# IBM MobileFirst Protect (SaaS)

The Terms of Use ("ToU") is composed of this IBM Terms of Use - SaaS Specific Offering Terms ("SaaS Specific Offering Terms") and a document entitled IBM Terms of Use - General Terms ("General Terms") available at the following URL: **www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/**.

In the event of a conflict, the SaaS Specific Offering Terms prevail over the General Terms. By ordering, accessing or using the IBM SaaS, Client agrees to the ToU.

The ToU is governed by the IBM International Passport Advantage Agreement, the IBM International Passport Advantage Express Agreement, or the IBM International Agreement for Selected IBM SaaS Offerings, as applicable ("Agreement") and together with the ToU make the complete agreement.

## 1. IBM SaaS

The following IBM SaaS offerings are covered by these SaaS Specific Offering Terms:

- IBM MobileFirst Protect - Devices (SaaS)
- IBM MobileFirst Protect - Devices (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Applications (SaaS)
- IBM MobileFirst Protect - Applications (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Application Security (SaaS)
- IBM MobileFirst Protect - Application Security (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Gateway for Apps (SaaS)
- IBM MobileFirst Protect - Gateway for Apps (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Content (SaaS)
- IBM MobileFirst Protect - Content (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Document Sync (SaaS)
- IBM MobileFirst Protect - Document Sync (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Document Editor (SaaS)
- IBM MobileFirst Protect - Document Editor (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Gateway for Documents (SaaS)
- IBM MobileFirst Protect - Gateway for Documents (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Email Management (SaaS)
- IBM MobileFirst Protect - Email Management (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Browser (SaaS)
- IBM MobileFirst Protect - Browser (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Gateway for Browser (SaaS)
- IBM MobileFirst Protect - Gateway for Browser (SaaS) Step up for existing customers
- IBM MobileFirst Protect for Blackberry (SaaS)
- IBM MobileFirst Protect for Blackberry (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Expenses (SaaS)
- IBM MobileFirst Protect - Expenses (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Management Suite (SaaS)
- IBM MobileFirst Protect - Management Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Productivity Suite (SaaS)
- IBM MobileFirst Protect - Productivity Suite (SaaS) Step up for existing customers

- IBM MobileFirst Protect - Secure Mail (SaaS)
- IBM MobileFirst Protect - Secure Mail (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Gateway Suite (SaaS)
- IBM MobileFirst Protect - Gateway Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Content Suite (SaaS)
- IBM MobileFirst Protect - Content Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect - Threat Management (SaaS)
- IBM MobileFirst Protect - Content Service (SaaS)
- IBM MobileFirst Protect - Content Service Storage (SaaS)
- IBM MobileFirst Protect - Content Service Bandwidth (SaaS)
- IBM MobileFirst Protect – Professional (SaaS)
- IBM MobileFirst Protect - Laptop (SaaS)
- IBM MobileFirst Protect - Laptop Location (SaaS)
- IBM MobileFirst Protect - Laptop Lifecycle Management (SaaS)
- IBM MobileFirst Protect - Laptop Security and Compliance (SaaS)
- IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)
- IBM MaaS360 Secure Productivity Suite Prime (SaaS)
- IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)
- IBM MaaS360 Professional Bundle Prime (SaaS)
- IBM MaaS360 Educational Bundle Prime (SaaS)
- IBM MaaS360 Advanced Laptop Management Prime (SaaS)

## 2. Charge Metrics

The IBM SaaS is sold under one of the following charge metric(s) as specified in the Transaction Document:

a. Authorized User is a unit of measure by which the IBM SaaS can be obtained. Client must obtain separate, dedicated entitlements for each unique Authorized User given access to the IBM SaaS in any manner directly or indirectly (for example: via a multiplexing program, device, or application server) through any means. Sufficient entitlements must be obtained to cover the number of Authorized Users given access to the IBM SaaS during the measurement period specified in Client's Proof of Entitlement (PoE) or Transaction Document.

b. Gigabyte is a unit of measure by which the IBM SaaS can be obtained. A Gigabyte is defined as 2 to the 30th power bytes of data (1,073,741,824 bytes). Sufficient entitlements must be obtained to cover the total number of Gigabytes processed by the IBM SaaS during the measurement period specified in Client's Proof of Entitlement (PoE) or Transaction Document.

c. Managed Client Device is a unit of measure by which IBM SaaS can be obtained. A Client Device is a single user computing device or special purpose sensor or telemetry device that requests the execution of or receives for execution a set of commands, procedures, or applications from or provides data to another computer system that is typically referred to as a server or is otherwise managed by the server. Multiple Client Devices may share access to a common server. A Client Device may have some processing capability or be programmable to allow a user to do work. Client must obtain Managed Client Device entitlements for every Client Device managed by the IBM SaaS during the measurement period specified in Client's Proof of Entitlement (PoE) or Transaction Document.

d. Client Device is a unit of measure by which the IBM SaaS can be obtained. A Client Device is a single user computing device or special purpose sensor or telemetry device that requests the execution of or receives for execution a set of commands, procedures, or applications from or provides data to another computer system that is typically referred to as a server or is otherwise managed by the server. Multiple Client Devices may share access to a common server. A Client Device may have some processing capability or be programmable to allow a user to do work. Client must obtain entitlements for every Client Device which runs, provides data to, uses services

provided by, or otherwise accesses the IBM SaaS during the measurement period specified in Client's Proof of Entitlement (PoE) or Transaction Document.

## 3. Charges and Billing

The amount payable for the IBM SaaS is specified in a Transaction Document.

### 3.1 Partial Month Charges

A partial month charge as specified in the Transaction Document may be assessed on a pro-rated basis.

### 3.2 Overage Charges

If Client's actual usage of the IBM SaaS during the measurement period exceeds the entitlement stated on the PoE, then Client will be invoiced for the overage, as set forth in the Transaction Document.

## 4. IBM SaaS Subscription Period Renewal Options

Client's PoE will set forth whether the IBM SaaS will renew at the end of the Subscription Period, by designating one of the following:

### 4.1 Automatic Renewal

If Client's PoE states that Client's renewal is automatic, Client may terminate the expiring IBM SaaS Subscription Period by written request to Client's IBM sales representative or IBM Business Partner, at least ninety (90) days prior to the expiration date as set forth in the PoE. If IBM or its IBM Business Partner does not receive such termination notice by the expiration date, the expiring Subscription Period will be automatically renewed for either one year or the same duration as the original Subscription Period as set forth in the PoE.

THE RENEWAL ENTITLEMENT QUANTITY WILL BE EQUAL TO THE GREATER OF THE ORIGINAL ORDER QUANTITY OR THE MONTHLY REPORTED USAGE FOR THE MONTH PRIOR TO GENERATION OF THE RENEWAL INVOICE UNLESS IBM RECEIVES A NOTIFICATION SPECIFYING A DIFFERENT ENTITLEMENT QUANTITY.

THE RENEWAL ENTITLEMENT QUANTITY FOR STEP UP OFFERING WILL BE EQUAL TO THE ORIGINAL ORDER QUANTITY.

### 4.2 Continuous Billing

When the PoE states that Client's renewal is continuous, Client will continue to have access to the IBM SaaS and will be billed for the usage of the IBM SaaS on a continuous basis. To discontinue use of the IBM SaaS and stop the continuous billing process, Client will need to provide IBM or its IBM Business Partner with ninety (90) days written notice requesting that Client's IBM SaaS be cancelled. Upon cancellation of Client's access, Client will be billed for any outstanding access charges through the month in which the cancellation took effect.

### 4.3 Renewal Required

When the PoE states that Client's renewal type is "terminate", the IBM SaaS will terminate at the end of the Subscription Period and Client's access to the IBM SaaS will be removed. To continue to use the IBM SaaS beyond the end date, Client will need to place an order with Client's IBM sales representative or IBM Business Partner to purchase a new Subscription Period.

## 5. Technical Support

Technical support for IBM SaaS is structured 2nd level support to a customer's Operation team, not End User support and is available during the subscription period. .

Support is provided through multiple channels; 24 x 7. Information regarding support of the IBM SaaS solution can be found on product portal.

Expected Responsiveness targets:

| Severity | Severity Definition | Initial Response Time Objectives | Response Time Coverage |
|---|---|---|---|
| 1 | **Critical business impact/service down:** Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an | 30 Minutes | 24x7 |

| | | | |
|---|---|---|---|
| | inability to access services resulting in a critical impact on operations. This condition requires an immediate solution. | | |
| 2 | **High business impact:** A service business feature or function of the service is severely restricted in its use or you are in jeopardy of missing business deadlines. | 1 business hour | 24 x 7 |
| 3 | **Medium business impact:** Indicates the service or functionality is usable and it is not a critical impact on operations. | 2 business hours | 24 x 7 |
| 4 | **Low business impact:** An inquiry or non-technical request | 3 business hours | 24 x 7 |

# 6. IBM SaaS Offering Additional Terms

## 6.1 Step up Limitation

For IBM SaaS offerings designated as "Step up for existing Customers" ("Step up SaaS"), Client must have previously or simultaneously acquired appropriate license entitlements to the associated IBM program as identified in the name of the Step up SaaS offering. For example, Client who purchases "IBM MobileFirst Protect - Devices (SaaS) Step up for existing customers" must have licensed entitlements to the associated IBM program of IBM MobileFirst Protect. Client's entitlements to the Step up SaaS cannot exceed Client's entitlements to the associated IBM program.

When acquiring Step up SaaS, Client may not use the same associated IBM program license entitlements within their on-premise installed environment as well as with the Step up SaaS entitlements. For example, if Client has 250 Managed Client Device entitlements to the associated IBM program and chooses to purchase 100 Step up SaaS Managed Client Device entitlements, Client can manage 100 Step up SaaS Managed Client Devices from the IBM SaaS environment and 150 Managed Client Devices from the software installed on-premise.

Client represents they have acquired the applicable (1) license entitlements and (2) Subscription and Support for the associated IBM program(s). During the Subscription Period of the Step up SaaS, Client must maintain current Subscription and Support for the IBM program entitlements used in conjunction with the Step up SaaS entitlements. In the event either Client's license to use the associated IBM program(s) or Client's Subscription and Support for the associated IBM program(s) is terminated, Client's right to use the Step Up SaaS will terminate.

## 6.2 Cookies

Client agrees that IBM may use cookies and tracking technologies to collect personally identifiable information in gathering usage statistics and information designed to help improve user experience and/or to tailor interactions with users in accordance with http://www-01.ibm.com/software/info/product-privacy/index.html

## 6.3 Cross Border Transfers

If Client makes Personal Information available to IBM SaaS offerings in the EU Member States, Iceland, Liechtenstein, Norway, or Switzerland, Turkey, and any other European country that has enacted local data privacy or protection legislation, Client agrees that IBM may process the Content, including any Personal Information, under relevant laws and requirements across a country border to processors and sub-processors in the following countries outside of the European Economic Area and countries considered by the European Commission to have adequate levels of security:

| Name of Processor/Subprocessor | Role (Data Processor or Subprocessor) | Location |
|---|---|---|
| IBM Corporation | Sub-processor | 1 New Orchard Rd.<br>Armonk, NY 10504, USA I |
| IBM India Private Limited | Sub-processor | No. 12, Subramanya Arcade<br>Bannerghatta Road,<br>Bangalore 560029 India |

Client agrees that IBM may, on notice, vary this list of country locations when it reasonably determines it necessary for the provision of the IBM SaaS.

## 6.4 EU Data Privacy

If Client makes personal data available to IBM SaaS offerings in the EU Member States, Iceland, Liechtenstein, Norway, or Switzerland, Turkey, and any other European country that has enacted local data privacy or protection legislation, or if Client has authorized users or devices in those countries, then Client as the sole controller appoint IBM as a processor to process (as those terms are defined in EU Directive 95/46/EC) Personal Information. IBM will only process such Personal Information to the extent required to make the IBM SaaS offering available in accordance with IBM's published descriptions of the IBM SaaS and Client agrees that any such processing is in accordance with Client's instructions.

## 6.5 Safe Harbor Compliance

The IBM SaaS offerings are included in Fiberlink Communications Corporation (IBM Subsidiary) US-EU Safe Harbor certification. Both IBM and Fiberlink abide by the U.S. - EU Safe Harbor Framework as set forth by the United States Department of Commerce regarding the collection, use and retention of information collected from the European Union. For more information about Safe Harbor or to access Fiberlink's certification statement, go to **http://www.export.gov/safeharbor/**.

When IBM's US-EU Safe Harbor Framework does not apply to a transfer of EEA Personal Information, the parties or their relevant affiliates may enter into separate standard unmodified EU Model Clause agreements in their corresponding roles pursuant to EC Decision 2010/87/EU with optional clauses removed. All disputes or liability arising under these agreements, even if entered into by affiliates, will be treated by the parties as if the dispute or liability arose between them under the terms of this Agreement.

## 6.6 Derived Benefit Locations

Where applicable, taxes are based upon the location(s) Client identifies as receiving benefit of the IBM SaaS. IBM will apply taxes based upon the business address listed when ordering an IBM SaaS as the primary benefit location unless Client provides additional information to IBM. Client is responsible for keeping such information current and providing any changes to IBM.

## 6.7 Normative Data

Notwithstanding anything to the contrary, for normative research, analysis, demonstration and reporting purposes only, IBM may retain and use in aggregated and anonymous format (i.e., so that you or your authorized users cannot be identified as the source of the data and so that personally identifiable information allowing identification of Client or Client's authorized users is removed) data reflecting Client's authorized users' individual experiences with the IBM SaaS.

## 6.8 Lawful Use and Consent

### 6.8.1 Authorization to Collect and Process Data

The IBM SaaS is designed to provision, manage, secure, monitor and control mobile devices. The IBM SaaS will collect information from users and devices that are authorized by you to interact with the IBM SaaS for which Client has subscribed. The IBM SaaS collects information that alone or in combination may be considered Personal Information in some jurisdictions. Collected data may include authorized user name, telephone number, registered email address and device location, userID and secure browsing history, information about end user device hardware, software and settings, and information generated by the device. Client authorizes IBM to collect, process, and use this information in accordance with the terms of this Terms of Use.

### 6.8.2 Informed Consent from Data Subjects

Use of the IBM SaaS may implicate various laws and regulations. The IBM SaaS may be used only for lawful purposes and in a lawful manner. Client agrees to use the IBM SaaS pursuant to, and assume all responsibility for complying with, applicable laws, regulations and policies.

Client agrees that it has obtained or will obtain any fully informed consents, permissions, or licenses necessary to enable lawful use of the IBM SaaS and to permit collection and processing of the information by IBM as your data processor through the IBM SaaS. Client hereby authorizes IBM to obtain fully informed consents necessary to enable lawful use of the IBM SaaS and to collect and process the information as described in the end user license agreement available at http://www.ibm.com/software/sla/sladb.nsf/.

## 6.9 Data Retention

IBM will delete any collected information, which may include Personal Information, following termination of this Terms of Use, except for that which is required to be retained for the purposes set forth above, or by applicable law, rule or regulation. In such case, IBM will retain the collected information for the duration required by such purpose, applicable law, rule or regulation.

# Appendix A

MobileFirst Protect is an easy-to-use cloud platform with all of the essential functionality for end-to-end management of today's mobile devices including iPhones, iPads, Androids, Kindle Fire devices, Windows Phones and BlackBerry smartphones. Following is a short description of the IBM SaaS offerings:

## 1. IBM MobileFirst Protect - Devices (SaaS)

The core mobility device management (MDM) features includes device enrollment, configuration, security policy management and device actions, such as send message, locate, lock, and wipe. The Advanced MDM features include automated compliance rules, bring your own device (BYOD) privacy settings, and Mobility Intelligence dashboards and reporting.

## 2. IBM MobileFirst Protect - Applications (SaaS)

MobileFirst Protect Applications provides the ability to add applications and distribute them to supported devices managed by MobileFirst Protect. This includes MobileFirst Protect App Catalog, an on-device application for users to view, install, and be alerted to updated, managed applications.

## 3. IBM MobileFirst Protect - Application Security (SaaS)

MobileFirst Protect Application Security provides additional data protection for enterprise applications that use the WorkPlace SDK during development, or for iOS apps upload the application (.ipa), provisioning profile, and signing certificate to be automatically integrated. Mobile Application Security integrates the app with the Secure Productivity Suite. This enables single sign on, Intranet access through the Mobile Enterprise Gateway, and enforcement of data security settings.

## 4. IBM MobileFirst Protect - Gateway for Apps (SaaS)

MobileFirst Protect Gateway for Apps provides users outside the enterprise network secure, seamless access to internal application resources without requiring a full-device, VPN connection.

## 5. IBM MobileFirst Protect - Content (SaaS)

MobileFirst Protect Content allows the administrator to add and distribute documents to the supported devices that are managed by IBM MobileFirst Protect Devices. Includes IBM MobileFirst Protect Doc Catalogue, an on-device, password-protected container that provides a secure and simple way for users to access, view, and share documents. It includes seamless access to distributed content and repositories such as SharePoint, Box, and Google Drive. Access to private SharePoint and Windows files shares are available with the MobileFirst Protect Mobile Enterprise Gateway. Documents managed through MobileFirst Protect can be version controlled, audited, and secured through data loss prevention (DLP) policy options, such as require authentication, restrict copy-paste functionality, and block from being opened or shared in other applications.

## 6. IBM MobileFirst Protect - Document Sync (SaaS)

MobileFirst Protect Document Sync provides users with the ability to easily and securely synchronize user content across managed mobile devices. Administrators can ensure that policies, such as restricting cut-copy-paste, and blocking content from being opened or shared in other apps or are in place for user content across devices. Content is stored securely, both in the cloud and on the device, and accessed only through the MobileFirst Protect Doc Catalogue.

## 7. IBM MobileFirst Protect - Document Editor (SaaS)

MobileFirst Protect Document Editor is a powerful office suite that allows users to work with business documents while on the go. MobileFirst Protect Secure Editor enables to:

- Create and edit .DOC, .PPT, and .XLS files
- Presentation mode for slides
- Easily work with email attachments and other files from MobileFirst Protect for iOS

## 8. IBM MobileFirst Protect - Gateway for Documents (SaaS)

With MobileFirst Protect Gateway for Documents, organizations can use MobileFirst Protect Content to additionally offer devices outside the enterprise network secure seamless access to internal Connections

sites, SharePoint sites, Windows File Shares and other file stores without requiring a full device VPN connection. Use of MobileFirst Protect Gateway for Documents requires also purchasing MobileFirst Protect Content. Supports iOS 5.0 and Android 4.0 or above.

## 9. IBM MobileFirst Protect - Email Management (SaaS)

MobileFirst Protect Email Management includes key features in support of Microsoft Exchange ActiveSync and Lotus Traveler.

- Exchange ActiveSync: Provides support for mobile devices connecting to Microsoft Exchange over the ActiveSync protocol. Features include core mobile device management functions, such as the ability to configure devices, create; enforce ActiveSync policies (passcode, block, or allow access to email); and take device actions, such as lock and wipe, and detailed report on device attributes.
- Lotus Traveler: Provides support for mobile devices that connect to IBM Lotus Notes® over the Lotus Traveler protocol. Features include the ability to configure devices, block or allow devices, enforce passcode policies, wipe devices, and develop detailed report on device attributes.

## 10. IBM MobileFirst Protect - Browser (SaaS)

MobileFirst Protect Browser is a full-featured web browser to enable secure access to corporate intranet sites and enforce compliance of content policies by defining website filtering and security policies to ensure that users only access approved web content that is based on a number of content categories, such as social networking, explicit, or malware sites. Includes the ability to disable native and third-party web browsers either through application policy or blacklisting when combined with MobileFirst Protect Devices. It allows whitelist exceptions to websites, restrict cookies; copy, paste, and print features; and enable Kiosk mode.

## 11. IBM MobileFirst Protect - Gateway for Browser (SaaS)

MobileFirst Protect Gateway for Browser allows supported devices to access approved internal web sites without requiring a full-device level, VPN connection.

## 12. IBM MobileFirst Protect for Blackberry (SaaS)

Provides support for BlackBerry Enterprise Server (BES) connected mobile devices by utilizing BlackBerry APIs. Features include remote actions such as send a message, reset passcode, assign BES policy and wipe, as well as detailed reporting on device attributes. Installation of MobileFirst Protect Cloud Extender is required. Available only for devices viewed or managed with MobileFirst Protect through BES 5.0.

## 13. IBM MobileFirst Protect - Expenses (SaaS)

MobileFirst Protect Expenses allows the administrator to create data usage policies and assign them to supported devices that are managed by MobileFirst Protect, and assign these policies at a device, group, or global level and configure alert thresholds and messaging for both in network and roaming data usage.

## 14. IBM MobileFirst Protect - Management Suite (SaaS)

Suite/Bundle of products including MobileFirst Protect Devices, MobileFirst Protect Applications, MobileFirst Protect Content, and MobileFirst Protect Expenses.

## 15. IBM MobileFirst Protect - Productivity Suite (SaaS)

Suite/Bundle of products including MobileFirst Protect Secure Mail, MobileFirst Protect Applications, MobileFirst Protect Application Security, MobileFirst Protect Content, and MobileFirst Protect Browser.

## 16. IBM MobileFirst Protect - Secure Mail (SaaS)

MobileFirst Protect Secure Mail provides a separate and secure office productivity application for users to access and manage email, calendar, and contacts with the ability to control emails and attachments to prevent data leakage by restricting the ability to forward or move content to other applications, to enforce authentication, restrict cut-copy-paste, and lock down email attachments for view only.

## 17. IBM MobileFirst Protect - Gateway Suite (SaaS)

MobileFirst Protect Gateway Suite allows supported apps on iOS and Android to securely and seamless communicate back to resources on the company's internal network.

## 18. IBM MobileFirst Protect - Content Suite (SaaS)

Suite/Bundle of products including MobileFirst Protect Content, MobileFirst Protect Document Editor, and MobileFirst Protect Document Sync.

## 19. IBM MobileFirst Protect - Threat Management (SaaS)

MobileFirst Protect Threat Management provides enhanced mobile security with mobile malware detection and advanced jailbreak/root detection. With MobileFirst Protect Threat Management, Client will be able to set and manage compliance policies around detected malware and other security vulnerabilities.

## 20. IBM MobileFirst Protect - Content Service (SaaS)

MobileFirst Protect Content Service (SaaS) provides users with the ability to upload application packages and documents to MobileFirst Protect Content Distribution system.

Clients with MobileFirst Protect Content Service will also need to purchase at least one entitlement of both MobileFirst Protect Content Service Storage (SaaS) and MobileFirst Protect Content Service Bandwidth (SaaS).

## 21. IBM MobileFirst Protect - Content Service Storage (SaaS)

MobileFirst Protect Content Service Storage (SaaS) provides users the ability to purchase a total amount of data storage available for use with the MobileFirst Protect Content Service (SaaS)

## 22. IBM MobileFirst Protect - Content Service Bandwidth (SaaS)

MobileFirst Protect Content Service Bandwidth (SaaS) provides users the ability to purchase the total amount of bandwidth available for use with the MobileFirst Protect Content Service (SaaS)

## 23. IBM MobileFirst Protect – Professional (SaaS)

Provides small and medium-sized businesses with a fast and simple way to remotely configure smartphones and tablets, enforce security policies, push apps and docs, and protect the data on corporate and personal devices. You can gain access to the right mobility management capabilities for your business quickly, easily, and affordably.

## 24. IBM MobileFirst Protect - Laptop (SaaS)

Provides Client the ability to enroll, configure, manage, secure, and report on OS X and Windows PC based devices alongside smartphones and tablets. Organizations can maintain consistent security policies and profiles across both corporate and employee-owned devices within the same MobileFirst Protect management console.

### 24.1 Windows

MobileFirst Protect - Laptop (SaaS) for Windows-based PCs provides over-the-air enrollment and inventory management reporting on hardware, operating system, and software information. The endpoint security reporting module provides interactive reporting and data analysis for Client provided applications such as anti-virus, backup/recovery, data encryption and personal firewall as well as missing operating system patches. The data protection module provides interactive reporting and analysis for security services, including data encryption, data leak prevention, and backup/recovery, and other integrated applications. Supports Windows XP SP3, Windows Vista, Windows 7, Windows 8+, and Windows 8+ Pro (including 32-bit and 64-bit where applicable).

Device actions include:

- Send message to the device
- Lock the device
- Locate Device (Requires MobileFirst Protect Laptop Location)
- Stop/Start/Restart Services
- Shutdown/Reboot
- Wipe the hard drive
- Configure patch settings
- Distribute software

### 24.2 Mac OS X

MobileFirst Protect - Laptop (SaaS) for Mac OS X provides over the air enrollment and inventory management reporting on hardware, operating system, and software information. The endpoint security reporting module provides interactive reporting and data analysis for Client provided applications such as anti-virus, backup/recovery, data encryption and personal firewall as well as missing operating system patches. The data protection module provides interactive reporting and analysis for data security services, including data encryption. The configuration management module provides remote management of a number of device and user settings, including: password, email, VPN, and Wi-Fi. Supports Mac OS X version 10.7.3 or higher.

Device actions include:

- Lock the device
- Wipe the hard drive
- Change device policy

## 25. IBM MobileFirst Protect - Laptop Location (SaaS)

MobileFirst Protect Laptop Location (SaaS) enabled the ability to locate supported laptops and tablets. MobileFirst Protect reports the location of the Wi-Fi or IP address coordinates and translates this data into an easily recognizable address. When a device is online, its current location can be retrieved. MobileFirst Protect stores reported locations over time, so location history is available for review. Requires IBM MobileFirst Protect Laptop (SaaS) for Windows. Supports Windows XP SP3, Windows Vista, Windows 7, Windows 8+, and Windows 8+ Pro (including 32-bit and 64-bit where applicable).

## 26. IBM MobileFirst Protect - Laptop Lifecycle Management (SaaS)

Provides the capabilities of the MobileFirst Protect - Laptop (SaaS) offering and adds the following capabilities:

- Allows you to upload packages to the MobileFirst Protect Content Service (SaaS) platform and schedule distribution of payload to devices, which are managed by the MobileFirst Protect Laptop (SaaS) service for Microsoft Windows. You control all aspects of distribution, including installation instructions and targeting at a device, group, or global level. You are responsible for all packaging and installation file creation. IBM does not provide installation package creation support.

## 27. IBM MobileFirst Protect - Laptop Security and Compliance (SaaS)

Provides organizations the ability to maintain consistent security policies and profiles across both corporate and employee-owned devices within the same management console.

## 28. IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)

The core mobility device management (MDM) features includes device enrollment, configuration, security policy management and device actions, such as send message, locate, lock, and wipe. The Advanced MDM features include automated compliance rules, bring your own device (BYOD) privacy settings, and Mobility Intelligence dashboards and reporting.

## 29. IBM MaaS360 Secure Productivity Suite Prime (SaaS)

Provides the ability to securely access email, store, distribute and manage applications and provide access to intranet site using the Secure Browser.

## 30. IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)

Provides the ability to remotely manage and configure smartphones and tablets, enforce security policies, distribute data, report on Wi-Fi usage which can be used to track data usage and expenses along with content storage and distribution for applications and documents.

## 31. IBM MaaS360 Professional Bundle Prime (SaaS)

Provides small and medium-sized businesses with a way to remotely configure smartphones and tablets, enforce security policies, push apps and docs, and protect the data on corporate and personal devices.

## 32. IBM MaaS360 Educational Bundle Prime (SaaS)

Provides educational organizations the ability to remotely manage and configure smartphones and tablets, enforce security policies distribute data, along with content storage and distribution for applications and management of applications.

## 33. IBM MaaS360 Advanced Laptop Management Prime (SaaS)

Provides organizations the ability to manage, update, locate and distribute software to laptops providing consistent security policies across all laptop/desktops reporting into the MaaS360 management console.

# Appendix B

IBM provides the following availability service level agreement ("SLA") for the IBM SaaS and is applicable if specified in Client's Proof of Entitlement (PoE) or Transaction Document.

The version of this SLA that is current at the commencement or renewal of the term of your subscription will apply. You understand that the SLA does not constitute a warranty to you.

## 1. Definitions

a. "Authorized Contact" means the individual you have specified to IBM who is authorized to submit Claims under this SLA.

b. "Availability Credit" means the remedy IBM will provide for a validated Claim. The Availability Credit will be applied in the form of a credit or discount against a future invoice of subscription charges for the IBM SaaS.

c. "Claim" means a claim submitted by your Authorized Contact to IBM pursuant to this SLA that a Service Level has not been met during a Contracted Month.

d. "Contracted Month" means each full month during the term of the IBM SaaS measured from 12:00 a.m. GMT on the first day of the month through 11:59 p.m. GMT on the last day of the month.

e. "Client" or "you" or "your" means an entity that is subscribing for the IBM SaaS directly from IBM, and that is not in default of any material obligations, including payment obligations, under its contract with IBM for the IBM SaaS.

f. "Downtime" means Application Downtime and/or Inbound Processing Downtime applicable to the corresponding Service Level shown on the table below. Downtime does not include the period of time when the IBM SaaS is not available as a result of:

- Planned System Downtime;
- Force Majeure;
- Problems with Client or third party applications, equipment, or data;
- Client or third party acts or omissions (including anyone gaining access to the IBM SaaS by means of your passwords or equipment);
- Failure to adhere to required system configurations and supported platforms for accessing the IBM SaaS; or
- IBM's compliance with any designs, specifications, or instructions provided by Client or a third party on Client's behalf.

g. "Event" means a circumstance or set of circumstances taken together, resulting in a failure to meet a Service Level.

h. "Force Majeure" means acts of God, terrorism, labor action, fire, flood, earthquake, riot, war, governmental acts, orders or restrictions, viruses, denial of service attacks and other malicious conduct, utility and network connectivity failures, or any other cause of the IBM SaaS unavailability that was outside IBM's reasonable control.

i. "Planned System Downtime" means a scheduled outage of the IBM SaaS for the purpose of maintenance.

j. "Service Level" means the standard set forth below by which IBM measures the level of service it provides in this SLA.

## 2. Availability Credits

a. In order to be eligible to submit a Claim you must have logged a support ticket for each Event with the IBM customer support help desk for the applicable IBM SaaS, in accordance with IBM procedure for reporting Severity 1 support issues. You must provide all necessary detailed information about the Event and reasonably assist IBM with the diagnosis and resolution of the Event to the extent required for Severity 1 support tickets. Such ticket must be logged within twenty-four (24) hours of your first becoming aware that the Event has impacted your use of the IBM SaaS.

b. Your Authorized Contact must submit your Claim for an Availability Credit no later than three (3) business days after the end of the Contracted Month that is the subject of the Claim.

c. Your Authorized Contact must provide to IBM all reasonable details regarding the Claim, including but not limited to, detailed descriptions of all relevant Events and the Service Level claimed not to have been met.

d. IBM will measure internally total combined Downtime during each Contracted Month applicable to the corresponding Service Level shown on the table below. Availability Credits will be based on the duration of the Downtime measured from the time you report that you were first impacted by the Downtime. If Client reports an Event of Application Downtime and an Event of Inbound Data Processing Downtime occurring simultaneously, then IBM will treat the overlapping periods of Downtime as a single period of Downtime, and not as two separate periods of Downtime. For each valid Claim, IBM will apply the highest applicable Availability Credit based on the achieved Service Level during each Contracted Month, as shown on the tables below. IBM will not be liable for multiple Availability Credits for the same Event(s) in the same Contracted Month.

e. For Bundled Service (individual IBM SaaS packaged and sold together for a single combined price), the Availability Credit will be calculated based on the single combined monthly price for the Bundled Service, and not the monthly subscription fee for each individual IBM SaaS. You may only submit Claims relating to one individual IBM SaaS in a bundle in any Contracted Month, and IBM will not be liable for Availability Credits with respect to more than one IBM SaaS in a bundle in any Contracted Month.

f. If you purchased the IBM SaaS from a valid IBM reseller in a remarketing transaction in which IBM maintains primary responsibility for fulfilling the IBM SaaS and SLA commitments, then the Availability Credit will be based on the then-current Relationship Suggested Value Price (RSVP) for the IBM SaaS in effect for the Contracted Month which is the subject of a Claim, discounted at a rate of 50%.

g. The total Availability Credits awarded with respect to any Contracted Month shall not, under any circumstance, exceed ten percent (10%) of one twelfth (1/12th) of the annual charge paid by you to IBM for the IBM SaaS.

h. IBM will use its reasonable judgment to validate Claims based on information available in IBM's records, which will prevail in the event of a conflict with data in your records.

i. THE AVAILABILITY CREDITS PROVIDED TO YOU IN ACCORDANCE WITH THIS SLA ARE YOUR SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM.

## 3. Service Levels – Availability of the IBM SaaS during a Contracted Month

| **Achieved Service Level (during a Contracted Month)** | **Availability Credit (% of Monthly Subscription Fee for Contracted Month which is the subject of a Claim)** |
|---|---|
| Less than 99.8% | 2% |
| Less than 98.8% | 5% |
| Less than 95.0% | 10% |

“Achieved Service Level”, expressed as a percentage is calculated as: (a) the total number of minutes in a Contracted Month, minus (b) the total number of minutes of Downtime in a Contracted Month, divided by (c) the total number of minutes in a Contracted Month.

Example: 50 minutes total Downtime during Contracted Month

| | |
|---|---|
| 43,200 total minutes in a 30 day Contracted Month -- 50 minutes Downtime = 43,150 minutes<br>_____<br>43,200 total minutes | = 2% Availability Credit for 99.8% Achieved Service Level during the Contracted Month |

## 4. Exclusions

This SLA is made available only to IBM Clients. This SLA does not apply to the following:

- Beta and trial Services.
- Non-production environments, including but not limited to, test, disaster recovery, quality assurance, or development.
- Claims made by an IBM Client's users, guests, participants and permitted invitees of the IBM SaaS.
- Enabling Software