IBM MaaS360 (SaaS)

본 서비스 명세서는 IBM 이 고객에게 제공하는 클라우드 서비스(Cloud Service)에 대해 설명합니다. 고객이란 클라우드 서비스의 계약 당사자, 승인된 사용자 및 수령자를 의미합니다. 관련 견적서와 라이센스 증서(PoE)는 별도의 거래서류(Transaction Documents)로 제공됩니다.

1. 클라우드 서비스

MaaS360 은 iOS, Android, Windows 및 Blackberry 운영 체제를 활용하는 최신 모바일 디바이스의 엔드투엔드 관리를 위한 핵심 기능이 포함된, 사용이 간편한 클라우드 플랫폼입니다. 클라우드 서비스 오퍼링에 대한 간단한 설명은 다음과 같습니다.

1.1 IBM MaaS360 Mobile Device Management (SaaS) 및 IBM MaaS360 Mobile Device Management (SaaS) Step up for existing customers

핵심 MDM(Mobility Device Management) 기능에는 디바이스 등록, 구성, 보안 정책 관리, 및 메시지 전송, 찾기, 잠금, 지우기 등의 디바이스 조치가 포함됩니다. 고급 MDM 기능에는 자동화된 준수 룰, BYOD(bring your own device) 개인 정보 설정, Mobility Intelligence 대시보드 및 보고 기능이 포함됩니다.

1.2 IBM MaaS360 Mobile Application Management (SaaS) 및 IBM MaaS360 Mobile Application Management (SaaS) Step up for existing customers

MaaS360 Mobile Application Management 는 애플리케이션을 추가하고 MaaS360 관리하에서 지원되는 디바이스에 해당 애플리케이션을 배포하는 기능을 제공합니다. 이에는 사용자가 관리 대상 애플리케이션을 보고 설치하며 업데이트 경보를 제공하는 on-device 애플리케이션인 MaaS360 App Catalog 가 포함됩니다.

1.3 IBM MaaS360 Mobile Application Security (SaaS) 및 IBM MaaS360 Mobile Application Security (SaaS) Step up for existing customers

MaaS360 Mobile Application Security 는 개발 시 WorkPlace SDK 를 사용하는 엔터프라이즈 애플리케이션이나 애플리케이션(.ipa), 프로비저닝 프로파일, 서명 인증이 자동으로 통합되는 iOS 앱 업로드에 대한 추가적인 데이터 보호 기능을 제공합니다. Mobile Application Security 는 앱과 Productivity Suite 를 통합합니다. 이를 통해 단일 사인온(single sign on), Mobile Enterprise Gateway 를 통한 인트라넷 액세스, 데이터 보안 설정 실행이 가능합니다.

1.4 IBM MaaS360 Gateway for Apps (SaaS) 및 IBM MaaS360 Gateway for Apps (SaaS) Step up for existing customers

MaaS360 Gateway for Apps 는 전체 디바이스 VPN 연결 없이 내부 애플리케이션 자원에 대한 매끄러운 액세스 경로를 엔터프라이즈 네트워크 외부의 사용자에게 제공합니다.

1.5 IBM MaaS360 Mobile Content Management (SaaS) 및 IBM MaaS360 Mobile Content Management (SaaS) Step up for existing customers

MaaS360 Mobile Content Management 를 통해 관리자는 IBM MaaS360 Mobile Device Management 관리 하의 지원되는 디바이스에 문서를 추가하고 배포할 수 있습니다. 사용자가 문서를 보호되어 간편하게 액세스, 확인 및 공유할 수 있는, 비밀번호로 보호된 on-device 컨테이너인 IBM MaaS360 Doc Catalogue 가 포함됩니다. 이에는 배포된 컨텐츠와 저장소(예: SharePoint, Box, Google Drive)에 대한 유연한 액세스가 포함됩니다. MaaS360 Gateway for Documents 에서 개인용 SharePoint 액세스와 Windows 파일 공유가 가능합니다. MaaS360 에서 관리하는 문서는 인증 필수, 복사-붙여쓰기 기능 제한, 다른 애플리케이션에서 열기나 공유 금지 등의 DLP(data loss prevention) 정책 옵션을 통해 버전 제어되고 감사되며 보호됩니다.

1.6 IBM MaaS360 Mobile Document Sync (SaaS) 및 IBM MaaS360 Mobile Document Sync (SaaS) Step up for existing customers

MaaS360 Mobile Document Sync 는 관리 모바일 디바이스에서 사용자 컨텐츠를 동기화하는 기능을 사용자에게 제공합니다. 관리자는 잘라내기-복사-붙여넣기 제한, 다른 앱에서 컨텐츠 열기나 공유 금지 등의 정책이 디바이스의 사용자 컨텐츠에 적용되는지 확인할 수 있습니다. 컨텐츠는 클라우드와 디바이스에 보호된 방식으로 저장되며 MaaS360 Doc Catalogue 를 통해서만 액세스됩니다.

1.7 IBM MaaS360 Mobile Document Editor (SaaS) 및 IBM MaaS360 Mobile Document Editor (SaaS) Step up for existing customers

MaaS360 Mobile Document Editor 는 사용자가 업무 중에 비즈니스 문서 작업을 수행할 수 있는 강력한 오피스 스위트입니다. MaaS360 Mobile Document Editor 로 다음을 수행할 수 있습니다.

- .DOC, .PPT 및 .XLS 파일 작성 및 편집
- 프리젠테이션 모드의 슬라이드
- MaaS360 for iOS 의 이메일 첨부 문서 및 기타 파일에 대한 작업 용이

1.8 IBM MaaS360 Gateway for Documents (SaaS) 및 IBM MaaS360 Gateway for Documents (SaaS) Step up for existing customers

MaaS360 Gateway for Documents 와 함께 조직은 MaaS360 Mobile Content Management 를 사용하여 전체 디바이스 VPN 연결 없이 내부 Connections 사이트, SharePoint 사이트, Windows File Shares 및 기타 파일 저장소에 대한 매끄러운 액세스를 엔터프라이즈 네트워크의 외부 디바이스에 추가로 제공할 수 있습니다. MaaS360 Gateway for Documents 를 사용하려면 MaaS360 Mobile Content Management 도 구입해야 합니다. iOS 5.0 및 Android 4.0 이상을 지원합니다.

1.9 IBM MaaS360 Email Management (SaaS) 및 IBM MaaS360 Email Management (SaaS) Step up for existing customers

MaaS360 Email Management 에는 Microsoft Exchange ActiveSync 및 Lotus Traveler 를 지원하기 위한 중요 기능이 포함됩니다.

- Exchange ActiveSync: ActiveSync 프로토콜을 통해 Microsoft Exchange 에 연결하는 모바일 디바이스에 대한 지원을 제공합니다. 디바이스 구성, ActiveSync 정책(패스코드, 이메일 액세스 허용 또는 차단) 작성 및 실행, 디바이스 조치 수행(예: 잠금, 지우기, 디바이스 속성 세부 보고서) 등의 핵심 MDM 기능이 포함됩니다.
- Lotus Traveler: Lotus Traveler 프로토콜을 통해 IBM Lotus Notes®에 연결하는 모바일 디바이스에 대한 지원을 제공합니다. 디바이스 구성, 디바이스 차단 또는 허용, 패스코드 정책 실행, 디바이스 삭제, 디바이스 속성 세부 보고서 개발 기능이 포함됩니다.

1.10 IBM MaaS360 Secure Mobile Browser (SaaS) 및 IBM MaaS360 Secure Mobile Browser (SaaS) Step up for existing customers

MaaS360 Browser 는 소셜 네트워킹, 유해 컨텐츠, 악성 사이트 등 다양한 컨텐츠 카테고리에 따라 사용자가 승인된 웹 컨텐츠에만 액세스할 수 있도록 웹 사이트 필터링 및 보안 정책을 정의하여 사내 인트라넷 사이트의 액세스를 제공하고 컨텐츠 정책 준수를 실행하는 완전한 기능의 웹 브라우저입니다. MobileFirst Protect 디바이스와 결합 시 블랙리스팅 또는 애플리케이션 정책을 통해 기본 웹 브라우저와 써드파티(third-party) 웹 브라우저를 사용 불가능하게 하는 기능이 포함됩니다. 웹 사이트의 화이트리스트 예외사항, 쿠키 제한, 기능 복사, 붙여넣기 및 인쇄, 키오스크 모드를 사용할 수 있습니다.

1.11 IBM MaaS360 Gateway for Browser (SaaS) 및 IBM MaaS360 Gateway for Browser (SaaS) Step up for existing customers

지원되는 디바이스에서는 MaaS360 Gateway for Browser 를 사용하여 전체 디바이스 레벨의 VPN 연결 없이 승인된 내부 웹 사이트에 액세스할 수 있습니다.

1.12 IBM MaaS360 for BlackBerry (SaaS) 및 IBM MaaS360 for BlackBerry (SaaS) Step up for existing customers

BlackBerry API 를 사용하여 BES(BlackBerry Enterprise Server) 연결 모바일 디바이스에 대한 지원을 제공합니다. 메시지 전송, 패스코드 재설정, BES 정책 지정 및 삭제, 디바이스 속성 세부 보고 등의 원격 조치가 포함됩니다. MaaS360 Cloud Extender 를 반드시 설치해야 합니다. BES 5.0 을 통해 MaaS360 로 보거나 관리하는 디바이스에만 사용 가능합니다.

1.13 IBM MaaS360 Mobile Expense Management (SaaS) 및 IBM MaaS360 Mobile Expense Management (SaaS) Step up for existing customers

MaaS360 Mobile Expense Management 를 통해 관리자는 데이터 사용량 정책을 작성하여 MaaS360 관리 하의 지원되는 디바이스에 지정할 수 있으며 해당 정책을 디바이스, 그룹 또는 글로벌 레벨로 할당하고 네트워크 및 로밍 데이터 사용량 모두에 대한 경보 임계값과 메시징을 구성할 수 있습니다.

1.14 IBM MaaS360 Productivity Suite (SaaS) 및 IBM MaaS360 Productivity Suite (SaaS) Step up for existing customers

MaaS360 Secure Mobile Mail, MaaS360 Mobile Application Management, MaaS360 Mobile Application Security, MaaS360 Content Service 및 MaaS360 Secure Mobile Browser 를 포함한 제품의 스위트/번들입니다.

1.15 IBM MaaS360 Secure Mobile Mail (SaaS) 및 IBM MaaS360 Secure Mobile Mail (SaaS) Step up for existing customers

MaaS360 Secure Mobile Mail 은 다른 애플리케이션으로 컨텐츠 전달 또는 이동을 제한하여 데이터 유출을 방지하고 인증을 실행하고 잘라내기-복사-붙여넣기를 제한하고 이메일 첨부 문서를 보기 전용으로 잠가 이메일 및 첨부 문서를 제어하는 기능을 사용하여 사용자가 이메일, 캘린더 및 연락처를 액세스 및 관리할 수 있는 별도의 오피스 생산성 애플리케이션을 제공합니다.

1.16 IBM MaaS360 Gateway Suite (SaaS) 및 IBM MaaS360 Gateway Suite (SaaS) Step up for existing customers

MaaS360 Gateway Suite 를 통해 iOS 및 Android 에서 지원되는 앱은 사내 네트워크의 자원에 대해 매끈하게 통신할 수 있습니다.

1.17 IBM MaaS360 Content Suite (SaaS) 및 IBM MaaS360 Content Suite (SaaS) Step up for existing customers

MaaS360 Mobile Content Management, MaaS360 Mobile Document Editor 및 MaaS360 Mobile Document Sync 를 포함한 제품의 스위트/번들입니다.

1.18 IBM MaaS360 Mobile Threat Management (SaaS)

MaaS360 Mobile Threat Management 는 모바일 악성 코드 감지 및 고급 jailbreak/root 감지 기능을 비롯한 개선된 모바일 보안을 제공합니다. MaaS360 Mobile Threat Management 를 사용하여 고객은 감지된 악성 코드 및 기타 보안 취약점에 대한 준수 정책을 설정하고 관리할 수 있습니다.

1.19 IBM MaaS360 Content Service (SaaS)

MaaS360 Content Service (SaaS)는 MaaS360 Content Distribution 시스템에 애플리케이션 패키지와 문서를 업로드하는 기능을 사용자에게 제공합니다.

IBM MaaS360 은 각 고객에게 1GB 의 스토리지를 제공합니다. IBM MaaS360 은 또한 연간 디바이스당 6GB 의 대역폭 활용량을 대역폭의 공유 풀로 제공합니다. 모든 디바이스에서 전체 대역폭 풀을 공유합니다. 이러한 기본 스토리지와 대역폭 할당량은 구입한 제품 번들이나 라인 품목의 수에 관계 없이 늘어나지 않습니다. 고객은 제공된 기본 용량을 초과하여 사용하고자 하거나 초과 용량이 필요한 경우 스토리지 및/또는 대역폭을 추가로 구입해야 합니다.

1.20 IBM MaaS360 Content Service Storage (SaaS)

MaaS360 Content Service Storage (SaaS)는 MaaS360 Content Service (SaaS)에서 사용 가능한 데이터 스토리지의 총 용량을 구입하는 기능을 사용자에게 제공합니다.

1.21 IBM MaaS360 Content Service Bandwidth (SaaS)

MaaS360 Content Service Bandwidth (SaaS)는 MaaS360 Content Service (SaaS)에서 사용 가능한 대역폭의 총 용량을 구입하는 기능을 사용자에게 제공합니다.

1.22 IBM MaaS360 Professional (SaaS)

회사 및 개인 디바이스에 원격으로 스마트폰과 태블릿을 구성하고 보안 정책을 시행하며 애플리케이션과 문서를 푸시하고 데이터를 보호할 수 있는 빠르고 간단한 방법을 중소 기업에 제공합니다. 고객은 고객의 비즈니스에 적합한 이동성 관리 기능에 신속하고 용이하고 알맞은 가격으로 액세스할 수 있는 권한을 확보할 수 있습니다.

1.23 IBM MaaS360 VPN (SaaS)

IBM MaaS360 VPN 은 사용자가 모바일 디바이스에서 회사 네트워크로 매끈하게 연결할 수 있도록 하는 가상 사설망(VPN) 솔루션입니다. 이 솔루션은 모바일 디바이스의 클라이언트와 VPN 서버로 구성되며 Device VPN, On-demand VPN, Always on VPN, Per-app VPN, 분할 터널링(Split tunneling) 등의 피처를 지원합니다.

1.24 IBM MaaS360 Laptop Location (SaaS)

MaaS360 Laptop Location (SaaS)에서는 지원되는 랩탑 및 태블릿을 찾는 기능을 사용할 수 있습니다. MaaS360 은 IP 주소 좌표 또는 Wi-Fi 위치를 보고하고 이러한 데이터를 쉽게 인식할 수 있는 주소로 변환합니다. 디바이스가 온라인 상태이면 디바이스의 현재 위치를 검색할 수 있습니다. MaaS360 은 시간의 경과에 따라 보고된 위치를 저장하므로 위치 히스토리를 검토할 수 있습니다. MaaS360 Suite 중 하나가 필요합니다. Windows Vista, Windows 7, Windows 8+를 지원합니다.

1.25 IBM MaaS360 Suites

IBM MaaS360 Suites 는 고객이 자신의 유스 케이스를 구동하는 데 가장 적합한 기능을 선택할 수 있도록 합니다. 아래 표에는 각 MaaS360 Suite 에 포함된 기본 피처와 기능이 설명되어 있습니다.

피처	MANAGEMENT (*)	ESSENTIAL	DELUXE	PREMIER	ENTERPRISE
Mobile Device Management (iOS, Android, Windows Mobile, Windows & macOS)	✓	✓	✓	✓	✓
Mobile Application Management (iOS, Android, Windows Mobile, Windows & macOS)	✓	✓	✓	✓	✓
Patch and Update Management (**)	✓	✓	✓	✓	✓
Advisor	✓	✓	✓	✓	✓
Container App	✓	✓	✓	✓	✓
Mobile Expense Management	✓	✓	✓	✓	✓
Identity Management (***)		✓	✓	✓	✓
Secure Mobile Mail			✓	✓	✓
Secure Mobile Chat			✓	✓	✓
VPN				✓	✓
Secure Browser				✓	✓

피처	MANAGEMENT (*)	ESSENTIAL	DELUXE	PREMIER	ENTERPRISE
Gateway for Browser				✓	✓
Content Management				✓	✓
Gateway for Documents				✓	✓
App Security				✓	✓
Gateway for Apps				✓	✓
Mobile Document Editor					✓
Mobile Document Sync					✓
Mobile Threat Management					✓

* IBM MaaS360 Management Suite(SaaS)는 Step Up 파트로서, 기존 고객이 사용할 수도 있습니다.

** Patch and Update Management 기능은 Windows 및 macOS 엔드포인트에서 실행 중인 운영 체제와 애플리케이션의 패치 및 업데이트를 식별, 보고, 배포 및 설치하는 기능을 제공합니다.

*** Identity Management 기능은 고객이 사용 중인 다른 퍼블릭 클라우드 애플리케이션에 대한 싱글 사인온(SSO)을 제공하는 IBM Cloud Identity Essentials 오퍼링의 기능을 포함함으로써 제공됩니다.

1.26 IBM MaaS360 Mobility Success Services

IBM MaaS360 Mobility Success Services 는 고객의 현재 등록(subscription) 기간 이내에 사용하는 인게이지먼트(Engagement)로 구입되며 다음 특정 서비스를 포함합니다. 이 원격 제공 서비스에서는 IBM 컨설턴트를 통해 우수 사례, 구성 및 트레이닝에 대한 지침과 지원을 제공합니다.

a. IBM MaaS360 Quick Start Setup Service

IBM MaaS360 Quick Start Setup Service 는 지식 이전을 기본 목표로 최대 3 개의 Cloud Extender, 하나의 게이트웨이, 최대 4 개의 정책, 최대 10 개의 디바이스 등록을 포함하여 대상 환경에 대한 MaaS360 SaaS 배치를 구현하기 위한 전문 지식과 지침을 제공합니다. IBM 은 일련의 웹 컨퍼런스를 제공하고 고객의 배치를 지원하기 위한 40 시간 이내의 컨설팅 전문 지식을 제공합니다. 컨설턴트는 BYOD(Bring Your Own Device) 프로그램의 우수 사례, 배치에 영향을 주는 내부 비즈니스 사례와 정책 배치에 대해 논의하고 하드웨어 선행 조건, 프로덕션 아키텍처 및 디바이스 등록 전략을 결정하는 데 도움을 줍니다.

컨설턴트는 고객의 인증 기관, 기업 디렉토리 및 이메일 시스템과의 통합을 포함하여 Cloud Extender 와 Enterprise Gateway 의 설치 및 구성에 대해서도 지원합니다. 또한 컨설턴트는 최대 3 명의 사용자에 대한 포털 둘러보기 및 인에이블먼트 세션을 포함한 MaaS360 포털과 솔루션 트레이닝, 디바이스 정책 및 준수 프로파일 설정을 포함한 하나의 컨테이너, 하나의 iOS 정책, 하나의 Android 정책, 하나의 Windows 폰 정책의 최대 4 개 정책에 대한 구성 지원을 제공합니다. 컨설턴트는 정책 및 사용자 관리, 보고, 준수 규칙, 애플리케이션 관리, 앱 및 문서 관리에 관한 우수 사례와 산업 표준에 대해 논의하며 최대 10 개의 디바이스에서 구현된 솔루션에 대한 QA 를 제공합니다. 인게이지먼트 종료 후에는 2 주에서 4 주 간, 상황 점검을 수행하여 고객의 MaaS360 사용 및 적용 성공 여부를 검토하고 완전한 적용에 필요한 후속 서비스를 파악합니다.

b. IBM MaaS360 Health Check Service

IBM MaaS360 Health Check Service 는 고객의 MaaS360 환경과 구현을 검토하는 전문 지식과 지침을 원격으로 제공하고 사용자 경험, 보안 및 인프라스트럭처 스케일링에 대한 권장사항을 작성합니다. IBM 컨설턴트는 스케일링, 엔터프라이즈 통합, 등록 프로세스의 중요한 측면을 검토하여 고객의 배치를 지원하기 위한 8 시간 이내의 컨설팅 전문 지식을 제공하는 일련의 웹 컨퍼런스를 실시하고 성과와 사용자 경험에 대한 테스트 케이스 평가를 실시하여 안정된 구현에 필요한 필수 시스템과 네트워크 변경사항을 이해하고 문서화합니다. IBM 컨설턴트는 인게이지먼트 종료 시 테스트 케이스 세부사항과 결과, 사용자 경험과 적용, 보안 및 인프라스트럭처 스케일링을 향상시키기 위한 권장사항을 제공하는 상황 점검 보고서 카드를 제공합니다.

c. IBM MaaS360 Mobility Training Workshop

IBM MaaS360 Mobility Training Workshop 은 MaaS360 솔루션을 지원하는 툴과 지식을 관리 직원과 보조 직원에게 제공하는 주제에 대한 정식 커리큘럼이 포함된 원격 제공 트레이닝을 최대 12 명의 개인에게 웹 및 비디오 컨퍼런스를 통해 영어로 제공합니다.

IBM 트레이너는 관리 직원과 운영 팀에게 2 일 간의 워크샵을 제공합니다. 고객 헬프 데스크 팀(level 1)은 사용자 요청을 관리하고 대응하는 방법, IBM MaaS360 기본사항, 관리, 에스컬레이션, 고객 배치 관련 사항을 포함한 level 1 지원 처리 과정에 대해 교육받습니다. 고객의 모바일 운영 팀(level 2)에게는 컨테이너 및 엔터프라이즈 통합 영역의 과정과 내부의 다른 팀에 대한 지원을 이해하기 위한 추가 교육을 제공합니다. 기타 고객 모바일 관리 직원(이메일, 보안, 인프라스트럭처, 모바일 관리 팀)에게는 멀티테넌시, 모바일 디바이스 및 컨텐츠 보안을 포함하여 제품을 효과적으로 안전하게 관리하는 방법에 대한 추가 교육을 제공합니다. 교육 세션용으로 개발된 자료는 모든 참가자에게 소프트 카피로 제공됩니다.

d. IBM MaaS360 Advisor on Demand

IBM MaaS360 Advisor on Demand 서비스는 IBM MaaS360 제품 최적화 및 배치 작업과 관련된 활동에 사용할 수 있는 최대 20 시간의 IBM 전문 서비스 컨설턴트 시간을 제공합니다. IBM 컨설턴트는 구현 또는 마이그레이션 프로세스 동안 일반 전략, 기술 설계, 프로세스, 테스트 및 프로덕션 운영 우수 사례를 자문하는 전담 지원을 제공하기 위한 자문 기술 논의를 돕습니다. IBM 은 프로젝트 목표, 관련 기술, 적합한 타임라인, 예상 인도물 및 예상 Advisor on Demand 서비스 인게이지먼트 수를 포함하여, 고객의 특정 요구사항이 반영된 프로젝트 스케줄을 이해하고 작성하도록 고객과 협력합니다. 고객은 서비스 수행에 필요한 필수 애플리케이션, 시스템 및 문서에 대한 액세스 권한을 제공해야 합니다. Advisor on Demand 서비스는 최대 20 시간의 보안 전문 기술을 수행한 경우, 및/또는 프로젝트 스케줄 및/또는 프로젝트 스케줄에 정의되어 있는 문서화된 인도물이 고객에게 전달되고 나면 완료됩니다.

1.26.1 IBM MaaS360 Mobility Success Services 책임사항

IBM 은 다음을 수행합니다.

- 고객이 구입한 Mobility Success Services 를 제공하며,
- 고객 프로젝트 관리자와 협력하여 인게이지먼트를 스케줄링하고 자원을 조정하는 IBM Engagement Manager 역할을 수행할 담당자를 지정합니다.

고객은 다음에 동의합니다.

- 계약 기간 동안 고객이 요청한 모든 인게이지먼트 요청과 관련된 모든 대금 청구에 대해 책임을 집니다.
- 구입한 인게이지먼트는 최초 계약 기간 내에 반드시 사용해야 하며 계약 기간 종료일까지 미사용된 경우에는 만료된다는 점을 인정합니다.
- 모든 Set Up 서비스에 대한 공식 요청은 사용등록 종료일에서 최소 30 일 전에 시작합니다.

IBM 은 Mobility Success Service 를 수행하는 과정에서 고객에게 정보 및 합당한 협조를 요청할 수 있습니다. 고객이 요청된 정보나 협조를 적절하게 제공하지 못하는 경우 IBM 의 판단에 따라 서비스에서 필요한 대로 인게이지먼트 요금을 부과하거나 관련 서비스의 수행이 지연될 수 있습니다.

고객은 IBM 이 테스트를 정확하게 수행하도록 필요한 경우 인게이지먼트 기간 동안 환경 준비와 유지보수에 관한 IBM 지침을 준수한다는 데 동의합니다.

2. 보안 설명

이 클라우드 서비스는 IBM SaaS 에 관한 IBM 데이터 보안 및 개인정보 보호 정책(http://www.ibm.com/cloud/data-security 참조)과 본 조건에서 제공한 추가 조건을 준수합니다. IBM 데이터 보안 및 개인 정보 보호 정책이 변경되더라도 클라우드 서비스의 보안 수준은 저하되지 않습니다.

고객이 데이터 관리자로서, 기술적 및 조직적 보안 조치가 처리 시 발생된 위험과 보호할 데이터의 성격에 적합하다고 판단한 경우 이 클라우드 서비스에서 개인 데이터가 포함된 디바이스 정보, 사용자 이름 및 이메일 주소를 처리할 수 있습니다. 고객은 이 클라우드 서비스는 민감한 개인 데이터나

추가적인 규제 요건이 적용되는 데이터를 보호하기 위한 기능을 제공하지 않는다는 점을 인지합니다. 고객은 IBM 은 고객의 컨텐츠에 포함된 데이터 유형에 대해 알 수 없으며 클라우드 서비스나 포함된 보안 조치의 적합성을 평가할 수 없다는 점을 인정합니다.

2.1 보안 기능 및 책임사항

클라우드 서비스는 다음 보안 기능을 구현합니다.

클라우드 서비스에서는 IBM 네트워크 외부에서 데이터가 전송되는 동안 컨텐츠를 암호화합니다. 클라우드 서비스는 데이터 전송을 대기하는 정지 기간 동안 컨텐츠를 암호화합니다.

본 클라우드 서비스는 고객이 미국에 소재하는 데이터 센터에서 클라우드 서비스를 호스팅하도록 선택하는 경우 IBM Privacy Shield 인증에 포함되어 적용되며 IBM Privacy Shield 개인정보 보호정책(http://www.ibm.com/privacy/details/us/en/privacy_shield.html 참조)의 적용을 받습니다.

3. SLA(Service Level Agreement)

IBM 은 라이센스 증서에 명시된 바와 같이 클라우드 서비스의 가용성에 관한 "서비스 레벨 계약"(이하 SLA)을 제공합니다. SLA 는 보증이 아닙니다. SLA 는 고객에게만 제공되며 프로덕션 환경의 사용에만 적용됩니다.

3.1 가용성 크레디트

고객은 중대한 업무 영향이 있고 클라우드 서비스가 사용 불가능하다는 것을 처음으로 인지한 시점으로부터 24 시간 이내에 심각도 1 지원 티켓을 IBM 기술 지원 헬프 데스크에 로그(log)해야 합니다. 고객은 문제점의 진단과 해결에 있어서 합리적으로 IBM 을 지원해야 합니다.

SLA 를 충족하지 못한 데 대한 지원 티켓 클레임은 약정 월 말일 이후 3 영업일 이내에 제출되어야 합니다. 유효한 SLA 클레임에 대한 보상은 클라우드 서비스의 프로덕션 시스템 처리가 불가능한 시간 동안의 지속 기간(이하 "Downtime")을 기준으로 클라우드 서비스의 추후 청구서에 대한 크레디트가 됩니다. Downtime 은 고객이 이벤트를 보고한 시간부터 클라우드 서비스가 복원된 시간까지로 측정되며 스케줄되거나 발표된 유지보수 중단 시간, IBM 의 통제를 벗어난 원인, 고객 또는 제 3 자 컨텐츠나 기술, 설계나 지침의 문제점, 지원되지 않는 시스템 구성 및 플랫폼 또는 기타 고객의 오류, 고객으로 인한 보안 사고 또는 고객 보안 테스트는 포함되지 않습니다. IBM 은 아래 표와 같이 각 약정된 월 동안의 누적 클라우드 서비스 가용성에 따라 적용 가능한 최대의 보상을 적용합니다. 약정 월에 적용되는 보상의 총 금액은 클라우드 서비스의 연간 대금의 12 분의 1(1/12)의 10%를 초과할 수 없습니다.

번들 클라우드 서비스(bundled Cloud Services)(단일 통합 가격의 단일 오퍼링으로 함께 패키지되고 판매되는 개별 클라우드 서비스 오퍼링)의 보상은 번들 클라우드 서비스에 대하여 월별로 통합된 단일 가격을 기준으로 산출되며 각 개별 클라우드 서비스의 월별 등록료를 기준으로 하지 않습니다. 고객은 주어진 시점에 번들 중 하나의 개별 클라우드 서비스와 관련된 클레임만을 제출할 수 있습니다.

3.2 서비스 레벨

약정 월 동안 클라우드 서비스 가용성

약정 월 동안 가용성	보상 (클레임 대상이 되는 약정 월의 월 사용등록(Subscription) 사용료*의 %)
< 99.8%	2%
< 98.8%	5%
< 95%	10%

* IBM 비즈니스 파트너로부터 클라우드 서비스를 취득한 경우, 월 등록 사용료는 클레임 대상이 되는 약정 월에 유효한, 50%의 할인이 제공된 클라우드 서비스의 당시 적용되는 정가를 기준으로 산정됩니다. IBM 은 고객이 직접 사용할 수 있는 장려금을 제공합니다.

백분율로 표시된 가용성은 약정 월의 총 시간(분)에서 약정 월의 총 Downtime(분)을 차감한 후 이를 약정 월의 총 시간(분)으로 나누어 산출합니다.

4. 기술 지원

클라우드 서비스에 대한 기술 지원은 다음 방법으로 제공됩니다.

- 이메일
- 전화 번호
- 라이브 채팅

IBM 은 기술 지원 담당자 연락처 정보 및 기타 정보와 절차에 대해 설명하는 IBM Software as a Service Support Handbook 을 제공합니다. 기술 지원은 클라우드 서비스에 포함되며 별도의 오퍼링으로 제공되지 않습니다.

5. 권한 부여 및 대금 청구 정보

5.1 청구 체계

본 클라우드 서비스는 거래서류에 명시된 바와 같이 다음 청구 체계 하에서 제공됩니다.

a. 승인된 사용자(Authorized User)는 클라우드 서비스 오퍼링이 구매되는 경우 이용되는 산정 단위입니다. 고객은 어떠한 방법으로든(예: 다중 송신 프로그램, 디바이스 또는 애플리케이션 서버 등을 통해) 직접 또는 간접적으로 클라우드 서비스에 접속할 수 있는 액세스 권한이 부여된 각 고유한 승인된 사용자에 대해 별도의 전용 권한을 취득해야 합니다. 고객의 라이센스 증서 또는 거래서류에 명시된 산정 기간 동안 클라우드 서비스에 대한 액세스 권한이 제공된 승인된 사용자 수를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

b. 기가바이트(Gigabyte)는 클라우드 서비스가 구매되는 경우 이용되는 산정 단위입니다. 기가바이트는 2 의 30 승 데이터(1,073,741,824 바이트)로 정의됩니다. 고객의 라이센스 증서 또는 거래서류에 명시된 산정 기간 동안 클라우드 서비스에서 처리한 총 기가바이트 수를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

c. 관리 대상 클라이언트 디바이스(Managed Client Device)는 클라우드 서비스 구입 시 사용되는 측정 단위입니다. 클라이언트 디바이스란 일반적으로 서버라고 부르거나 서버에 의해 관리되는 다른 컴퓨터 시스템에서 명령, 프로시저 또는 애플리케이션 세트에 대한 실행을 요청하거나 수신하는 단일 사용자 컴퓨팅 디바이스 또는 특수 용도의 센서나 원격 측정 디바이스를 의미합니다. 다중 클라이언트 디바이스는 공통 서버에 대한 액세스를 공유할 수 있습니다. 클라이언트 디바이스는 일부 처리 기능을 갖추고 있거나 사용자가 작업을 수행할 수 있도록 프로그램화될 수 있습니다. 고객은 고객의 라이센스 증서 또는 거래서류에 명시된 산정 기간 동안 클라우드 서비스에서 관리한 각 클라이언트 디바이스에 대한 관리 대상 클라이언트 디바이스 권한을 취득해야 합니다.

d. 클라이언트 디바이스(Client Device)는 클라우드 서비스가 구매되는 경우 이용되는 산정 단위입니다. 클라이언트 디바이스란 일반적으로 서버라고 부르거나 서버에 의해 관리되는 다른 컴퓨터 시스템에서 명령, 프로시저 또는 애플리케이션 세트에 대한 실행을 요청하거나 수신하는 단일 사용자 컴퓨팅 디바이스 또는 특수 용도의 센서나 원격 측정 디바이스를 의미합니다. 다중 클라이언트 디바이스는 공통 서버에 대한 액세스를 공유할 수 있습니다. 클라이언트 디바이스는 일부 처리 기능을 갖추고 있거나 사용자가 작업을 수행할 수 있도록 프로그램화될 수 있습니다. 고객은 고객의 라이센스 증서 또는 거래서류에 명시된 산정 기간 동안 클라우드 서비스를 실행하거나 클라우드 서비스에 데이터를 제공하거나 클라우드 서비스가 제공한 서비스를 이용하거나 클라우드 서비스에 달리 액세스하는 각 클라이언트 디바이스에 대한 권한을 취득해야 합니다.

e. 인게이지먼트(Engagement)는 서비스가 구매되는 경우 이용되는 산정 단위입니다. 인게이지먼트는 클라우드 서비스와 관련된 전문 서비스 및/또는 교육 서비스로 구성됩니다. 각 인게이지먼트(Engagement)를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

5.2 설치(Set-Up) 요금

일시불 설치 요금은 주문된 각 설치 서비스의 거래서류에 지정된 요율로 청구됩니다.

5.3 추가 요금

산정 기간 동안 클라우드 서비스 실제 사용량이 라이센스 증서에 명시된 권한을 초과하면 거래서류에 지정된 요율에 따라 초과 사용한 그 다음 달에 초과분에 대한 요금이 고객에게 부과됩니다.

6. 기간 및 갱신 옵션

클라우드 서비스의 기간은 라이센스 증서에 명시된 바와 같이, IBM 이 고객에게 클라우드 서비스에 대한 고객의 액세스(접근) 권한에 대해 통지한 날부터 시작됩니다. 클라우드 서비스를 자동으로 갱신할지, 사용 계속 여부에 따라 갱신할지 또는 기간 만료 시 종료할지 여부는 라이센스 증서에 명시합니다.

자동 갱신의 경우, 고객이 기간 만료일로부터 최소 90 일 이전에 갱신하지 않겠다는 서면 통지를 제공하지 않으면 클라우드 서비스는 라이센스 증서에 명시된 기간에 대해 자동으로 갱신됩니다.

갱신 권한 수량은 IBM 이 상이한 권한 수량이 명시된 통지서를 수신하지 않는 한, 원래 주문 수량과 갱신 청구서 작성 이전의 해당 월에 대해 보고된 월별 수량 중 더 큰 수량과 동일합니다.

STEP UP 오퍼링의 갱신 권한 수량은 원래 주문 수량과 동일합니다.

계속적인 사용의 경우, 고객이 사전 90 일의 서면 종료 통지를 제출할 때까지 클라우드 서비스를 월단위로 계속 사용할 수 있습니다. 90 일 기간 이후에는 해당 역월(calendar month)의 말일까지 클라우드 서비스가 계속 제공됩니다.

7. 추가 조건

7.1 인에이블링 소프트웨어(Enabling Software)

고객은 클라우드 서비스의 사용이 용이하도록 인에이블링 소프트웨어를 고객 시스템에 다운로드하여 사용해야 합니다. 고객은 클라우드 서비스의 사용과 관련해서만 인에이블링 소프트웨어를 사용할 수 있습니다.

다음 IBM 소프트웨어 프로그램이, 해당 IBM 프로그램 라이센스의 조항에 의거해서 아래 제한사항에 추가하여 인에이블링 소프트웨어로서 포함되어 있습니다.

a. IBM MaaS360 Cloud Extender

b. IBM MaaS360 Mobile Enterprise Gateway

c. IBM MaaS360 Mobile Device

d. IBM Security Access Manager

- 사용 제한사항: 고객은 이 클라우드 서비스에서 관리하는 모바일 디바이스에서 엔터프라이즈 이메일 서버로의 프록시 연결에 대해서만 IBM Security Access Manager 를 사용할 수 있습니다.

7.2 Step Up 제한사항

"Step up for existing Customers"로 표시된 클라우드 서비스 오퍼링의 경우("Step up SaaS"), 고객은 해당 Step up SaaS 오퍼링 이름으로 식별되는 연관된 IBM 프로그램에 대한 적절한 라이센스 권한을 미리 또는 동시에 취득해야 합니다. 예를 들어, "IBM MobileFirst Protect - Devices (SaaS) Step up for existing customers"를 구입한 고객은 연관된 IBM 프로그램인 IBM MobileFirst Protect 에 대한 권한을 취득해야 합니다. Step up SaaS 에 대한 고객의 권한은 고객의 연관된 IBM 프로그램에 대한 권한을 초과할 수 없습니다.

고객이 Step up SaaS 를 취득하는 경우 Step up SaaS 권한과 함께 on-premise 설치 환경에서 동일한 IBM 프로그램 라이센스 권한을 사용할 수 없습니다. 예를 들어, 고객이 연관된 IBM 프로그램에 대한 250 부의 관리 대상 클라이언트 디바이스 권한을 보유하고 있고 100 부의 Step up SaaS 관리 대상 클라이언트 디바이스 권한을 구입하는 경우, 고객은 클라우드 서비스 환경에서 100 대의 Step up SaaS 관리 대상 클라이언트 디바이스를 관리하고 설치된 on-premise 소프트웨어에서 150 대의 관리 대상 클라이언트 디바이스를 관리할 수 있습니다.

고객은 고객이 관련 IBM 프로그램에 적용되는 (1)라이센스 권한과 (2)Subscription and Support 를 이미 확보했음을 보증합니다. Step up SaaS 의 사용등록(Subscription) 기간 동안, 고객은 Step up SaaS 권한과 관련해서 사용하는 IBM 프로그램 권한에 대해 유효한 Subscription and Support 를 유지해야

합니다. 연관된 IBM 프로그램을 사용할 수 있는 고객의 라이센스 또는 연관된 IBM 프로그램에 대한 고객의 Subscription and Support 가 종료되면 고객의 Step up SaaS 에 대한 사용 권한은 종료됩니다.

7.3 규범 데이터

다른 조건에도 불구하고, 규범적 연구, 분석, 데모 및 보고 목적에 한해서 IBM 은 클라우드 서비스에 대한 고객의 승인된 사용자 개인의 경험을 반영하는 데이터를 집계 및 익명의 형식으로 보관하고 사용할 수 있습니다(즉, 고객이나 고객의 승인된 사용자를 정보의 출처로 식별할 수 없으며 고객이나 고객의 승인된 사용자를 확인할 수 있는 개인 식별 정보(personally identifiable information)는 삭제됩니다).

7.4 데이터 수집 및 처리 권한

클라우드 서비스는 모바일 디바이스를 프로비저닝, 관리, 모니터링 및 제어하도록 설계되었습니다. 클라우드 서비스는 고객이 등록한 클라우드 서비스와 상호작동하도록 고객이 허가한 사용자와 디바이스로부터 정보를 수집합니다. 일부 지역의 경우 클라우드 서비스는 개인 정보로 간주될 수 있는 정보를 단독 또는 결합 형태로 수집합니다. 수집되는 데이터에는 허가된 사용자 이름, 전화번호, 등록된 이메일 주소, 디바이스 위치, 사용자 ID 및 MaaS360 브라우저의 브라우징 히스토리, 최종 사용자 디바이스 하드웨어, 소프트웨어 및 설정에 대한 정보, 디바이스에서 생성된 정보가 포함될 수 있습니다. 고객은 IBM 이 본 서비스 명세의 조건에 따라 해당 정보를 수집하고 처리하고 사용하도록 허용합니다.

7.5 데이터 보유

IBM 은 수집된 모든 정보(개인 정보도 포함될 수 있음)를 본 서비스 명세가 만료되거나 해지된 후 삭제합니다. 단, 상기한 용도나 적용되는 법률, 규정 또는 규제에 따라 데이터를 보유해야 하는 경우는 제외합니다. 이 경우 IBM 은 그러한 용도, 해당 법률, 규정 또는 규제에서 요구한 기간 동안 수집된 정보를 보유합니다.

7.6 보안 데이터

IBM 은 보안 활동을 포함하는 클라우드 서비스의 일부로 클라우드 서비스에서 수집된 비식별화 정보 및/또는 집계 정보("Security Data, 보안 데이터")를 준비하고 관리합니다. 보안 데이터는 아래 (d)에서 제공한 경우를 제외하고, 고객 또는 개인을 식별하지 않습니다. 고객은 또한 IBM 이 다음 용도로만 보안 데이터를 사용하거나 및/또는 복사할 수 있다는 데 동의합니다.

a. 보안 데이터(Security Data)의 게시 및/또는 배포(예: 사이버 보안 관련 분석 및/또는 컴파일)

b. 제품이나 서비스 개발 또는 개선

c. 내부적으로 또는 제 3 자와의 연구 수행

d. 확인된 제 3 자 범죄자 정보의 합법적 공유.