

IBM MaaS360 (SaaS)

Diese Servicebeschreibung bezieht sich auf den von IBM für den Kunden bereitgestellten Cloud-Service. Als Kunde werden das Unternehmen und seine berechtigten Benutzer sowie die Empfänger des Cloud-Service bezeichnet. Das maßgebliche Angebot und der Berechtigungsnachweis (Proof of Entitlement = PoE) werden als separate Auftragsdokumente zur Verfügung gestellt.

1. Cloud-Service

MaaS360 ist eine benutzerfreundliche Cloudplattform mit allen wesentlichen Funktionen für das End-to-End-Management moderner Mobilgeräte, auf denen die Betriebssysteme iOS, Android, Windows und Blackberry ausgeführt werden. Im Folgenden werden die Cloud-Service-Angebote in einer Kurzbeschreibung vorgestellt:

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

Zu den zentralen Mobility Device Management-Funktionen (MDM) gehören Geräteregistrierung, Konfiguration, Verwaltung von Sicherheitsrichtlinien und Aktionen für Geräte wie das Senden von Nachrichten und das Lokalisieren, Sperren und Löschen von Geräten. Die Advanced MDM-Features bieten automatisierte Konformitätsregeln, Datenschutzeinstellungen für Bring Your Own Device (BYOD) sowie Mobility Intelligence-Dashboards und Berichterstellung.

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

MaaS360 Mobile Application Management ermöglicht das Hinzufügen von Anwendungen und deren Verteilung an unterstützte Geräte, die von MaaS360 verwaltet werden. Bestandteil dieses Angebots ist der MaaS360 App Catalog, eine auf dem Gerät vorhandene Anwendung für Benutzer zum Anzeigen und Installieren verwalteter Anwendungen, die außerdem auf Updates für verwaltete Anwendungen aufmerksam macht.

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

MaaS360 Mobile Application Security bietet zusätzlichen Datenschutz für Unternehmensanwendungen, wenn bei der Entwicklung das WorkPlace SDK verwendet wird, sowie die Möglichkeit zum Hochladen von iOS-Apps als Anwendung (.ipa), ein Bereitstellungsprofil und die automatische Integration eines Signaturzertifikats. Mobile Application Security integriert die App mit der Productivity Suite. Auf diese Weise werden Single Sign-on, Intranetzugang über das Mobile Enterprise Gateway und die Durchsetzung der Datensicherheitseinstellungen ermöglicht.

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

Das MaaS360 Gateway for Apps bietet Benutzern außerhalb des Unternehmensnetzes einen nahtlosen Zugriffspfad auf interne Anwendungsressourcen, ohne dass dafür eine gerätebasierte VPN-Verbindung erforderlich ist.

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

MaaS360 Mobile Content Management ermöglicht dem Administrator das Hinzufügen und Verteilen von Dokumenten an die unterstützten Geräte, die von IBM MaaS360 Mobile Device Management verwaltet werden. Bestandteil dieses Angebots ist der IBM MaaS360 Doc Catalogue, ein auf dem Gerät befindlicher kennwortgeschützter Container, der Benutzern auf geschützte und einfache Weise den Zugriff auf Dokumente sowie das Anzeigen und Teilen von Dokumenten ermöglicht. Dieses Angebot bietet einen nahtlosen Zugriff auf verteilte Inhalte und Repositories wie SharePoint, Box und Google Drive. Der Zugriff auf private SharePoint- und Windows-Dateifreigaben erfolgt über das MaaS360 Gateway for Documents. Für Dokumente, die über MaaS360 verwaltet werden, wird Versionssteuerung unterstützt, sie können geprüft und über Richtlinienoptionen zum Schutz vor Datenverlusten (Data Loss Prevention, DLP), wie Authentifizierungsanforderung, Einschränkung der Kopier- und Einfügefunktion sowie

Blockierung der Dokumente, damit sie nicht in anderen Anwendungen geöffnet oder geteilt werden können, geschützt werden.

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

MaaS360 Mobile Document Sync bietet Benutzern die Möglichkeit, Benutzerinhalte über verwaltete Mobilgeräte hinweg zu synchronisieren. Administratoren können sicherstellen, dass Richtlinien, die beispielsweise das Ausschneiden, Kopieren und Einfügen von Inhalten einschränken oder das Öffnen oder Teilen von Inhalten in anderen Apps verhindern, für sämtliche Benutzerinhalte auf allen Geräten aktiviert sind. Inhalte werden sowohl in der Cloud als auch auf dem Gerät geschützt gespeichert und der Zugriff kann nur über den MaaS360 Doc Catalogue erfolgen.

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

MaaS360 Mobile Document Editor ist eine leistungsfähige Office-Suite, mit der Geschäftsdokumente auch unterwegs bearbeitet werden können. Der MaaS360 Mobile Document Editor:

- ermöglicht die Erstellung und Bearbeitung von DOC-, PPT- und XLS-Dateien
- verfügt über einen Präsentationsmodus für Folien
- ermöglicht die problemlose Bearbeitung von E-Mail-Anhängen und anderen Dateien aus MaaS360 for iOS

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

Unternehmen können MaaS360 Mobile Content Management in Verbindung mit dem MaaS360 Gateway for Documents einsetzen, um auch Geräten außerhalb des Unternehmensnetzes nahtlosen Zugriff auf interne Connections-Sites, SharePoint-Sites, Windows File Shares und andere Dateispeicher anzubieten, ohne dass dafür eine gerätebasierte VPN-Verbindung erforderlich ist. Um das MaaS360 Gateway for Documents nutzen zu können, muss zusätzlich MaaS360 Mobile Content Management erworben werden. Unterstützt werden iOS 5.0 und Android 4.0 oder höhere Versionen.

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

MaaS360 Email Management enthält Schlüsselfunktionen zur Unterstützung von Microsoft Exchange ActiveSync und Lotus Traveler.

- Exchange ActiveSync: Bietet Unterstützung für Mobilgeräte, die über das ActiveSync-Protokoll eine Verbindung zu Microsoft Exchange herstellen. Zu den Features gehören zentrale Managementfunktionen für Mobilgeräte wie das Konfigurieren von Geräten, das Erstellen und Durchsetzen von ActiveSync-Richtlinien (Passcode, Zugriff auf E-Mail sperren oder zulassen), das Durchführen von Aktionen für Geräte wie Sperren und Löschen sowie detaillierte Berichte über Geräteattribute.
- Lotus Traveler: Bietet Unterstützung für Mobilgeräte, die über das Lotus Traveler-Protokoll eine Verbindung zu IBM Lotus Notes® herstellen. Zu den Features gehören das Konfigurieren von Geräten, das Sperren oder Freigeben von Geräten, das Durchsetzen von Passcoderrichtlinien, das Löschen von Geräten und das Erstellen detaillierter Berichte über Geräteattribute.

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

Der MaaS360 Browser ist ein mit vielen Funktionen ausgestatteter Web-Browser, der den Zugriff auf die Intranet-Sites des Unternehmens ermöglicht und die Einhaltung von Inhaltsrichtlinien durchsetzt, indem Richtlinien für Website-Filterung und Sicherheitsrichtlinien definiert werden, um sicherzustellen, dass Benutzer nur auf genehmigte Webinhalte zugreifen, die auf einer Reihe von Inhaltskategorien, wie beispielsweise Social-Networking-Sites, Sites mit bestimmten Inhalten oder Malware-Sites, basieren. Dazu gehört auch die Möglichkeit, native Web-Browser und Web-Browser anderer Anbieter bei der Nutzung in Verbindung mit MobileFirst Protect Devices entweder durch eine Anwendungsrichtlinie oder durch Blacklisting zu inaktivieren. Whitelist-Ausnahmen in Bezug auf bestimmte Websites, die Beschränkung von Cookies sowie der Funktionen Kopieren, Einfügen und Drucken und die Aktivierung des Kiosk-Modus sind weitere mögliche Optionen.

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

Das MaaS360 Gateway for Browser ermöglicht unterstützten Geräten den Zugriff auf genehmigte interne Websites, ohne dass dafür eine gerätebasierte VPN-Verbindung erforderlich ist.

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

Bietet über BlackBerry-APIs Unterstützung für Mobilgeräte, die mit einem BlackBerry Enterprise Server (BES) verbunden sind. Zu den Features gehören fern ausgeführte Aktionen, wie das Senden von Nachrichten, das Zurücksetzen des Passcodes, die Zuordnung einer BES-Richtlinie und die Löschung eines Geräts sowie die Erstellung detaillierter Berichte über Geräteattribute. Die Installation von MaaS360 Cloud Extender ist erforderlich. Diese Unterstützung ist nur für Geräte verfügbar, die mit MaaS360 über BES 5.0 angezeigt oder verwaltet werden.

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

MaaS360 Mobile Expense Management ermöglicht dem Administrator die Erstellung von Datennutzungsrichtlinien und deren Zuordnung zu unterstützten Geräten, die über MaaS360 verwaltet werden. Diese Richtlinien können auf Geräte-, Gruppen- oder globaler Ebene zugeordnet werden, und es können Schwellenwerte für Warnhinweise und Benachrichtigungen sowohl für die Nutzung innerhalb des Netzes als auch für Daten-Roaming konfiguriert werden.

1.14 IBM MaaS360 Management Suite (SaaS) und IBM MaaS360 Management Suite (SaaS) Step up for existing IBM MaaS360 customers

Produkt-Suite/Produkt-Bundle bestehend aus MaaS360 Mobile Device Management, MaaS360 Mobile Application Management, MaaS360 Content Service und MaaS360 Mobile Expense Management.

1.15 IBM MaaS360 Productivity Suite (SaaS) und IBM MaaS360 Productivity Suite (SaaS) Step up for existing customers

Produkt-Suite/Produkt-Bundle bestehend aus MaaS360 Secure Mobile Mail, MaaS360 Mobile Application Management, MaaS360 Mobile Application Security, MaaS360 Content Service und MaaS360 Secure Mobile Browser.

1.16 IBM MaaS360 Secure Mobile Mail (SaaS) und IBM MaaS360 Secure Mobile Mail (SaaS) Step up for existing customers

MaaS360 Secure Mobile Mail stellt Benutzern eine separate Officeproduktivitätsanwendung für den Zugriff und die Verwaltung von E-Mail, Kalender und Kontakten bereit. Sie bietet die Möglichkeit, E-Mails und Anhänge zu kontrollieren, das Ausspähen von Daten (Datenlecks) zu verhindern, indem das Weiterleiten oder Verschieben von Inhalten in andere Anwendungen eingeschränkt wird, eine Authentifizierung zu erzwingen, das Ausschneiden, Kopieren und Einfügen von Inhalten einzuschränken und E-Mail-Anhänge zu sperren, damit sie nur im Ansichtsmodus aufrufbar sind.

1.17 IBM MaaS360 Gateway Suite (SaaS) und IBM MaaS360 Gateway Suite (SaaS) Step up for existing customers

MaaS360 Gateway Suite ermöglicht unterstützten Apps auf iOS und Android die nahtlose Kommunikation mit Ressourcen im internen Netz des Unternehmens.

1.18 IBM MaaS360 Content Suite (SaaS) und IBM MaaS360 Content Suite (SaaS) Step up for existing customers

Produkt-Suite/Produkt-Bundle bestehend aus MaaS360 Mobile Content Management, MaaS360 Mobile Document Editor und MaaS360 Mobile Document Sync.

1.19 IBM MaaS360 Mobile Threat Management (SaaS)

MaaS360 Mobile Threat Management verbessert die mobile Sicherheit durch das Erkennen mobiler Malware und die erweiterte Erkennung von Jailbreak/Rooting. Mit MaaS360 Mobile Threat Management ist der Kunde in der Lage, Konformitätsrichtlinien im Zusammenhang mit erkannter Malware und anderen Sicherheitslücken festzulegen und zu verwalten.

1.20 IBM MaaS360 Content Service (SaaS)

MaaS360 Content Service (SaaS) ermöglicht Benutzern den Upload von Anwendungspaketen und Dokumenten in das MaaS360 Content Distribution-System.

IBM MaaS360 stellt für jeden Kunden 1 GB an Speicher bereit. IBM MaaS360 bietet außerdem eine Bandbreitennutzung von 6 GB pro Gerät und Jahr über einen gemeinsamen Bandbreitenpool. Der gesamte Bandbreitenpool wird von allen Geräten gemeinsam genutzt. Dieser Basisspeicher und die Bandbreitenzuordnung erhöhen sich nicht, unabhängig davon, wie viele Produkt-Bundles oder Einzelprodukte erworben werden. Die Kunden müssen zusätzlichen Speicher und/oder zusätzliche Bandbreite erwerben, wenn das bereitgestellte Basisvolumen überschritten wird oder mehr Speicher bzw. Bandbreite erforderlich ist.

1.21 IBM MaaS360 Content Service Storage (SaaS)

MaaS360 Content Service Storage (SaaS) ermöglicht Benutzern den Erwerb des gesamten Datenspeichers, der für die Nutzung mit dem MaaS360 Content Service (SaaS) verfügbar ist.

1.22 IBM MaaS360 Content Service Bandwidth (SaaS)

MaaS360 Content Service Bandwidth (SaaS) ermöglicht Benutzern den Erwerb der gesamten Bandbreite, die für die Nutzung mit dem MaaS360 Content Service (SaaS) verfügbar ist.

1.23 IBM MaaS360 Professional (SaaS)

Bietet kleinen und mittelständischen Unternehmen eine schnelle und einfache Möglichkeit, Smartphones und Tablets über Fernzugriff zu konfigurieren, Sicherheitsrichtlinien durchzusetzen, Apps und Dokumente mit Push-Operationen zu übertragen sowie die Daten auf Unternehmensgeräten und privaten Geräten zu schützen. Dieses Angebot ermöglicht dem Kunden schnellen, einfachen und bezahlbaren Zugriff auf die für sein Unternehmen geeigneten Mobilitätsmanagementfunktionen.

1.24 IBM MaaS360 Laptop Management (SaaS)

Bietet dem Kunden die Möglichkeit, OS X- und Windows-basierte PCs sowie Smartphones und Tablets zu registrieren, zu konfigurieren, zu verwalten und Berichte über diese Geräte zu erstellen. Unternehmen können über dieselbe MaaS360-Managementkonsole konsistente Sicherheitsrichtlinien und Profile sowohl für unternehmenseigene als auch für mitarbeitereigene Geräte verwalten.

1.24.1 Windows

MaaS360 Laptop Management (SaaS) für Windows-basierte PCs ermöglicht die Registrierung über eine Funkschnittstelle (Over the Air = OTA) sowie die Erstellung von Bestandsmanagementberichten mit Informationen über Hardware, Betriebssysteme und Software. Das Berichterstellungsmodul für Endpunktsicherheit bietet interaktive Berichterstellung und Datenanalyse für vom Kunden bereitgestellte Anwendungen, wie beispielsweise Virenschutz, Backup/Recovery, Datenverschlüsselung, persönliche Firewall und fehlende Betriebssystempatches. Das Datenschutzmodul bietet interaktive Berichterstellung und Analyse für Sicherheitsservices, einschließlich Datenverschlüsselung, Vermeidung von Datenlecks (Data Leak Prevention), Backup/Recovery und weitere integrierte Anwendungen. Unterstützt werden XP SP3, Windows Vista, Windows 7, Windows 8+ und Windows 8+ Pro (sofern zutreffend, die 32-Bit- als auch die 64-Bit-Version).

Zu den für die Geräte ausführbaren Aktionen gehören:

- Senden einer Nachricht an ein Gerät
- Sperren eines Geräts
- Lokalisieren eines Geräts (dazu ist MaaS360 Laptop Location erforderlich)
- Stoppen/Starten/Erneutes Starten von Services
- Herunterfahren/Warmstart
- Löschen der Daten auf der Festplatte
- Konfigurieren der Patcheinstellungen
- Verteilen der Software

1.24.2 Mac OS X

MaaS360 Laptop Management (SaaS) für Mac OS X ermöglicht die Registrierung über eine Funkschnittstelle (Over the Air = OTA) sowie die Erstellung von Bestandsmanagementberichten mit

Informationen über Hardware, Betriebssysteme und Software. Das Berichterstellungsmodul für Endpunktsicherheit bietet interaktive Berichterstellung und Datenanalyse für vom Kunden bereitgestellte Anwendungen, wie beispielsweise Virenschutz, Backup/Recovery, Datenverschlüsselung, persönliche Firewall und fehlende Betriebssystempatches. Das Datenschutzmodul bietet interaktive Berichterstellung und Analyse für Datensicherheitsservices, einschließlich Datenverschlüsselung. Das Konfigurationsmanagementmodul ermöglicht die Fernverwaltung einer Reihe von Geräte- und Benutzereinstellungen, einschließlich Kennwort, E-Mail, VPN und WiFi. Unterstützt wird Mac OS X Version 10.7.3 oder eine höhere Version.

Zu den für die Geräte ausführbaren Aktionen gehören:

- Sperren eines Geräts
- Löschen der Daten auf der Festplatte
- Ändern der Geräterichtlinie

1.25 IBM MaaS360 Laptop Location (SaaS)

MaaS360 Laptop Location (SaaS) ermöglicht das Lokalisieren unterstützter Laptops und Tablets. MaaS360 meldet die Position der Wifi- oder IP-Adresskoordinaten und übersetzt diese Daten in eine leicht erkennbare Adresse. Wenn ein Gerät online ist, kann die aktuelle Position abgerufen werden. Die gemeldeten Daten werden von MaaS360 gespeichert, sodass im Laufe der Zeit ein Protokoll aufgebaut wird, das zu Prüfungszwecken verfügbar ist. Voraussetzung dafür ist MaaS360 Laptop Management (SaaS) for Windows. Unterstützt werden XP SP3, Windows Vista, Windows 7, Windows 8+ und Windows 8+ Pro (sofern zutreffend, die 32-Bit- als auch die 64-Bit-Version).

1.26 IBM MaaS360 Laptop Lifecycle Management (SaaS)

Enthält die Funktionalität des Angebots MaaS360 Laptop Management (SaaS) und bietet darüber hinaus die folgenden Funktionen:

- Ermöglicht dem Kunden den Upload von Paketen auf die MaaS360 Content Service (SaaS)-Plattform und die Planung der Nutzdatenverteilung an die Geräte, die vom MaaS360 Laptop Management (SaaS)-Service für Microsoft Windows verwaltet werden. Die Steuerung sämtlicher Aspekte der Verteilung, einschließlich der Installationsanweisungen, und die Verteilung auf Geräte-, Gruppen- oder globaler Ebene liegt beim Kunden. Der Kunde trägt die gesamte Verantwortung für die Paketierung und die Erstellung der Installationsdatei. IBM leistet keine Unterstützung bei der Erstellung des Installationspakets.

1.27 IBM MaaS360 Laptop Security (SaaS)

Ermöglicht Unternehmen die Verwaltung konsistenter Sicherheitsrichtlinien und Profile sowohl für unternehmenseigene als auch für mitarbeitereigene Geräte über dieselbe Managementkonsole.

1.28 IBM MaaS360 Essentials Suite (SaaS)

Diese Suite ermöglicht dem Kunden die Anzeige und Kontrolle der mobilen Geräte und Apps, die seinem Unternehmen hinzugefügt werden. Die Suite bietet unternehmensweites Management für mobile Geräte, Anwendungen und Ausgaben über eine einzige Anzeige.

1.29 IBM MaaS360 Deluxe Suite (SaaS)

Diese Suite umfasst das gesamte Leistungsspektrum der MaaS360 Essentials Suite und bietet den Benutzern darüber hinaus eine separate, mit umfassenden Sicherheitsfunktionen ausgestattete Officeproduktivitätsanwendung für den Zugriff und die Verwaltung ihrer E-Mail, Kalender, Kontakte und Chats.

1.30 IBM MaaS360 Premier Suite (SaaS)

Diese Suite umfasst das gesamte Leistungsspektrum der MaaS360 Deluxe Suite und bietet darüber hinaus Sicherheit für mobile Anwendungen, einen sicheren mobilen Browser und ein Gateway sowie Management für mobil abrufbare Inhalte.

1.31 IBM MaaS360 Enterprise Suite (SaaS)

Diese Suite umfasst das gesamte Leistungsspektrum der MaaS360 Premier Suite und bietet darüber hinaus Management für mobile Sicherheitsbedrohungen, einen Dokumenteditor und Dokumentsynchronisation.

2. Sicherheitsbeschreibung

Dieser Cloud-Service orientiert sich an den unter <http://www-03.ibm.com/software/sla/slabd.nsf/sla/dsp> verfügbaren IBM Datensicherheits- und Datenschutzrichtlinien für IBM SaaS sowie weiteren Bedingungen in diesem Abschnitt. Eventuelle Änderungen der IBM Datensicherheitsrichtlinien führen nicht zu einer Beeinträchtigung der Sicherheit des Cloud-Service.

Dieser Cloud-Service wurde nach den Grundsätzen des Safe-Harbor-Abkommens zwischen den USA und der EU zertifiziert.

3. Service-Level-Agreement

Das folgende Verfügbarkeits-Service-Level-Agreement („SLA“) wird von IBM, so wie im Berechtigungsnachweis angegeben, für den Cloud-Service bereitgestellt. Das SLA stellt keine Gewährleistung dar und gilt nicht für Aktivierungssoftware. Es wird nur Kunden zur Verfügung gestellt und gilt ausschließlich für Produktionsumgebungen.

3.1 Gutschriften für Ausfallzeiten

Der Kunde muss innerhalb von 24 Stunden, nachdem er zum ersten Mal festgestellt hat, dass ein Vorfall die Verfügbarkeit des Cloud-Service beeinträchtigt, ein Support-Ticket der Fehlerklasse 1 beim IBM Help-Desk für technische Unterstützung öffnen. Der Kunde ist verpflichtet, IBM in angemessener Weise bei der Diagnose und Lösung des Problems zu unterstützen.

Der Anspruch aus einem Support-Ticket aufgrund der Nichteinhaltung eines SLA muss innerhalb von drei (3) Arbeitstagen nach Ablauf des Vertragsmonats geltend gemacht werden. Die Entschädigung für einen berechtigten Anspruch aus einem SLA wird als Gutschrift gewährt und mit einer künftigen Rechnung für den Cloud-Service verrechnet. Sie basiert auf dem Zeitraum, in dem das Produktionssystem nicht zur Verarbeitung des Cloud-Service zur Verfügung stand („Ausfallzeit“). Die Erfassung der Ausfallzeit beginnt mit der Meldung des Vorfalls durch den Kunden und endet, wenn der Cloud-Service wiederhergestellt ist. Als Ausfallzeit zählen nicht: Zeiten für vorab geplante oder angekündigte Unterbrechungen zur Durchführung von Wartungsarbeiten; Gründe, die IBM nicht zu vertreten hat; Probleme mit dem Inhalt, der Technologie, den Entwürfen oder den Anweisungen des Kunden oder Dritter; nicht unterstützte Systemkonfigurationen und Plattformen oder andere Fehler des Kunden; vom Kunden verursachte Sicherheitsvorfälle oder vom Kunden durchgeführte Sicherheitstests. IBM wird die höchstmögliche Entschädigung basierend auf der kumulierten Verfügbarkeit des Cloud-Service während jedes einzelnen Vertragsmonats anwenden (siehe die nachstehende Tabelle). Die Gesamtentschädigung für einen beliebigen Vertragsmonat wird 10 Prozent (%) von einem Zwölftel (1/12) der Jahresgebühr für den Cloud-Service nicht überschreiten.

3.2 Service-Levels

Verfügbarkeit des Cloud-Service in einem Vertragsmonat

| Verfügbarkeit in einem Vertragsmonat | Gutschrift für Ausfallzeiten (in Prozent (%) der monatlichen Subscription-Gebühr* für den Vertragsmonat, der Gegenstand des Anspruchs ist) |
|--------------------------------------|---|
| Unter 99,8 % | 2 % |
| Unter 98,8 % | 5 % |
| Unter 95,0 % | 10 % |

* Wurde der Cloud-Service von einem IBM Business Partner erworben, so wird die monatliche Subscription-Gebühr auf der Basis des zum jeweiligen Zeitpunkt gültigen Listenpreises für den Cloud-Service berechnet, der in dem Vertragsmonat wirksam war, der Gegenstand des Anspruchs ist, mit einem Abschlag von 50 Prozent (%). Eine eventuelle Rückvergütung von IBM wird direkt an den Kunden geleistet.

Die Verfügbarkeit, ausgedrückt als Prozentsatz, wird wie folgt berechnet: Gesamtzahl der Minuten in einem Vertragsmonat, minus der Gesamtzahl der Ausfallminuten in einem Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in einem Vertragsmonat.

Beispiel: 425 Minuten Gesamtausfallzeit in einem Vertragsmonat

| | |
|---|---|
| 43.200 Minuten insgesamt in einem Vertragsmonat mit 30 Tagen - 425 Minuten Ausfallzeit = 42.775 Minuten <hr style="width: 50%; margin: 10px auto;"/> 43.200 Minuten insgesamt | = Gutschrift für Ausfallzeiten in Höhe von 2 % bei einer Verfügbarkeit von 99,0 % in einem Vertragsmonat |
|---|---|

4. Technische Unterstützung

Technische Unterstützung für den Cloud-Service wird per Chat, Telefon und E-Mail bereitgestellt.

IBM stellt das IBM Software as a Service Support Handbook zur Verfügung, das Kontaktinformationen für die technische Unterstützung sowie weitere Informationen und Prozesse enthält.

| Fehlerklasse | Definition der Fehlerklasse |
|--------------|--|
| 1 | Fehler oder Probleme mit dem Service, die bei der Gesamtheit der Kunden zu Unterbrechungen oder Beeinträchtigungen des regulären Geschäftsbetriebs führen Durch den Service verursachte Fehler oder Probleme, die katastrophale Auswirkungen auf den regulären Geschäftsbetrieb haben |
| 2 | Fehler oder Probleme mit dem Service, die bei einem erheblichen Prozentsatz der Kunden zu Unterbrechungen oder Beeinträchtigungen des regulären Geschäftsbetriebs führen Durch den Service verursachte Fehler oder Probleme, die schwerwiegende Auswirkungen auf den regulären Geschäftsbetrieb haben |
| 3 | Fehler oder Probleme mit dem Service, die bei einem kleinen Prozentsatz der Kunden zu Unterbrechungen oder Beeinträchtigungen des regulären Geschäftsbetriebs führen Durch den Service verursachte Fehler oder Probleme, die erhebliche Auswirkungen auf den regulären Geschäftsbetrieb haben |
| 4 | Fehler oder Probleme mit dem Service, die bei einem einzelnen Benutzer zu Unterbrechungen oder Beeinträchtigungen des regulären Geschäftsbetriebs führen Durch den Service verursachte Fehler oder Probleme, die geringfügige Auswirkungen auf den regulären Geschäftsbetrieb haben |

5. Informationen zu Berechtigungen und Abrechnung

5.1 Gebührenmetriken

Der Cloud-Service ist mit der im Auftragsdokument angegebenen Gebührenmetrik verfügbar:

- a. **Berechtigter Benutzer** ist eine Maßeinheit für den Erwerb des Cloud-Service. Der Kunde muss für jeden einzelnen berechtigten Benutzer, dem auf beliebige Weise direkt oder indirekt (z. B. über ein Multiplexing-Programm, eine Einheit oder einen Anwendungsserver) Zugriff auf den Cloud-Service erteilt wird, eine separate, dedizierte Berechtigung erwerben. Es müssen ausreichende Berechtigungen erworben werden, um die Anzahl der berechtigten Benutzer abzudecken, denen während des Messzeitraums, der im Berechtigungsnachweis oder Auftragsdokument des Kunden angegeben ist, Zugriff auf den Cloud-Service erteilt wird.
- b. **Gigabyte** ist eine Maßeinheit für den Erwerb des Cloud-Service. Ein Gigabyte entspricht 2 hoch 30 Byte (1.073.741.824 Byte). Der Kunde muss ausreichende Berechtigungen erwerben, um die Gesamtzahl der Gigabyte abzudecken, die während des Messzeitraums, der im Berechtigungsnachweis oder Auftragsdokument angegeben ist, vom Cloud-Service verarbeitet werden.
- c. **Verwaltete Clienteinheit** ist eine Maßeinheit für den Erwerb des Cloud-Service. Eine Clienteinheit ist eine Datenverarbeitungseinheit eines einzelnen Benutzers, ein Spezialelement oder ein Telemetriegerät, das eine Reihe von Befehlen, Prozeduren oder Anwendungen zur Ausführung an ein anderes Computersystem, das üblicherweise als Server bezeichnet wird, übergibt oder von diesem zur Ausführung empfängt, Daten für den Server bereitstellt oder vom Server verwaltet wird. Mehrere Clienteinheiten können gemeinsam auf einen Server zugreifen. Eine Clienteinheit kann

über gewisse Verarbeitungsfunktionen verfügen oder programmierbar sein, sodass ein Benutzer Arbeiten ausführen kann. Der Kunde muss für jede Clienteinheit, die während des im Berechtigungsnachweis oder Auftragsdokument angegebenen Abrechnungszeitraums vom Cloud-Service verwaltet wird, eine Berechtigung für eine verwaltete Clienteinheit erwerben.

- d. **Clienteinheit** ist eine Maßeinheit für den Erwerb des Cloud-Service. Eine Clienteinheit ist eine Datenverarbeitungseinheit eines einzelnen Benutzers, ein Spezielsensor oder ein Telemetriegerät, das eine Reihe von Befehlen, Prozeduren oder Anwendungen zur Ausführung an ein anderes Computersystem, das üblicherweise als Server bezeichnet wird, übergibt oder von diesem zur Ausführung empfängt, Daten für den Server bereitstellt oder vom Server verwaltet wird. Mehrere Clienteinheiten können gemeinsam auf einen Server zugreifen. Eine Clienteinheit kann über gewisse Verarbeitungsfunktionen verfügen oder programmierbar sein, sodass ein Benutzer Arbeiten ausführen kann. Der Kunde muss für jede Clienteinheit, die während des im Berechtigungsnachweis oder Auftragsdokument angegebenen Messzeitraums in Verbindung mit dem Cloud-Service ausgeführt wird, Daten an den Cloud-Service liefert, vom Cloud-Service bereitgestellte Services nutzt oder auf andere Weise auf den Cloud-Service zugreift, eine Berechtigung erwerben.

5.2 Anteilige Monatsgebühren

Die im Auftragsdokument angegebene anteilige Monatsgebühr wird anteilig basierend auf der Nutzung ermittelt.

5.3 Zusatzgebühren

Wenn die tatsächliche Nutzung des Cloud-Service während des Messzeitraums die im Berechtigungsnachweis angegebene Berechtigung überschreitet, wird dem Kunden die Nutzungsüberschreitung gemäß dem Auftragsdokument in Rechnung gestellt.

6. Laufzeit und Verlängerungsoptionen

Die Laufzeit des Cloud-Service beginnt an dem Datum, an dem IBM dem Kunden mitteilt, dass sein Zugriff auf den Cloud-Service gemäß der Angabe im Berechtigungsnachweis freigeschaltet ist. Im Berechtigungsnachweis ist festgelegt, ob sich der Cloud-Service automatisch verlängert, auf fortlaufender Basis genutzt werden kann oder am Ende der Laufzeit abläuft.

6.1 Automatische Verlängerung

Bei automatischer Verlängerung wird der Cloud-Service automatisch um die im Berechtigungsnachweis angegebene Laufzeit verlängert, es sei denn, der Kunde teilt IBM mindestens 90 Tage vor dem Ablaufdatum schriftlich mit, dass er keine Verlängerung wünscht.

Die Anzahl oder das Volumen der Verlängerungsberechtigungen entspricht der ursprünglichen Bestellmenge oder der monatlichen Nutzung, die für den Monat vor der Erstellung der Rechnung für die Verlängerung gemeldet wird (es gilt der höhere Wert), es sei denn, IBM erhält eine Mitteilung mit abweichenden Angaben zur Verlängerung der Berechtigungen.

Verlängerungsberechtigungen für Step-up-Angebote basieren auf der ursprünglichen Bestellmenge.

6.2 Fortlaufende Abrechnung

Bei fortlaufender Nutzung steht der Cloud-Service auf monatlicher Basis ununterbrochen zur Verfügung, bis der Kunde unter Einhaltung einer Frist von 90 Tagen schriftlich kündigt. Der Cloud-Service bleibt nach Ablauf der 90-Tage-Frist bis zum Ende des Kalendermonats verfügbar.

7. Aktivierungssoftware

Dieser Cloud-Service enthält Aktivierungssoftware, die nur in Verbindung mit dem Cloud-Service während der Laufzeit verwendet werden darf.

8. Zusätzliche Informationen

8.1 Step-up-Beschränkung

Als Voraussetzung für die als „Step up for existing Customers“ (nachfolgend „Step-up SaaS“ genannt) gekennzeichneten Cloud-Service-Angebote muss der Kunde zuvor oder gleichzeitig entsprechende Lizenzberechtigungen für das zugehörige IBM Programm erworben haben, das im Namen des Step-up SaaS-Angebots angegeben ist. Wenn der Kunde beispielsweise „IBM MobileFirst Protect – Devices (SaaS) Step up for existing customers“ erwirbt, muss er über Lizenzberechtigungen für das zugehörige

IBM MobileFirst Protect-Programm verfügen. Die Berechtigungen des Kunden für das Step-up SaaS-Angebot dürfen seine Berechtigungen für das zugehörige IBM Programm nicht überschreiten.

Wenn der Kunde das Step-up SaaS-Angebot erwirbt, darf er die Lizenzberechtigungen für das zugehörige IBM Programm, die er in Verbindung mit den Step-up SaaS-Berechtigungen nutzt, nicht mehr innerhalb seiner On-Premise-Umgebung einsetzen. Angenommen, der Kunde verfügt über 250 Berechtigungen für verwaltete Clienteinheiten für das zugehörige IBM Programm und erwirbt 100 Step-up SaaS-Berechtigungen für verwaltete Clienteinheiten, dann beziehen sich die 100 Step-up SaaS-Berechtigungen auf die Verwaltung der Clienteinheiten in der Cloud-Service-Umgebung und 150 Clienteinheiten können weiterhin über die vor Ort installierte Software verwaltet werden.

Der Kunde versichert, dass er (1) die erforderlichen Lizenzberechtigungen und (2) Subscription und Support für das zugehörige IBM Programm erworben hat. Während der Subscription-Laufzeit für das Step-up SaaS-Angebot muss der Kunde seinen laufenden Subscription- und Support-Vertrag für die IBM Programmberechtigungen aufrechterhalten, die in Verbindung mit den Step-up SaaS-Berechtigungen genutzt werden. Falls entweder die Lizenz des Kunden oder sein Subscription- und Support-Vertrag für das jeweilige zugehörige IBM Programm ausläuft, erlischt auch sein Recht zur Nutzung des Step-up SaaS-Angebots.

8.2 Cookies

Der Kunde stimmt zu, dass IBM gemäß der IBM Datenschutzrichtlinie unter <http://www-01.ibm.com/software/info/product-privacy/index.html> Cookies und Tracking-Technologien zur Erfassung personenbezogener Daten für die Erstellung von Nutzungsstatistiken und -informationen verwenden darf, die dazu beitragen sollen, das Benutzererlebnis zu verbessern und/oder Interaktionen mit Benutzern anzupassen.

8.3 Keine persönlichen Gesundheitsdaten

Der Cloud-Service ist nicht für die Einhaltung des von den USA erlassenen Health Insurance Portability and Accountability Act („HIPAA“) ausgelegt und darf nicht für die Übermittlung oder Speicherung persönlicher Gesundheitsdaten verwendet werden.

8.4 Normative Daten

Ungeachtet gegenteiliger Regelungen darf IBM Daten, welche die individuellen Erfahrungen der berechtigten Benutzer des Kunden mit den Cloud-Services widerspiegeln, nur für normative Recherche sowie für Analyse-, Demonstrations- und Berichtszwecke in einem aggregierten, anonymen Format aufbewahren und verwenden (d. h., der Kunde oder die berechtigten Benutzer des Kunden können nicht als Quelle der Daten identifiziert werden und personenbezogene Daten, die eine Identifizierung des Kunden oder der berechtigten Benutzer des Kunden ermöglichen, werden entfernt).

8.5 Rechtmäßige Nutzung und Zustimmung

8.5.1 Ermächtigung zur Erfassung und Verarbeitung von Daten

Der Cloud-Service ist für die Einrichtung, Verwaltung, Überwachung und Kontrolle von Mobilgeräten ausgelegt. Er erfasst Informationen von Benutzern und Geräten, die vom Kunden zur Interaktion mit dem Cloud-Service berechtigt wurden, den er per Subscription erworben hat. Die vom Cloud-Service erfassten Informationen können allein oder in Kombination in einigen Rechtsordnungen als personenbezogene Daten gelten. Zu den erfassten Informationen können der Name des berechtigten Benutzers, seine Telefonnummer, seine registrierte E-Mail-Adresse und der Gerätestandort, seine Benutzer-ID und der Browserverlauf des MaaS360-Browsers, Informationen über die Gerätehardware des Endbenutzers, die Software und die Einstellungen sowie von dem Gerät generierte Informationen gehören. Der Kunde ermächtigt IBM, diese Informationen gemäß den Bestimmungen dieser Servicebeschreibung zu erfassen, zu verarbeiten und zu verwenden.

8.5.2 Einverständniserklärung der betroffenen Personen

Bei der Nutzung des Cloud-Service können mehrere Gesetze und Bestimmungen zur Anwendung kommen. Der Cloud-Service darf nur für gesetzlich zulässige Zwecke und in rechtmäßiger Weise verwendet werden. Der Kunde willigt ein, den Cloud-Service gemäß den anwendbaren Gesetzen, Bestimmungen und Richtlinien zu verwenden und die gesamte Verantwortung für deren Einhaltung zu übernehmen.

Der Kunde versichert, dass er alle Einverständniserklärungen, Genehmigungen oder Lizenzen eingeholt hat oder einholen wird, die für die rechtmäßige Nutzung der Cloud-Services sowie für die Erfassung und Verarbeitung der Informationen über die Cloud-Services durch IBM als Auftragsverarbeiter des Kunden

erforderlich sind. Der Kunde ermächtigt hiermit IBM, die Einverständniserklärungen einzuholen, die für die rechtmäßige Nutzung des Cloud-Service sowie die Erfassung und Verarbeitung der Informationen gemäß der Beschreibung in der Endbenutzerlizenzvereinbarung erforderlich sind, die unter <http://www.ibm.com/software/sla/sladb.nsf/> verfügbar ist.

8.6 Datenaufbewahrung

IBM wird alle erfassten Informationen, einschließlich der ggf. enthaltenen personenbezogenen Daten, nach Ablauf oder Beendigung dieser Servicebeschreibung löschen, außer den Informationen, die für die vorstehend genannten Zwecke oder per Gesetz, Vorschrift oder Verordnung aufbewahrt werden müssen. In einem solchen Fall wird IBM die erfassten Informationen für die zu diesem Zweck erforderliche oder für die per Gesetz, Vorschrift oder Verordnung vorgeschriebene Frist aufbewahren.

8.7 Datenschutz

8.7.1 Grenzüberschreitende Datenübermittlung

Wenn der Kunde personenbezogene Daten innerhalb der IBM Cloud-Services in den EU-Mitgliedstaaten sowie in Island, Liechtenstein, Norwegen, in der Schweiz, in der Türkei und in anderen europäischen Ländern, die nationale Datenschutzbestimmungen eingeführt haben, verfügbar macht, willigt er ein, dass IBM die Inhalte, einschließlich der personenbezogenen Daten, unter Einhaltung der einschlägigen Gesetze und Anforderungen grenzüberschreitend durch Auftragsverarbeiter und Unterauftragsverarbeiter in den folgenden Ländern außerhalb des Europäischen Wirtschaftsraums (EWR) und in Ländern, die von der Europäischen Kommission als Länder mit einem angemessenen Schutzniveau eingestuft werden, verarbeiten lassen kann:

| Name des Auftragsverarbeiters/Unterauftragsverarbeiters | Rolle (Auftragsverarbeiter oder Unterauftragsverarbeiter) | Standort |
|---|---|--|
| IBM Corporation | Unterauftragsverarbeiter | 1 New Orchard Rd. Armonk, NY 10504, USA |
| IBM India Private Limited | Unterauftragsverarbeiter | No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 Indien |

Der Kunde erklärt sich damit einverstanden, dass IBM nach vorheriger Mitteilung diese Länderliste ändern kann, wenn dies zur Erbringung der Cloud-Services für notwendig erachtet wird.

8.7.2 EU-Datenschutz

Wenn der Kunde personenbezogene Daten innerhalb der IBM Cloud-Services in den EU-Mitgliedstaaten sowie in Island, Liechtenstein, Norwegen, in der Schweiz, in der Türkei und in anderen europäischen Ländern, die nationale Datenschutzbestimmungen eingeführt haben, verfügbar macht oder wenn sich berechnete Benutzer oder Geräte des Kunden in diesen Ländern befinden, beauftragt der Kunde als alleiniger Verantwortlicher IBM als Auftragsverarbeiter mit der Verarbeitung der personenbezogenen Daten (gemäß der Definition dieser Begriffe in der EU-Richtlinie 95/46/EG). IBM wird personenbezogene Daten nur in dem Umfang verarbeiten, der zur Bereitstellung der IBM Cloud-Services gemäß den von IBM veröffentlichten Beschreibungen der IBM Cloud-Services erforderlich ist, und der Kunde stimmt zu, dass eine solche Verarbeitung seinen Anweisungen entspricht.

8.8 Sicherheitsdaten

Im Rahmen des Cloud-Service, der eine Berichterstattung beinhaltet, wird IBM anonymisierte und/oder aggregierte Informationen, die aus dem Cloud-Service erfasst wurden, aufbereiten und verwalten („Sicherheitsdaten“). Die Sicherheitsdaten lassen keine Rückschlüsse auf den Kunden oder eine Person zu, außer wie unten in Absatz (d) vorgesehen. Der Kunde erklärt sich außerdem damit einverstanden, dass IBM die Sicherheitsdaten nur für folgende Zwecke verwenden und/oder kopieren darf:

- Veröffentlichung und/oder Weitergabe der Sicherheitsdaten (z. B. in Datensammlungen und/oder Analysen im Zusammenhang mit Cybersicherheit)
- Entwicklung oder Verbesserung von Produkten oder Services
- Durchführung interner Recherchen oder mit Dritten
- Rechtmäßige Weitergabe von bestätigten Informationen über externe Täter