



주요 장점

- 단일 콘솔에서 장치 프로비저닝, 보호, 관리
 - 이메일, 캘린더, 연락처, Wi-Fi 및 VPN 프로필을 구성하여 접속 중인 사용자에게 무선으로 전달
 - iOS, Android 및 Windows Phone 및 BlackBerry용 최신 모바일 운영 체제 출시 시의 개시일 지원 체험
 - 보안 정책 수립, 그리고 장치 비밀번호 요구 및 훼손된 장치 차단과 같은 자동화된 규정 준수 조치를 통해 보안 정책 강제 실행
 - 강력한 대시보드와 기업 및 개인 장치를 모두 관리하는 보고 기능 사용
-

IBM MaaS360 Mobile Device Management

오늘날의 모바일 장치 보호 및 관리

IBM® MaaS360® Mobile Device Management는 빠른 전체 기능 솔루션으로서, 스마트폰 및 태블릿 등 모든 단일 화면에서 기업 데이터에 대해 엔터프라이즈 액세스 및 보호 기능을 제공하도록 장치를 구성합니다.

강력한 통합 클라우드 플랫폼으로서 MaaS360는 모바일 장치, 애플리케이션 및 문서 전반에 걸쳐 확장하는 빠른 배치, 가시성 및 통제를 통해 모바일 장치 관리(MDM)를 간편하게 합니다.

배치가 빠릅니다. 단 몇 번의 클릭만으로 IT 관리자는 장치 등록을 시작하고 등록부터 엔터프라이즈 통합, 구성 및 관리, 모니터링과 보안, 지원 및 분석 도구와 보고까지 전체적인 모바일 장치 수명 주기를 빠르게 관리할 수 있습니다.

MDM 문제 해결

- 보안 및 규제 준수 실행 향상
- 모바일 자산 지원 비용 절감
- 애플리케이션 및 성능 관리 향상
- 개선된 업무의 연속성 보장 지원
- 생산성 및 직원 만족도 증가

왜 MaaS360인가?

- 엔터프라이즈 이동성 관리에 있어서 입증된 접근법
- 강력한 관리와 보안으로 전체적인 이동성 수명 주기 해결
- 기존 인프라와 쉽게 통합
- 간편함 및 신속함을 통한 놀라운 고객 경험

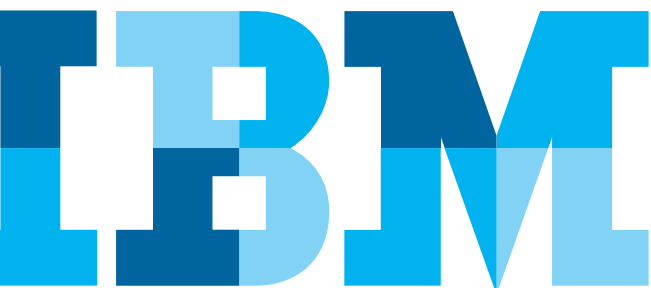




그림 1: 다양한 기기에서 보이는 MaaS360 사례

모바일 장치의 빠른 등록

MaaS360 Mobile Device Management는 플랫폼 설정과 장치 등록 프로세스를 효율화해 IT 및 직원의 업무를 간편화합니다.

- MDM 서비스 선택 및 장치 등록 설정 구성
- SMS, 이메일 또는 사용자 정의 URL을 사용해 이동통신망(OTA)으로 등록 요청 보내기
- 일회용 암호 또는 SAML을 활용해 Active Directory/LDAP 인증
- 사용자 정의된 허용 가능 사용 정책 및 EULA 생성 및 분배
- 기업 및 직원 소유 BYOD(자신만의 장치를 가지고 다니다) 등록
- 개인 또는 대규모 장치 등록 시작
- 기본 장치 정책 설정 적용 또는 수정

엔터프라이즈 시스템과 모바일 장치 통합

MaaS360 Cloud Extender를 통해 엔터프라이즈 시스템 통합이 사내 서버 또는 네트워크를 재구성할 필요 없이 쉽고 간단해집니다.

- 엔터프라이즈 시스템에 액세스하는 장치의 즉각적인 발견
- Microsoft Exchange, Lotus Notes, Microsoft Office 365 및 Gmail과의 통합
- 기존 Active Directory/LDAP 및 인증 기관(Certificate Authorities) 상에 구축
- BlackBerry Enterprise Server (BES) 정책 관리
- 강력한 웹 API를 통해 다른 운영 체제 연결

모바일 장치의 중앙 관리

MaaS360은 여러 플랫폼 전반에 걸친 중앙집중식 정책과 제어를 활용하는 스마트폰과 태블릿을 위한 통합 모바일 관리 콘솔입니다.

- 이메일, 캘린더, 연락처, Wi-Fi 및 VPN 프로필을 이동통신망(OTA)으로 구성
- 네트워크 상에서 새로운 모바일 장치 승인 또는 격리
- 세밀화된 관리를 위한 사용자 정의 그룹 생성
- 공용 및 기업 애플리케이션 분배 및 관리
- 문서 및 콘텐츠를 안전하게 공유 및 업데이트
- MaaS360 Mobile Device Management 내에서 역할 기반 관리 포털 액세스 권한 정의
- 기업 데이터와 MDM 통제를 제거함으로써 장치 해체

사전대처식 모바일 장치 보호

MaaS360 Mobile Device Management는 동적이고 강력한 안전 및 규정 준수 관리 기능을 제공해 지속적으로 장치를 모니터링하고 적절한 조치를 취합니다.

- 구성이 가능한 품질, 길이 및 기간을 갖춘 비밀번호 정책 요구
- 암호화 및 비밀번호 가시성 설정 실행
- 기능, 애플리케이션, iCloud 및 콘텐츠 등급에 대한 장치 제한 설정
- 탈옥 및 루팅된 장치 감지 및 제한
- 잃어버리거나 도난 당한 장치의 원격 위치찾기, 잠금 및 지우기
- 개인 데이터는 온전히 둔 채로 기업 데이터의 선택적 지우기
- 자동화 조치로 거의 실시간에 가까운 규정 준수 역할 구현
- 지오펜싱(geo-fencing) 규칙을 통해 위치 기반 규제 준수 실행

MDM 지원 효율화

MaaS360 Mobile Device Management는 웹 기반 포털에서 지속적으로 장치, 사용자 또는 애플리케이션 문제를 진단 및 해결하는 능력을 제공하고, IT 세부 가시성 및 통제를 제공하며, 최적의 모바일 사용자 생산성을 촉진합니다.

- 장치 보기 접속을 통해 문제 진단 및 해결
- 잃어버리거나 도난 당한 장치 위치 추적
- 잊어버린 비밀번호 재설정
- 장치에 메시지 전송
- 필요 시 구성 설정 업데이트
- 셀프 서비스 포털을 통한 사용자 자가 지원

모바일 장치 상에서 모니터링 및 보고

Mobility Intelligence™ 대시보드에서 모바일 장치 관리 운영 및 규제 준수에 대한 대화형 그래픽 요약을 확인하고 IT 부서는 회사 전체에 걸쳐 필요에 따른 보고를 할 수 있습니다.

- 하드웨어 및 소프트웨어 재고에 대한 세부 보고
- 구성 및 취약성 세부 정보
- 거의 모든 속성 전체에 걸쳐 스마트한 검색 기능 통합
- 사용자 정의 감시 대상 목록을 통한 경보 추적 및 수신
- BYOD 개인정보보호 설정으로 개인 식별 가능한 정보 수집 차단
- 지속적인 데이터 사용 모니터링 및 알림을 위한 모바일 비용 관리 옵션

즉시의 모바일 장치 관리

MaaS360 Mobile Device Management는 iPhones, iPads, Androids, Kindle Fire, Windows Phone, Windows 10 및 BlackBerry 스마트폰과 태블릿 등 오늘날 모바일 장치의 전체적인 수명 주기 관리를 위한 필수 기능을 갖춘 사용이 용이한 MDM 플랫폼입니다.

MDM 필수 요소

- SMS, 이메일 또는 URL 이동통신망(OTA) 등록
- 비밀번호 및 암호화 실행
- 이메일, VPN 및 Wi-Fi 프로필
- 장치 제한 설정
- 원격 위치추적, 잠금 및 지우기(전체 및 선택적)
- 탈옥 및 루팅 감지
- 정책 수정 및 변경
- 규제준수 보고

강력한 이동성 관리

- 이메일 접속 통제
- 기업 디렉토리 통합
- 인증서 관리
- BYOD 개인정보보호 설정
- 장치가 아닌 사용자별 페르소나 정책
- 거의 실시간에 가까운 조치 실행을 위한 자동화 규제준수 엔진
- 위치 추적 및 지오펜싱(geofencing)
- 대시보드 및 경보

IBM 보안 사기 방지 솔루션에 관한 자세한 내용은 가까운 IBM 담당자 또는 IBM 비즈니스 파트너사에 문의하시거나 다음 웹사이트를 참조하십시오. ibm.com/security.



© Copyright IBM Corporation 2016

IBM Corporation
Software Group
Route 100
Somers, NY 10589

제조:미국
2016년 3월

IBM, IBM 로고, ibm.com 및 X-Force는 전 세계 많은 관할지에 등록된 International Business Machines Corp.의 상표입니다. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® 및 장치, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility®, Trusted Workplace™, Visibility360® 및 We do IT in the Cloud.™와 장치들은 IBM Company인 Fiberlink Communications Corporation의 상표 또는 등록 상표입니다. 그 밖의 제품 및 서비스 이름은 IBM 또는 해당 회사의 상표입니다. 현재 IBM 상표 목록은 다음 웹사이트의 “저작권 및 상표 정보”에서 확인할 수 있습니다. ibm.com/legal/copytrade.shtml

Apple, iPhone, iPad, iPod touch 및 iOS는 미국 및 기타 국가에서 사용되는 Apple Inc.의 등록 상표 또는 상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 및/또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

본 문서는 출판 시점에 유효한 문서로서, IBM에서 언제든지 변경할 수 있습니다. IBM이 사업을 운영하는 모든 국가에서 모든 제안이 제외되는 것은 아닙니다.

본문에 인용된 실적 데이터 및 고객 사례는 단순한 예시용입니다. 실제 실적 결과는 특정 구성 및 운영 조건에 따라 다를 수 있습니다. IBM 제품 및 프로그램과 함께 사용하는 기타 제품 또는 프로그램의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

이 문서의 정보는 상품성, 특정 목적에의 적합성 및 타인의 권리 비침해에 대한 보증이나 조건을 포함하여 명시적이든 묵시적이든 일체의 보증 없이 “있는 그대로” 제공됩니다. IBM 제품은 제품과 함께 제공되는 계약서의 이용 약관에 따라 보상을 받으실 수 있습니다.

관련법과 규정을 준수해야 할 책임은 고객에게 있습니다. IBM은 법률 자문을 제공하지 않으며, IBM이 고객에게 서비스 또는 제품을 제공한다는 사실이 고객이 관련 법률 또는 규제를 준수하고 있음을 IBM이 확인하거나 보증하는 것은 아닙니다.

IBM의 향후 방향에 대한 언급 역시 통보 없이 변경 또는 철회될 수 있으며 목표에 대한 표현과 목적에 대해서도 마찬가지입니다.

올바른 보안 관행 진술: IT 시스템 보안은 기업 내외에서의 부적절한 접속에 대한 예방, 탐지 및 대응을 통하여 시스템 및 정보를 보호하는 일을 담당합니다. 부적절한 접속으로써 정보를 변개, 파괴 또는 악용하거나 다른 정보를 공격하는 등 시스템 손상 또는 시스템 오용으로 이어질 수 있습니다. 어떠한 IT 시스템 또는 제품도 완전히 안전하다고 간주되지 않으며, 어떠한 단일 제품 또는 보안 조치도 부적절한 접속 방지에 완전히 효과적일 수는 없습니다. IBM 시스템 및 제품은 포괄적인 보안 접근법의 일환으로 설계되었고, 추가 운영 절차에 필연적으로 관여하며, 효과를 최대화하기 위해 기타 시스템, 제품 또는 서비스를 요구할 수도 있습니다. IBM은 시스템 및 제품이 제3자의 악성 또는 불법적인 행위로부터 면역되어 있다고 보증하지 않습니다.



재활용하세요