Realize your vision

Samsung SDS
EMM

사용자 매뉴얼

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

사용 대상

이 매뉴얼은 Samsung SDS EMM (이하 EMM) 의 Client 설치 및 서비스 활성화 방법 , EMM App Store 사용 방법 , Secure Browser 사용 방법 및 사용자 포털 사용 방법을 담고 있습니다 . 또한 모바일 단말에서 EMM 와 관련한 서비스나 애플리케이션을 사용하는 사용자를 대상으로 합니다 .

매뉴얼 구성

이 매뉴얼은 다음과 같은 내용으로 구성되어 있습니다 .

- **1장. Samsung SDS EMM 개요**
  EMM의 개요 및 주요 기능에 대해 설명합니다.
- **2장. 설치하기**
  EMM의 설치 환경 및 사용자 단말에 Client파일 설치에 대해 설명합니다.
- **3장. 시작하기**
  EMM에 로그인하여 초기 설정하는 방법과 홈화면 구조에 대해 설명합니다.
- **4장. 애플리케이션 활용하기**
  EMM에서 제공하는 앱스토어를 활용하는 방법에 대해 설명합니다.
- **5장. Secure Browser 사용하기**
  EMM Secure Browser의 설치 및 사용 방법에 대해 설명합니다.
- **6장. SecuCamera 사용하기**
  EMM SecuCamera의 설치 및 사용 방법에 대해 설명합니다.
- **7장. Wearable EMM 사용하기**
  웨어러블 단말에서 EMM 로그인 및 사용 방법에 대해 설명합니다.
- **8장. EMM 원격지원 받기**
  원격지원을 받기 위한 툴을 설치하여 시작하는 방법에 대해 설명합니다.
- **9장. 방문자용 EMM 사용하기**
  방문자용 EMM의 설치와 사용 방법에 대해 설명합니다.
- **10장. 사용자 포털 사용하기**
  EMM의 사용자 포털의 소개 및 사용 방법에 대해 설명합니다.

- **부록 A. 해결하기**
  사용자 단말이 잠긴 경우와 단말의 비밀번호를 잊은 경우의 방법에 대해 설명합니다.
- **부록 B. Client 에러 코드 및 설명**
  사용자 단말의 EMM에서 보여질 수 있는 에러 코드에 대해 설명합니다.

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 또는 문서의 다른 장을 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, 스크린캡처 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: 실행 배치 파일은 Windows의 관리자 권한으로 수행합니다.

개정 이력

솔루션 버전	매뉴얼 버전	매뉴얼 변경 일자	매뉴얼 변경 사항
1.0.0	1.0.0	2014.10	버전 1.0.0 매뉴얼 발행
1.0.3	1.0.3	2015.2	버전 1.0.3 매뉴얼 발행
1.1.0	1.1.0	2015.3	버전 1.1.0 매뉴얼 발행
1.1.1	1.1.1	2015.6	버전 1.1.1 매뉴얼 발행
1.1.2	1.1.2	2015.6	버전 1.1.2 매뉴얼 발행
1.1.3	1.1.3	2015.7	버전 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	Secure Browser 기능 개선
1.2.3	1.2.3a	2015.12	방문자용 EMM 정책 추가
1.3.0	1.3.0a	2016.4	단말내 UI, UX 개선
1.4.0	1.4.0a	2016.7	- QR Code 활용 단말 활성화 등 IT관리자 및 사용자 편의 기능 강화 - Windows10 지원(폰, 테블릿)
1.4.1	1.4.1a	2016.8	디바이스 관리자 권한 개수 변경으로 UI변경은 없음
1.5.0	1.5.0a	2016.10	메인화면 UI변경, Knox Shared Device 사용하기 추가
1.5.1	1.5.1a	2016.12	단말 지원 범위 변경
1.6.0	1.6.0a	2017.3	Tizen Wearable 지원 추가
1.6.1	1.6.1a	2017.5	EMM 앱 스토어 UI/UX 개선
2.0	2.0a	2017.10	SecuCamera 사용하기 추가
2.0.2	2.0.2a	2018.2	- 단말 지원 범위 변경 - 단말에 설정된 전체 정책 조회 기능 추가

목차

1 Samsung SDS EMM 개요

Samsung SDS EMM(Enterprise Mobility Management) 은 BYOD(Bring Your Own Device) 와 COPE(Corporate-Owned, Personally Enabled) 환경에서 보안이 강화된 기업용 EMM 솔루션입니다 . Samsung SDS EMM 은 단말 내의 개인 영역과 업무 영역을 분리하여 기업 정보에 대한 접근 관리를 강화하는 동시에 개인 프라이버시 데이터를 보호합니다 . 또한 삼성전자 컨테이너 솔루션인 Knox 를 지원하고 기업내에 필요한 다양한 애플리케이션을 다운로드 받아 설치할 수 있도록 비지니스 앱 스토어를 제공하고 있습니다 .

Samsung SDS EMM의 주요 기능

Samsung SDS EMM(이하 EMM) 은 EMM 서버 인증을 통한 사용자별 정책 적용과 애플리케이션 배포관리 그리고 애플리케이션 내부 보안기능 (text copy/paste, print, Open In, wipeout 등) 등 다양한 기능을 제공하고 있습니다 .

또한 Samsung SDS Push 솔루션을 통해 사용 권한 제어를 위한 정책을 실시간으로 EMM 서버에서 전송하여 관리하고 , 특정 사이트 접근이 가능하도록 암호화된 웹 브라우저인 Secure Browser 를 제공합니다 .

필요에 따라 원격으로 단말 화면을 공유하며 문의사항을 지원받을 수도 있습니다 .

EMM 은 기본적으로 세로모드의 UI 를 지원하고 일반 단말과 태블릿 , PC 에서 모두 사용 가능하며 Android 와 iOS, Windows, Tizen Wearable 플랫폼에 따라 지원되는 기능이 다를 수 있습니다 .

자세한 내용은 이 매뉴얼의 2 페이지의 " 설치 및 실행 환경 " 과 6 페이지의 "3 시작하기 ", 15 페이지의 "4 단말 정책 확인하기 ", 34 페이지의 "7 Wearable EMM 사용하기 " 를 각각 참고하세요 .

2 설치하기

EMM 을 단말에 설치하는데 필요한 단말 기기와 OS 버전 및 사전 확인 사항에 대해 설명합니다 . 또한 사용자포털을 사용하기 위한 실행 환경에 대해 설명합니다 .
EMM 을 단말에 설치하는 것은 가이드에서 제시하는 방법 외에 각 고객의 특성에 맞추어 웹페이지를 통한 배포 등 다양한 방법으로 가능합니다 .

설치 및 실행 환경

EMM 을 단말에 설치하는데 필요한 환경과 사용자포털을 이용하기 위한 설명입니다 .

Android™ OS

EMM 의 라이선스에 따라 지원하는 OS 정보는 다음과 같습니다 .

- 고보안 라이선스: Android 4.4(Kitkat) ~ Android 8.0 (Oreo)의 삼성 단말
- 일반보안 라이선스: Android 4.4(Kitkat) ~ Android 8.0 (Oreo)의 삼성 및 타사 단말

iOS™ OS

EMM 이 지원하는 OS 정보는 다음과 같습니다 .

- 고보안 및 일반보안 라이선스: iOS 8.0 이상

Windows OS

EMM 이 지원하는 OS 정보는 다음과 같습니다 .

- 고보안 및 일반보안 라이선스: Windows10 1703 이상의 데스크탑 (Pro/Enterprise/Home)

Tizen Wearable OS

EMM 이 지원하는 OS 정보는 다음과 같으며 일반보안을 기본으로 동작합니다 .
즉 , 고보안 서버가 설치된 환경에서도 Tizen Wearable 환경을 구성하면 일반 보안으로 동작합니다 .

- 일반보안 라이선스: Tizen 2.3.2 이상

Note: 사업장을 출입하는 방문자를 위한 EMM의 설치 및 실행은 일반보안 라이선스에서만 지원합니다.

사용자 포털

EMM 의 사용자 포털을 실행하기 위한 PC 의 최적화 환경은 다음과 같습니다 .

- OS: Windows XP 이상
- 브라우저: Chrome 20 이상, Firefox 15 이상, Internet Explorer 9, 10, 11
- 해상도: 1,680 x 1,050(px) 이상 권장

EMM 설치하기

EMM 을 사용하기 위해서는 관리자가 제공하는 다운로드 URL 에 따라 사용자의 단말에 관련 파일들을 직접 설치하거나 다운로드한 후 설치를 해야 합니다 . 관리자가 설정한 환경에 따라 인증서 파일과 EMM 설치 파일이 모두 제공되거나 , EMM 설치 파일만 제공될 수 있습니다 . 전자의 경우 인증서 파일을 실행하여 설치한 후 , EMM 설치 파일을 실행합니다 .

모바일 단말의 경우

EMM 의 설치는 EMM 관리자의 설정에 따라 Client 파일만 단말에 설치한 후 EMM 에 최초 로그인 시 나머지 설치 파일들을 자동으로 설치하거나 , EMM Client 파일 , EMM Agent 파일 , Push Agent 파일을 모두 단말에 설치한 후 EMM 에 로그인하는 두가지 방법이 있습니다 . 후자의 경우 EMM 을 설치하려면 다음의 절차를 따르세요 .

1. 단말에서 다운로드된 EMM Client 파일이 위치한 폴더로 이동하세요.
2. EMM Client 파일을 실행한 후, **다음** 혹은 **설치**를 탭하세요.
3. 설치 완료 화면에서 **완료**를 탭하세요.
4. Android 단말에 설치하려면,
    가. EMM Agent파일과 Push Agent파일을 각각 실행한 후, **다음** 혹은 **설치**를 탭하세요.
    나. EMM Agent와 Push Agent 설치 완료 화면에서 **완료**를 탭하세요.
5. 단말 홈에 생성된  SDS EMM을 탭하세요.

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

KME 연계 단말의 경우

운영자에 의해 미리 일괄 등록된 KME 연계 단말의 경우 단말이 최초 부팅 또는 Wi-Fi 연결 시 자동으로 EMM 이 다운로드된 후 설치되어 로그인까지 진행됩니다 . KME 를 설정하려면 “Samsung SDS EMM 관리자 매뉴얼 ” 의 Knox Mobile Enrollment 를 참고하세요 .

1. Mobile Enrollment 안내가 나타나면 **다음**을 탭하세요.
2. 보안 정책 및 Knox 개인정보 취급방침을 읽고 **위 모든 내용에 동의함**을 선택 후 **다음**을 탭합니다.
3. 인증과 등록 과정을 자동으로 거쳐 EMM이 활성화 됩니다.

Note:
- Android 단말의 경우 EMM 설치를 위해 단말의 **설정 > 보안**으로 이동하여 **출처를 알 수 없는 앱** 항목을 탭한 후, **허용**을 선택합니다.
- iOS 단말의 경우 EMM 설치를 위해 단말의 **설정 > Safari > 고급**으로 이동하여 **JavaScript** 항목을 **On**으로 설정합니다.
- Windows10 단말의 경우 EMM 설치를 위해 사전에
  - 단말의 **설정 > 업데이트 및 보안 > 개발자용**으로 이동하여 개발자 기능 사용 항목을 **개발자 모드**로 설정합니다.
  - 기존에 EMM을 설치했던 단말의 경우 설정 > 계정 > 프로비저닝으로 이동하여 설치되어 있는 패키지 파일을 삭제합니다.
- 의존성 라이브러리 파일(Microsoft.NET.Native.Framework.1.3, Microsoft.NET.Native.Runtime.1.3)을 설치합니다.

Windows 10 데스크탑의 경우

Windows 10 용 EMM 설치 파일은 32 비트용과 64 비트용이 별도 압축파일로 제공됩니다 . 설치 파일을 단말 내의 적당한 위치에 압축 해제한 후 설치하려면 다음의 절차를 따르세요 .

1. 단말에서 압축해제한 EMM Client 파일이 위치한 폴더로 이동하세요.
2. **Add-AppPackage.ps1**파일을 오른쪽 클릭한 후, **PowerShell에서 실행**을 선택하세요.
3. “Windows PowerShell”창의 “계속하려면 <Enter> 키를 누르십시오” 메시지에서 **Enter**를 누르세요.
4. 사용자 계정 컨트롤 팝업창이 열리면 **예**를 클릭하세요.
5. 개발자 모드 안내 팝업창이 열리면 내용 중 **개발자 설정** 링크를 클릭한 후 **설정 > 업데이트 및 복구 > 개발자용**으로 이동하세요.
6. **개발자 기능 사용** 항목 중 **개발자 모드**를 선택한 후 확인창에서 **예**를 클릭하세요.
7. “설정”창을 닫은 후 개발자 모드 안내 팝업창에서 **확인**을 클릭하세요.
8. 설치 중 “계속하려면 <Enter> 키를 누르십시오” 메시지에서 대기 상태에 있으면 **Enter**를 누르세요.

웨어러블 단말의 경우

EMM 의 설치는 SMS 메시지 수신이 가능한 경우 Tizen 스토어의 제품 페이지로 연결되는 Deep Link 를 이용하고 , SMS 메시지 수신이 불가능한 경우 KME(Bulk installation) 를 이용하여 EMM Agent 를 설치합니다 . KME 를 이용하려면 관리자에 의해 미리 기어 단말이 Knox 포털에 일괄 등록되어 있어야 합니다 . 자세한 내용을 “Samsung SDS 관리매뉴얼 ” 의 Knox Mobile Enrollment 를 참고하세요 .

Deep Link 를 이용하여 EMM 을 설치하려면 다음의 절차를 따르세요 .

1. 사용자의 웨어러블 단말에 메시지 앱으로 이동하여, 수신된 SMS 메시지의 Deep Link(설치 정보 URL)를 여세요.
2. **설치**를 탭하여 EMM 앱을 다운로드하세요.
3. 앱 사용 권한 확인 메시지가 나타나면  을 탭하세요.
4. 웨어러블 단말에 생성된  SDS EMM 아이콘을 탭하거나 위젯을 등록한 후 위젯을 탭하세요.

KME 를 이용하여 EMM 을 설치하려면 다음의 절차를 따르세요 .

1. 사용자의 웨어러블 단말에서 Wi-Fi를 설정합니다.
   - KME를 사용하려면 Wi-Fi에 연결되어야 하고 배터리 잔량이 50% 이상이어야 합니다.
2. Knox Mobile Enrollment 메시지가 나타나면 스크롤 후 **Next**를 탭하세요.
3. 이용 약관을 확인한 후 동의를 선택하고 **Next**를 탭하세요.
   EMM 앱이 자동으로 다운로드되며 설치가 완료됩니다.
4. 웨어러블 단말에 생성된  SDS EMM 아이콘을 탭하거나 위젯을 등록한 후 위젯을 탭하여 로그인을 진행하세요. Wearable EMM 사용에 대한 자세한 내용은 34 페이지의 "7 Wearable EMM 사용하기"를 참고하세요.

Note:
- 설치 및 로그인 정보 전달을 위한 SMS 전송을 위해서는 전화번호가 등록되야 합니다.
- Tizen Wearable 2.3.2.1 이하 버전은 KME를 지원하지 않으므로 펌웨어 업데이트가 필요합니다. 기어 단말에서 **설정 > Gear 정보 > Gear 소프트웨어 업데이트**를 탭하여 펌웨어를 업데이트합니다.

3 시작하기

EMM 은 로그인 시 사용자 정책이 즉시 적용되며 , 애플리케이션 관리 및 애플리케이션 내부 Secure (text copy 및 paste, print, Open In, wipeout 등) 기능을 제공합니다 . 또한 EMM 은 Samsung SDS Push 를 통해 실시간으로 단말 사용 제어를 위한 정책을 EMM 서버로부터 전송 받습니다 . 그 외 사용자의 사이트 접근 보안을 위하여 Secure Browser 를 제공합니다 .

EMM Agent 및 Client 실행 시 자가진단

단말 애플리케이션은 단말 자체가 단말 내부의 OpenSSL 을 사용하여 자가 진단을 합니다 . Samsung SDS EMM Agent 역시 MDM Agent 가 제대로 작동하는지 확인하기 위해 전원을 켤 때마다 자가 진단을 실행하고 , 단말이 켜지면 레지스트리 확인을 위해 Samsung SDS EMM Agent 와 통신을 시작합니다 . 단말 레지스트리가 위변조된 경우 된 경우 , EMM 서버는 단말 사용이 불가능하도록 EMM Agent 와 서버간의 통신을 차단합니다 . 또한 EMM Agent 는 정책과 단말상에 등록된 다른 애플리케이션 데이터의 무결성을 확인합니다 . 단말이 EMM 서버에 등록되었거나 EMM Agent 에 로그인 된 경우 , EMM Agent 는 EMM 서버로부터 정책 및 다른 애플리케이션 데이터를 받습니다 . 정책과 다른 애플리케이션 데이터는 암호화되어 저장됩니다 .

정책과 애플리케이션 데이터가 암호화되어 저장되는 경우는 다음과 같습니다 .

- 해시 알고리즘 Secure Hash Algorithm (SHA) 256을 사용하여 데이터 object가 해쉬값을 받는 경우
- 암호화 알고리즘 Advanced Encryption Standard (AES) 256으로 데이터 object를 암호화하는 경우
- 완벽한 보안을 위해 AES 256과 해쉬값을 이중 암호화하는 경우

단말이 켜지면 Samsung SDS EMM Agent 는 암호화된 정책과 애플리케이션 데이터를 읽고 , 다음과 같은 무결성 확인을 실행합니다 .

1. Double 암호화된 데이터와 해쉬값을 해독합니다.
2. 해독된 데이터는 SHA 256을 사용해 해쉬값을 받습니다.
3. 저장하였을 때와 사용할 때 데이터들의 해쉬값을 비교합니다.

정책 또는 다른 어플리케이션 데이터가 위변조 된 경우 , EMM 서버는 단말 사용이 불가능하도록 EMM Agent 와 서버간의 통신을 차단합니다 .

EMM 로그인하기

EMM 에 로그인하는 방법은 QR 코드를 이용하는 방법과 직접 입력하는 방법이 있습니다 . 단 , Windows10 과 Tizen Wearable 단말의 경우 직접 입력하여 로그인하는 방법만 가능합니다 . Wearable EMM 의 로그인 방법 및 사용 방법은 34 페이지의 " Wearable EMM 로그인하기 " 를 참고하세요 . 최초 로그인은 Tenant ID 를 서버에서 확인해야 하므로 로그인 소요시간이 평소보다 오래 걸릴 수 있습니다 .

Note: EMM 최초 실행 시, iOS단말의 경우 iOS9부터는 단말의 **설정 > 일반 > 기기관리** 에서 해당 애플리케이션에 대하여 신뢰를 선택한 후 실행이 가능합니다.

QR코드로 로그인하기

Android 단말과 iOS 단말의 경우 QR 코드로 로그인할 수 있습니다 . QR 코드는 관리자로부터 사전에 이메일로 전송받아야 하며 , QR 코드로 로그인하려면 다음의 절차를 따르세요 .

1. EMM을 실행하기 위하여 사용자 단말에 설치된  SDS EMM을 탭하세요.
   단, EMM 서버가 Custom의 Single-Tenant 모드이거나 EMM에 처음 로그인하는 것이 아닌 경우, 사용자 ID, 모바일 ID, 비밀 번호를 입력하는 화면이 나타날 수 있습니다.
2. 화면 우측 상단의 QR코드 이미지를 탭하세요.
3. 관리자로부터 전달받은 QR코드를 사각형 안에 인식시키세요.
   또는, 사전에 단말에 QR코드를 저장한 경우 **불러오기**를 탭하여 QR코드를 선택하세요.
4. QR코드로 부터 읽혀진 **사용자 ID**, **모바일 ID**가 입력되어 있는 화면에 **비밀번호**를 입력한 후 **로그인**을 탭하세요.
   최초 로그인 시 비밀번호는 사용자 ID와 동일합니다.
5. 최종 사용자 라이선스 동의서를 읽은 후 **예**를 탭하세요.
6. 기기 관리자 실행 안내가 나타나면 **실행**을 탭하세요.
7. 개인정보 취급방침에 대한 안내가 나타나면 동의 확인란을 선택한 후, **확인**을 탭하세요.
8. 사용자 ID와 동일하게 설정되어 있는 임시 비밀번호를 변경하기 위해 **비밀번호**에 현재의 비밀번호를 입력한 다음 **새로운 비밀번호**와 **새로운 비밀번호 확인**에 새로운 비밀번호를 입력한 후 **변경**을 탭하세요.
9. 화면잠금 비밀번호를 설정하세요.
   화면잠금 비밀번호에 대한 자세한 내용은 9페이지의 " 화면 잠금 비밀번호 설정하기"를 참고하세요.
10. iOS 단말에서로그인하려면 **설정 > 일반 > 프로파일**에서 단말 등록한 다음 프로파일을 설치한 후 SDS EMM을 다시 실행하세요.

직접 입력하여 로그인하기

로그인 시 필요한 정보를 직접 입력하여 로그인하려면 다음의 절차를 따르세요 .

1. EMM을 실행하기 위하여 사용자 단말에 설치된  SDS EMM을 탭하세요.
   단, EMM 서버가 Custom의 Single-Tenant 모드이거나 EMM에 처음 로그인하는 것이 아닌 경우, 사용자 ID, 비밀 번호, 모바일 ID를 입력하는 화면이 나타날 수 있습니다.
2. 미리 관리자로부터 발급받은 서버 주소(https, Access URL, Port)와 Tenant ID를 입력한 **후 다음**을 탭하세요.
   Tenant ID와 서버 주소(https, Access URL, Port)는 최초 로그인할 때만 입력하며, Single-Tenant 모드의 경우, Tenant ID 입력란은 선택하지 않습니다.
3. 관리자에게 안내받은 **사용자 ID**, **비밀번호**, 모바일 ID를 입력한 후 **로그인**을 탭하세요. 최초 로그인 시 **비밀번호**는 **사용자 ID**와 동일합니다.
4. 최종 사용자 라이선스 동의서를 읽은 후 **예**를 탭하세요.
5. 기기 관리자 실행 안내가 나타나면 **실행**을 탭하세요.
6. 개인정보 취급방침에 대한 안내가 나타나면 동의 확인란을 선택한 후, **확인**을 탭하세요.
7. 사용자 ID와 동일하게 설정되어 있는 임시 비밀번호를 변경하기 위해 **비밀번호**에 현재의 비밀번호를 입력한 다음 **새로운 비밀번호**와 **새로운 비밀번호 확인**에 새로운 비밀번호를 입력한 후 **변경**을 탭하세요.
8. 화면잠금 비밀번호를 설정하세요.
   화면잠금 비밀번호에 대한 자세한 내용은 9페이지의 " 화면 잠금 비밀번호 설정하기"를 참고하세요.
9. iOS 단말에서 로그인 하려면 **설정 > 일반 > 프로파일**에서 단말 등록한 다음 프로파일을 설치한 후 SDS EMM을 다시 실행하세요.

Note:

- EMM에 로그인 하려면 관리자가 **사용자 ID**와 **비밀번호**를 EMM 관리자 포털에 미리 등록해야 로그인이 가능합니다.
- Android 단말 사용자는 관리자가 사용자의 단말로 전송하는 정책에 Knox 컨테이너가 포함되어 있어야 EMM 설치 후 Knox 컨테이너를 추가로 설치할 수 있습니다.
- 다음은 EMM 고보안 버전에서만 적용되는 사항입니다.
  - Samsung SDS EMM이 활성화된 상태에서 단말 자체의 화면 잠금을 설정한 경우 기존에 등록된 인증서는 삭제됩니다.
  - 단말에 인증서를 설치하려면 단말 자체에 최소 PIN 수준 이상의 보안설정이 되어있어야 합니다. 또한 단말 재부팅 시 EMM 서비스와 인증서 접근을 위해 PIN을 입력해야 합니다.

화면 잠금 비밀번호 설정하기

EMM 의 최초 로그인 시 개인 정보 보호를 위해 화면 잠금 비밀번호를 설정합니다 . 화면 잠금 비밀번호 정책은 EMM 서버에 설정된 정책에 따라 다르게 제한되며 EMM 서버에 설정한 일정 시간 동안 사용자가 단말을 사용하지 않으면 단말의 화면 잠금이 즉시 실행됩니다 . 화면 잠금 비밀번호를 설정하려면 다음의 절차를 따르세요 .

1. 화면 잠금을 위한 비밀번호를 입력하세요.
   - 비밀번호 입력란에 영문, 숫자, 특수 문자, 대문자 등을 혼용하여 최소 6자 최대 20자의 비밀번호를 입력하세요.
   - 비밀번호 정책은 EMM 관리자 포털에서 설정한 비밀번호 정책에 따라 변경될 수 있습니다.
2. 비밀번호를 다시 한번 입력한 후, **설정**을 탭하세요.

Note: 화면 잠금 비밀번호 입력 시, 연속 5회 동안 비밀번호를 잘못 입력하면 다음 중 하나의 통제 동작이 실행됩니다. 해당 내용은 EMM 정책에 따라 다를 수 있습니다.
- 통제하지 않습니다.
- 단말 잠금을 실행합니다.
- 단말을 공장 초기화합니다.
- EMM 잠금을 실행합니다.

자동 설치 애플리케이션 확인하기

EMM 애플리케이션 설치

EMM 에 로그인 시 설치가 필요한 EMM 애플리케이션이 있는 경우 알림 팝업이 나타납니다 . 확인을 탭하면 해당 애플리케이션이 자동으로 설치됩니다 . 또한 설치해야 할 EMM 애플리케이션이 여러 개인 경우 순서대로 자동 설치됩니다 .

필수 애플리케이션 설치하기

EMM 에 로그인 시 운영자가 관리자 포털에서 등록한 필수 애플리케이션이 있는 경우 알림 메시지가 표시되며 해당 애플리케이션이 자동으로 설치됩니다 . 또한 설치해야 할 필수 애플리케이션이 여러 개인 경우 순서대로 자동 설치됩니다 .

Note:
- 애플리케이션의 경우 관리자 포털의 설정에 따라 삭제가 불가능할 수 있습니다.
- Kiosk 모드가 적용된 경우, 필수 앱 설치 완료 후 Kiosk 모드가 실행됩니다.

EMM 홈 살펴보기

Android, iOS 단말의 경우

EMM 을 실행하면 다음과 같이 EMM 홈이 나타납니다 .

Android 플랫폼의 삼성 단말인 경우 , 운영자가 단말 관리 프로파일에 Knox 컨테이너를 등록한 경우 하단의 **KNOX 컨테이너 설치**가 표시됩니다 .

EMM 홈 중앙에는 현재 사용자 ID 와 단말의 모델 정보가 표시됩니다 .

홈 화면 하단에는 EMM 의 앱 스토어를 통하여 설치한 앱이 있는 경우 아이콘들이 나타나며 , 애플리케이션 관련 자세한 내용은 16 페이지의 "4 애플리케이션 활용하기 " 를 참고하세요 .

Note: Knox 사용자의 경우 홈 하단의 **Knox 컨테이너 설치**를 탭하여 Knox를 설치할 수 있으며, Knox 사용자가 아니면 홈 하단에 **Knox 컨테이너 설치** 버튼은 나타나지 않습니다. 또한, 루팅된 삼성 단말의 경우, Knox 스펙에 의해 Knox 컨테이너가 설치되지 않습니다.

- 운영자의 설정에 따라 Knox 컨테이너 설치 알림이 단말의 알림바에 나타납니다. Knox 컨테이너가 설치되면 알림 메시지는 사라집니다.
- Knox 컨테이너 알림의 삭제 가능 여부는 관리자의 설정에 따라 다릅니다.

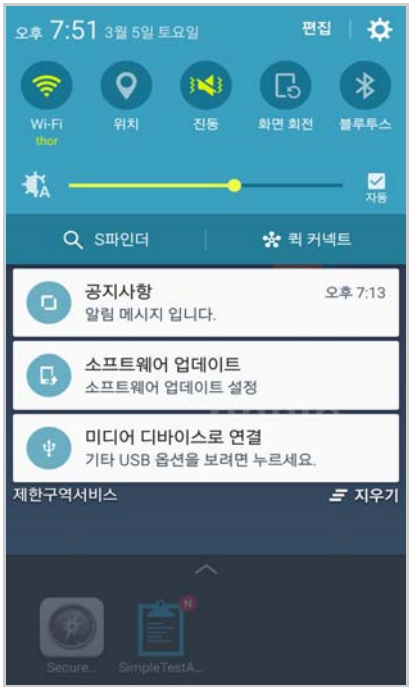
Windows10 단말의 경우

EMM 을 실행하면 다음과 같이 EMM 홈이 나타납니다 .

- **화면 잠금**: 탭하면 즉시 단말이 잠금 상태가 되며, 화면잠금 비밀번호 입력 시 잠금이 해제됩니다.
- **공지사항**: EMM 관리자가 게시한 공지 사항을 확인할 수 있습니다.
- **서비스데스크**: 고객 지원 관련 전화번호와 이메일 안내를 하며 단말에서 발생한 오류를 관리자에게 보내는 로그 전송 기능을 제공합니다.
- **설정**: EMM 화면 잠금 비밀번호의 변경을 할 수 있습니다.
- **ABOUT**: 현재 EMM 버전과 오픈소스 라이선스를 확인할 수 있으며 EMM의 새로운 버전이 있을 시 하단의 업데이트 버튼을 이용하여 업데이트를 할 수 있습니다.

관리자의 알림 메시지

EMM 서버에서 사용자의 단말로 알림 메시지를 전송하면 , 다음과 같이 단말의 알림바에 알림 메시지가 표시됩니다 .



사이드 메뉴 살펴보기

EMM 홈 좌측상단의 ☰ 을 탭하면 사이드 메뉴가 보입니다 . Knox Manage 에서 제공되는 메뉴는 다음과 같습니다 .

단 , Windows10 단말의 경우 사이드 메뉴의 내용을 홈 화면에서 제공합니다 .

- 기본 정보: 접속한 사용자 ID/모바일 ID가 조회되며, ⌄를 탭하면 Tenant ID와 접속 서버 정보가 조회됩니다.
- **공지사항**: 운영자가 게시한 공지 사항을 확인할 수 있습니다.
- **정책보기**: 사용자 단말에 적용된 단말의 전체 정책 목록을 확인할 수 있습니다.
- **앱 스토어**: EMM에서 제공하는 사내 애플리케이션과 외부 애플리케이션 목록을 조회하고, 선택한 애플리케이션을 다운로드 받아 설치할 수 있습니다. 자세한 내용은 16페이지의 " 앱 스토어 사용하기"를 참고하세요.

  Note:
  - Knox 사용자의 경우 Knox 컨테이너 안의 EMM에서 앱 스토어를 사용할 수 있습니다.
  - Android for Work을 사용하거나, 삼성그룹용 EMM의 경우 EMM의 앱 스토어는 제공하지 않습니다.

- **설정 내려 받기**: Android 단말에만 적용되는 메뉴이며, 운영자가 배포한 Wi-Fi, VPN, Exchange 등의 보안 환경을 설치할 수 있습니다. EMM 홈 우측상단의 ⬇ 을 탭하여도 동일한 기능의 메뉴로 이동합니다. 자세한 내용은 15페이지의 " 설정 내려 받기"를 참고하세요.
- **설정**: EMM 관련 알림의 설정, 화면 잠금 비밀번호의 변경 및 서비스 해지를 할 수 있습니다. Knox영역의 EMM인 경우 화면 잠금 비밀번호의 변경만 가능하며, iOS 단말의 EMM의 경우 서비스 해지를 제공하지 않습니다.
- **서비스 데스크**: 서비스 데스크 전화번호와 이메일 안내를 하며 단말에서 발생한 오류를 관리자에게 보내는 로그 전송 기능을 제공합니다.
- About: 현재 EMM 버전과 오픈소스 라이선스를 확인할 수 있으며 EMM의 새로운 버전이 있을 시 하단의 업데이트 버튼을 이용하여 업데이트를 할 수 있습니다.

서비스 설정하기

사이드 메뉴의 **설정**은 이벤트 정책 적용 관련 알림을 설정하는 부분과 화면잠금 비밀번호를 변경하는 부분 , 서비스를 해지할 수 있는 부분으로 이루어져 있습니다 . 화면 잠금 기능은 관리자 포털의 정책 설정에 따라 제어 여부가 결정됩니다 .

- **이벤트 알림**: **이벤트 적용 시 알림 허용**과 **이벤트 해제 시 알림 허용** 중 On으로 설정한 옵션은 알림을 받고 Off로 설정한 옵션은 알림을 받지 않습니다. **이벤트 알림 삭제 금지**를 On으로 설정한 경우 Android 단말에서 이벤트관련 알림을 쓸어넘겨 지울 수 없으며 알림바에 고정되며, iOS 단말에서는 앱 내부의 상단에 5초간 알림을 보여줍니다.
- **화면잠금**: 기 설정되어 있는 화면잠금 비밀번호를 변경하여 설정할 수 있습니다.

- **비활성화**: 서비스 비활성화 코드를 입력하여 EMM 서비스를 해지할 수 있습니다. 서비스 비활성화 코드는 관리자가 제공하는 정보이며, 코드가 유효하지 않은 경우, 에러 메시지가 나타나므로 반드시 관리자에게 재문의합니다.

  Note: 관리자 설정에 따라 EMM 서비스 비활성화 시에 EMM에서 관리되는 앱이 사용자의 단말에서 자동 삭제될 수 있습니다.

서비스 데스크 정보 확인 및 로그 전송하기

사이드 메뉴의 **서비스 데스크**에서는 EMM 관련 지원을 받을 수 있는 이메일과 전화 연결을 안내합니다 . 또한 로그 전송은 사용자가 EMM 사용 중 문제가 발생할 경우 문제 해결을 위해 서버로 로그를 보내는 기능입니다 . EMM 서버로 전송된 로그는 관리자가 확인 후 조치를 취하게 됩니다 . 단 , 로그가 수집되지 않은 경우 , 로그 전송이 불가능할 수 있습니다 .

버전 정보 확인 및 업데이트하기

사이드 메뉴의 **About** 에서는 EMM 의 현재 버전 정보를 확인하고 업데이트 버전이 있는 경우 하단에 업데이트 버튼이 나타납니다 .

- 개인정보 취급방침를 탭하면 회사의 개인정보 취급방침관련 사이트로 이동할 수 있습니다.
- 오픈소스 라이선스를 탭하면 EMM Client 및 Agent 등에서 사용되는 Open Source 에 대한 라이선스 공지 내용을 확인할 수 있습니다.
- Restricted Rights를 탭하면 제한권에 대한 설명을 확인할 수 있습니다.

Note: EMM 버전 1.2.0부터는 EMM서버에 등록된 라이선스에 따라 단말에 고보안 또는 일반보안 기능이 적용됩니다. 예를 들어 기존의 고보안 버전(1.1.0, 1.1.3)에서 업데이트할 경우 사용자의 단말에는 고보안 기능이 적용되며, 일반보안 버전(1.1.1, 1.1.2)에서 업데이트할 경우 일반보안 기능이 적용됩니다.

화면 잠그기와 정책 새로 받기

EMM 사이드 메뉴 중간에는 **화면잠금**과 **정책 새로 받기** 의 두가지 기능이 있습니다 . 화면 잠금 기능은 관리자 포털의 정책 설정에 따라 제어 여부가 결정됩니다 .

- 관리자가 설정한 일정 시간 이상 단말을 사용하지 않거나, EMM 사이드 메뉴 중간의 **화면잠금**을 탭하고 화면잠금 확인 메시지에 확인을 탭하면 화면이 즉시 잠깁니다.
  - 화면 잠금을 해제하려면 하단의 을 탭하고 화면 잠금 비밀번호를 입력 후 해제를 탭합니다.
  - 화면 잠금 비밀번호의 변경은 사이드 메뉴의 **설정 > 화면 잠금 비밀번호**에서 가능합니다.

- 관리자가 정의한 단말의 정책이 사용자 단말에 적용되지 않았을 경우, EMM 사이드 메뉴 중간의 **정책 새로 받기**를 탭하여 관리자에게 최신 단말 정책을 요청할 수 있습니다.

설정 내려 받기

Android 단말의 경우만 제공하는 보안 환경에 관한 메뉴입니다 . EMM 홈 우측 상단의 을 탭하거나 사이드메뉴의 **설정 내려 받기**를 탭하여 관리자가 배포한 보안 환경 관련 세부내용을 확인하고 설치 혹은 삭제할 수 있습니다 .

사용자는 관리자가 미리 지정해 놓은 설정 항목만 볼 수 있으며 사용자의 단말에 설치된 설정과 미설치된 설정을 구분하여 조회합니다 .

Note:
- 설치된 VPN을 삭제할 경우, 프로파일 제거를 위해 단말을 재부팅해야 합니다.
- Generic VPN의 경우, 개인영역 또는 Knox영역 상관없이 한 단말에 하나의 Generic VPN만 설치할 수 있습니다.

보안 환경 설정 설치, 삭제하기

Android 단말에서 보안 환경 설정을 설치하거나 삭제하려면 다음의 절차를 따르세요 .

1. EMM 홈 우측 상단의 을 탭하거나, 사이드 메뉴의 **설정 내려 받기**를 탭하세요.
2. 설치하려는 항목 우측의 **설치**를 탭하세요.
3. 설치한 항목을 삭제하려면 삭제하려는 항목 우측의 **삭제**를 탭하세요.
   단, 관리자에 의해 삭제 방지로 설정된 항목은 삭제가 불가합니다.

4 애플리케이션 활용하기

EMM 홈 하단에는 EMM 의 앱 스토어를 통하여 설치한 앱 아이콘들이 나타나게 됩니다 . 설치한 애플리케이션이 많은 경우 하단 화면을 위로 쓸어넘겨 추가적인 애플리케이션을 확인할 수 있습니다 .

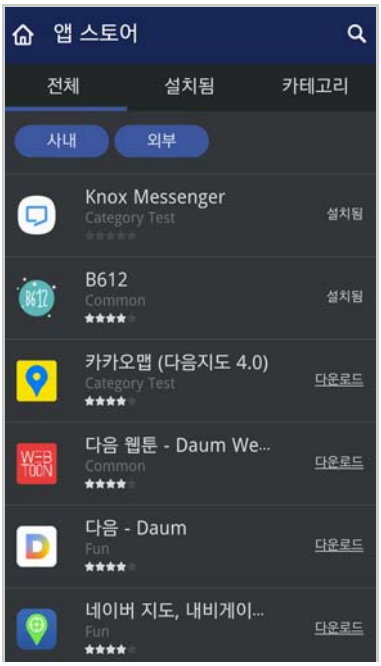
Note:
- Knox를 사용하는 경우 Knox컨테이너의 EMM 앱 스토어를 통해 설치한 애플리케이션을 조회하고 실행할 수 있습니다.
- MDM2.0용 EMM, Windows10, Tizen Wearable 단말용 EMM의 경우 EMM 내의 앱 스토어와 홈 화면 하단의 애플리케이션 아이콘은 제공하지 않습니다

앱 스토어 사용하기

EMM 앱 스토어는 EMM에서 제공하는 사내 애플리케이션과 외부 애플리케이션 목록을 조회하고 , 선택한 애플리케이션을 다운로드 받아 설치하는 기능을 제공합니다 .

애플리케이션 목록보기

EMM 앱 스토어에서 관리하는 사내 애플리케이션 및 외부 애플리케이션 목록 전체를 조회하거나 설치된 애플리케이션 목록을 조회하려면 다음의 절차를 따르세요 .



1. EMM 앱 스토어에 등록된 전체 애플리케이션 목록을 조회하려면 상단의 **전체**를 탭하세요.
   목록에 애플리케이션 명, 카테고리, 별점 등이 조회됩니다.
2. 단말에 설치된 애플리케이션 목록만 조회하려면 **설치됨**을 탭하세요
3. 특정 애플리케이션을 찾으려면 우측 상단의  을 탭한 후 검색란에 검색어를 입력하고  을 탭하세요.
4. 검색하여 찾아낸 애플리케이션을 다운로드하여 설치하기 위해 **다운로드**를 탭하세요. 정책 설정에 따라 앱 다운로드 진행 현황을 확인할 수 있습니다.

사내/외부 애플리케이션 사용하기

전체 애플리케이션 목록 , 설치된 앱 목록 , 또는 카테고리별 앱 목록에서 필터를 사용하여 사내 또는 외부 애플리케이션을 조회할 수 있습니다 .

사내 애플리케이션은 EMM 커넥터와 SDK 를 활용하여 기업내에서 자체적으로 개발한 업무용 모바일 애플리케이션을 의미합니다 . 외부 애플리케이션은 Google Play Store 또는 iOS 의 App Store 와 같이 Public App Store 에 등록된 애플리케이션을 의미하며 외부 애플리케이션 목록에는 관리자가 허용한 외부 애플리케이션만 나타납니다 .

애플리케이션 필터를 사용하여 사내 또는 외부 앱을 조회한 후 설치하려면 다음의 절차를 따르세요 .

1. EMM 앱 스토어에서 사내 앱만 조회하려면, 앱 목록 상단의 **외부**을 탭하여 선택을 해제하세요. 사내 버튼이 파란색으로 표시되면 사내 애플리케이션 목록이 조회됩니다.
   - 애플리케이션 필터는 버튼 형태의 on/off 방식이며 기본 값으로 **사내**와 **외부**가 선택되어 있습니다.
2. 외부 앱만 조회하려면 앱 목록 상단의 **외부**를 탭하여 선택한 후 다시 **사내**를 탭하여 선택을 해제하세요. 외부 버튼이 파란색으로 표시되면 외부 애플리케이션 목록이 조회됩니다.
3. 검색란에 애플리케이션명을 입력한 후 돋보기를 탭하세요.
4. 해당 애플리케이션을 다운로드하여 설치하려면 **다운로드**를 탭하세요.

애플리케이션 상세보기

애플리케이션의 상세 정보를 확인하려면 다음의 절차를 따르세요 .

1. 애플리케이션의 상세 정보(애플리케이션 소개 및 스크린샷)를 확인하려면 애플리케이션 목록에서 애플리케이션을 탭하세요.
   - 상세 정보에서 **다운로드**를 탭하여 애플리케이션을 설치할 수 있습니다.
   - 사용자 단말에 이미 설치된 애플리케이션의 경우 **설치됨**으로 표시되며 업데이트가 필요한 앱은 **업데이트**로 표시됩니다. 상세 화면 하단의 애플리케이션 **스크린샷**을 탭하세요. 스크린샷이 팝업으로 확대됩니다.

- 해당 애플리케이션을 설치한 사용자들의 평점과 평가 사용 후기가 조회됩니다.

2. 애플리케이션 상세보기 좌측 상단의 을 탭하여 이전 상태로 돌아갈 수 있습니다.
   - 애플리케이션 목록 상단의 을 탭하여 EMM 앱 스토어를 종료하고, EMM 홈으로 돌아갑니다.

애플리케이션 사용 후기 사용하기

애플리케이션 사용자는 다른 사용자들의 애플리케이션에 대한 사용 후기를 조회하거나 본인이 직접 애플리케이션을 사용한 후 , 사용 후기를 작성할 수 있습니다 .

애플리케이션 사용 후기 조회와 작성은 사내 애플리케이션의 경우에만 가능합니다 .

애플리케이션 사용 후기를 사용하려면 다음의 절차를 따르세요 .

1. EMM 앱 스토어 상단 **사내** 애플리케이션 필터를 선택한 후 애플리케이션을 탭하세요.
2. 상세 정보 화면에서 사용자들이 등록한 애플리케이션의 사용 후기 및 평점을 조회하세요.
3. 사용 후기를 작성하려면 상세 정보 화면의 **리뷰** 우측의 을 탭한 다음, 사용한 애플리케이션에 대해 별점과 사용 후기를 기록한 후 을 탭하세요.
   작성한 내용이 저장됩니다.
4. 작성한 사용 후기를 취소하려면 리뷰 수정에서 좌측 상단의 을 탭하세요.
   작성이 취소되고 이전 화면으로 이동합니다.

애플리케이션 카테고리 사용하기

애플리케이션 카테고리는 사용자의 필요에 따라 EMM 앱 스토어에 등록된 애플리케이션을 분류하고 분류된 애플리케이션을 검색하기 위한 용도로 사용합니다 .

애플리케이션 카테고리를 사용하려면 다음의 절차를 따르세요 .

1. 카테고리 목록을 조회하기 위해 EMM 앱 스토어 상단 **카테고리**를 탭하세요.
   각 카테고리 목록마다 사용자가 조회 및 설치 가능한 애플리케이션의 개수가 표시됩니다.
2. 각 카테고리를 탭하세요.
   카테고리 별로 등록되어 있는 애플리케이션 목록이 나타납니다.
3. 특정 카테고리에 분류된 애플리케이션을 검색하려면, 카테고리를 탭한 후 검색란에 해당 애플리케이션을 입력하세요.
4. 애플리케이션을 설치하려면 검색하여 찾은 애플리케이션의 **다운로드**를 탭하세요 . 애플리케이션을 다운로드한 후, 설치할 수 있습니다.

애플리케이션 업데이트하기

사용자가 설치한 애플리케이션 중 업데이트가 필요한 경우 , 앱 목록의 우측에 업데이트 버튼이 표시됩니다 . **업데이트**를 탭하여 업데이트를 실행합니다 .

애플리케이션을 업데이트하려면 다음의 절차를 따르세요 .

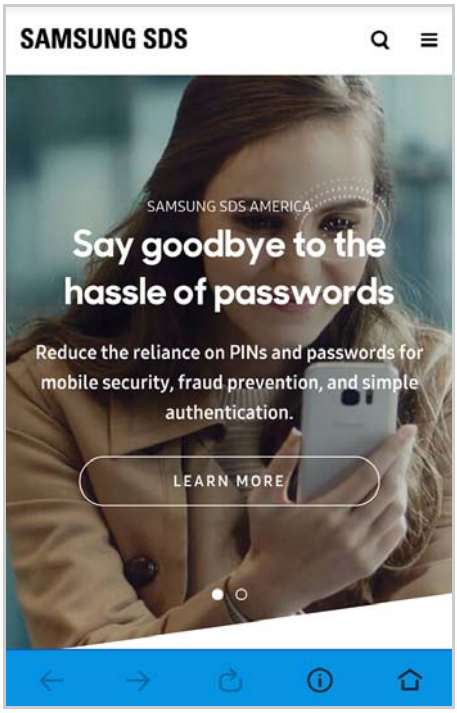
1. EMM 앱스토어 상단의 **설치됨**을 탭하세요.
   단말에 설치된 애플리케이션 목록이 조회됩니다.
2. 애플리케이션 목록 우측에 **업데이트** 버튼을 탭하여 앱별로 업데이트를 진행하거나, 우측 상단의 **모두 업데이트**를 탭하여 전체 앱을 업데이트합니다.
   - 전체 앱 목록 또는 카테고리에서도 업데이트가 가능합니다.

Note: 애플리케이션을 삭제하면 애플리케이션과 관련된 모든 데이터도 함께 삭제됩니다.

Kiosk Browser 사용하기

관리자가 하나의 웹사이트를 고정적으로 이용하도록 사용자 단말에 kiosk 정책을 배포한 경우 이것을 설치한 후에는 단말의 다른 기능은 사용하지 못하고 지정된 웹사이트만을 이용하게 됩니다 . 이를 Kiosk Browser 라고 하며 , 관리자가 해당 정책을 유지하는 동안 사용하게 됩니다 . Kiosk Browser 는 Android 단말에만 제공됩니다 .

단말 유형에 따라 Kiosk browser 화면의 하단 혹은 상단에 나타나는 메뉴에 대한 설명은 다음과 같습니다 .



항목	명칭	설명
	뒤로 가기	이전 페이지로 이동합니다.
	앞으로 가기	다음 페이지를 보여 줍니다.
	새로고침	새로고침을 합니다.
	오픈소스 라이선스	오픈소스 라이선스 고지를 보여준다.
	홈페이지	설정된 홈페이지로 이동 한다.

5 Secure Browser 사용하기

EMM 애플리케이션 중 하나인 Secure Browser 는 URL, JavaScript, 자동 입력 , 보안 경고 표시 , Cache, 쿠키 , Proxy 설정 , 파일 다운로드와 같이 다양한 웹 브라우저의 기능에 보안을 강화한 기업용 웹 브라우저입니다 . Secure Browser 의 다양한 보안 기능들은 모바일에서 뿐만 아니라 태블릿에서도 동일하게 사용할 수 있습니다 .

관리자가 Secure Browser 를 필수 애플리케이션으로 등록하면 , 사용자가 EMM 에 로그인 시 자동으로 Secure Browser 가 설치되며 EMM 홈 하단과 단말 홈에 Secure Browser 가 나타납니다 . 관리자가 Secure Browser 를 필수 애플리케이션으로 등록하지 않으면 Secure Browser 가 제공되지 않습니다 . Android 단말을 기준으로 설명하나 , iOS 단말에서도 동일한 방법으로 사용이 가능합니다 .

홈 화면 및 기본 UI

을 탭하여 Secure Browser 를 실행시키면 Secure Browser 홈이 나타납니다 .

그림 5-1. Secure Browser 홈 (모바일)

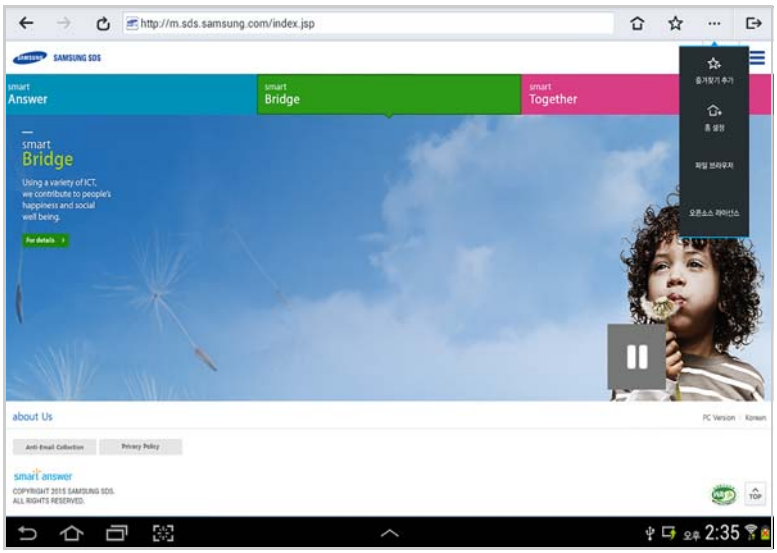


그림 5-2. Secure Browser 홈 (태블릿)

항목	설명
	Secure Browser 홈 상단 좌측의 을 탭하면 설정한 홈으로 이동합니다.
	Secure Browser 홈의 을 탭하면 URL 입력 박스에 로딩된 홈페이지의 Favicon이 나타납니다.
	Secure Browser 홈 상단 우측의 을 탭하면 현재 페이지를 새로 고침합니다.
	페이지를 이동하는 경우 나타나며 을 탭하면 로딩이 취소됩니다.
	페이지 이동으로 로딩시 로딩 상태가 표시됩니다.
	Secure Browser 홈 하단의 을 탭하면 자주 이용하는 웹 페이지를 즐겨찾기에 추가합니다.
	Secure Browser 홈 하단의 을 탭하면 현재 페이지를 홈으로 설정합니다.
파일 브라우저	관리자에 의해 파일 다운로드 권한이 주어진 사용자에게만 보여지는 메뉴입니다. 자세한 내용은 25페이지의 " 파일 브라우저 사용하기"를 참고하세요.
오픈소스 라이선스	Secure Browser에서 사용되는 오픈 소스 라이선스 공지의 내용입니다. 자세한 내용은 28페이지의 " 오픈소스 라이선스 확인하기"를 참고하세요.
	Secure Browser 홈 하단의 을 탭하면 이전 페이지로 이동합니다.
	Secure Browser 홈 하단의 을 탭하면 다음 페이지로 이동합니다.
	Secure Browser 홈 하단의 을 탭하면 현재 페이지를 새로고침합니다.
	Secure Browser 홈 하단의 을 탭하면 즐겨찾기로 이동합니다.
	Secure Browser 홈 하단의 을 탭하면 더보기 메뉴가 나타납니다.
	Secure Browser 홈 하단의 을 탭하면 Secure Browser를 종료합니다.

즐겨찾기 관리하기

자주 사용하는 URL 주소를 즐겨찾기에 등록하여 관리할 수 있습니다 .

즐겨찾기 추가하기

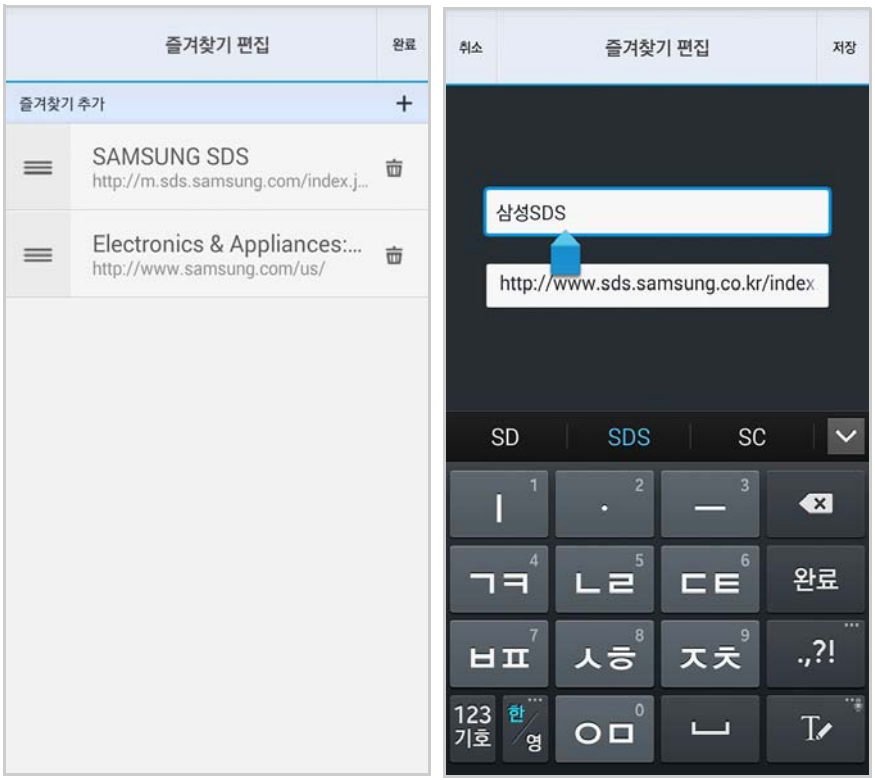
자주 사용하는 URL 주소를 즐겨찾기에 추가하려면 다음의 절차를 따르세요 .

1. 즐겨찾기로 이동하기 위해 Secure Browser 홈 하단의 ⋯을 탭한 후, ☆+을 탭하세요.
   - 또는즐겨찾기로 이동하기위해 Secure Browser 홈 하단의 ☆을 탭하세요. 화면 상단의 **편집**을 탭한 **다음**, ＋를 탭하세요.
2. 즐겨찾기로 추가하려는 URL주소와 이름을 입력하세요.
   - 즐겨찾기 이름은 50자까지 입력 가능합니다.
3. 저장하려면 상단 우측의 **저장**을 탭하세요.

Note: 즐겨찾기 등록이 실패하는 경우, 실패 안내 메시지가 나타나며 **확인**을 탭하면 즐겨찾기 추가 화면으로 다시 돌아갑니다. 만약 계속하여 실패하는 경우 관리자에게 문의하시기 바랍니다.

즐겨찾기 편집하기

즐겨찾기에 등록된 URL 주소를 편집하려면 다음의 절차를 따르세요 .



1. 즐겨찾기 편집으로 이동하기 위해 즐겨찾기 우측 상단의 **편집**을 탭하세요.

2. 즐겨찾기 편집에서 ☰ 을 탭한 후, 끌어다 놓아 우선순위를 변경하세요.
3. 즐겨찾기 목록을 탭하여 즐겨찾기 수정으로 이동한 후, 즐겨찾기 이름과 URL 주소를 입력하세요.
   - 즐겨찾기 편집에서는 즐겨찾기 이름만 변경할 수 있으며 URL주소를 수정하려면 삭제한 후, 다시 등록해야 합니다.
4. 편집을 종료하려면 화면 상단 우측의 **완료**를 탭하세요.

즐겨찾기 삭제하기

즐겨찾기에 등록된 URL 주소를 삭제하려면 다음의 절차를 따르세요 .

1. 즐겨찾기로 이동하기 위해 Secure Browser 홈 하단의 ☆ 을 탭하세요.
2. 등록된 즐겨찾기를 삭제하려면 즐겨찾기 우측의 🗑 을 탭합니다.
3. 삭제 확인 메시지가 나타나면 **확인**을 탭합니다.
4. 종료하려면 상단 우측의 **완료**를 탭하세요.

Note: 즐겨찾기 삭제가 실패하는 경우, 삭제 실패 안내 메시지가 나타나며 **확인**을 탭하면 즐겨찾기 삭제 화면으로 다시 돌아갑니다. 만약 계속하여 실패하는 경우 관리자에게 문의하시기 바랍니다.

Secure Browser 홈 설정하기

Secure Browser 홈을 설정하려면 다음의 절차를 따르세요 .

1. Secure Browser 홈 하단의 ... 을 탭한 후, ⌂+ 을 탭하세요.

2. 다음의 두가지 방법 중 하나로 홈 화면을 설정하세요.
   - Secure Browser 홈을 빈 페이지로 설정하려면 **빈 페이지**를 선택하세요.
   - Secure Browser 홈을 특정 URL주소로 입력하려면 **URL 입력**을 선택한 후, 아래 입력란에 URL주소를 입력하세요.
3. 저장하려면 상단 우측의 **저장**을 탭하세요.
   - Secure Browser에서 허용하지 않는 URL주소를 홈으로 설정하는 경우, 차단 안내 메시지가 나타나고 등록되지 않습니다.

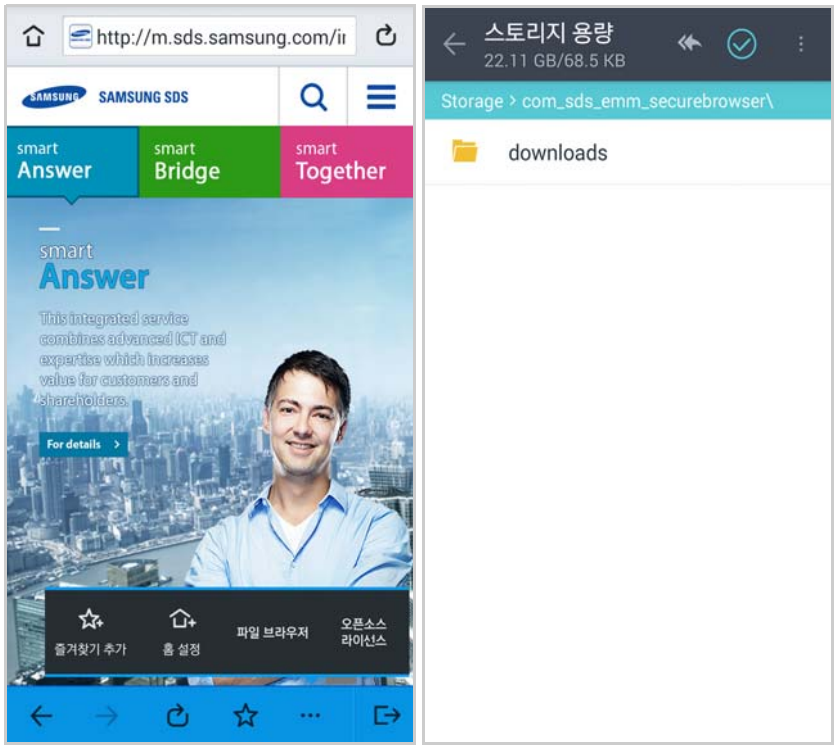
파일 브라우저 사용하기

파일 브라우저는 관리자에 의해 파일 다운로드 권한이 허용된 사용자에게만 보여지는 메뉴입니다 . 파일 다운로드 권한이 있는 사용자는 Secure Browser 를 통해 다운로드 받은 파일을 관리할 수 있습니다 .

Note:
- Secure Browser가 Knox 내부에 설치된 경우, 파일 브라우저 메뉴 선택 시 Android에서 제공하는 기본 파일 브라우저가 실행됩니다.
- 파일 브라우저는 Android 단말만 지원합니다.

파일 브라우저 살펴보기

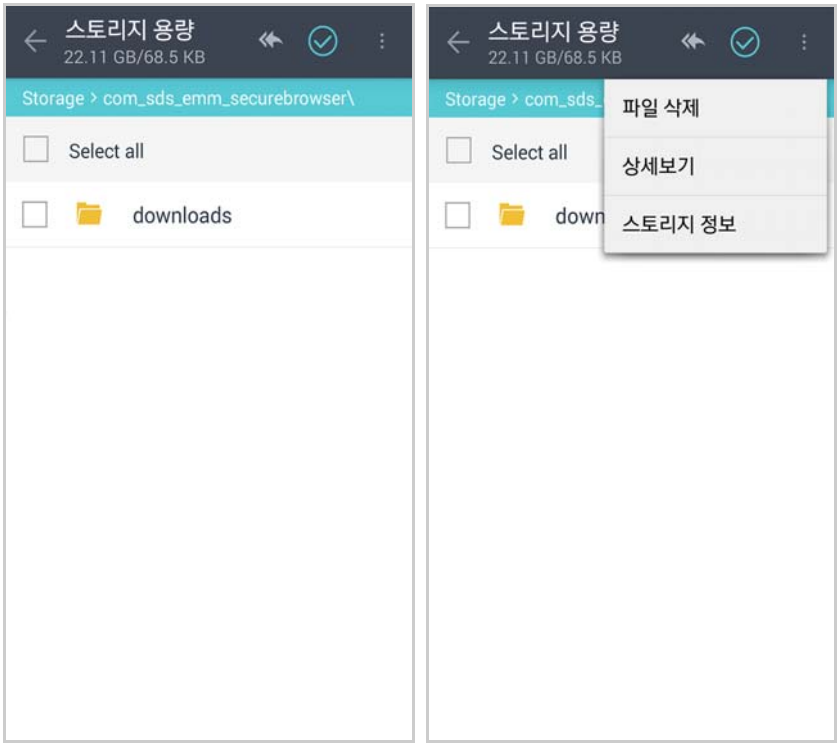
Secure Browser 홈 하단의 ...을 탭한 후 , **파일 브라우저**를 탭합니다 .



항목	설명
	파일 브라우저 상단 좌측의 을 탭하면 파일 브라우저가 종료됩니다.
	파일 브라우저 상단 우측의 을 탭하면 상위 폴더로 이동합니다.
	파일 브라우저 상단 우측의 을 탭하면 편집 모드로 이동합니다.
	파일 브라우저 상단 우측의 을 탭하면 더보기가 나타납니다.

파일 브라우저의 파일 및 폴더 관리하기

Secure Browser 를 통해 다운로드 받은 파일을 관리하려면 다음의 절차를 따르세요 .

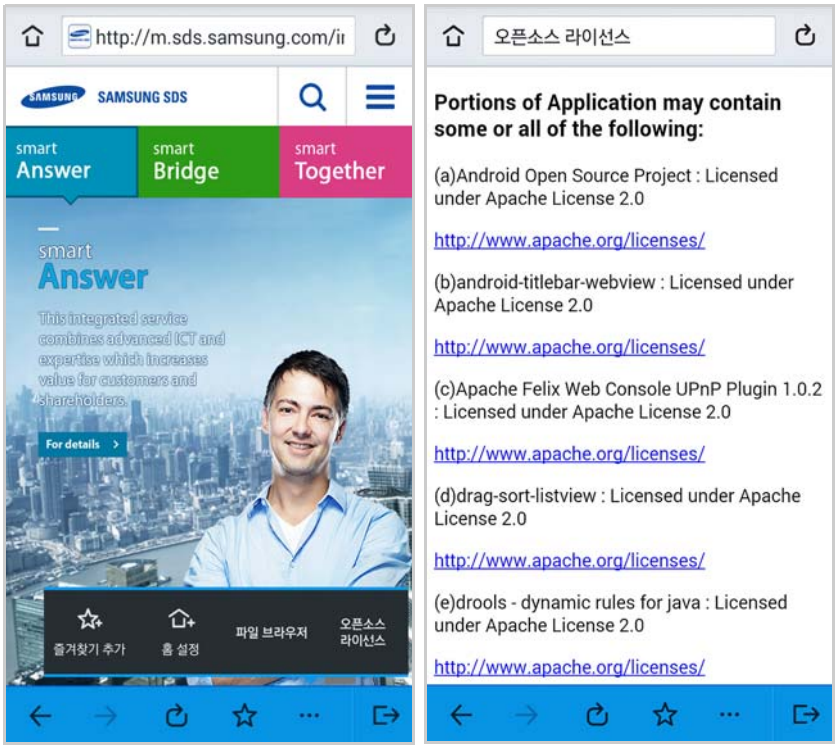


1. Secure Browser 홈 하단의 ...을 탭한 후, **파일 브라우저**를 탭하세요.
2. 파일 브라우저의 파일 및 폴더를 관리하려면 상단 우측의 을 탭하세요.
   을 탭하면 파일 브라우저 편집 모드로 전환되며 폴더에 체크박스가 나타납니다.
3. 를 탭하세요.
   Secure Browser를 통해 다운로드 받은 파일을 관리하기 위해 삭제, 상세보기 및 스토리지 정보 확인을 할 수 있습니다.

Note: Secure Browser를 통한 파일 다운로드는 EMM 정책에 따라 다를 수 있으므로 관리자에게 문의하시기 바랍니다.

오픈소스 라이선스 확인하기

오픈소스 라이선스는 Secure Browser 에서 사용되는 Open Source 에 대한 라이선스 공지의 내용입니다 . 오픈소스 라이선스를 확인하려면 다음의 절차를 따르세요 .



1. Secure Browser 홈 하단의 ...을 탭한 후, **오픈소스 라이선스**를 탭하세요.
2. 종료하려면 ←을 탭하세요.

심플 브라우저 사용하기

심플 브라우저 모드는 Secure Browser 상단에 URL 주소 입력창이 없어 사용자가 URL 을 입력하여 다른 웹 페이지로 이동할 수 없는 모드입니다 . 사용자에게 제공되는 URL Link 를 클릭하는 경우 해당 페이지에만 실행되며 , Secure Browser 아이콘을 탭하는 경우 홈 페이지 URL 로 설정한 페이지만 실행됩니다 .

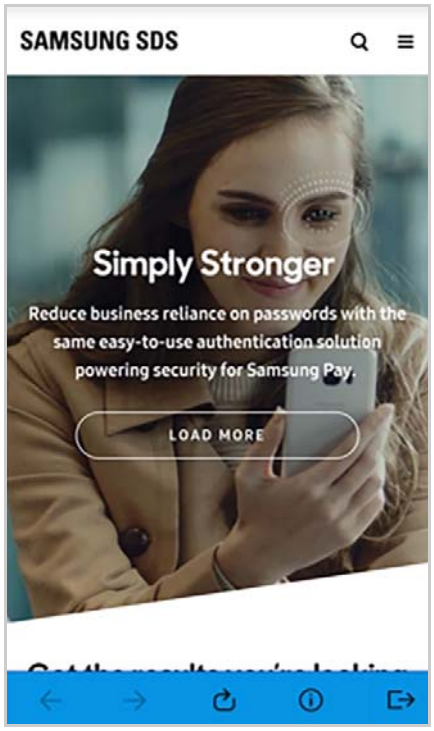
심플 브라우저를 사용하려면 관리자 포털에서 **프로파일 > 앱 관리 프로파일**로 이동하여 Secure Browser 에서 **Tiny Mode 사용**을 선택한 후 정책을 단말에 적용합니다 .
관리자에 의해 심플 브라우저 사용 권한이 허용되는 사용자에게는 홈 버튼 , URL 주소창 , 즐겨찾기 추가 , 파일 브라우저 메뉴가 나타나지 않습니다 .

Note:
- 심플 브라우저는 Android 단말만 지원합니다.
- 심플 브라우저 사용 시, 파일 다운로드는 불가합니다.

심플 브라우저 살펴보기

다음은 심플 브라우저 모드 상태에서 Secure Browser 를 실행한 화면입니다 .

하단의 메뉴 설명은 다음과 같습니다 .



항목	설명
	Secure Browser 홈 하단의 을 탭하면 이전 페이지로 이동합니다.
	Secure Browser 홈 하단의 을 탭하면 다음 페이지로 이동합니다.
	Secure Browser 홈 하단의 을 탭하면 현재 페이지를 새로고침합니다.
	Secure Browser에서 사용되는 오픈 소스 라이선스 공지의 내용입니다. 자세한 내용은 28페이지의 " 오픈소스 라이선스 확인하기"를 참고하세요.
	Secure Browser 홈 하단의 을 탭하면 Secure Browser를 종료합니다.

6 SecuCamera 사용하기

SecuCamera 는 기본 카메라 기능인 화면 확대 또는 축소 , 포커스 등과 같이 카메라 기능에 보안을 강화한 기업용 카메라 애플리케이션입니다 .
카메라 사용이 금지된 사용자의 단말에서 Secure Camera 를 실행하여 사진을 촬영할 수 있습니다 . 촬영된 이미지는 EMM 관리자 포털에 등록된 이메일로 전송되어 회사 정보를 보호할 수 있습니다 .
관리자가 SecuCamera 를 EMM 애플리케이션으로 등록한 후 앱 정책을 배포하면 , SecuCamera 가 자동으로 설치됩니다 .

다음 조건에서 SecuCamera 앱이 정상적으로 실행되고 , 그외에는 SecuCamera 앱이 실행되지 않거나 종료됩니다 .

SecuCamera 가 정상적으로 실행되려면 다음의 조건을 만족해야 합니다 .

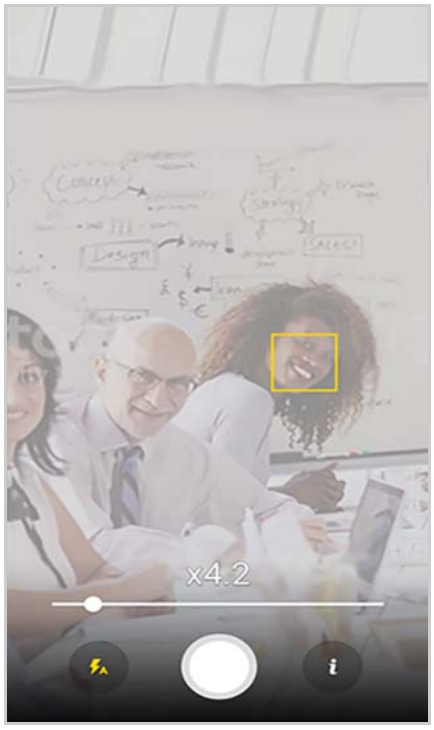
- 단말 OS가 Android KitKat 이상인 경우
- SecuCamera 설치 시 앱 권한에 동의한 경우
- 사용자 단말 H/W에 카메라가 있는 경우
- 네트워크 사용이 가능한 경우
- EMM이 활성화된 경우
- EMM 관리자 포털의 사용자 정보에 SecuCamera 사용으로 등록된 경우
- SecuCamera 라이선스가 있으며, 사용자 라이선스 수를 초과하지 않은 경우
- SecuCamera를 사용할 수 있는 이벤트 정책이 사용자 단말에 배포된 경우

Note: SecuCamera로 촬영이 가능할때도 단말에서 사용하는 다른 카메라 애플리케이션은 보안 정책에 따라 촬영이 불가능합니다.

SecuCamera 실행하기

EMM Client 실행 시 자동으로 다운로드 된 SecuCamera 를 실행합니다 .

다음의 이미지는 SecuCamera 가 정상적으로 실행된 화면입니다 .



1. EMM 앱 내부 또는 단말의 홈 화면의 을 클릭하여 SecuCamera를 실행하세요.
2. **앱 접근 권한**에 대한 안내를 확인 후 **다음**을 클릭하세요.
3. SecuCamera가 실행 화면에서 포커스를 맞추거나, 플래쉬를 조정한 후 을 탭하세요.
   - 카메라 기능에 대한 자세한 사항은 32페이지의 " SecuCamera 기능"을 참고하세요.
4. SecuCamera로 찍은 사진의 화질을 선택한 후, **전송**을 클릭하세요.
   촬영된 데이터는 단말에 저장되지 않고, EMM 관리자 포털에 등록된 사용자의 이메일로 전송됩니다.
   - 화질
     - 원본화질: 카메라 H/W 최대 pixel (JPEG 품질 90%)
     - 일반화질: 원본 화질의 품질 70%
   - 파일명 규칙
     - [SecuCam]사용자이메일_YYYYMMDDHHMMSS.jpeg

Note: 이메일로 사진 전송이 실패하는 경우, 실패 안내 메시지가 나타나며 **다시찍기** 또는 **재전송**을 선택할수 있습니다. 만약 계속하여 실패하는 경우 EMM 관리자에게 문의하시기 바랍니다.

SecuCamera 기능

항목	설명
플래쉬 동작	플래쉬 세가지 모드 지원 • on: 사진 촬영시 항상 플래쉬가 켜진 상태로 동작 • off: 사진 촬영시 플래쉬가 꺼진 상태로 동작 • Auto: 사진 촬영시 주위 환경의 밝기에 따라 자동으로 플래쉬가 on/off으로 동작
포커스	사진의 촛점을 맞추는 기능을 자동 또는 수동으로 지원 • 수동: 원하는 특정 영역을 클릭하여 해당 부분에 포커스를 맞춤 • 자동: 특정 영역을 클릭하지 않으면 자동으로 포커스를 맞춤 - 노란 박스: 화면 포커스가 정상적으로 맞춰진 경우 - 빨간 박스: 화면 포커스를 맞추지 못한 경우
화면 확대/축소	촬영시 화면에서 손가락을 펴거나 오므려서 확대/축소 가능 • 확대 배율: 0~7배 까지 지원 • 확대 배율이 1이상이면 Scroll bar 생성됨

SecuCamera 서비스 정보 확인하기

사용자는 SecuCamera 앱 정보 , 오픈소스의 라이선스를 확인할 수 있습니다 .

SecuCamera 앱 정보를 확인하려면 다음 절차를 따르세요 .

1. SecuCamera 하단의 을 탭한 후, 서비스 정보에서 확인하려는 항목을 탭하세요.

- **서비스 데스크**: 서비스 데스크의 전화번호와 이메일을 안내합니다.
- **로그 보내기**: SecuCamera의 로그를 Secure Camera 서버로 전송합니다.

- **오픈소스 라이선스**: SecuCamera에서 사용되는 오픈 소스에 대한 라이선스 고지 내용을 확인합니다.

2. 종료하려면 을 탭하세요.

7 Wearable EMM 사용하기

삼성전자 웨어러블 단말에서 Samsung SDS EMM 을 사용할 수 있습니다 . 웨어러블 단말에서 EMM 로그인 시 단말 정책이 즉시 적용되며 , 필수 애플리케이션 설치 기능을 제공합니다 . 또한 EMM 은 Tizen Push 를 통해 실시간으로 단말 사용 제어를 위한 정책을 EMM 서버로부터 전송 받습니다 .

Wearable EMM 로그인하기

Wearable EMM 에 로그인을 하려면 EMM 서버 정보와 인증 코드를 입력합니다 . 웨어러블 단말에서 EMM 서버 정보를 간편하게 입력하기 위해서는 단축 URL 사용을권장합니다 . 최초 로그인은 Tenant ID 를 서버에서 확인해야 하므로 로그인 소요 시간이 평소보다 오래 걸릴 수 있습니다 . 로그인 시 필수 입력 정보는 SMS 메시지 또는 이메일로 전달됩니다 . Wearable EMM 에 로그인하려면 다음의 절차를 따르세요 .

1. EMM을 실행하기 위하여 사용자 웨어러블 단말에 설치된 SDS EMM 아이콘을 탭하세요. 또는 EMM 위젯을 등록한 후 위젯을 탭하세요.
2. 서비스 URL 타입을 선택하고 **접속 URL**을 입력한 후 **다음**을 탭하세요.
   - 자동 입력: 관리자 포털에서 EMM 설치 정보를 발송하면 웨어러블 단말에 수신된 SMS 메시지에서 정보를 추출하여 EMM 설치 URL이 자동으로 입력됩니다.
   - 수동 입력: SMS 메시지 수신이 불가한 경우, 이메일 등 기타 경로로 전달된 **접속 URL**을 직접 입력하세요.
     - 서비스 URL 타입을 선택한 후 '/'뒤의 상세 주소만 입력하거나, **Manual**로 선택한 후 전체 URL 주소를 입력하세요.
       예) EMM 설치 URL이 https://goo.gl/7VgJuk인 경우, **서비스 URL 타입**을 **goo.gl**으로 선택하고 아래 입력란에는 **7VgJuk**만 입력하세요.

3. 관리자로부터 전달받은 8자리 인증 코드를 입력하고 **LOGIN**을 탭하세요.
   인증 코드 입력 실패 등으로 인증 코드 재발급이 필요하면 사용자가 재발급 받거나 관리자에게 문의하세요. 재발급 방법에 대한 자세한 내용은 35페이지의 " Wearable EMM 인증 코드 생성하기"를 참고하세요.
   - 자동 입력: 웨어러블 단말에 수신된 EMM 설치 정보 SMS 메시지에서 정보를 추출하여 EMM 인증 코드가 자동으로 입력됩니다.

4. 최종 사용자 라이선스 동의서를 읽은 후 ☑를 탭하세요.
5. Knox 라이선스 안내가 나타나면 맨 아래 끝까지 스크롤하여 **동의**를 선택한 후, **확인**을 탭하세요.

Note:
- EMM에 로그인 하려면 관리자가 사용자와 단말 정보를 관리자 포털에 미리 등록해야 합니다.
- SMS 메시지 수신이 불가한 웨어러블 단말은 수동 입력으로만 로그인이 가능합니다.

Wearable EMM 인증 코드 생성하기

Wearable EMM 로그인 시 인증 코드 입력 실패 횟수를 초과하거나 유효 기간이 지나면 관리자에게 인증 코드 재발송을 요청하거나 사용자가 직접 인증 코드를 재발급 받습니다 . 인증 코드 생성을 위한 정보는 설치 시에 전달된 SMS 메시지 또는 이메일에 존재합니다 . 인증 코드를 재발급받으려면 다음의 절차를 따르세요 .

1. SMS 메시지 또는 이메일로 전달된 **인증코드 발급 URL(OTP URL)**을 인터넷 브라우저에서 입력하세요.
2. 관리자로부터 전달받은 **회사명(Tenant ID)**, **사용자 ID**, **비밀번호**, **모바일 ID**를 입력한 후 **발급**을 클릭하세요.
3. 발급받은 8자리 인증 코드를 Wearable EMM 로그인 화면에 입력하세요.

화면 잠금 비밀번호 설정하기

관리자 포털의 Tizen Wearable 정책에 따라 화면 잠금 비밀번호를 설정합니다 . 화면 잠금 비밀번호 정책은 관리자 포털에 설정된 정책에 따라 다르게 제한됩니다 . 화면 잠금 비밀번호를 설정하려면 다음의 절차를 따르세요 .

1. 화면 잠금을 위한 비밀번호를 입력하세요.
   - 비밀번호 입력란에 PIN 또는 영숫자를 혼용하여 최소 0자 최대 20자의 비밀번호를 입력합니다.
   - 비밀번호 정책은 관리자 포털에서 설정한 비밀번호 정책에 따라 변경될 수 있습니다.
2. 비밀번호를 다시 한번 입력한 후, **설정**을 탭하세요.

Note: 화면 잠금 비밀번호 입력 시, 관리자 포털에 설정된 **비밀번호 입력 실패 허용 횟수** 이상으로 비밀번호를 잘못 입력하면 공장 초기화가 실행됩니다.

자동 설치 애플리케이션 설치하기

EMM 에 로그인 시 관리자가 EMM 서버에서 등록한 필수 애플리케이션이 있는 경우 알림 메시지가 표시되며 해당 애플리케이션이 자동으로 설치됩니다 . 또한 설치해야할 필수 애플리케이션이 여러 개인 경우 순서대로 자동 설치됩니다 .

Note:
- 자동 설치 애플리케이션의 경우 EMM 관리자의 설정에 따라 삭제가 불가능할 수 있습니다.
- 앱을 자동 설치하려면 Tizen 2.3.2.3 버전 이상 기기 환경과 앱에 대한 Stub API 권한이 있어야합니다. 두가지 조건을 만족시키지 않으면 수동 설치가 진행됩니다.

Wearable EMM 홈 살펴보기

웨어러블 단말에서 EMM 앱에 진입하는 방법에는 위젯을 등록하여 선택하는 방법과 앱 보기에서 직접 EMM 아이콘 을 선택하는 방법이 있습니다 . 좌측의 위젯 화면을 탭하면 우측의 Wearable EMM 홈 화면이 나타납니다 .

그림 7-1. Wearable EMM 위젯(좌)과 홈 화면(우)

Wearable EMM 위젯에는 단말 상태가 조회되고 홈 중앙에는 단말 상태 , 사용자 ID 정보가 조회됩니다 .

- **단말 정책 확인하기**: 단말 정책 중에 GPS와 NFC 정책의 적용 여부가 조회되며, 금지된 정책은 슬래쉬 아이콘으로 표시됩니다.
- **Wi-Fi Quick Link**: 홈 화면의 우측 을 탭하면 **Setting > Wi-Fi Setting**으로 이동합니다.

웨어러블 단말 설정하기

홈 화면에서 을 탭하면 **Setting** 으로 이동합니다 . 화면에서 스크롤 또는 물리 베젤을 회전시킨 후 하위 메뉴를 탭합니다 .

- **Wi-Fi Setting**: 웨어러블 단말의 Wi-Fi 설정 메뉴로 이동하기 위한 바로가기를 제공합니다.
- **Device Log**: 사용자가 Wearable EMM 사용 중 문제가 발생한 경우 문제 해결을 위해 서버로 단말의 로그를 보내는 기능입니다. **OK**를 탭한 후, 를 탭하여 단말의 로그를 전송합니다.
- **Account**: 사용자 ID, 모바일 ID, EMM 버전을 확인합니다.
- **Deactivcation**: 서비스 비활성화 코드를 입력하여 Wearable EMM 서비스를 해지할 수 있습니다. 서비스 비활성화 코드는 관리자가 제공하는 정보이며, 코드가 유효하지 않은경우, 에러 메시지가 나타나므로 반드시 관리자에게 재문의합니다.
- **Open source Licenses**: 오픈 소스 라이선스를 확인합니다.
- **Restricted Rights**: 소프트웨어 사용권 제약 사항을 확인합니다.

단말 잠김 해제하기

EMM 관리자는 사용자의 단말을 잠그기 위해 단말 제어 명령을 전송할 수 있습니다 .

EMM 정책으로 단말이 잠긴 경우 , 잠김을 해제하려면 다음의 절차를 따르세요 .

1. 관리자에게 사용자 ID와 단말 ID로 단말의 잠김을 문의하세요.
2. 관리자 포털에서 생성된 랜덤 4자리 숫자를 전달받아 화면 잠금을 해제하세요. 단말 해제 코드는 단말 잠금 제어 전송 시에 재생성됩니다.
3. 웨어러블 단말에서 **설정 > 화면잠금 > 사용 안함**으로 설정하세요.

8 EMM 원격지원 받기

EMM 원격 지원 서비스는 사용자의 요청에 의해 사용자 단말 화면을 공유하며 원격으로 지원 받는 것으로 일반 보안 라이선스에서만 가능합니다 . 본 서비스는 직접 사용자의 단말 화면을 공유하여 볼 수 있기 때문에 문의사항에 대하여 보다 정확하고 신속하게 지원 받을 수 있습니다 .

원격 지원 설치하기

지원 단말 플랫폼

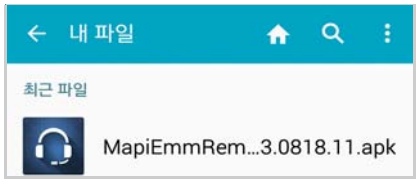
권장하는 단말의 플랫폼은 다음과 같습니다 .

- Android 4.4(Kitkat) 이상의 삼성 갤럭시 단말

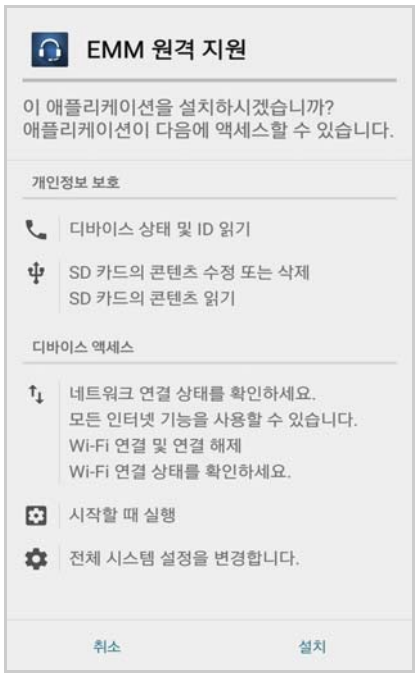
모바일 Agent 설치

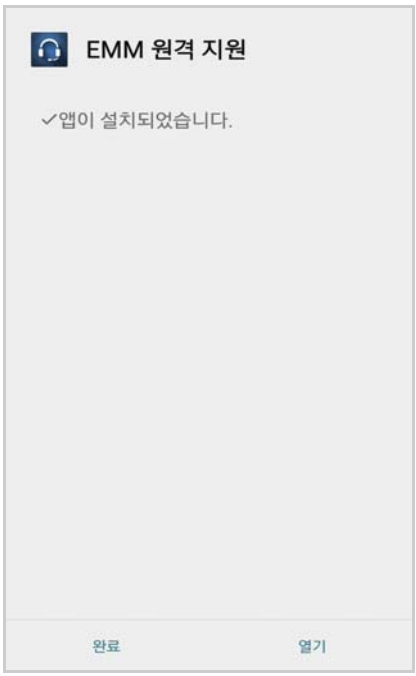
단말에 원격지원을 받을 수 있는 애플리케이션을 설치하려면 다음의 절차를 따르세요 .

1. 관리자로 부터 전달받은 APK 파일을 단말에서 실행하여 설치를 진행하세요.

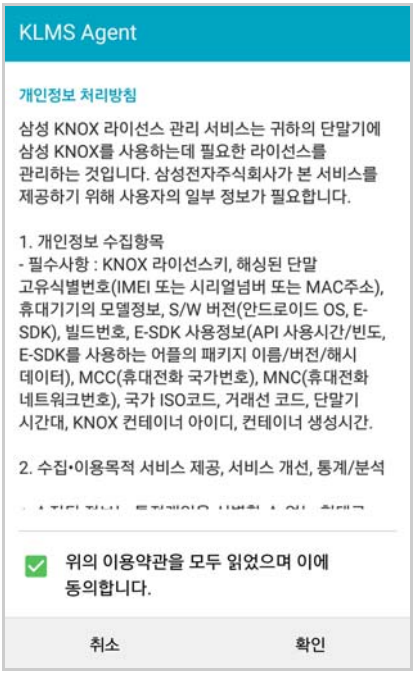


2. 개인 정보 보호 및 기기 액세스 정보를 확인한 후 **다음** 혹은 **설치**를 탭하세요.
   EMM의 원격 지원 애플리케이션이 설치됩니다.





3. **열기**를 탭하거나 단말 화면에 나타난 **EMM 원격 지원**을 탭하세요.
4. **Knox 라이선스 확인**을 탭하세요.
5. 개인정보 처리 방침 내용을 확인한 다음 이용약관 동의 확인란을 선택한 후 **확인**을 탭하세요.



원격 지원 설정 확인하기

EMM 원격 지원 화면 우측 상단의 ⓘ을 탭하면 설정 화면이 나타납니다 .

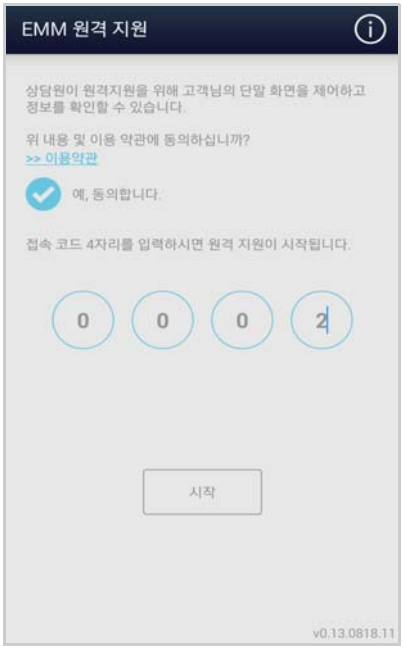
- **단말 정보**: 원격 지원 앱의 버전과 사용자의 단말 IP 및 Port 정보를 확인합니다.
- **서버**: 원격지원 서버의 IP 및 Port 정보를 확인합니다. Replay 서버의 IP와 Port 정보를 설정하려면 EMM 운영자에게 문의바랍니다.
- **애플리케이션**:
  - **오픈소스 라이선스**를 탭하여 내용을 확인할 수 있습니다.
  - **애플리케이션 삭제**를 탭하여 사용자 단말에서 EMM 원격 지원 애플리케이션을 삭제할 수 있습니다.

원격 지원 서비스 시작하기

원격 지원 서비스를 시작하려면 다음의 절차를 따르세요 .

1. 단말에 설치된 **EMM 원격 지원**을 탭하세요.
2. 애플리케이션 홈화면의 **이용약관**을 탭한 다음 이용약관 내용을 확인한 후 **닫기**를 탭하세요.
3. 애플리케이션 홈 화면의 **예, 동의합니다**를 선택하세요.

4. 관리자에게 전달 받은 4자리 접속 코드를 단말에 입력한 후 **시작**을 탭하세요.
   원격지원 서비스가 시작됩니다.



5. 원격 지원을 종료하려면 사용자가 EMM 원격 지원 화면의 **종료**를 탭하거나 관리자가 원격 지원을 종료 처리하세요.

9 방문자용 EMM 사용하기

사업장의 보안과 방문자의 편의를 위하여 사업장에 출입하는 방문자는 방문자용 EMM 을 사용할 수 있습니다 . 방문자용 EMM 은 방문관리자가 설정한 보안 정책이 적용되며 , 사업장 내에 머무르는 동안 방문자의 단말 사용은 방문자 정책에 따라 제한될 수 있습니다 .

EMM 로그인하기

방문자용 EMM 을 실행하면 초기 화면이 나타납니다 . 방문자는 서버 인증을 통해 EMM 에 로그인하려면 다음의 절차를 따르세요 .

1.  을 탭하여 EMM을 실행하세요.
   로그인 화면이 나타납니다.
2. 미리 발급받은 Tenant ID와 서버 주소(http/https, Access URL, Port)를 입력한 후 **확인**을 탭하세요.
   사용자 인증 화면이 나타납니다.
   - Tenant ID와 서버 주소(http/https, Access URL, Port)는 최초 로그인할 때만 입력합니다.
   - 최초 로그인시 Tenant ID를 서버에서 확인해야 하므로 로그인 소요시간이 평소보다 오래 걸릴 수 있습니다.

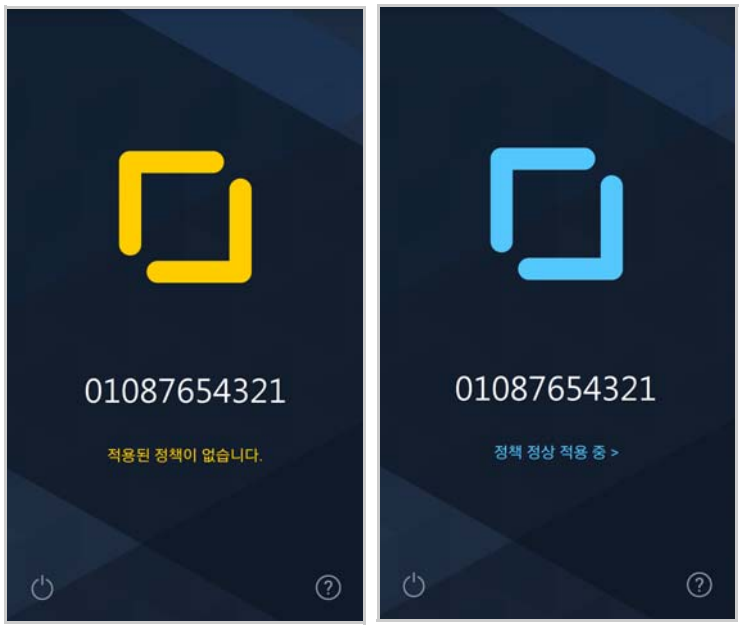
EMM 활성화하기

사용자 인증은 다음과 같은 단계로 수행됩니다 . 사용자 인증이 실행되고 나면 EMM 서비스가 활성화됩니다 . EMM 을 활성화하려면 다음의 절차를 따르세요 .

1. Tenant ID를 확인한 후, **EMM 실행**을 탭하세요.
2. EMM 서비스가 활성화되면 Knox 라이선스의 개인정보 취급방침에 동의를 선택한 후, **확인**을 탭하세요.

사용하기

EMM 에 로그인 시 다음과 같은 화면이 나타납니다 . EMM 에서 적용된 정책이 없는 경우 왼쪽 화면이 나타나고 , 정책이 적용된 경우 오른쪽 화면이 단말에 나타납니다 .



적용 정책 확인하기

단말의 중앙 하단에 위치한 **정책 정상 적용 중**을 탭하면 아래와 같이 현재 적용 중인 정책들이 보여집니다 .

서비스데스크 사용하기

서비스데스크에서는 EMM 버전 확인 및 오픈소스 라이선스 확인 , 그리고 단말에서 발생하는 오류를 서버로 보내는 로그 전송 기능을 제공합니다 .

버전 정보 확인하기

서비스데스크의 버전 정보에서 설치된 EMM의 현재 버전 정보를 확인하려면 다음의 절차를 따르세요 .

1. EMM 홈 우측 하단의  을 탭하세요.
2. 서비스 데스크의 **버전 정보**에서 버전을 확인하세요.

오픈소스 라이선스보기

EMM Client 및 Agent 등에서 사용되는 Open Source 에 대한 라이선스 공지 내용을 확인하려면 다음의 절차를 따르세요 .

1. EMM 홈 우측 하단의  을 탭허세요.
2. 서비스데스크에서 **오픈소스 라이선스**를 탭하세요.

로그 전송하기

서비스데스크의 로그 전송은 사용자가 EMM 사용 중 문제가 발생할 경우 문제 해결을 위해 서버로 로그를 보내는 기능입니다 . EMM 서버로 전송된 로그는 관리자가 확인 후 조치를 취하게 됩니다 . EMM 서버로 로그를 전송하려면 다음의 절차를 따르세요 .

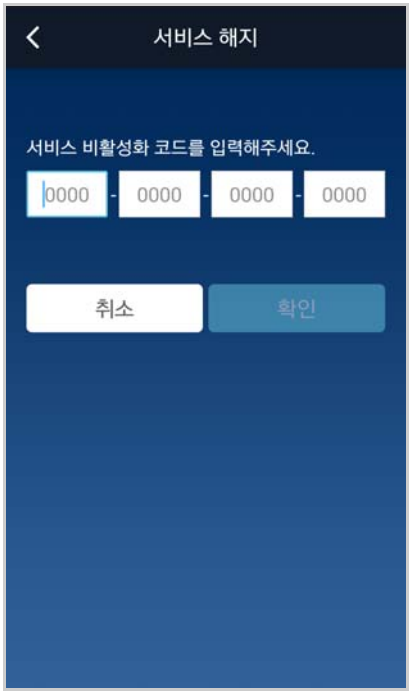
1. EMM 홈 우측 하단의  을 탭하세요.
2. 서비스데스크에서 **로그 전송**의  을 탭하세요.
   - 로그가 수집되지 않은 경우, 로그 전송이 불가능할 수 있습니다.
3. **확인**을 탭하세요.
   로그를 전송합니다.

서비스 종료하기

방문자 단말에서 EMM 서비스를 종료하려면 사업장에서 나갈 때 안내받은 서비스 비활성화 코드를 입력한 후 , EMM 을 종료합니다 . EMM 을 종료하려면 다음의 절차를 따르세요 .

1. EMM 좌측 하단의  을 탭하세요.
2. 안내받은 서비스 비활성화 코드를 입력한 후, **확인**을 탭하세요.
   - 서비스 비활성화 코드는 방문관리자가 제공하는 정보이므로, 반드시 관리자에게 문의하시기 바랍니다.

- 서비스 비활성화 코드가 유효하지 않은 경우 에러 메시지가 나타나며, 반드시 관리자에게 문의하시기 바랍니다.



단말 제어 기능

관리자의 설정에 따라 방문자의 단말에 다음과 같은 기능들이 제어될 수 있습니다 .

단말 제어기능은 다음 표를 참고하세요 .

기능	설명
카메라	카메라 사용을 제어합니다.
마이크	마이크 기능을 제어합니다. 마이크 기능 사용이 가능할 경우에도 iOS 단말의 경우 녹음 기록이 남고, 녹음 사실을 관리자에게 알려줍니다.
화면 캡쳐	단말 스크린 캡쳐를 제어합니다.
Wi-Fi	Wi-Fi 사용을 제어합니다.
Wi-Fi 핫스팟	Wi-Fi 핫스팟 사용을 제어합니다.
Wi-Fi SSID 화이트리스트	특정 SSID를 가진 Wi-Fi만 연결을 허용합니다.
블루투스	블루투스 기능을 제어합니다.
블루투스 테더링	블루투스 테더링 기능을 제어합니다.
PC 연결	PC 연결을 제어합니다.
USB 테더링 활성화	USB 테더링을 제어합니다.
앱 실행 블랙리스트	단말에서 특정 앱의 실행을 차단합니다.
앱 실행 화이트리스트	단말에서 특정 앱만 실행을 허용합니다.

플랫폼별 제어 기능

플랫폼의 종류에 따라 제어되는 기능들이 다를 수 있습니다. 플랫폼별 제어기능은 다음 표를 참고하세요 .

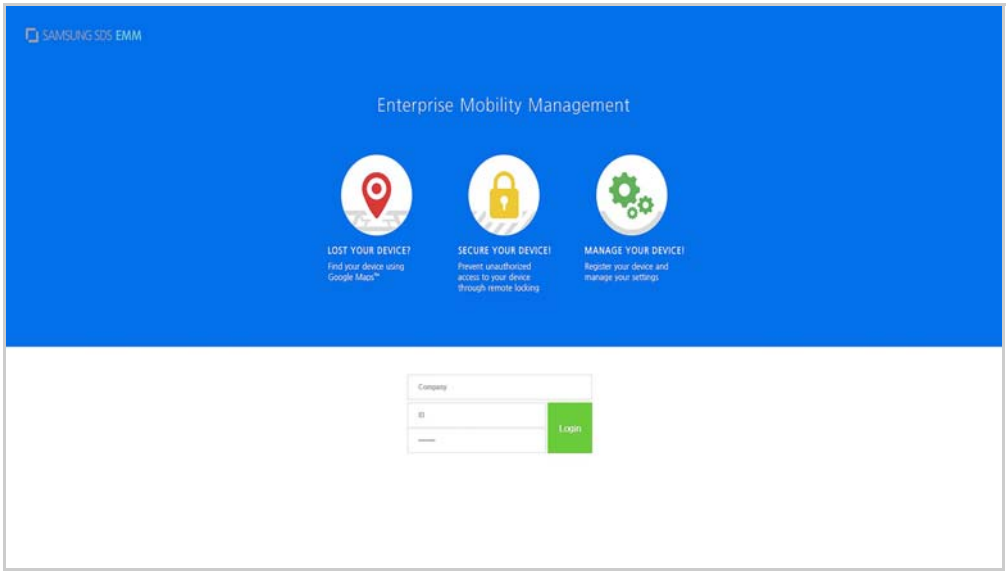
기능	Android		iOS
	Samsung	Others	
카메라	●	●	●
마이크	●	●	●
화면 캡쳐	●	●	●
Wi-Fi	●	●	-
Wi-Fi 핫스팟	●	●	-
Wi-Fi SSID 화이트리스트	●	●	-
블루투스	●	●	-
블루투스 테더링	●	●	-
PC 연결	●	●	-
USB 테더링 활성화	●	●	-
앱 실행 블랙리스트	●	●	●
앱 실행 화이트리스트	●	●	●

10 사용자 포털 사용하기

사용자 포털은 사용자가 직접 단말을 관리할 수 있는 포털을 의미합니다 . 사용자는 사용자 포털을 통해 EMM 을 사용하려는 단말을 직접 등록하고 단말의 상세 정보를 조회할 수 있습니다 . 만약 단말을 분실했을 경우 사용자는 사용자 포털을 통해 단말의 위치를 파악할 수 있고 단말의 잠금 처리를 하거나 단말의 초기화로 타인의 단말 도용을 미리 방지할 수 있습니다 . 사용자 포털의 사용법에 대해 설명합니다 .

로그인하기

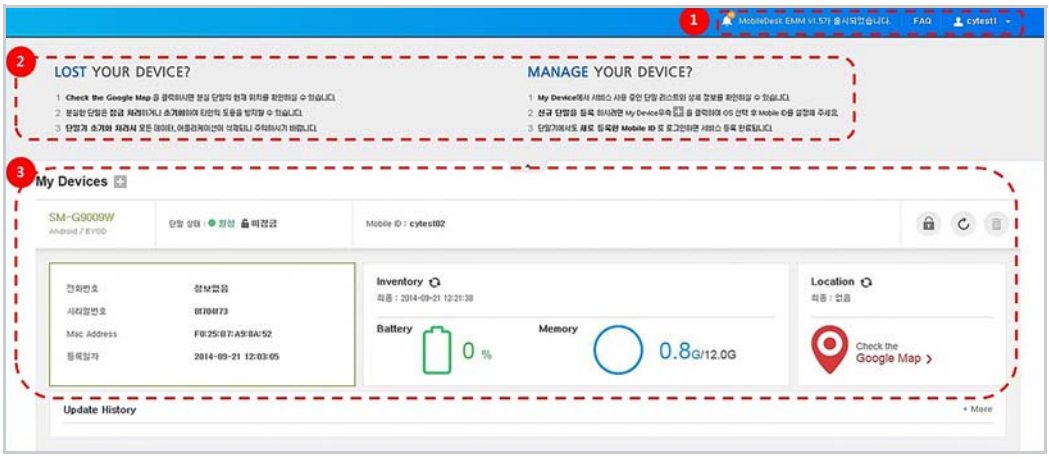
사용자 포털은 관리자 포털에 등록된 사용자 ID 와 비밀번호로 로그인합니다 .



사용자 포털에 로그인하려면 다음의 절차를 따르세요 .

1. EMM 사용자 포털의 로그인 페이지에 접속하세요.
2. 회사명(Tenant ID), 사용자 ID, 비밀번호를 입력하세요.
3. **로그인**을 클릭하세요.

사용자 포털 살펴보기



번호	영역	설명
1	알림	• 공지사항 조회 • 접속이력 조회 • 로그아웃
2	보안	• 단말 분실 시 조치방법 • 단말 신규 등록 방법 • 가이드 하단 버튼을 클릭하여 더 많은 내용 조회
3	내 단말	• 단말 등록 • 단말 잠금 • 단말 초기화 • Google Maps™를 이용한 단말 추적

단말 등록하기

사용자 포털에 사용자의 신규 단말을 등록하는 방법은 두 가지가 있습니다. 관리자가 관리자 포털을 통해 단말을 등록하거나 또는 사용자가 사용자 포털에서 직접 등록하는 방법입니다.

사용자가 사용자 포털에서 직접 단말을 등록할 경우 새로 등록한 Mobile ID 로 EMM 에 로그인하면 EMM 사용을 위한 EMM 서비스가 활성화되고, 활성화 이후 단말은 사용자 포털에서 관리가 가능한 상태가 됩니다. 사용자별 등록 가능한 단말의 개수는 최대 10 대입니다.

사용자가 사용자 포털을 통해 직접 단말을 등록하려면 다음의 절차를 따르세요.

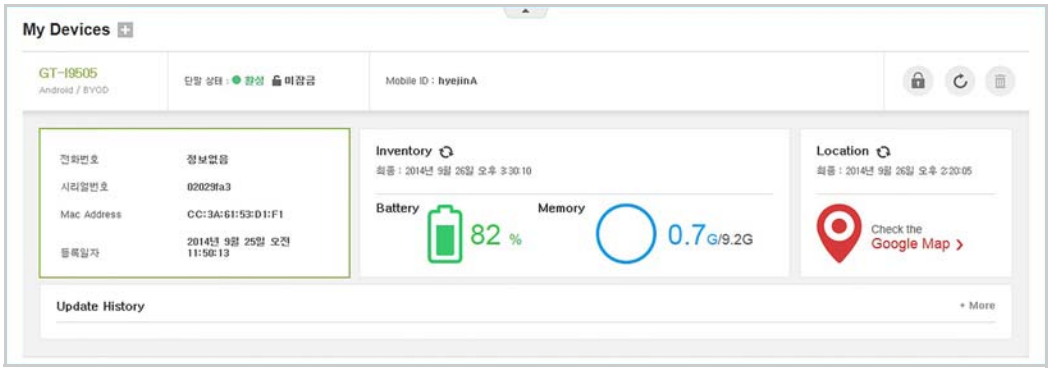
1. **사용자 포털에 로그인한 후 My Device** 우측의 ＋을 클릭하세요.
2. "단말 추가" 창에서 **Mobile ID**를 입력한 후, **플랫폼**을 선택하세요.

3. **확인**을 클릭한 후, 단말 등록 확인 메시지가 나타나면 **OK**를 클릭하세요.

Note: 단말에 EMM을 설치하고 EMM 서비스를 활성화하는 자세한 설명은 6 페이지의 "3 시작하기" 또는 15페이지의 "4 단말 정책 확인하기"를 참고하세요.

단말 관리하기

사용자 포털에서 사용자가 등록한 단말을 사용자 스스로 관리할 수 있습니다 . 만약 한 사용자가 여러개의 단말을 보유한 경우 각 단말은 단말 고유 ID 로 관리됩니다 . 등록한 단말의 상세 정보를 확인하려면 단말의 기본 정보란을 클릭하여 하단의 추가 정보들을 확인할 수 있습니다 .



- **단말의 기본 정보**
  모델명, 플랫폼(Android, iOS), 소유구분(BYOD, COPE, Company), 단말 상태(활성여부, 잠금여부), Mobile ID
- **단말의 상태 변경**
  단말 잠금( ), 단말 초기화( ), 단말 삭제( )
- **단말의 상세 정보**
  전화 번호, 시리얼 번호, Mac Address, 등록일자
- **단말의 Inventory**
  단말의 배터리 잔량, 사용 메모리/총 메모리 용량, 최종 Inventory 업데이트 시각
- **단말의 Location**
  단말의 위치, 최종 Location 업데이트 시각
- **Update History**
  단말의 잠금처리, 초기화한 히스토리 조회

단말 잠금하기

단말 잠금 기능은 단말 잠금이 필요한 상황이거나 또는 사용자가 단말을 분실한 경우 EMM 정보 보호를 위해 일시적으로 단말을 사용하지 못하도록 하는 기능입니다 . 단말 잠금 기능을 통해 EMM 정보를 보호하고 타인의 단말 도용을 방지할 수 있습니다 . 사용

자에 의해 단말 잠금 처리 후 잠금 해제는 관리자를 통해서만 가능하며 단말 잠금이 요청된 시각과 요청 PC 의 IP 는 **Update History** 에서 조회됩니다 . 단말을 잠그려면 다음의 절차를 따르세요 .

1. 단말 잠금을 위해 을 클릭하세요.
2. 사용자 포털 로그인 시 비밀번호 입력하세요.
3. **잠금 실행**을 클릭하세요.
4. 단말 제어 전송 확인 팝업 메시지가 나타나면 **OK**를 클릭하세요.

단말 초기화하기

단말 초기화 기능은 단말의 EMM 정보가 누출되지 않도록 단말을 초기화시키는 기능입니다 . 사용자가 단말을 분실한 경우 단말을 공장초기화하여 EMM 정보를 보호하고 타인의 도용을 방지할 수 있습니다 . 만약 단말 초기화 이전에 별도 단말 백업을 하지 않았다면 단말에 저장된 데이터의 복구가 불가능할 수 있습니다 . 단말 초기화가 요청된 시각과 요청 PC 의 IP 는 **Update History** 에서 조회가 가능합니다 . 단말을 초기화하려면 다음의 절차를 따르세요 .

1. 단말 초기화를 위해 을 클릭하세요.
2. 사용자 포털 로그인 시 비밀번호 입력하세요.
3. **초기화 실행**을 클릭하세요.
4. 단말 제어 전송 확인 팝업 메시지가 나타나면 **OK**를 클릭하세요.

Note: 프로파일에서 EMM 무력화 방지 기능이 설정되어 있을 경우, 공장초기화 후 모바일 단말에 EMM Client를 다운 받을 수 있는 URL 링크를 제공하여 다운로드 후 재등록 할 수 있게 합니다.

단말 삭제하기

사용자가 잘못 등록한 단말이거나 일정 기간동안 사용하지 않는 단말은 **My Devices** 의 우측 상단 를 클릭하여 삭제할 수 있습니다 . 단 , 단말이 비활성화 상태일 경우만 삭제가 가능합니다 .

단말 인벤토리 정보 보기

단말의 인벤토리 (배터리 잔량 , 저장소 사용량) 정보를 확인하려면 다음의 절차를 따르세요 .

1. Inventory 우측의 을 클릭하세요.
2. 단말 제어 전송 확인 팝업 메시지가 나타나면 **OK**를 클릭하세요.

3. 단말의 인벤토리 정보 **Battery**, **Memory**를 받아 최종 정보를 가져온 날짜와 시각을 확인하세요.
   - 통신, 전원 등 단말의 상태에 따라 확인이 지연될 수 있습니다.

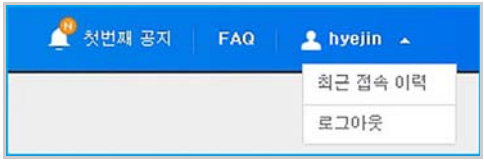
단말 위치 정보 보기

단말을 분실한 경우 단말 위치 정보 보기로 대략적인 단말 위치 정보를 확인할 수 있습니다 . 단말의 최종 위치 정보와 날짜 , 시각을 조회하려면 다음의 절차를 따르세요 .

1. Location 우측의 을 클릭하세요.
2. 단말 제어 전송 확인 팝업 메시지가 나타나면 **OK**를 클릭하세요.
3. 단말의 최종 위치 정보와 날짜 및 시각을 확인하세요.
   - 통신, 전원 등 단말의 상태에 따라 확인이 지연될 수 있습니다.
4. **Check the Google Map**을 클릭한후 단말의 위치 정보를 확인하세요.

기타 정보 조회

사용자 포털 화면 우측 상단에서 기타 정보 조회가 가능합니다.



공지사항

사용자 포털 우측 상단의 **공지사항**을(최근 공지사항의 제목이 표시됨) 클릭 시 포털 관리자가 게시한 공지사항 내용을 확인할 수 있습니다.

Note: 공지사항 등록은 관리자 포털의 운영자가 사용자포털에 로그인하여 등록할 수 있으며, 공지사항 목록 우측 하단의 **새글 작성**을 클릭 후 작성합니다.

FAQ

사용자 포털 우측 상단의 FAQ 클릭 시 자주하는 질문에 대한 답변을 확인할 수 있습니다.

Note: FAQ 등록은 관리자 포털의 운영자가 사용자포털에 로그인하여 등록할 수 있으며, FAQ 목록의 우측 하단의 **새글 작성**을 클릭 후 작성합니다.

최근 접속 이력

사용자 포털 우측 상단의 **사용자 ID > 최근 접속 이력**을 클릭하면 사용자 포털에 로그인 한 최근 이력 (날짜 , 시각 , 접속 IP) 을 확인할 수 있습니다.

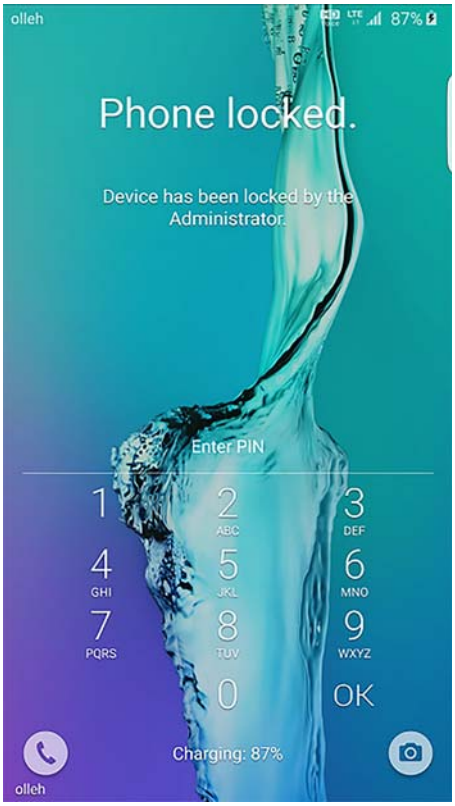
로그아웃

사용자 포털 우측 상단의 **사용자 ID > 로그아웃**을 클릭하면 사용자 포털에서 로그아웃됩니다 . 사용자 포털에 로그인 후 30 분이 지날 때까지 사용하지 않으면 자동으로 로그아웃됩니다 .

부록 A 해결하기

A.1 단말 잠김 해결하기

EMM 관리자는 사용자의 단말을 잠그기 위해 단말 제어 메시지를 전송할 수 있으며 , 특정 정책에 의해 단말이 잠기도록 설정할 수 있습니다 .



이처럼 EMM 의 정책으로 단말이 잠긴 경우 해제하려면 다음의 절차를 따르세요 .

1. EMM 관리자에게 사용자 ID와 단말 ID로 단말의 잠김을 문의하세요.
   EMM 관리자는 사용자의 단말이 EMM 서버와 통신이 가능한지를 체크합니다.
2. 단말과 EMM 서버의 통신이 가능하면, 관리자가 단말 제어를 단말에 보내어 단말 잠김이 바로 해제됩니다.
   단말과 EMM 서버의 통신이 불가능하면, 관리자가 생성하여 알려주는 단말 잠금 해제 코드를 사용자가 단말에 입력하세요.
   단말 잠김이 바로 해제됩니다.

Note: 그 외 기타 사유로 인하여 단말이 잠긴 경우, 위의 단계로 해결이 되지 않으므로 단말의 서비스 센터로 문의하여 단말의 공장초기화를 진행합니다.

A.2 비밀번호 해결하기

사용자 단말의 비밀번호는 3 가지가 있습니다 .

- EMM로그인 시 사용자 ID와 함께 입력하는 “로그인 비밀번호”
- EMM로그인 후 EMM화면 잠금을 풀 수 있는 “화면잠금 비밀번호”
- 단말 자체의 “단말잠금 비밀번호”

설정한 비밀번호를 잊어버린 경우 해결하려면 다음의 절차를 따르세요 .

- 로그인 비밀번호를 잊어버린 경우:

  관리자에게 비밀번호 초기화를 요청하세요.
  사용자의 이메일로 임시비밀번호를 전송받습니다.

  임시비밀번호로 EMM을 로그인 시 비밀번호를 재설정하세요.
- 화면잠금 비밀번호를 잊어버린 경우:

  관리자에게 “계정 삭제”라는 단말 제어를 요청하세요.
  사용자 단말의 EMM이 로그아웃되며 다시 로그인합니다.

  로그인 시 화면 잠금 비밀번호를 설정하세요.
- 단말잠금 비밀번호를 잊어버린 경우:

  관리자에게 “단말잠금 비밀번호 초기화”라는 단말 제어를 요청하세요.
  사용자 단말에 기존에 설정했던 단말잠금 비밀번호는 없어지며 바로 비밀번호 설정화면이 나타납니다.

  단말잠금 비밀번호를 새로 설정하세요.

부록 B Client 에러 코드 및 설명

사용자 단말의 EMM 에서 보여질 수 있는 에러 코드의 리스트입니다 . 에러 발생 시 아래의 설명을 참고하며 관리자에게 해당 에러코드로 문의 가능합니다 .

대분류	모듈	코드	설명
Client	Self-signed Certificate	A1010	사설 인증서를 설치하지 않았거나, 잘못된 인증서가 설치된 경우
	Service Provision	F100	서버 정보를 찾을 수 없습니다.
		F210	Tenant가 존재하지 않을 경우
		F220	사용자 동의서에 동의하지 않았음
		F230	Tenant의 라이선스 기간 만료
	Provisioning	B5015	입력한 Mobile Alias가 이전에 프로비저닝한 값과 다른 경우
		B2001	사용자 ID가 Null일 경우
		B2002	사용자 비밀번호가 Null일 경우
		B2003	Mobile Alias가 Null일 경우
		B3001	서버 주소를 지정하지 않을 경우
		B3002	서버 연결 중 timeout 발생
		B3003	서버 연결 시도 중 예외 상황 발생
		B3004	서버 페이지 오류 (HTTP 오류코드)
		B4001	서버 내부 오류
		B5002	서버 GetPublicKey Runtime 오류
		B5003	서버에 단말 정보가 없을 경우
		B5004	서버에 등록된 단말이 없을 경우
		B5005	단말 Block상태
		B5010	서버에 단말이 이미 Provision 되어있는 경우
		B5012	사용자 ID를 찾을 수 없는 경우
		B5013	ID 또는 비밀번호 불일치로 인증이 실패한 경우
		B5019	사용자별 등록가능 단말 개수가 초과할 경우
	Device Certificate	A1011	디바이스 인증서 발급 실패

대분류	모듈	코드	설명
	Login	A1004	로그인 실패(서버에서 잘못된 형식의 데이터를 받은 경우)
		A5001	사용자 ID가 삭제된 경우
		A5003	기타 알 수 없는 이유
		C1001	네트워크 오류 발생
		C1003	인증 실패, ID 또는 비밀번호 확인 필요
		C1004	사용자 ID를 찾을 수 없는 경우
		C1005	서버에 단말 정보가 없을 경우, 서버에 등록된 단말이 없을 경우
		C1006	서버에 등록된 단말 정보와 일치하지 않을 경우
		C1008	단말 Block상태
		C1009	서버에 PrivateKey가 존재하지 않을 경우
		C1011	입력한 Mobile ID가 서버에 등록Push된 Mobile ID와 일치하지 않는 경우
	Client Profile	A3000	Client 프로파일을 받아오지 못한 경우
	AppTunnel	A1021	AppTunnel 초기화 성공
		A1022	잘못된 파라미터가 입력된 경우
		A1023	라이선스 정보가 잘 못 되었을 때
		A1024	AppTunnel 초기화 실패
		A1025	네트워크 연결 실패
	Push	A3001	Push 등록 Retry 실패
		A3002	Push 등록 실패
	Agent	F3001	메시지 버전이 정의되지 않은 경우
		F3002	EMM Client 등록된 앱 버전과 일치하지 않는 경우
		F3003	EMM Agent 등록된 앱 버전과 일치하지 않는 경우
		F2001	Push Agent가 존재하지 않음
		F2002	Push 등록 실패
		F2003	Push 등록 시 예외 발생
		F2004	푸시 등록 타임 아웃
		F5014	디바이스 인증서 발급 실패

대분류	모듈	코드	설명
Provisioning Library	Common	B1001	성공
		B1002	DeviceId가 단말에 없을 경우 발생
		B1003	SQLite 오류
		B1004	암호화 오류
		B1005	Get Public Key 오류
		B1006	입력한 Mobile Alias가 이전에 프로비저닝한 값과 다른 경우
		B1007	복호화 에러
		B1008	키생성 에러
	Parameter	B2001	사용자 ID가 Null일 경우
		B2002	사용자 비밀번호가 Null일 경우
		B2003	Mobile Alias가 Null일 경우
		B2004	테넌트ID가 없을 경우
		B2005	서버 공개키가 없을 경우
		B2006	어플리케이션명 또는 버전이 Null 일 경우
		B2007	setProvisioningInfo() 함수의 파라미터 누락된 경우
	Connection	B3001	서버 주소를 지정하지 않을 경우
		B3002	서버 연결 중 timeout 발생
		B3003	서버 연결 시도 중 예외상황 발생시
		B3004	서버 페이지 오류(HTTP 오류코드)

대분류	모듈	코드	설명
	Etc.	B4001	Server Internal 오류
		B4002	예상치 못한 예외상황 발생
	Provision Server	B5001	서버에 PublicKey가 존재하지 않을 경우
		B5002	서버 GetPublicKey Runtime 오류
		B5003	서버에 단말 정보가 없을 경우
		B5004	서버에 등록된 단말이 없을 경우
		B5005	단말이 Block상태일 때
		B5006	서버 Provision Runtime 오류
		B5007	서버에 PrivateKey가 존재하지 않을 경우
		B5008	서버의 단말 상태가 initProvision을 못 하는 경우
		B5009	InitProvision을 하기 위해 매칭되는 단말이 없는 경우
		B5010	서버에 단말이 이미 Provision 되어있는 경우
		B5011	서버 InitProvision Runtime 오류
		B5012	사용자 ID를 찾을 수 없는 경우
		B5013	ID 또는 비밀번호 불일치로 인증이 실패한 경우
		B5014	네트워크 Communication 오류
		B5015	자동등록 단말 허용 개수 초과
		B5016	device ID가 유효하지 않은 값일 경우
		B5017	라이선스 정보 읽어오기 실패
		B5018	단말상태가 block(System block)일 경우
		B5019	사용자별 등록가능 단말 개수가 초과할 경우
		B5020	단말에서 전송한 Platform 정보와 서버에 저장된 Platform 정보가 일치하지 않을 경우
		B5021	Wi-Fi 전용 단말이 아니지만 Mac address 와 IMEI 정보가 없는 경우
		B5022	Wi-Fi 전용 단말이면서 Serial number 정보가 없는 경우

대분류	모듈	코드	설명
Login		C1001	네트워크 오류 발생
		C1002	알 수 없는 오류 발생
		C1003	인증 실패, ID 또는 비밀번호 확인 필요
		C1004	사용자 ID를 찾을 수 없음, 사용자 ID 확인 필요
		C1005	사용가능 단말이 없음
		C1006	일치하는 사용자 단말을 찾을 수 없음
		C1007	비밀번호 암호와 실패
		C1008	단말 Block 상태
		C1009	단말 비활성화 상태
		C1010	유효하지 않은 라이선스
		C1011	모바일 ID 불일치
Profile	common	D1001	Header의 파라미터 정보 없음
		D1002	압축실패
		D1003	암호화 실패
		D1004	없는 command
		D1005	유효하지 않은 버전
		D1006	Device ID 없음
		D1007	유효하지 않은 Device ID
		D1008	Device ID 정보를 조회할 수 없음
	Device Command	D2001	Device Command 전송 실패
		D2002	어플리케이션 정보 조회 실패
		D2003	KNOX ID 조회실패
		D2004	사용자 ID없음
		D2005	어플리케이션 ID 없음
		D2006	패키지명 없음
		D2007	knox ID 파라미터 없음
		D2008	knoxcontainer ID가 없음
		D2009	앱정보 없음
		D2010	유효하지 않은 Device Command 코드
		D2011	설치 요청한 앱이 화이트리스트에 포함되지 않거나 블랙리스트에 포함인 경우
	homepage	D3001	사용자 ID없음
		D3002	홈페이지 정보 insert 실패
	bookmark	D4001	사용자 ID 없음
		D4002	북마크 index 없음
		D4003	북마크 정보 insert 실패

대분류	모듈	코드	설명
	update profile	D5001	devicetoken 업데이트 실패
		D5002	프로파일 조회 실패
		D5003	앱정보 조회 실패
		D5004	프로파일 생성 실패
		D5005	최종프로파일 업데이트 시간 업데이트 실패
		D5006	앱정보 조회 실패
	client report	D6001	위치정보 및 jailbreak정보등 업데이트 실패
		D6002	유효하지 않은 report type
	Push	D7001	푸시 매직 데이터 없음
Push	Push	E1001	입력 파라미터 오류인 경우
		E1002	APID 가 오류인 경우
		E1003	SERVER 가 오류인 경우
		E1004	SUID 가 오류인 경우
		E1005	Data 가 오류인 경우
		E1006	Push service 등록 중인 상태
		E1007	Push service 대기 중인 상태
		E1008	Push service 등록 완료 상태
		E1009	Push service 등록 실패
		E1010	인증서 오류
		E1011	단말 Network가 연결되어 있지 않을 경우
		E1012	DCM 서버가 없는 경우
		E1013	메시지 전달 실패
		E1014	Device Agent ID 차단
		E1015	Application ID 차단

대분류	모듈	코드	설명
Agent	Provision	F1001	Provision 실패한 경우
		F1002	Provision 시 예외 상황이 발생한 경우
		F1003	Device ID가 Null일 경우
		F1004	RsaKey 가 Null일 경우
	Push	F2001	Push Agent가 존재하지 않음
		F2002	Push Agent 등록 실패
		F2003	Push 등록 시 예외 발생
		F2004	푸시 등록 타임 아웃
	Enrollmentspec	F3001	메시지 버전이 정의되지 않은 경우
		F3002	EMM Client 등록된 앱 버전과 일치하지 않는 경우
		F3003	EMM Agent 등록된 앱 버전과 일치하지 않는 경우
	ActivateDpm	F4001	Timeout
		F4002	Disagree
	UpdateElmLicense	F5001	Timeout
		F5002	None
		F5003	파라미터 정보 없음
		F5004	Unknown
		F5005	EML라이선스 정보가 유효하지 않은 경우
		F5006	EML라이선스가 만료된 경우
		F5007	Internal 오류
		F5008	Server Internal 오류
		F5009	Network가 연결되어 있지 않을 경우
		F5010	NetworkGeneral
		F5011	UserDisagreesLicenseAgreement
		F5012	InvalidPackageName
		F5013	NotCurrentDate
	UpdateKlmLicense	F6001	Timeout
		F6002	None
		F6003	파라미터 정보 없음
		F6004	Unknown
		F6005	KML라이선스정보가 유효하지 않은 경우
		F6006	KLM라이선스가 만료된 경우
		F6007	InvalidPackageName
		F6008	NotCurrentDate
		F6009	Internal 오류

대분류	모듈	코드	설명
		F6010	Internal 오류
		F6011	Network가 연결되어 있지 않을 경우
		F6012	NetworkGeneral
		F6013	USerDisagreesLicenseAgreement
Agent	Agent (iOS)	1500000	Command에 대한 Request가 3번 이상
		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	이미 UDID가 존재함
		1500013	TENANT ID에 해당 DEVICE ID가 없음
		1500014	Push 발송 실패
		1500015	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	앱 블랙&화이트리스트 조회 실패
		1500101	지금 명령을 수행할 수 없음
		1500102	MDM Command 형식에 어긋남

SAMSUNG SDS

Realize your vision

www.samsungsds.com