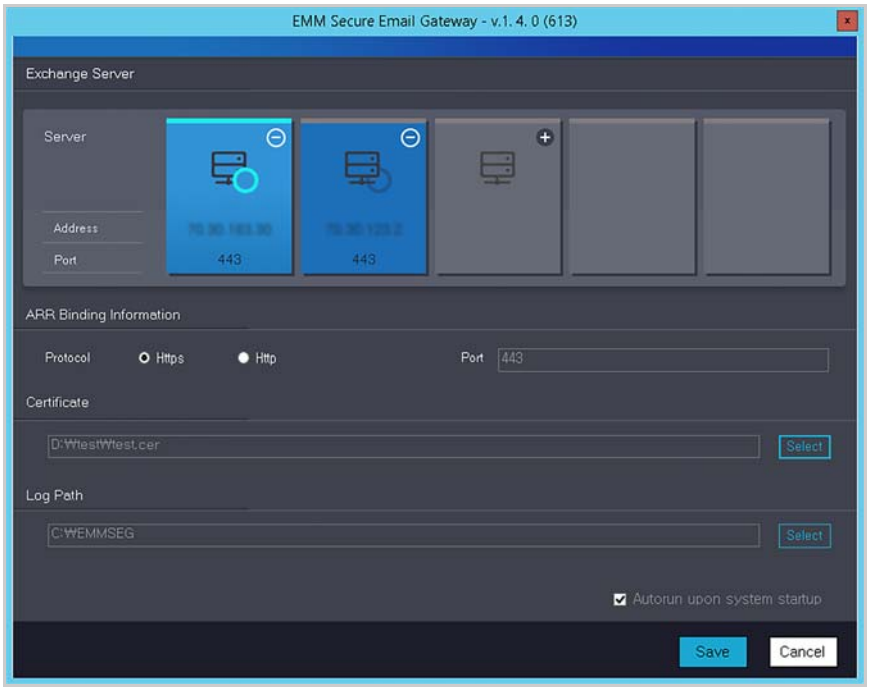
Secure Email Gateway Manager

SEG(Secure Email Gateway) 는 Microsoft Exchange 서버와 단말 사용자를 중계해주는 서버로 웹 방화벽 기능을 활용하여 해당 서비스를 필터링합니다. 외부에서 내부로 들어오는 트래픽을 분산시키고 외부 공격을 차단하여 웹기반의 공격으로부터 보호할 수 있습니다 . 또한 SEG Manager 를 통해 Exchange 서버를 등록하고 서버 상태를 조회할 수 있습니다. Exchange 서버를 등록하려면 Exchange 서버의 인증서를 등록하고 로그의 저장 위치를 설정한 후 , 단말과 애플리케이션의 통신 정보를 등록합니다 .

Note: SEG Manager 설치는 “Samsung SDS EMM 설치매뉴얼”을 참고하세요.

SEG Manger 사용하기

SEG Manager를 이용하여 사용하려는 Exchange 서버 정보를 관리할 수 있습니다. 관리 가능한 항목은 다음과 같습니다 .



4. **Exchange Server**에서 ➕을 클릭하여 Exchange 서버 IP 주소와 Port 정보를 입력하세요.
   - 등록된 Exchange 서버의 상태가 아래 조회되며, 오프라인일 경우에는 색이 어둡게 표시됩니다. ⊖을 클릭하면 등록된 서버를 삭제할 수 있습니다.
   - 최소 1개의 Exchange 서버 등록이 필요합니다.
5. **ARR Binding**에서 SEG 서버와 단말 애플리케이션간 통신 정보를 등록 및 수정하세요.
   - 통신 Protocol을 Https 또는 Http로 선택하고 Port 번호를 입력합니다.
6. **Certificate**에서 **Select**를 클릭하여 SEG 서버에서 사용할 인증서를 등록하세요.

- 해당 인증서는 https 통신시 binding할 인증서입니다. 공인 인증서 또는 SEG 서버에서 생성한 self signed 인증서를 사용합니다.

7. **Log Path**에서 **Select**를 클릭하여 로그가 저장될 파일 디렉토리를 선택하세요.
   - 로그 저장 기한은 일주일입니다.
8. **Autorun upon system startup** 항목을 체크하면 시스템 시작 시 SEG Manager가 자동 실행됩니다.
9. **Save**를 클릭하세요.
   - 인증서를 등록하거나 변경했을 경우, 인증서 비밀번호 입력 팝업창이 조회되며 인증서 비밀번호 입력이 필요합니다.
   - 필수값이 입력되지 않으면 항목 타이틀 옆에 메시지가 노출됩니다.
   - 기존 설정값이 있는 경우, 수정사항을 반영 후 **Save**를 클릭하여 저장합니다.

Knox Mobile Enrollment

KME(Knox Mobile Enrollment) 를 이용하면 IT 운영자는 대량의 단말을 빠르고 쉽게 등록 및 배포할 수 있습니다 . KME 를 통해 사용자에게 배포된 단말은 사용자가 단말을 켜고 Wi-Fi 에 연결하면 자동으로 EMM 이 설치되고 활성화 상태가 되며 , EMM 에 단말이 등록된 후 , 단말이 초기화되더라도 EMM 에 자동으로 재 등록됩니다 .

준비하기

- KME를 이용하려면 단말을 다음과 같은 reseller나 통신사에서 구입합니다.
  자세한 내용은 Knox 지원센터로 문의합니다.
  - Knox Mobile Enrollment에서 승인한 대리점
  - IMEI/일련 번호 정보를 삼성 담당자와 직접 공유하는 대리점
- Knox 2.4 이상의 삼성 단말로 지원되는 단말 모델인지 확인합니다.
  자세한 내용은 Knox 포털 내의 안내를 참고합니다.
- KME를 사용할 수 있는 국가인지 확인합니다.
  자세한 내용은 Knox 포털 내의 사용가능 국가 리스트를 참고합니다.
- Knox 포털의 계정을 준비합니다.
- KME 단말에서 EMM을 설치 시 단말의 배터리 잔량이 50% 이상인지 확인합니다.

KME 시작하기

1. Knox 포털(www.samsungknox.com)에 계정을 생성하거나 기존의 계정으로 로그인한 후, KNOX Mobile Enrollment 포털(이하 KME 포털)로 이동합니다.
2. KME 포털에서 MDM 프로파일 구성하기
3. KME 단말 구성하기
   - 리셀러에 의해 구입된 단말의 경우, 리셀러 포털에 등록된 단말 정보는 KME 포털에서 바로 확인이 가능하며, 추가적인 등록 절차가 필요하지 않습니다.
   - 리셀러에 의해 구입되지 않은 경우, 앱을 통해 NFC 태깅으로 단말을 등록할 수 있습니다.
4. KME 포털에서 등록된 단말 확인하기
5. 사용자가 KME 단말을 켜고 Wi-Fi에 연결 시 자동으로 단말에 EMM이 설치되고 활성화 상태가되며, 사용자의 계정 정보를 입력하면 로그인이 가능해집니다.

KME 포털 접속하기

KME 를 이용하려면 Knox 포털 로그인 계정으로 KME 사용 승인을 받아야합니다 .

1. Knox 포털 (www.samsungknox.com)에 미리 준비한 계정으로 로그인 한 후, Knox 포털의 상단 **Samsung Knox 대시보드**을 클릭하세요.

2. My Solutions 영역에서 KNOX Mobile Enrollment의 **시작**을 클릭하세요.
3. 각 항목에 값을 입력한 후, **신청**을 클릭하세요.
   신청이 승인되면 Knox Mobile Enrollment를 사용하는 방법에 대한 지침이 담긴 환영 이메일을 받게 됩니다.

MDM 프로파일 만들기

Knox Mobile Enrollment 포털에서 단말을 등록하기 전에 MDM 클라이언트 APK 및 기타 정보가 있는 MDM 프로파일을 만들어야 합니다 .

MDM 프로파일을 생성하려면 다음의 절차를 따르세요 .

1. Knox Device Enrollment 포털의 **MDM 프로필** 탭의 **추가**를 클릭하세요.
2. MDM 활성화를 위한 **MDM 서버 URI**를 입력하고 **다음**을 클릭하세요.
   예) https://sample.manage.samsungknox.com
3. MDM 프로필 상세 정보를 입력하세요.
   - **프로필 이름**: 내 프로필을 식별할 이름을 입력하세요.
   - **설명(선택 사항)**: 프로필에 대한 추가 정보를 입력하세요.
   - **MDM Agent APK**: 단말에 자동으로 다운로드되는 MDM 애플리케이션을 추가합니다. **MDM 애플리케이션 추가**를 클릭하여 단말에 다운로드 할 APK의 URL을 입력하고 **저장**을 클릭하세요.
     - 웨어러블 단말의 경우, Tizen 스토어에 등록된 MDM 애플리케이션의 Deep Link를 추가하세요.
     - 사용자가 단말을 Wi-Fi 네트워크에 연결하면 해당 애플리케이션이 다운로드되어 단말에 설치됩니다.
     - **사용자 지정 JSON 데이터(MDM에 정의됨)**: 사용자 지정 설정 방식을 정의할 수 있습니다. EMM의 경우, Tenant 정보를 다음과 같이 입력하세요.
       - Multi-Tenant : {"TenantId":"테넌트명","TenantType":"M"}
       - Single-Tenant: {"TenantId":"EMM","TenantType":"S"}
   - **EULA**, **이용 약관**, **사용자 동의서**: **사용자 동의서 추가**를 클릭하여 최종 사용자 라이선스 동의서, 이용약관, 기타 사용자 동의서를 추가하세요.
     - **Knox 관련 EULA 추가**를 클릭하면 단말을 최초 등록 시 Knox와 관련된 모든 EULA(라이선스 EULA)를 한 번에 표시하여 팝업 창의 수를 줄일 수 있습니다.
   - **Knox 라이선스를 이 프로필에 연결**: Mobile Enrollment와는 별개이나, 운영자는 EMM 관리자 포털을 사용하지 않고도 단말 등록 중에 활성화를 위해 Knox 라이선스 키를 입력할 수 있습니다.
4. **저장**을 클릭합니다.

> **Note:** MDM URI는 URL 형태로 된 MDM 서버의 주소입니다. MDM URI에 대한 정보는 MDM 제공업체에 문의하세요.

MDM 프로파일을 수정하는 방법

프로파일을 이미 만든 경우 MDM URI 는 변경할 수 없습니다 . MDM URI 를 변경하려면 MDM 프로파일을 새로 만들어야하며 , 이미 만들어진 MDM 프로파일의 내용을 수정하려면 다음의 절차를 따르세요 .

1. **MDM프로필** 탭을 클릭하세요.
2. 수정할 프로필을 선택한 후, **편집**을 클릭하세요.
3. 수정하려는 정보를 입력하고 **저장**을 클릭하세요.

단말 등록하기

Knox Mobile Enrollment 포털에서 .csv 파일을 사용하여 단말을 일괄 등록하거나 , Mobile Enrollment 스캐너 앱을 통해 단말을 등록할 수 있습니다 .

.csv 파일을 만드는 방법

단말 등록을 위하여 csv 파일을 만들려면 다음의 절차를 따르세요 .

1. **디바이스 > 제출완료**로 이동하여 **새 디바이스 제출**을 클릭하세요.
2. CSV 파일 템플릿을 클릭하여 템플릿을 다운로드 받거나 MS Excel의 새 파일을 여세요.
3. 다음의 안내에 따라 해당하는 열에 다음 정보를 입력하세요.
   - IMEI 또는 일련 번호: 첫번째 열에 단말 IMEI를 입력하세요. 해당 정보는 **설정 > 디바이스 정보** 또는 단말의 포장에서 확인할 수 있습니다.
   - 사용자 이름: 두 번째 열에 사용자 ID를 필수로 입력하세요. 사용자 ID는 EMM 관리자 포털에 미리 등록되어 있어야 합니다.
   - 비밀번호: 세번째 열에 사용자의 비밀번호를 입력하세요. 비밀번호 입력은 활성화를 위한 필수값이지만 비밀 번호를 입력하지 않는 경우, 단말에서 사용자의 직접 입력을 통해 인증됩니다.
   - 추가 정보: 네번째 열에 모바일 ID를 필수로 입력하세요. csv 파일 업로드 시 해당 모바일 ID로 EMM 관리자 포털에 자동으로 단말이 등록됩니다.
4. 단말 정보를 모두 입력했다면, **파일 > 다른 이름으로 저장**을 선택한 후, 파일 형식에서 **CSV (쉼표로 분리) (*.csv)**를 선택하여 CSV 파일로 저장하세요.

> **Note:** 제목 행은 추가하지 말아야 하며, 비어 있는 행이 있어서는 안됩니다.

.csv 파일을 사용한 단말 등록 방법

csv 파일을 이용하여 단말을 등록하려면 다음의 절차를 따르세요 .

1. **디바이스 > 제출완료**로 이동하여 **새 디바이스 제출**을 클릭하세요.
2. 단말정보가 저장된 csv 파일을 찾으려면 **선택**을 클릭하세요.

3. 등록할 .csv 파일을 선택하고 **열기**를 클릭하세요.
4. **업로드**를 클릭하세요.
5. 구입 상세 정보를 입력하세요.
   - 디바이스 구입처에서 판매자정보를 선택하세요. 등록되지 않은 재판매인의 경우 구매 영수증이나 판매 영수증의 사번을 첨부합니다.
   - **MDM 프로필 할당**에서 할당할 MDM 프로파일을 선택하세요.
   - 같은 사용자 ID와 비밀번호를 일괄로 적용하려면 **같은 사용자 ID와 비밀번호를 모든 디바이스에 설정합니다.**를 선택하고 **사용자 ID**와 **비밀번호**를 입력하세요.
6. **제출**을 클릭하세요.

스캔된 디바이스 등록 방법

스캔한 디바이스를 등록하려면 다음의 절차를 따르세요 .

1. Knox 포털 계정에 로그인하고 **Mobile Enrollment 시작**을 클릭하세요.
2. **디바이스 > 스캔 완료**를 클릭하여 추가된 모든 단말을 확인하세요. 해당 정보는 앱 스토어에서 KME 앱을 다운받아 설치한 후, SCAN DEVICES기능을 이용하여 단말의 IMEI 또는 Serial number를 스캔한 단말의 정보입니다.
3. 등록할 단말을 선택한 후, **모든 디바이스를 CSV로 다운로드**를 클릭한 다음 다운로드하세요.
4. 다운로드 받은 csv 파일은 단말의 IMEI 또는 Serial number 만을 포함하므로 사용자 ID, 비밀번호, 모바일 ID를 추가하여 csv 파일을 저장하세요.
   - 모바일 ID는 unique한 값을 가져야 하므로 단말의 IMEI 또는 Serial number를 사용합니다.
   - 사용자 ID와 비밀번호는 csv 파일에 직접 입력하거나 KME 포털에서 제공하는 일괄입력을 이용할 수 있습니다.
5. **디바이스 > 제출완료**로 이동하여 **새 디바이스 제출**을 클릭하세요.
6. 단말정보가 저장된 csv 파일을 찾기 위해 **선택**을 클릭하세요.
7. 등록할 .csv 파일(4번 단계에서 저장한 파일)을 선택하고 **열기**를 클릭하세요.
8. **업로드**를 클릭한 후, 구입 상세 정보를 다음과 같이 입력하세요.
   - 디바이스 구입처에서 판매자정보를 선택하세요.
     등록되지 않은 재판매인의 경우 구매영수증이나 판매영수증의 사번을 첨부합니다.
   - **MDM 프로필 할당**에서 할당할 MDM 프로파일을 선택하세요.
   - 같은 사용자 ID와 비밀번호를 일괄로 적용하려면 **같은 사용자 ID와 비밀번호를 모든 디바이스에 설정합니다.**를 선택하고 **사용자 ID**와 **비밀번호**를 입력하세요.
9. **제출**을 클릭하세요.

- 단말 정보가 검증되면 확인 이메일을 받게 됩니다. 최종 사용자는 자신의 단말에서 등록 프로세스를 완료하라는 메시지를 받게됩니다.

단말에 사용자 이름 또는 비밀번호 정보를 추가하는 방법

단말의 사용자 정보를 수정하려면 다음의 절차를 따르세요 .

1. Knox Mobile Enrollment 포털에서 **디바이스 > 제출완료**를 클릭하세요.
2. 수정할 단말을 선택하고, 사용자 ID와 비밀번호를 입력하세요.
   - 모든 단말에서 동일한 사용자 ID와 비밀번호를 사용하려면 모든 단말을 선택하고 **편집**을 클릭하세요.
3. **저장**을 클릭하세요.

등록된 단말을 보는 방법

KME 로 등록된 단말 목록을 확인하려면 다음의 절차를 따르세요 .

1. Knox Mobile Enrollment 포털에서 **디바이스**를 클릭하세요.
2. **제출완료**를 클릭하면 제출된 모든 IMEI 또는 일련 번호가 보여집니다. 단말 모델, 단말이 등록된 MDM 프로필, 특정 단말의 상태 등과 같은 추가 정보도 볼 수 있습니다.

KME 단말 구성하기

- KME 단말을 구성하기 위한 방법은 다음과 같습니다. 리셀러 포털에서 KME 단말 등록을 위해 리셀러가 단말의 IMEI 정보를 등록합니다. 등록된 단말은 KME 포털의 **다비이스 > 업로드**에서 리셀러 정보, 등록된 날짜 및 단말 수, 단말의 IMEI 정보, 적용된 프로파일 등을 확인합니다. 리셀러 포털 사용에 대한 자세한 내용은 Knox 포털에서 Knox 리셀러 가이드(https://configure.samsungknox.com/files/samsung-reseller-guide/Content/manage-devices.htm)를 참고하세요.
- 삼성전자가 승인하지 않은 리셀러에게 구입한 단말의 경우, 앱을 사용하여 개별로 등록해야 합니다. 자세한 내용은 474페이지의 "앱을 사용하여 KME에 단말 등록하기"를 참고하세요.

앱을 사용하여 KME에 단말 등록하기

삼성전자가 승인하지 않은 리셀러에게 구입했거나 또는 테스트 용도로 단말을 개별 등록하려면 다음의 절차를 따르세요 . 사용자 정보는 EMM 관리자 포털에 반드시 먼저 등록되어 있어야 합니다 .

1. Google Play Store에서 Knox Deployment 앱을 설치하세요.
2. 사용자의 단말에서 Knox 포털 사용자의 ID와 비밀번호를 입력한 후, **SIGN IN**을 탭하세요.

3. **ENROL VIA NFC**를 탭하세요.
   - 단말의 NFC 기능이 활성화 되어있어야 합니다.
4. **START**를 탭한 후, MDM 프로파일을 선택하고 사용자 정보를 입력하세요.
5. 사용자 단말을 태그하여 등록하세요.
6. 사용자 단말에서 NFC 태깅을 통해 등록이 완료되면, KME 포털의 **디바이스 > 모든 디바이스**에서 해당 단말을 확인하세요.

KME에 등록된 단말 확인하기

KME 포털에 등록된 단말 목록을 확인하려면 다음의 절차를 따르세요 .

1. KME 포털에서 **디바이스 > 모든 디바이스**를 클릭하세요.
   - 등록된 모든 단말의 IMEI/MEID 및 일련번호 정보가 나타납니다. 그외 단말 모델, 사용자 ID, MDM 프로파일, 단말 상태 등 추가 정보 확인이 가능합니다.

KME에 등록된 단말의 사용자 정보 수정하기

단말의 사용자 이름 또는 비밀번호를 수정하려면 다음의 절차를 따르세요 .

1. KME 포털에서 **디바이스 > 모든 디바이스**를 클릭하세요.
2. 사용자 정보를 개별로 수정하려면, 사용자 ID를 클릭하여 사용자 ID와 비밀번호를 입력하세요.
   - 또는 수정할 단말의 **IMEI / MEID** 또는 **일련번호**를 클릭하여 “디바이스 상세정보” 팝업 창에서 **사용자 ID**와 **비밀번호**를 입력한 후, **저장**을 클릭하세요.
3. 모든 단말에서 동일한 사용자 ID와 비밀번호를 사용하려면 모든 단말을 선택한 후, 화면 상단의 **정책구성**을 클릭하세요.
   - “선택된 디바이스 정책구성” 팝업 창의 **사용자 계정 정보**에서 **사용자 계정 정보 덮어쓰기**를 선택하고, 사용자 ID와 비밀번호를 입력한 후, **저장**을 클릭하세요.

KME 단말 해제하기

KME 단말을 해제하려면 EMM 관리자 포털에서 KME 단말을 비활성화한 후 , KME 포털에 등록된 KME 단말 정보를 삭제해야 합니다 . 그렇지 않은 경우 , Wi-Fi 에 연결 시 KME 단말 진행 절차가 계속 실행됩니다 . EMM 관리자 포털에서 단말을 비활성화하는 방법은 104 페이지 10 장의 " 단말 상태 변경하기 " 를 참고하세요 .

KME 에 등록된 단말을 해제하려면 다음의 절차를 따르세요 .

1. KME 포털에서 **디바이스 > 모든 디바이스**를 클릭하세요.
2. KME 단말에서 해제하려는 단말을 검색한 후, 해당 단말 또는 전체를 클릭한 다음 상단 우측의 **Delete devices**를 클릭하세요.

- “Delete devices” 창에서 **Delete**를 클릭하면 해당 단말이 KME 포털에서 삭제됩니다. 이후 KME 단말로 재 등록시 리셀러에게 문의하시기 바랍니다.

EMM AppWrapper

EMM AppWrapper (이하 AppWrapper) 는 EMM 의 SDK 로 구현된 기능을 사내 애플리케이션에서 간편하게 구현할 수 있는 툴입니다 . AppWrapper 가 지원하는 EMM SDK 의 기능으로는 사용자 인증 , 화면 캡쳐 , 화면 잠금 , 단말 Copy& Paste 차단 등이 있습니다 . AppWrapper 툴로 변환한 앱을 관리자 포털에서 사내 애플리케이션으로 등록한 후 , 앱 관리 프로파일에서 애플리케이션 해당 정책을 설정할 수 있습니다 . 사용자 단말에 설치된 사내 애플리케이션에서 해당 기능이 제어됩니다 .

EMM 에서 제공하는 AppWrapper 를 설치하고 사내 애플리케이션에 EMM SDK 의 기능을 구현하는 방법은 다음과 같습니다 .

사전 준비 사항

단말 플랫폼에 맞는 AppWrapper 를 사용하기 위하여 다음을 준비합니다 .

- Android용 EMM AppWrapper 툴 설치 환경
  : JDK 1.7 이상이 설치된 Windows 환경
- iOS용 AppWrapper 툴 설치 환경
  : Mac OS 10.7 이상
- 사내 애플리케이션을 AppWrapper 후 제어되는 기능

지원여부	Android	iOS
사용자 인증	O	O
화면 캡쳐 방지	O	X
화면 잠금	O	O
단말 Copy& Paste 차단	O	O
사용자 로그	O	X
암호화 기능	O	O

Android앱용 AppWrapper 설치하기

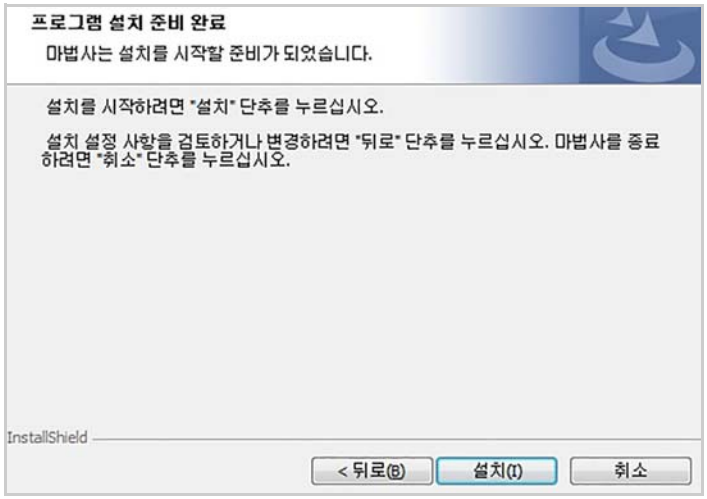
AppWrapper 의 다운로드와 설치는 기술 운영팀의 안내에 따라 진행합니다 . `EMM_AppWrapper.exe` 를 설치하려면 다음의 절차를 따르세요 . 프로그램 설치 중 설치를 취소하려면 **취소**를 클릭하세요 .

1. `EMM_AppWrapper.exe` 파일을 다운로드 하세요. 또는 기술 운영팀에게 파일을 전달 받으세요.
   - AppWrapper 툴은 Window의 관리자 권한으로 설치합니다.
2. 설치할 언어를 선택하고, **확인**을 클릭하세요.

3. InstallShield Wizard가 시작되면 **다음**을 클릭하세요.

4. AppWrapper의 사용권 계약서를 자세히 읽고, **사용권 계약서의 조건에 동의함**을 선택한 후 **다음**을 클릭하세요.

5. AppWrapper 설치를 시작하려면 **설치**를 클릭하세요.



6. AppWrapper 설치가 완료되면 **마침**을 클릭하세요.

Android앱용 AppWrapper 삭제하기

AppWrapper 를 더이상 사용하지 않는 경우에는 Window 제어판에서 해당 프로그램을 삭제합니다 .

- **Windows > 제어판 > 프로그램 > 프로그램 제거** 또는 **변경**에서 AppWrapper를 선택하여 마우스 오른쪽 버튼을 클릭한 후 제거를 클릭하세요.

Android앱용 AppWrapper 사용 하기

IT 운영자는 AppWrapper 명령어를 이용하여 사내 애플리케이션에 원하는 기능을 wrapping 합니다 . Wrapping 시 필요한 필수 항목 및 명령어에 대한 자세한 설명은 480 페이지 18 장의 “Android 앱용 AppWrapper 명령어의 매개 변수 " 을 참고하세요 .

1. AppWrapper 가 설치되어 있는 폴더로 이동하세요.

2. Windows의 커맨드 창에서 `EMMWrapper.jar`와 AppWrapping 시 필요한 명령어를 실행하세요.

   - AppWrapping 명령어의 필수 매개 변수에 대한 설명과 예시입니다.
     -s : Wrapping하려는 사내 애플리케이션의 APK 파일
     -k: 사내 애플리케이션 keystore의 파일 경로
     -p: keystore의 비밀번호
     -a: keystore의 별칭

```
java -jar EMMWrapper.jar
-s "D:\\redex\\AppWrappingTest.apk"
-k "D:\\Knox Manage.keystore"
-p "sdspasswd!!"
-a "aliase"
```

Android앱용 AppWrapper 명령어의 매개 변수

Tag	Param	설명	필수 여부	값
srcAPKPath	-s	AppWrapping할 사내애플리케이션 원본 apk파일 위치의 절대 경로	필수	
keyStorePath	-k	keystore 파일 위치의 절대 경로	필수	
storePass	-p	keystore 의 비밀번호	필수	
alias	-a	keystore 파일의 별칭	필수	
destAPKpath	-dpath	AppWrapping된 사내앱apk 파일 위치의 절대 경로		/현재폴더/redex.apk
tempSpacePath	-tpath	• 앱의 크기를 줄이는 redex 과정을 위한 임시 폴더 • tmp 폴더로 준비		/현재폴더/tmp
unSignedApkPath	-upath	Singing할 apk파일 위치의 절대 경로		/현재폴더/redex.apk
storeType	-ktype	• keystore의 storetype • 사용하지 않을 경우 null		null
jdkBinPath	-jpath	• jarsigner.exe 파일이 포함된 jdk의 bin폴더의 경로 • null 경우 서버 환경 변수의 파일 경로를 따름		서버 환경 변수
proxyDexPath	-dex	proxy용 dex파일 위치의 절대 경로		installer 설치/현재폴더/sdsemm.dex
soLibDir	-so	• .so용 폴더의 절대 경로 • 추가할 .so 파일이 없어도 해당 경로는 있어야 함		installer 설치 /현재폴더/libs
frameworkResDir	-res	resources_framework.arsc 파일 위치의 절대 경로		installer 설치 /현재폴더/res
packagePrefix	-pre	• 기존 package명에 추가할 prefix명 붙임 • isRePackage가 false일 경우 사용 안함		emmsds
isRePackage	-ispre	기존 package명에 prefix를 붙이면 true, 아니면 false		• true • false (기본값)

Tag	Param	설명	필수 여부	값
isEMMSecureFileMode	-sfile	• secure파일을 통한 파일 입출력 지원 여부 암호화 기능 사용방법 : - isSecureFileMode를 true함. file에 관련된 read/write 암호화로 처리되므로 로그 사용시 유의		• true • false (기본값)
isEMMSdkExistCheckMode	-isemm	apk파일에 EMM SDK가 포함되는지 API의 동작으로 확인		• true • false (기본값)

Android앱용 AppWrapper 에러 코드

AppWrapper를 이용하여 사내 애플리케이션을 wrapping할때 보여질 수 있는 에러 코드의 리스트입니다. 에러 발생 시 아래의 설명과 확인사항을 참고하여 wrapping시 발생하는 간단한 오류에 대해 조치를 취할수 있습니다.

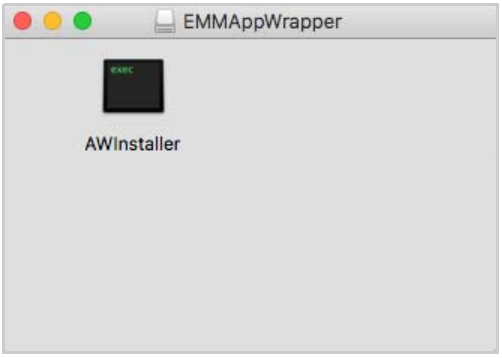
정의	ErrorCode	설명	확인사항
SUCCESS	0	Wrapper 성공	
EMM_SDK_EXIST	SUCCESS + 1	EMM check mode일 경우,해당 apk파일에 EMM SDK가 포함된 경우	
EMM_SDK_NOT_EXIST	SUCCESS + 2	EMM check mode일 경우, 해당 apk파일에 EMM SDK가 포함되지 않은 경우	
SRC_APK_NOT_EXIST	-1000	Wrapping할 원본 apk파일이 해당 경로에 없는경우	원본 apk파일 유무 확인
TMP_DIR_NOT_EXIST	SRC_APK_NOT_EXIST -1	redex시 필요한 tmp 임시 폴더가 없는경우	redex할 tmp 임시폴더 유무 확인
KEYSTORE_FILE_NOT_EXIST	SRC_APK_NOT_EXIST -2	signing을 위한 keystore 파일이 해당 경로에 없음	keystore 파일 유무 확인
DEX_FILE_NOT_EXIST	SRC_APK_NOT_EXIST -3	Wrapper가 설치된 폴더에 sdsemm.dex 파일 유무 확인	sdsemm.dex 파일 유무 확인
SO_LIB_DIR_NOT EXIST	SRC_APK_NOT_EXIST -4	INI Push에 사용될 so lib폴더가 해당 경로에 없는 경우	Wrapper가 설치된 폴더/libs 밑에 so파일 유무 확인

정의	ErrorCode	설명	확인사항
FRAMEWORK_RES_FILE_NOT_EXIST	SRC_APK_NOT_EXIST -5	resource_framework.arsc파일이 해당 경로에 없음	Wrapper가 설치된 폴더/res 밑에 resources_framework.arsc 파일 존재 유무 확인
EMM_SDK_ALREADY_INCLUDED	SRC_APK_NOT_EXIST -6	Wrapping하려는 apk파일에 EMM SDK가 포함됨	해당 apk파일에 EMM SDK가 포함되어 있으므로 Wrapping할수 없음
SIGNING_FAILED	SRC_APK_NOT_EXIST -7	Wrapping된 apk파일에 singing 실패한 경우	storePass,alias,sotreType,jdkBinPath 정보 확인 • Error 로그 ('Runtime.getRunTime0.exec result:' 로그)
APPWRAPPER_VER_CHECK	SRC_APK_NOT_EXIST -10	해당 apk파일이 같은 버전의 AppWrapper로 wrapping된 이력 확인	해당 apk파일은 AppWrapping 불가
UNKNOWN	-99999		

iOS앱용 AppWrapper 설치하기

AppWrapper 의 다운로드와 설치는 기술 운영팀의 안내에 따라 진행합니다 . EMMAp-pWrapper.dmg 를 설치하려면 다음의 절차를 따르세요 .

1. EMMAppWrapper.dmg 파일을 다운로드 하세요. 또는 기술 운영팀에게 파일을 전달 받으세요.
2. EMMAppWrapper.dmg을 실행한 후, EMMAppWrapper창 안에 AWInstaller를 클릭하여 자동으로 설치하세요.



3. EMMAppWrapper 설치 완료를 확인하세요.

iOS앱용 AppWrapper 삭제하기

AppWrapper 를 더이상 사용하지 않는 경우에는 Mac OS 의 터미널에서 다음 명령어로 EMMApprWrapper.app 를 삭제하세요 .

- rm -r / Applications/ EMMApprWrapper.app/

```
bas1-quebec13-70-30-184-42:~ daehyeogim$
rm -r /Applications/EMMAppWrapper.app/
```

iOS앱용 AppWrapper 사용 하기

운영자는 AppWrapper 명령어를 이용하여 사내 애플리케이션에 원하는 기능을 wrap-ping 합니다 . Wrapping 시 필요한 필수 항목 및 명령어에 대한 자세한 설명은 484 페이지의 "iOS 앱용 AppWrapper 명령어의 매개 변수 " 를 참고하세요 .

1. Mac OS에서 터미널을 실행하세요.
2. 터미널에서 AppWrapping 시 필요한 명령어를 실행하세요.

```
~ — -bash
bas1-quebec13-70-30-184-42:~ daehyeogim$ EMMAppWrapper -s
~/work.test.ipa -b com.sds.emm.test -p ~/work/EMMTest.prov
isionprofile -k LLVDH2GU5H.com.sds.emm -i "iPhone Distribu
tion: SAMSUNG SDS"
```

- AppWrapping 명령어의 필수 매개 변수에 대한 설명과 예시입니다.
  -s : Wrapping하려는 사내 애플리케이션의 ipa 파일
  -b: iOS앱의 번들 아이디
  -p: iOS앱의 Provisioning profile 파일
  -k: 키체인 그룹
  -i: 배포용 인증서 이름

```
EMMAppWrapper
-s ~/work/test.ipa
-b com.sds.emm.test
-p ~/work/EMMTEST.provisionprofile
-k LLVDH2GU5H.com.sds.emm
-i “iPhone Distribution:SAMSUNG SDS”
```

iOS앱용 AppWrapper 명령어의 매개 변수

Tag	Param	설명	필수 여부	값
srcAPKPath	-s	AppWrapping할 사내 애플리케이션 원본 ipa파일 위치의 절대 경로	필수	
bundle_id	-b	앱 번들ID로 provising profile에 등록한 App ID내용과 일치해야 함 • 예) EMM Biz앱의 경우 com.sds.emm.*로 되어있고, wrapping할 사내 애플리케이션은 모두 com.sds.emm으로 시작하는 앱ID를 가지고 있어야함.	필수	
provisioning_profile	-p	앱을 signing 하기 위한 provisioning profile. • App ID와 키체인 공유를 위한 prefix값을 가짐	필수	
keychain_group	-k	키체인 공유 기능 사용을 위한 키체인 그룹 • 입력된 키체인 그룹은 EMM Client에 설정된 그룹과 동일해야함 (기본: LLVDH2GU5H.com.sds.emm) • 입력된 키체인 그룹의 prefix값은 provisioning_profile의 prefix값과 동일 해야함.	필수	
ios_certificate	-i	앱을 signing하기 위한 인증서		
client_scheme	-c	EMM Client의 URL Scheme		EMMClient
fcrypto	-f	파일 암호화 기능 사용 여부		• true • false(기본값)

Tag	Param	설명	필수 여부	값
dpath	-d	AppWrapping된 사내 애플리케이션 ipa파일 위치의 절대 경로		/현재폴더/redex.ipa
tpath	-t	사내 애플리케이션의 압축을 풀기위한 임시 폴더 경로		/현재폴더/tmp

iOS앱용 AppWrapper 에러 코드

AppWrapper를 이용하여 사내 애플리케이션을 wrapping할때 보여질 수 있는 에러 코드의 리스트입니다. 에러 발생 시 아래의 설명과 확인사항을 참고하여 wrapping시 발생하는 간단한 오류에 대해 조치를 취할수 있습니다.

정의	ErrorCode	설명	확인사항
SUCCESS	0	Wrapper 성공	
SRC_APK_NOT_EXIST	-1000	Wrapping할 원본 ipa파일이 해당 경로에 없는경우	입력된 경로에 ipa파일 유무 확인
EMM_SDK_ALREADY_INCLUDED	SRC_APK_NOT_EXIST -6	Wrapping하려는 ipa파일에 EMM SDK가 포함됨	해당 ipa파일에 EMM SDK가 포함되어 있으므로 Wrapping할수 없음
SIGNING_FAILED	SRC_APK_NOT_EXIST -7	Wrapping된 ipa파일에 singing 실패한 경우	• 인증서, provisioning profile의 유효기간 확인 • 인증서가 provisioning profile에 입력된 인증서와 동일한지 확인 • 앱의 번들ID가 provisioning profile의 App ID와 일치하는지 확인
APPWRAPPER_VER_CHECK	SRC_APK_NOT_EXIST -10	해당 ipa파일이 같은 버전의 AppWrapper로 wrapping된 이력 확인	해당 ipa파일은 AppWrapping 불가
PROVISIONFILE_NOT_EXIST	SRC_APK_NOT_EXIST -11	앱 signing을 위한 provisioning profile이 해당 경로에 없는 경우	입력된 경로에 provisioning profile 파일 유무 확인
BUNDLEID_NOT_MATCHED	SRC_APK_NOT_EXIST -12	입력된 앱의 번들ID와 provisioning profile의 App id가 다른 경우	provisioning profile의 App ID와 입력된 앱의 번들ID가 일치하는지 확인

정의	ErrorCode	설명	확인사항
KEYCHAIN_NOT_MATCHED	SRC_APK_NOT_EXIST -13	입력된 키체인 그룹의 prefix값과 provisioning profile의 prefix값이 다름	입력된 키체인 그룹의 prefix값과 provisioning profile의 prefix값이 일치하는지 확인
UNKNOWN	-99999		

용어 사전

A

AIDL

구글의 Android mobile device platform을 위한 IDL을 말합니다.

[관련 용어] android interface definition language, IDL

Air Command

삼성전자 단말 기능 중 하나로, 화면에 S펜을 가까이 대고 S펜 버튼을 클릭하여 에어 커맨드 메뉴를 실행할 수 있는 기능을 말합니다.

Air View

삼성전자 단말의 기능 중 하나로, 이메일, 사진 등에 S펜을 갖다대면 미리보기 할 수 있는 기능을 말합니다.

Android Beam

NFC를 이용해서 기기간에 브라우저 페이지, 유튜브 동영상 사이트, 연락처 등을 공유할 수 있는 기능을 말합니다.

[관련 용어] NFC

AP

인터넷 네트워크 신호를 무선으로 전송해 주는 기계를 말합니다. AP를 연결하게 되면 전파 수신 범위 안에 있는 한 인터넷을 쓸 수 있습니다.

[관련 용어] access point

API

운영체제와 응용 프로그램 사이의 통신에 사용되는 언어나 메시지 형식을 말합니다. API는 응용 프로그램이 운영체제나 데이터베이스 관리 시스템과 같은 시스템 프로그램과 통신할 때 사용되는 언어나 메시지 형식을 가집니다. API는 프로그램 내에서 실행을 위해 특정 서브루틴에 연결하는 함수를 호출하는 것으로 구현됩니다. 그러므로 하나의 API는 함수의 호출에 의해 요청되는 작업을 수행하기 위해 이미 존재하거나 연결되어야 하는 몇 개의 프로그램 모듈이나 루틴을 가집니다.

[관련 용어] application programming interface

APNS

애플의 Push 알림 서비스를 말합니다.

[관련 용어] Apple Push notification service

Attestation

단말의 정상 여부를 판단하기 위해, EMM Agent에서 API를 통해 인증 서버와 통신하는 것을 말합니다. 삼성전자 단말의 경우, Attestation 서버와의 통신을 통해 단말의 정상 여부를 판단할 수 있습니다.

[관련 용어] EMM Agent

B

BAPI

각 SAP 모듈별로 SAP Business Object라는 클래스를 만들어 놓았는데 이 클래스를 사용하기 위한 방법 중 하나로서 다른 Component 프로그램에서 사용할 수 있도록 해 줍니다.

[관련 용어] business application programming interface

BAS

기업 맞춤형 애플리케이션 스토어 솔루션으로 기업용 애플리케이션을 전사적으로 배포관리하여 업무나 회사 생활에 필요한 모바일 단말용 앱을 임직원에게 효율적으로 배포하고 관리할 수 있습니다.

[관련 용어] Biz App store

C

CA

전자서명을 위한 인증관리체계를 갖추고 정보통신망을 통해 가입자의 전자서명 검증키를 인증하는 인증기관입니다. 제3자에 의해 운영되거나 기업 내부에서 자체적으로 운영할 수 있습니다.

[관련 용어] certificate authority

CA Server

CA 서버는 인증 기관을 대신하여 디지털 인증서를 발급하는 서버입니다.

[관련 용어] CA

CA Root 인증서

CA 자체 인증서로서 기업용 단말이 MDM 서비스를 사용할 수 있도록 인증되었음을 증명하기 위해 CA서버가 발급하는 디지털 인증서를 말합니다.

[관련 용어] CA

CC

ISO 15408 표준으로 채택된 정보 보호 제품 평가 기준입니다. 정보 보호 기술 기준으로 정보화 제품의 정보 보호 기능과 이에 대한 사용 환경 등급을 정한 기준으로 제1부 시스템 평가 원칙과 평가 모델, 제2부 시스템 보안 기능 요구 사항(11개), 제3부 시스템의 7등급 평가를 위한 8개의 보증 요구 사항으로 되어 있습니다.

[관련 용어] common criteria

CDMA

이동 통신에서 코드를 이용한 다중접속 기술의 하나로서 코드를 이용하여 하나의 셀에 다중의 사용자가 접속할 수 있도록 하는 기술이다.

[관련 용어] code division multiple access

CertAgent

미국 Information Security Corporation의 CA 제품으로 애플리케이션의 보안 강화를 위하여 X.509 인증서를 발급하며 인증서 폐기 목록을 관리합니다. EMM에서는 CA 연계 어댑터를 사용하여 인증서를 발급할 수 있습니다.

CMP

인증서를 관리하기 위한 프로토콜을 말합니다.

[관련 용어] certificate management protocol, 프로토콜

COPE

기업소유 단말기기지만 사용자인 임직원의 개인적 사용도 허용됩니다.

[관련 용어] corporate-owned personally enabled

CRL

인증서 폐기 목록으로 폐기된 인증서를 사용자들이 확인할 수 있도록 그 목록을 배포, 공표하기 위한 메커니즘입니다. 주로 인증 기관에서 관리하며 메시지를 전달할 때 인증서와 함께 전달됩니다.

[관련 용어] certificate revocation list

CRM

고객 관계 관리를 말합니다. 기업이 고객 관계를 관리해 나가기 위해 필요한 방법론이나 소프트웨어 등을 가리키는 용어입니다. 현재의 고객과 잠재 고객에 대한 정보 자료를 정리, 분석해 마케팅 정보로 변환함으로써 고객의 구매 관련 행동을 지수화하고, 이를 바탕으로 마케팅 프로그램을 개발, 실현, 수정하는 고객 중심의 경영 기법을 말합니다.

[관련 용어] customer relationship management

CSR

인증서 서명 요청을 말합니다.

[관련 용어] certificate signing request

CSS

HTML이나 XHTML이 실제로 표시되는 방법을 기술하는 언어로 W3C의 표준이며 화면에 표현되는 레이아웃과 스타일을 정의할 때 주로 사용됩니다.

D

DBMS

다수의 컴퓨터 사용자들이 컴퓨터에 수록한 수많은 자료들을 쉽고 빠르게 추가, 수정, 삭제할 수 있도록 해주는 소프트웨어를 말합니다.

[관련 용어] database management system

DRM

디지털 콘텐츠의 무단 사용을 막아 제공자의 권리와 이익을 보호해주는 기술과 서비스를 통틀어 일컫는 말입니다. 불법 복제와 변조를 방지하는 기술 등을 제공합니다.

[관련 용어] digital rights management

E

EIP

기업 기간계와 연계를 위해 널리 사용되는 패턴 및 Best Practice라 할 수 있습니다.

[관련 용어] enterprise integration pattern

EMM

회사 내의 부서별, 개인별로 IT 정책을 정의하여 차별적으로 적용이 가능한 기업형 모바일 단말 관리 서비스를 말합니다.

[관련 용어] enterprise mobility management

EMM Console

EMM 서비스를 위한 관리자용 UI를 제공합니다.

EMM 등록 프로파일

EMM 서버의 URL을 포함한 iOS EMM 서비스를 받기 위한 최소한의 정보가 들어있는 프로파일로 단말이 EMM 서버에 등록될 때 단말에 설치됩니다. 이 프로파일이 설치되어 있지 않으면 iOS EMM 서비스를 받을 수 없습니다.

EMM 서버

EMM 서비스를 제공하는 서버로 기업용 단말을 관리하고 통제하는 기능을 제공합니다.

EMM Agent

단말에 설치되는 애플리케이션의 집합으로 단말을 통제하고 감시합니다.

EMM Agent 비활성화

EMM Agent가 서버로부터 비활성화 단말제어를 받으면 활성화 상태에서 비활성화 상태로 전환되고 이후 EMM Agent 활성화 단말 제어를 제외한 어떠한 단말 제어에도 반응하지 않고 단말을 더 이상 통제하지 않습니다.

EMM Agent 활성화

EMM Agent가 서버로부터 활성화 단말제어를 받으면 비활성화 상태에서 활성화 상태로 전환되고 이후 지속적으로 EMM서버와 통신을 하면서 단말을 통제하고 감시합니다.

EMM 정책 프로파일

EMM서버가 단말을 제어하는 정책 내용이 포함된 프로파일을 말합니다.

End Entity

공개키 기반 구조(PKI)에서 PKI 서비스를 이용하는 최종 사용자, 가입자, 하드웨어 장치 또는 응용 Software를 말합니다. 인증서의 공개키에 대응하는 개인키를 소유하고 있는 인증서 주체이며, CA나 RA도 EE가 될 수 있습니다.

[관련 용어] CA, RA

ENDPoint주소

통신 참여자나 통신 채널에 의해 드러나게 되는 인터페이스로 외부에서 접근 가능한 툴. 보통 IP주소를 말합니다.

ERP

기업 활동을 위해 사용되는 기업 내의 모든 인적, 물적 자원을 효율적으로 관리하여 궁극적으로 기업의 경쟁력을 강화시켜주는 역할을 하는 통합 정보 시스템을 말합니다. 기업은 경영 활동의 수행을 위해 여러 개의 시스템 즉 생산, 판매, 인사, 회계, 자금, 원가, 고정 자산 등의 운영 시스템을 갖고 있는데 ERP는 이처럼 전 부문에 걸쳐있는 경영 자원을 하나의 체계로 통합 시스템을 재구축함으로써 생산성을 극대화하려는 대표적인 기업 리엔지니어링 기법입니다.

[관련 용어] enterprise resource planning

F

FIPS

미국연방정부기관에서 사용하는 정보 처리 기계와 방식을 표준화하기 위해 미국 국립 표준 기술연구소(NIST)가 제정하는 표준 규격입니다.

[관련 용어] federal information processing standards

FTP

인터넷을 통해 한 컴퓨터에서 다른 컴퓨터로 파일을 전송할 수 있도록 하는 방법과 프로그램을 모두 일컫는 말입니다.

[관련 용어] file transfer protocol

G

Gateway

복수의 컴퓨터와 근거리 통신망(LAN; local area network)등을 상호 접속할 때 컴퓨터와 공중 통신망, LAN과 공중 통신망 등을 접속하는 장치를 가리킨다.

GCM

GCM은 구글의 Push 알림 서비스로 개발자가 서버에서 개인의 안드로이드 단말로 데이터를 전송하는 무료 서비스입니다. 적은 용량의 애플리케이션 알림 메시지 또는 4KB의 페이로드 데이터를 포함하는 메시지를 전송할 수 있습니다.

[관련 용어] Google cloud messaging

Groupware

기업의 구성원들이 컴퓨터로 연결된 작업장에서 서로 협력하여 업무를 수행하는 그룹 작업을 지원하기 위한 소프트웨어나 소프트웨어를 포함하는 구조를 말합니다. 개인용 소프트웨어와 반대되는 개념입니다.

GPS

위성에서 보내는 신호를 수신해 사용자의 현재 위치를 계산하는 위성항법 시스템입니다.

[관련 용어] global positioning system

GSM

유럽에서 서비스하고 있는 무선 이동통신 기술방식입니다. GSM은 시분할 다중접속 (

TDMA)의 변종으로서, TDMA, CDMA와 함께 널리 사용되는 디지털 무선전화기술 중 하나다.

[관련 용어] global system for mobile communications

H

HTML

인터넷 서비스의 하나인 월드 와이드 웹을 통해 볼 수 있는 문서를 만들 때 사용하는 프로그래밍 언어의 한 종류입니다. 특히 하이퍼텍스트를 작성하기 위해 개발되었으며 인터넷에서 웹을 통해 접근되는 대부분의 웹 페이지들은 HTML로 작성됩니다. HTML은 전자 문서의 서식을 정의하기 위해 만들어졌으며 국제 표준 SGML의 부분 집합으로 정의되었습니다.. HTML은 SGML에서 특히 하이퍼텍스트를 강조하여 만들어진 언어이며 ASCII 문자로 구성된 일반적인 텍스트로 구성되었습니다. HTML은 별도 컴파일러가 필요하지 않으며 웹 브라우저에서 해석이 가능한 사용하기 쉬운 언어로 각광받고 있습니다.

[관련 용어] hyperText markup language

HTML5

HTML의 차기 주요 제안 버전으로 월드 와이드 웹의 핵심 마크업 언어이며 HTML4, XHTML 1.0에 대한 차기 표준 제안이다. 이것은 어도비 플래쉬나 마이크로소프트의 실버라이트, 썬의 자바 FX와 같은 플러그인 기반의 리치 인터넷 애플리케이션에 대한 필요를 줄이는데 목적을 두고 있습니다.

[관련 용어] HTML

Hybrid Platform

Hybrid Platform은 HTML, JavaScript, CSS등의 웹 기술로 개발한 Mobile Web을 멀티 플랫폼에서 실행되는 Native App으로 만들 수 있는 OSMU (One Source Multi Use)를 지원하는 크로스 모바일 플랫폼입니다. 즉, Mobile Web은 다양한 단말에 동일한 화면을 보여줄 수 있지만 단말 리소스 접근의 한계가 있으며 Native App은 쉽게 단말 리소스 접근은 가능하지만 플랫폼별로 제작되어야 합니다. 이와 같이 웹 기술로 개발된 애플리케이션을 다양한 단말에서 사용할 수 있으며 쉽게 단말 리소스에 접근도 가능한 크로스 모바일 플랫폼이 Hybrid Platform입니다. 또한 Hybrid Platform으로 개발된 애플리케이션인 Hybrid App은 Native App과 동일한 방식으로 실행과 배포를 할 수 있으며 JavaScript API를 이용하여 Native feature를 사용할 수 있습니다.

[관련 용어] HTML, CSS

Hybrid 앱

Web app과 Hybrid Platform API를 사용한 앱을 말합니다. 즉, Web App과 Native App이 합쳐져 연동하는 Application을 말합니다. Native app의 형태이며 주요 화면 구성은 Webkit에 기반을 둔 Webview를 통해 보여지는 Mobile Web으로 구성되어 있습니다. Native Application과 설치 및 실행 방식은 동일하지만 Web 기술을 사용하여 동작되는 점이 일반 App과 다릅니다.

I

IDE

효율적으로 소프트웨어를 개발하기 위한 통합개발환경 소프트웨어 애플리케이션 인터페이스입니다. 코드 편집기, 디버거, 컴파일러, 인터프리터등을 포함하고 개발자에게 제공합니다.

[관련 용어] integrated development environment

IDL

소프트웨어 컴포넌트의 인터페이스를 묘사하기 위한 명세 언어를 말합니다.
[관련 용어] AIDL

IMEI

단말기 국제 고유 식별 번호를 말합니다. 휴대폰 제조사는 전 세계 수많은 휴대폰을 구별하기 위해 단말기마다 고유 번호를 부여하고 있습니다.

[관련 용어] international mobile equipment identity

J

JAR

클래스 파일의 효율적인 배포를 위해 여러 클래스 파일들을 하나로 묶어 단일의 파일로 만드는 포맷을 말합니다. 로컬(local)상에서 편리한 관리는 물론 자바(Java) 프로그램 실행 중에 원격지에서 하이퍼텍스트 전송 규약(HTTP) 등을 통해 내려받기(download)되어 바로 사용이 가능합니다.

[관련 용어] Java archiver

Java EE

자바를 이용한 서버측 개발을위한 플랫폼입니다. Java EE 플랫폼은 PC에서 동작하는 표준 플랫폼인 Java SE에 부가하여,웹 애플리케이션 서버에서 동작하는 장애 복구 및 분산 멀티티어를 제공하는 자바 소프트웨어의 기능을 추가한 서버를 위한 플랫폼입니다. 이전에는 J2EE라 불리었으나 버전 5.0 이후로 Java EE로 개칭되었습니다. 이러한 Java EE 스펙에 따라 제품으로 구현한 것을 웹 애플리케이션 서버 또는 WAS라 부릅니다.

[관련 용어] Java platform, enterprise edition

JBOSS

자바를 기반으로 하는 오픈 소스 미들웨어로서 일반적으로 WAS라고 부릅니다.

[관련 용어] WAS

JCA

JCA는 웹 애플리케이션 서버와 기간계를 연동할 수 있도록 하는 자바 기반 기술입니다. JDBC가 웹 애플리케이션 서버와 테이터베이스와의 연동에 사용된다면, JCA는 웹 애플리케이션 서버와 기간계(데이터베이스 포함)를 연동하는 보다 일반적인 방법입니다. JCA 1.0은 자바 커뮤니티 프러세스의 JSR 16에 의해 개발되었으며, 최신 버전은 JCA 1.5 (JSR 112)입니다.

JCE

자바 암호 구조(JCA)에서 지원하지 않는 대칭키 알고리즘과 암호화 구조를 위해 썬(SUN)사에서 제공하는 확장 패키지를 말합니다. 암호, 메시지 인증 코드(MAC), 키 생성, 키 일치 등의 구조를 제공하고 JCA와 동일한 구조를 가지고 있어 JCA와 함께 사용됩니다.

[관련 용어] Java cryptography extention, JCA

JDK

자바 애플릿이나 각종 애플리케이션을 개발자들이 쉽게 만들 수 있도록 해 주는 개발자용 도구를 말합니다. 각종 운영체제(OS) 및 애플리케이션과 연결시킬 수 있는 API와 클래스 라이브러리, 자바 가상 머신 등으로 구성됩니다.

[관련 용어] Java Development Kit, API

jQuery

jQuery는 HTML 속 클라이언트 사이드 스크립트 언어를 단순화하도록 설계된 브라우저 호환성이 있는 자바스크립트 라이브러리를 말합니다.

jQuery Mobile

HTML5를 기반으로 하고 jQuery로 개발된 사용자 UI 프레임워크를 말합니다. 모바일 환경에 맞는 다양한 위젯을 제공하고 터치 이벤트를 지원하며 크로스 브라우저를 특징으로 합니다.

JRE

자바로 실행되는 프로그램을 사용자 컴퓨터에서 실행하기 위한 환경을 말합니다.

[관련 용어] Java runtime environment

JSON / XML

웹상의 구조화된 문서를 전송하기 위한 표준화된 텍스트 형식을 말합니다.

[관련 용어] Java script object notation / extensible markup language

L

LDAP

X.500을 근거로 한 디렉터리 데이터베이스에 접속하기 위한 통신 규약을 말합니다. 미국 미시간 대학에서 개발되었으며 디렉터리 정보의 등록, 갱신, 삭제와 검색 등을 실행할 수 있습니다. 운영체제(OS)나 그룹웨어 제품들이 지원해 주고 있습니다. RFC 2251에 규정된 버전 3이 최신판이며 통신망을 이용한 이용자 메일 주소나 이용자의 정보를 검색하는 데 주로 사용됩니다.

[관련 용어] lightweight directory access protocol

Log4j

log4j는 자바 기반 로깅 유틸리티입니다. 디버그용 도구로 주로 사용되고 있습니다. log4j의 최근 버전에 의하면 높은 등급에서 낮은 등급으로의 6개 로그 레벨을 가지고 있습니다. 설정 파일에 대상별(자바에서는 패키지)로 레벨을 지정할 수 있고 그 등급 이상의 로그만 저장하는 방식입니다.

M

MAM

모바일 기기에 설치된 앱과 데이터를 선택적으로 관리하는 솔루션으로 모바일의 애플리케이션 관리 시스템을 말합니다.

[관련 용어] mobile application management

MDM

모바일 기기를 기업이 중앙에서 제어하는 솔루션으로 모바일 단말 관리 시스템을 말합니다.

[관련 용어] mobile device management

MBI

기존의 커넥터로 지원할 수 없는 프로토콜 또는 비즈니스 로직에 대해 커스터마이징할 수 있도록 지원하는 인터페이스를 말합니다.

[관련 용어] mobile business integrator

MBS

기업 내부에서 사용하는 공통 모듈(결재, 메일, 일정 등)을 표준화하여 외부에 연계 인터페이스만 노출하고 이를 기반으로 단말 애플리케이션에 재활용하여 개발하는 방식을 말합니다. MBS의 비즈니스 로직이 변경되더라도 기존 단말 애플리케이션에는 별도의 영향을 주지 않는 구조입니다.

[관련 용어] mobile Biz. service

MQ

메시지가 처리되거나 송신되기 위해 기다리고 있는 온라인 메시지의 대기 행렬을 말합니다.

[관련 용어] message queue

N

NFC

전자태그(RFID) 기술 중 하나로, 10cm 이내의 가가운 거리에서 다양한 무선 데이터를 주고받는 비접촉식 통신 기술을 말합니다. 블루투스 등 기존의 근거리 통신 기술과 비슷하지만 블루투스처럼 기기 간 설정을 하지 않아도 됩니다.

[관련 용어] near field communication

NVP

웹 기반의 URL 호출과 유사한 방식으로 파라미터를 구성하여 호출됩니다. EMM connector 서비스와 composite service designer 구성 시 사용되는 파라미터 전달 방식의 한 유형입니다.
예) name1=parameter1&name2=parameter2

[관련 용어] name & value parameter

O

OCSP

X.509를 이용한 전자 서명 인증서의 폐지 상태를 파악하는 데 사용되는 인터넷 프로토콜입니다. 인증서 폐기 목록을 대체하기 위해 만들어졌으며, 공개 키 기반 구조의 인증서 폐기 목록과 관련된 문제들을 검증하기 위한 것입니다.

[관련 용어] online certificate status protocol, 프로토콜

OTA

무선 네트워크환경에서 모바일 애플리케이션이나 펌웨어를 설치 및 변경하는 일반적인 방법으로 HTTP 기반의 URL을 통해 OTA가 제공됩니다.

[관련 용어] over the air

OTG

USB On-The-Go의 줄임말로 USB OTG 또는 OTG라고 합니다. 컴퓨터의 개입 없이, 디지털 오디오 기기, 디지털 카메라, 마우스, 키보드, 스마트폰과 같은 디지털 기기 간에 케이블을 연결해서 통신이 가능하도록 하는 USB 규격입니다.

[관련 용어] on the go

P

PKI

공개키 기반의 구조를 말합니다. 인터넷상의 거래 비밀을 보장하면서거래 당사자들의 신분을 확인시켜 주는 보안 기술입니다. 공개한 의미는 수신자만 열쇠를 갖고 있는 자물쇠를 여러 사람에게 나눠줬다는 것을 말합니다. 즉 자신에게 귀중품을 보낼 때 금고에 먼저 그것을 담고 금고 열쇠는 다시 자신만이 열수 있는 자물쇠로 봉합해 보내라는 것입니다. 데이터를 암호화하는 방법에는 공개키와 비밀키 방식이 있습니다. 비밀키 암호 시스템이 송수신자 양측에서 똑같은 비밀키를 공유하는 데 반해 공개키는 암호화와 복호화키가 다르기 때문에 데이터를 암호화하고 이를 다시 풀 수 있는 열쇠가 달라 거의 완벽한 데이터 보완이 가능하고 정보 유출의

가능성이 적은 시스템입니다. 공개키 암호 방식은 대칭키 암호 기술이 제공하는 기밀성, 무결성 기능뿐 아니라 인증, 부인 방지, 전자 서명과 같은 다양한 정보 보호 기능을 제공하고 키 분배 문제를 해결할 수 있는 가장 효과적인 대안으로 인식되고 있습니다. 이 시스템에는 공개키에 대한 인증서를 발급하는 인증 기관, 사용자들의 인증서 신청 시 인증 기관 대신 그들의 신분과 소속을 확인하는 등록 기관, 인증서와 사용자 관련 정보, 상호 인증서 및 인증서 취소 목록 등을 저장 검색하는 장소인 디렉터리 또한 다양한 응용에서 공개키를 이용하여 전자 서명을 생성하고 검증하며 데이터에 대한 암호, 복호를 수행하는 사용자 등이 포함됩니다.

[관련 용어] public key infrastructure

Podcast

오디오, 동영상, PDF 등의 형태로 뉴스, 강의, 드라마 등의 다양한 콘텐츠를 제공하는 서비스를 말합니다. 애플의 아이팟(iPod)과 방송(boadcasting)을 합성한 신조어입니다.

Push

인터넷 환경을 이용하여 이용자가 관심을 가지고 있는 정보 목록을 선택하기만 하면 자동적, 주기적으로 최신 정보를 컴퓨터 화면에 직접 밀어 넣어(push)주는 기술입니다. push 기술은 사용자가 원하는 정보를 서버가 자동적으로 제공하는 방식입니다. 사용자가 매번 요청하지 않아도 특정 정보를 전송 받을 수 있도록 자동화된 기술입니다.

R

RA

보안인증서 발급 신청 업무를 대행하는 인증서 등록 시스템입니다.

[관련 용어] registration authority

S

SA

Push 서비스 사용 시, 애플리케이션 서버(통합 시스템, Samsung SDS EMM 서버 또는 기타 모바일 서비스)에서 단말로 메시지를 송수신하기 위해 애플리케이션 서버에 설치되는 Agent입니다.

[관련 용어] Push

SAP

독일의 소프트웨어 전문기업으로 SAP R/3 또는 SAP ERP 등 ERP 제품을 생산하는 기업입니다.

SCEP

가장 많이 쓰이는 인증서 관리 프로토콜 중 하나이다.

[관련 용어] simple certificate enrollment protocol, 프로토콜

Scheduler Job Class

예약 작업을 수행하기 위한 실행 클래스를 말합니다.

SDK

응용 프로그램의 개발을 간편하고 용이하게 하기 위해 프로그래머에게 유상이나 무상으로 제공되는 개발 도구를 말합니다. 프로그래머들이 솔루션 개발 시 자사의 응용 프로그램 인터페이스(API)를 채택하게 하기 위한 목적으로 대부분 무료로 제공됩니다. 개발 도구 및 라이브러리, 관련 도큐먼트, 개발 툴 등으로 구성됩니다.

[관련 용어] software development kit

Service Broker

단말과 서버 간 통신 및 암호화를 위한 공통 모듈을 말합니다.

SMS

무선 단말에서 단문 형태의 텍스트를 주고받을 수 있도록 해주는 단문 메시지 서비스를 말합니다.

[관련 용어] short message service

SOAP

일반적으로 널리 알려진 HTTP, HTTPS, SMTP 등을 사용하여 XML 기반의 메시지를 컴퓨터 네트워크 상에서 교환하는 형태의 프로토콜을 말합니다. SOAP는 웹 서비스(Web Service)에서 기본적인 메시지를 전달하는 기반이 됩니다. SOAP에는 몇가지 형태의 메시지 패턴이 있지만 보통의 경우 원격 프로시저 호출(Remote Procedure Call: RPC) 패턴으로 네트워크 노드(클라이언트)에서 다른쪽 노드(서버) 쪽으로 메시지를 요청하고 서버는 메시지를 즉시 응답하게 됩니다. SOAP는 XML-RPC와 WDDX에서 envelope / header / body로 이루어진 구조와 전송(transport)과 상호 중립성(interaction neutrality)의 개념을 가져왔습니다. SOAP는 XML을 근간으로 header와 body를 조합하는 디자인 패턴으로 설계되어 있습니다. header는 선택 사항으로 반복이나 보안 및 트랜잭션을 정보로 하는 메타 정보를 가지고 있으며 body 부분은 주요한 정보를 가지고 있습니다.

[관련 용어] simple object access protocol

SQL

데이터베이스를 사용할 때 데이터베이스에 접근할 수 있는 데이터베이스 하부 언어를 말합니다. 구조화 질의어라고 합니다. 데이터 정의어(DDL)와 데이터 조작어(DML)를 포함한 데이터베이스용 질의언어(query language)의 일종입니다. 초기에는 IBM의 관계형 데이터베이스인 시스템에서만 사용되었으나 지금은 다른 데이터베이스에서도 널리 사용됩니다.

[관련 용어] structured query language

SSL

보안 소켓 계층을 이르는 말로 인터넷에서 데이터를 안전하게 전송하기 위한 인터넷 통신 규약 프로토콜을 말합니다. 넷스케이프사에서 전자상거래 등의 보안을 위해 개발한후 TLS라는 이름으로 표준화되었습니다. SSL은 특히 네트워크 레이어의 암호화 방식이기 때문에 HTTP 뿐만 아니라 NNTP, FTP등에도 사용할 수 있는 장점이 있습니다. 기본적으로 Authentication, Encryption, Integrity를 보장합니다.

[관련 용어] secure socket layer, TLS

SSO

사용자 인증을 위한 공통 모듈을 말합니다. 하나의 ID로 여러 사이트를 이용할 수 있는 시스템 으로 여러 개의 사이트를 운영하는 대기업이나 인터넷 관련 기업이 회원을 통합 관리할 필요성이 생김에 따라 개발된 방식입니다.

[관련 용어] single sign on

T

TCP/IP

인터넷 네트워크의 핵심 프로토콜입니다. 인터넷에서 전송되는 정보나 파일들이 일정한 크기의 패킷들로 나누어 네트워크상 수많은 노드들의 조합으로 생성되는 경로들을 거쳐 분산적으로 전송되고, 수신지에 도착한 패킷들이 원래의 정보나 파일로 재조립되도록 합니다.

[관련 용어] transmission control protocol/internet protocol

Tethering

USB 또는 블루투스 장치, Wi-Fi 등을 통해 스마트폰에 또 다른 스마트폰, 태블릿 PC, 노트북, PC 등 IT 기기들을 연결함으로써 연결된 기기들이 무선인터넷을 사용할 수 있는 기능을 말합니다.

TIMA

회피가 불가능한 Android 커널 무결성 모니터링을 지속적으로 수행하기 위한 아키텍처를 말합니다.

TIMA or TrustZone Integrity Measurement Architecture incorporates privacy and security functions at the embedded systems level, which acts as buffer between the Android OS Kernel and mobile processor hardware.

[관련 용어] trustzone-based integrity measurement architecture

TLS

인터넷상에서 데이터의 도청이나 변조를 막기 위해 사용되는 보안 소켓 계층(SSL) 프로토콜 보다 보안성이 강화된 프로토콜입니다. SSL과 기능적 차이는 거의 없으나, 해시 기반 메시지 인증 코드 계산과 암호 모음, 의사난수 계산 방식을 달리합니다., 1999년 TLS 1.0 (IETF RFC 2246)이 정의된 이후, 취약성 보완 및 확장성 강화를 위해 설계를 개선하여 2008년 TLS 1.2(IETF RFC 526)가 발표되었습니다.

[관련 용어] transport layer security, SSL

Token

일련의 문자열에서 구분할 수 있는 단위로 컴파일러나 어셈블러 등의 처리기에서 사용되는 어휘 분석 단위를 말합니다. 루프 또는 고리 형태의 망에서 사용권을 제어하는 데 사용됩니다. 토큰이 망을 순회하며 토큰을 잡은 노드에 사용권을 주는 방식입니다. 즉 공백, 구두점, 여는 괄호, 콜론, 세미콜론 등과 같은 특수 기호, 식별자, 지정어, 상수, 단말 기호들로 인식된다. 키워드, 변수, 연산자, 숫자 등이 있습니다.

TTE

메시지 유효 기간을 말합니다.

[관련 용어] time to expire

U

UI

사용자 인터페이스를 말합니다. 사용자 인터페이스는 사람(사용자)와 사물 또는 시스템, 특히 기계, 컴퓨터 프로그램 등 사이에서 의사소통을 할 수 있도록 일시적 또는 영구적인 접근을 목적으로 만들어진 물리적, 가상적 매개체를 뜻합니다.

[관련 용어] user interface

UI Component

위젯이라고도 불리며 애플리케이션 화면을 표현하는 GUI (Graphic User Interface)의 요소로서 정보를 다양한 방식으로 표시합니다. Button, Checkbox, Text box, Slider, Select 등 여러가지가 있습니다.

UI Framework

하이브리드 애플리케이션 개발을 위해서 새롭게 개발된 프레임워크로 HTML5 / Javascript / CSS로 구성되어 있습니다. jQuery Mobile을 기반으로 하며 다양한 모바일 위젯과 페이지 이력 관리, 터치 이벤트 처리 등 모바일 웹앱 개발에 필요한 환경을 제공합니다.

UMP

EMM의 Push 컴포넌트로 application server 와 client 사이에 신뢰할 수 있고 안전한 메시지의 송수신을 지원하는플랫폼입니다. 메시지의 특성에 따라 차별성 있는 전송 품질을 제공하며 서버와 단말 간의 양방향 Push 기능을 지원합니다. UMP는 구축형과 서비스형을 포함한 모든 환경에서 운영됩니다.

[관련 용어] unified messaging platform

USIM

비동기 3세대 이동 통신(WCDMA)의 단말기에 삽입되는 스마트 카드로 사용자 인증, 글로벌 로밍, 전자 상거래 등 다양한 기능을 한 장의 카드에 구현한 기술을 말합니다.

[관련 용어] universal subscriber identity module

V

VOC

관리 시스템 콜센터에 접수되는 고객불만 사항을 접수부터 처리가 완료될 때까지 처리 상황을 실시간으로 관리하고 처리결과를 관서별로 지표화하여 관리·평가함으로써 고객의 체감서비스를 향상시키는 고객관리시스템입니다.

[관련 용어] voice of customer

VPN

VPN (가상 사설망)이란 인터넷과 같은 공중망(public network)을 마치 전용선으로 사설망(private network)을 구축한 것처럼 이용해 회선 비용을 크게 절감할 수 있는 기업 통신 서비스로 인터넷망을 전용선처럼 사용할 수 있도록 특수 통신 체계와 암호화 기법을 제공하는 서비스를 말합니다.

[관련 용어] virtual private network

VPN 클라이언트

VPN 클라이언트는 단말기에 설치되어 가상 사설망 기능을 수행하는 클라이언트 프로그램을 말합니다.

W

WAP

Wireless Application Protocol

GSM, TDMA, CDMA 등을 포함한 모든 무선 네트워크에 연결할 수 있는 모바일용 아키텍처를 말합니다.

WAS

Web Application Server

Web Application을 수행할 수 있는 환경을 제공해주는 서버를 말합니다.

WSDL

Web Services Description Language

웹 서비스 기술 언어 또는 기술된 정의 파일의 총칭으로 XML로 기술된다. 웹서비스의 구체적 내용이 기술되어 있어 서비스 제공 장소, 서비스 메시지 포맷, 프로토콜 등이 기술된다.

개인키(Private Key)

Private Key공개키 기반구조(PKI)에서 공개키(Public Key)와 쌍으로 생성되어 비대칭 암호화 알고리즘(RSA 등)을 통하여 메시지 및 전자서명의 암호화/복호화에 사용되며 , 개인이 보유하고 관리하는 키이다.

공개키(Public Key)

공개키 기반구조(PKI)에서 개인키(Private Key)와 쌍으로 생성되어 비대칭 암호화 알고리즘(RSA등)을 통하여 메시지 및 전자서명의 암호화/복호화에 사용되며, 외부에 공개되는 키이다.

기간계

어떠한 솔루션을 도입하기 전에 고객이 이미 쓰고 있는 시스템을 말합니다.

네이티브 앱

단말, PC 등에 설치된 운영체제(Operating System, OS)의 기능을 이용하기 위해 해당 OS의 SDK를 이용하여 만들 어진 애플리케이션을 말합니다. 모바일의 경우에는 다양한 모바일 플랫폼에서 제공하는 SDK로 만들어진 애플리케이션을 말합니다.

단말기 방화벽

단말기에서 VPN 연결 시 단말기 내/외부에서의 부적절한 네트워크의 접근을 차단하는 기능을 말합니다.

단말기 프로비저닝

EMM 클라이언트가 설치된 단말에서 EMM Server에 인증을 통하여 단말을 등록하는 과정 또는 행위를 의미합니다.

단말제어

서버로부터 전달되어 즉시 반영되도록 하는 명령을 말합니다. 해당 명령은 단말에서 1회 실행됩니다.

모바일 웹(Mobile Web)

모바일 웹은 일반적인 웹 기술로 개발되고 모바일 브라우저에 의해 실행되는 웹 애플리케이션을 통칭합니다.

모바일 웹앱(Mobile Web App)

모바일 웹앱 역시 모바일 웹의 한 형태입니다. 하지만 모바일 웹앱은 일반적인 웹사이트보다 모바일에 더 최적화되고 네이티브 애플리케이션화된 형태를 한정하는 표현입니다. 웹앱은 웹과 애플리케이션의 합성어로 앱이라는 용어가 보편화되면서 생긴 일정의 신조어라 할 수 있습니다. 모바일 웹앱은 웹 기술만 사용해서 풀 스크린 모드, 애니메이션 효과, 터치 상호 작용, 비동기 통신, 로컬 저장소, 오프라인 지원, 향상된 스타일 등을 구현하여 모바일 환경에서 네이티브 애플리케이션과 유사한 실행 환경, 사용자 경험을 제공하는 형태의 애플리케이션입니다.

배타적 화이트리스트 애플리케이션

배타적 화이트리스트에 등록된 애플리케이션이 실행되면 해당 리스트에 등록된 애플리케이션을 제외한 나머지 애플리케이션의 실행을 금지합니다. 단, 배타적 화이트리스트 애플리케이션 이전에 수행된 애플리케이션은 실행 상태를 유지합니다.

블랙리스트 애플리케이션

반드시 실행되지 말아야하는 애플리케이션 목록입니다. 블랙리스트 애플리케이션을 추가하고 정책이 적용된 상태에서는 블랙리스트의 애플리케이션을 구동시키면 잠시 후 종료됩니다. 즉 EMM Agent가 블랙리스트를 강제로 종료시킵니다.

[관련 용어] EMM Agent

웹클립(Web Clip)

iOS 단말에 설치되는 아이콘으로 특정 웹 사이트의 URL을 가지고 있어서 실행 시 Safari를 통해 웹 사이트로 연결됩니다.

프로토콜(Protocol)

정보기기 사이 즉 컴퓨터끼리 또는 컴퓨터와 단말기 사이 등에서 정보교환이 필요한 경우, 이를 원할하게 하기 위하여 정한 여러 가지 통신규칙과 방법에 대한 약속 즉, 통신의 규약을 의미합니다.

화이트리스트 애플리케이션

반드시 실행되고 있어야 하는 애플리케이션의 목록입니다. 화이트리스트 애플리케이션을 추가하고 정책이 적용된 상태에서는 화이트리스트의 애플리케이션을 종료시켜도 잠시 후 다시 실행됩니다. 즉 EMM Agent가 화이트리스트를 강제로 재실행시킵니다.

[관련 용어] EMM Agent

SAMSUNG SDS

Realize your vision

www.samsungsds.com