

IBM MobileFirst Protect On-Premise



# Configuration Guide

*Version 2 Release 4*



IBM MobileFirst Protect On-Premise



# Configuration Guide

*Version 2 Release 4*

**Note**

Before using this information and the product it supports, read the information in "Notices" on page 63.

This edition applies to version 2, release 4, modification level 0 of IBM MobileFirst Protect (program number 5725-R11) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2014, 2016.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

|   |           |
|---|-----------|
| <b>Chapter 1. IBM MobileFirst Protect On-Premise Configuration Guide Overview . . . . .</b>             | <b>1</b>  |
| <b>Chapter 2. About IBM MaaS360 Accounts . . . . .</b>  | <b>3</b>  |
| <b>Chapter 3. Step 1: Creating an account . . . . .</b>   | <b>5</b>  |
| <b>Chapter 4. Step 2: Customizing Your Deployment . . . . .</b>   | <b>7</b>  |
| <b>Chapter 5. Step 3: Configuring the Portal Branding . . . . .</b>                                     | <b>9</b>  |
| <b>Chapter 6. Step 4: Configuring iOS MDM Branding . . . . .</b>  | <b>11</b> |
| <b>Chapter 7. Step 5: Configuring Email Settings . . . . .</b>  | <b>13</b> |
| <b>Chapter 8. Step 6: Enabling Web Services . . . . .</b>   | <b>15</b> |
| <b>Chapter 9. Step 7: Preparing to Manage Apple iOS Devices. . . . .</b>                                | <b>17</b> |
| <b>Chapter 10. Step 8: Preparing to Manage Windows Phone Devices . . . . .</b>                          | <b>21</b> |
| <b>Chapter 11. About Enterprise Mobile Device Management Agent Apps . . . . .</b>                       | <b>25</b> |
| <b>Chapter 12. Step 9: Downloading IBM MobileFirst Protect Apps . . . . .</b>                           | <b>27</b> |
| <b>Chapter 13. Step 10: Signing MaaS360 for Windows Phone Phone Apps . . . . .</b>                      | <b>29</b> |
| <b>Chapter 14. Uploading Apps . . . . .</b>   | <b>31</b> |
| App Upload Setting Options . . . . .  | 33        |
| Options for iOS apps . . . . .  | 34        |
| Options for Android apps . . . . .  | 34        |
| <b>Chapter 15. About the IBM MobileFirst Protect WorkPlace SDK . . . . .</b>                            | <b>37</b> |
| <b>Chapter 16. Configuring for the Apple Device Enrollment Program. . . . .</b>                         | <b>39</b> |
| <b>Chapter 17. Configuring IBM MobileFirst Protect for the Android for Work Program . . . . .</b>       | <b>45</b> |
| Making sure that your IBM MobileFirst Protect and Google Accounts are ready . . . . .                   | 45        |
| Configuring Android for Work in your Google for Work account. . . . .                                   | 45        |
| Creating Google accounts for your users. . . . .  | 46        |
| Enrolling users with IBM MobileFirst Protect and Android for Work . . . . .                             | 47        |
| <b>Chapter 18. About Security Information and Event Management (SIEM) Support With QRadar . . . . .</b> | <b>53</b> |
| <b>Chapter 19. Managing Certificates . . . . .</b>  | <b>55</b> |
| Managing SCEP Certificates . . . . .  | 55        |
| Checking SCEP Certificate Expiry . . . . .  | 55        |
| Renewing the SCEP Certificate . . . . .   | 55        |
| Renewing the SCEP Certificate in HA (High Availability) Environments . . . . .                          | 56        |
| Roll Back SCEP Certificate Renewal . . . . .  | 57        |
| About Self-Signed Certificates Support . . . . .  | 57        |
| <b>Chapter 20. Next Steps . . . . .</b>   | <b>61</b> |
| <b>Notices . . . . .</b>  | <b>63</b> |
| Trademarks . . . . .  | 65        |
| Terms and conditions for product documentation. . . . .   | 65        |



---

## Chapter 1. IBM MobileFirst Protect On-Premise Configuration Guide Overview

The goal of this document is to provide an overview of the steps required to customize your IBM MobileFirst™ Protect On-Premise deployment before you start directing end users to enroll their devices.

Before proceeding, your IBM MobileFirst Protect On-Premise instance must be deployed and configured as described in the IBM MobileFirst Protect On-Premise Installation Guide.





---

## Chapter 2. About IBM MaaS360 Accounts

IBM® MaaS360® provides three kinds of accounts:

- **Full Mobile Device Management (MDM) account**

A full MDM account installs an MDM profile on enrolled devices, and allows a wide range of control over those devices.

- **Secure Productivity Suite<sup>®</sup>™ (SPS) account**

A SPS account provides security by providing secure apps on devices. An SPS account does not install an MDM profile on the device. Instead, the IBM MaaS360 SPS app allows secure mail, calendar, contacts, and a secure browser.

Agent apps allow content such as email, calendars, contacts, and browsing to be performed in a secure container.

- **Mobile Application Management (MAM) account**

A MAM account installs an app catalog on the device facilitating enterprise app distribution and app life-cycle management on the device.

- **Reseller account**

A reseller account is automatically created when you deploy your instance. The reseller account allows you to create organization administration accounts to provide IBM MaaS360 as a SaaS offering to other clients.

The default username for the Reseller account is `partner_master` and the password for this account is sent to the email address used during the deployment of IBM MaaS360.

If you are not sure on what type of account should be created, please contact your IBM support contact.



## Chapter 3. Step 1: Creating an account

### About this task

You can use the account creation portal after your IBM MobileFirst Protect deployment is configured.

### Procedure

1. Using Chrome, Firefox, or Internet Explorer Browser version 11 or later, open `http://Configuration_VM_IP_Address`.

You could also directly open the account creation pages for the account type:

MDM accounts - `https://Portal_URL/tryMDM/SK_MDM_C`

SPS accounts - `https://Portal_URL/try_MDM/SK_SPS`

MAM accounts - `https://Portal_URL/try_MDM/SK_MAM`

2. Enter the username and password you created and click **Log In**.
3. Click the **Create MaaS360 Account** menu and select the type of account to create.



4. Enter the required fields to create your account.

A screenshot of the MaaS360 account creation form. The form is titled 'Create a MaaS360 Account' and includes a green 'Create MaaS360 Account' button. Below the button, there is a section for 'Your Login Details' with several input fields: 'Email' (with the example 'example@corporate.com'), 'Password' (with the prompt 'Enter a strong password'), 'Confirm Password' (with the prompt 'Confirm your password'), 'Company Name' (with the prompt 'Enter your company name'), 'Full Name' (with the prompt 'First name Last name'), and 'Phone Number' (with the prompt 'Enter phone number'). A 'Create Account' button is located at the bottom of the form. The MaaS360 logo and tagline 'See. Know. Go.' are visible at the top left of the form.

**Email:** Specify the email address used for creating an IBM MobileFirst Protect account. This email address will be used to log into the portal and manage your deployment's devices.

**Password and Confirm Password:** Specify the password for the account. Be sure to select a strong password.

**Company Name:** Specify your company name.

**Full Name:** Specify the name of the primary portal administrator.

**Phone Number:** Specify a contact number.

5. Click Create Account.

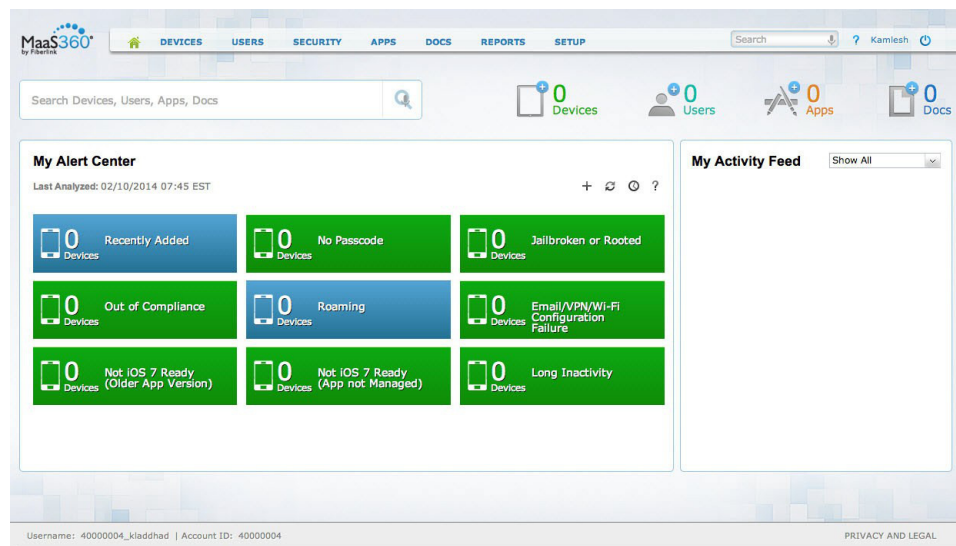
An account is created as well as an administrator login, and you are logged into the portal. The email address you specified will be sent an email with login details.

When the Portal is first displayed, some preliminary tips might be displayed.

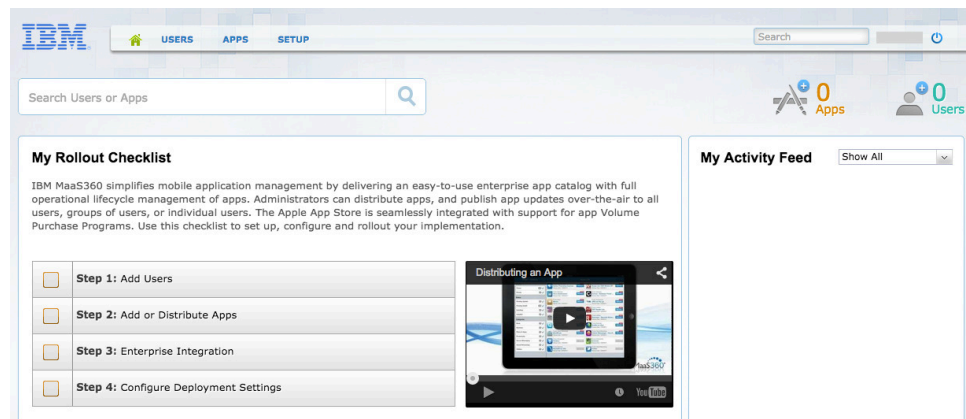
**Note:** If you get an error with the new customer account, and the ios-mdm and dp modules produce errors in the Administration Console, you probably have a problem with the certificates used in the configuration. Contact IBM Support to verify the integrity of the certificates.

6. Click Close to access the main portal page.

The MDM and SPS portals show a status and alert page.



The MAM portal shows a deployment checklist.



---

## Chapter 4. Step 2: Customizing Your Deployment

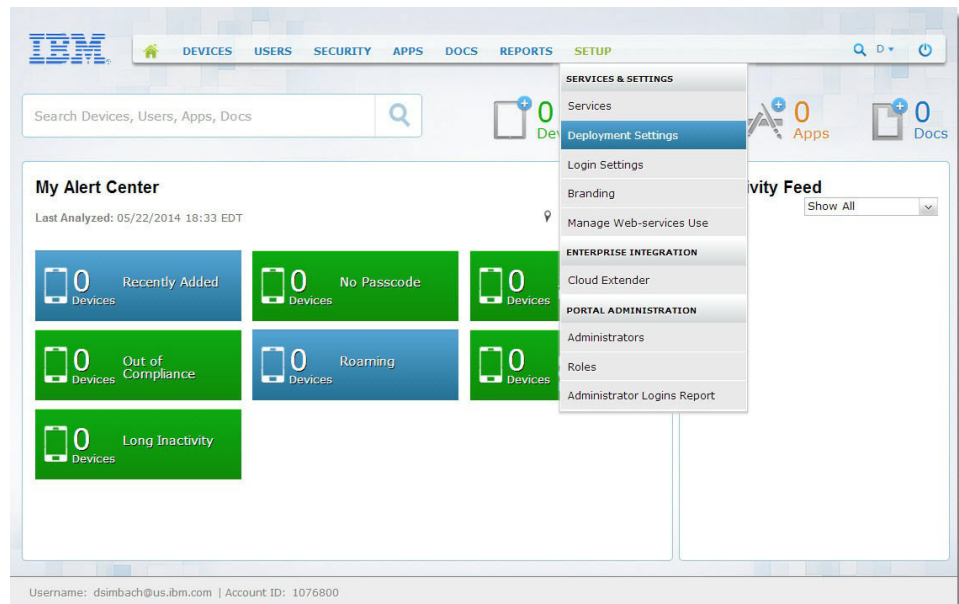
### About this task

With an account created, the first step is to make some basic changes to customize your IBM MobileFirst Protect deployment.

### Procedure

1. Log in to the main portal page.

From the top navigation bar, navigate to **Setup > Deployment Settings**.



2. Change the **Corporate Identifier** to better reflect your deployment.

This might be your company name, for example. This identifier is used in the enrollment URL and other locations.

The screenshot shows the 'Deployment Settings' page in the IBM MobileFirst console. At the top, there is a navigation bar with 'DEVICES', 'USERS', 'SECURITY', 'APPS', 'DOCS', 'REPORTS', and 'SETUP'. The 'Corporate Identifier' field is highlighted with a red box and contains the value '1076800'. Below this, there are several sections with checkboxes and radio buttons for configuration. The 'Corporate Information' section is also highlighted with a red box and contains the following fields: 'iOS Services Hostname' (with 'IBM ID' entered), 'Contact Email', 'Phone Number', and 'Custom Instructions'. A 'Save' button is located at the bottom right of the page. The footer shows the username 'dsimbach@us.ibm.com' and account ID '1076800'.

3. Under **Corporate Information**, enter the following information: **iOS Services Hostname** - Enter a string that is displayed during over-the-air actions scheduled for iOS 7 and iOS 8 devices.  
**Contact Email** - Enter an email address that is presented to end users as the primary contact email.  
**Phone Number** - Enter the phone number that is presented to end users as the primary contact number.  
**Custom Instructions** - A URL pointing to the information entered here is provided to users during device enrollment.
4. Click **Save**. You are prompted to enter your password and are directed back to the home page.

---

## Chapter 5. Step 3: Configuring the Portal Branding

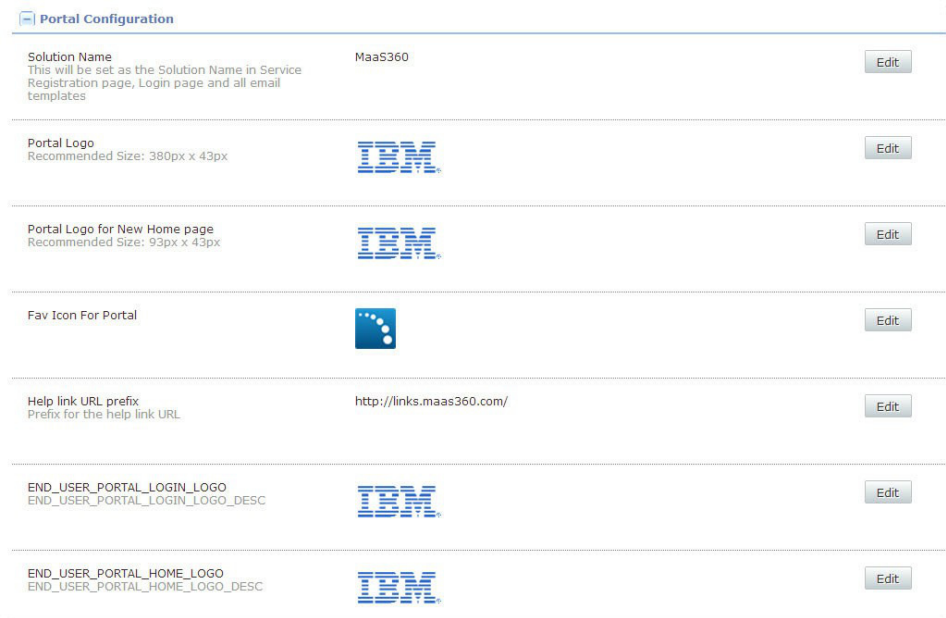
### About this task

Several elements of the portal can be branded to better represent your identity.






This includes your service name, portal logo, support details, and more. Some of these elements might have been set up during the configuration process outlined in the IBM MobileFirst Protect On-Premise Installation Guide.

### Procedure

1. Log in to the main portal page, and navigate to **Setup > Branding**.
2. Click **Portal Configuration**.



The screenshot displays the 'Portal Configuration' interface with the following settings:

| Setting  | Value   | Action |
|--|---|--------|
| <b>Solution Name</b><br>This will be set as the Solution Name in Service Registration page, Login page and all email templates | MaaS360   | Edit   |
| <b>Portal Logo</b><br>Recommended Size: 380px x 43px   |    | Edit   |
| <b>Portal Logo for New Home page</b><br>Recommended Size: 93px x 43px  |    | Edit   |
| <b>Fav Icon For Portal</b>   |  | Edit   |
| <b>Help link URL prefix</b><br>Prefix for the help link URL  | http://links.maas360.com/   | Edit   |
| <b>END_USER_PORTAL_LOGIN_LOGO</b><br>END_USER_PORTAL_LOGIN_LOGO_DESC   |  | Edit   |
| <b>END_USER_PORTAL_HOME_LOGO</b><br>END_USER_PORTAL_HOME_LOGO_DESC   |  | Edit   |

3. Click **Edit** next to each setting to configure it, as needed:

- **Solution Name**

This is the name displayed in the Service Registration page, Login page, and all email templates. Changing this will replace all references to your IBM MobileFirst Protect solution in email communications and portal messaging.

- **Portal Logo**

This is the main logo for your deployment.

- **Portal Logo for New Home Page**

Configure a smaller logo used in the portal.

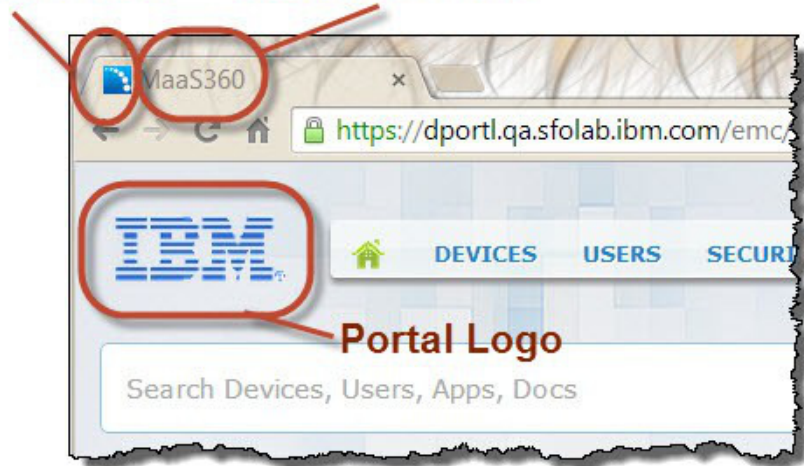
- **Favorite Icon**

This is the small icon used in browser tabs.

- **Help Link URL Prefix**

Host your own documentation using this URL for that content.

**Favorite Icon**      **Solution Name**





---

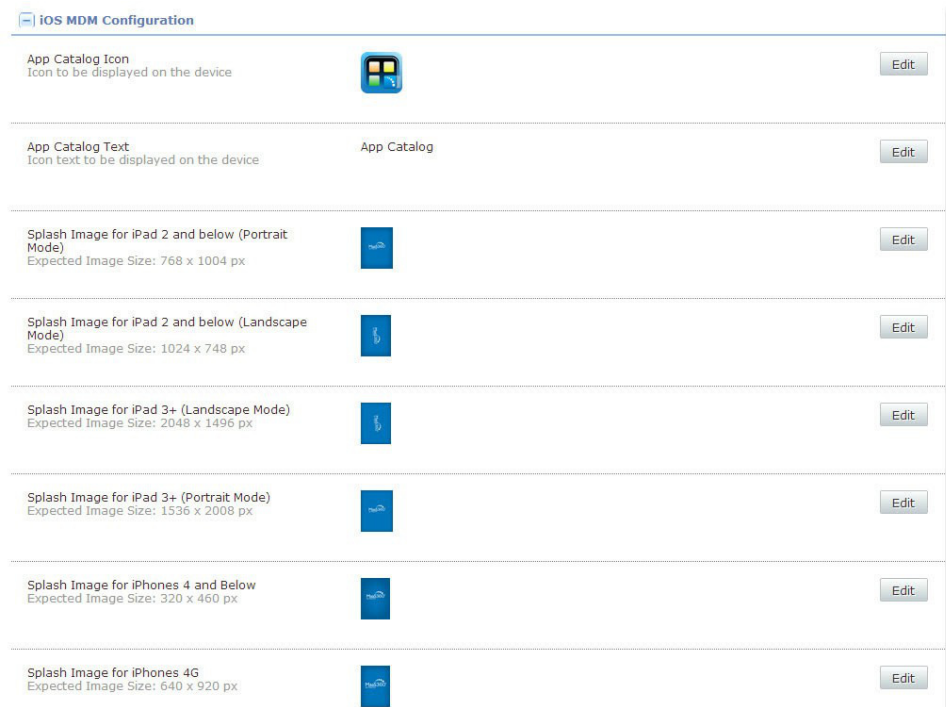
## Chapter 6. Step 4: Configuring iOS MDM Branding

### About this task

You can configure branding options that apply to iOS devices only.

### Procedure

1. Log in to the main portal page, and navigate to **Setup > Branding**.
2. Click **iOS MDM Configuration**.



3. Click **Edit** next to each setting to configure it, as needed:
  - **App Catalog Icon**  
This icon is used as the app icon on iOS devices.
  - **App Catalog Text**  
This is the text displayed for the app icon.
  - **Splash Images**  
A series of splash screen images can be uploaded for every type of iOS device.





## Chapter 7. Step 5: Configuring Email Settings

### About this task

You can configure the email options that affect the origin and look of all emails. Some of these settings might be populated from the Administration Console configuration process described in the IBM MobileFirst Protect On-Premise Installation Guide.

### Procedure

1. Log in to the main portal page, and navigate to **Setup > Branding**.
2. Click **Email Configuration**.

| Email Configuration  |   |      |
|--|---|------|
| Email Sender (Email Address)<br>Email Address specified in all emails sent   | maas360@fiberlink.com   | Edit |
| Email Sender Display Name<br>Name of the Email sender displayed in all emails sent                                 | MaaS360   | Edit |
| Email Logo<br>Image that will be used in all emails.<br>Recommended Size: 200 x 115 px                             |    | Edit |
| Email Background   |  | Edit |
| Support Email<br>Support email address specified in emails sent  | dsimbach@us.ibm.com   | Edit |
| Support Contact Number<br>Support contact number specified in emails sent  | 415 555 5555  | Edit |
| Additional Support Information<br>If specified, this will be displayed along with Support Email and Contact Number |   | Edit |

3. Click **Edit** next to each setting to configure it, as needed:

| Setting                          | Description   |
|----------------------------------|---|
| <b>Email Sender</b>              | Enter the email address that emails will originate from. This email must be setup on your SMTP server.  |
| <b>Email Sender Display Name</b> | The string entered here determines the name displayed as the email sender. This entry might be overridden by name associated in your SMTP server. |
| <b>Email Logo</b>                | Upload the image used in email communication. The recommended file size is 200x115 pixels.  |
| <b>Email Background</b>          | Upload an image to be used in the email header background.  |
| <b>Support Email</b>             | The email address entered here is presented as the contact information for support issues.  |

| <b>Setting</b>                        | <b>Description</b>   |
|---------------------------------------|--|
| <b>Support Contact Number</b>         | Similar to the Support Email, this number is presented to email recipients as the way to reach technical support.            |
| <b>Additional Support Information</b> | Any text entered here is displayed with the email and number provided. Use this area to highlight instructions, for example. |

## Chapter 8. Step 6: Enabling Web Services

### About this task

IBM MobileFirst Protect provides a REST style web-service Application Programming Interface (API) for integrating IBM MobileFirst Protect workflows with other applications.

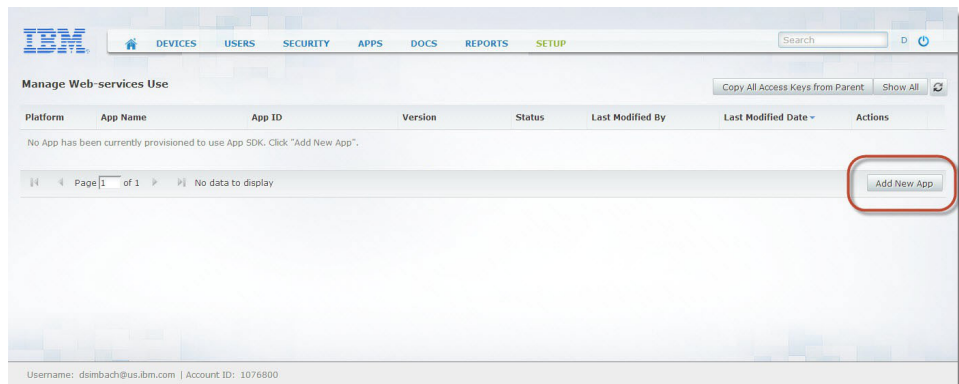
Enabling this API is a requirement for integration with or migration from IBM Endpoint Manager for Mobile Device Management. This is also a requirement for Worklight integration.

To use IBM MobileFirst Protect APIs, an API access key must be generated. You can generate multiple API access keys by creating multiple apps in this workflow. Apps can be deactivated, or their API access keys viewed by using the Actions button to the right of each app.

Complete the following steps to acquire an API access key:

### Procedure

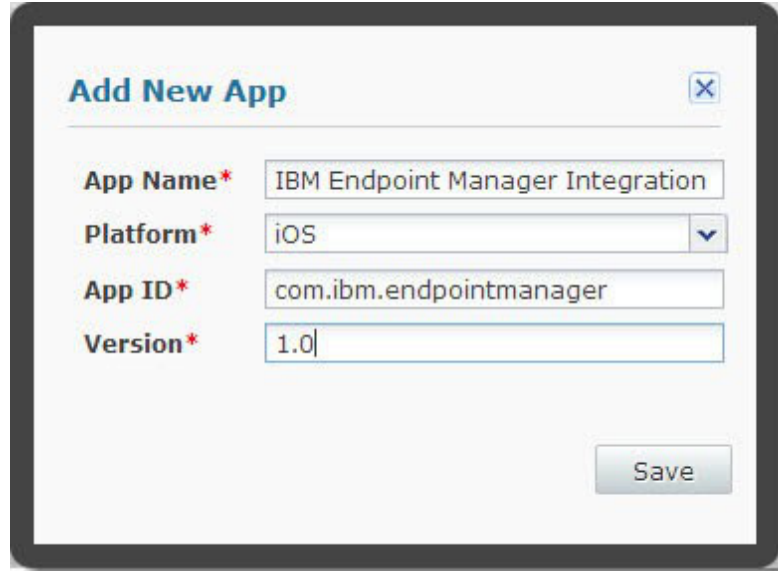
1. Log in to the main portal page, and navigate to **Setup > Manage Web-services Use**.
2. Click **Add New App**.



3. Enter the following information:

| Setting         | Description   |
|-----------------|---|
| <b>App Name</b> | Name of the application that you are planning to integrate using IBM MobileFirst Protect APIs.  |
| <b>Platform</b> | Select iOS or Android from the dropdown menu. This setting does not necessarily dictate the types of devices that can be managed using the APIs. If you are unsure, select iOS. |
| <b>App ID</b>   | Enter an identity for the application you are planning to integrate. For example, com.maas360.mycompany.myapplication.  |
| <b>Version</b>  | Version for the application. For example, 1.0.  |

**Note:** All of these fields are mandatory; however, the values are primarily for your reference.



**Add New App** [X]

**App Name\*** IBM Endpoint Manager Integration

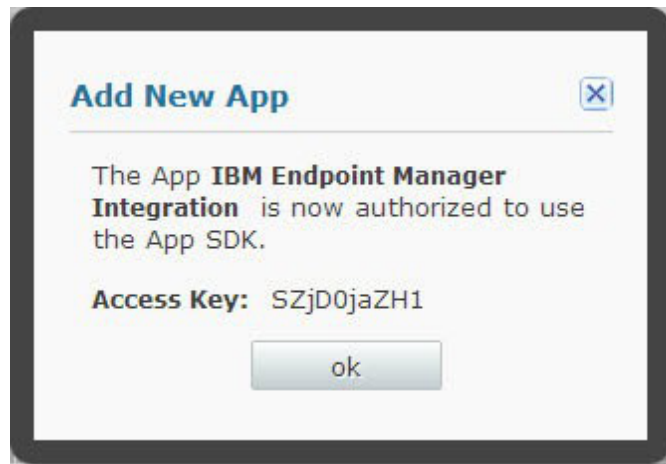
**Platform\*** iOS [v]

**App ID\*** com.ibm.endpointmanager

**Version\*** 1.0

Save

4. Click Save to generate an API access key.
5. Note the access key for future use.



**Add New App** [X]

The App **IBM Endpoint Manager Integration** is now authorized to use the App SDK.

**Access Key:** SZjD0jaZH1

ok

---

## Chapter 9. Step 7: Preparing to Manage Apple iOS Devices

If you do not plan to manage iOS devices in your deployment, the following components are not necessary.

If your IBM MobileFirst Protect On-Premise Instance (v2.4 or later) is configured to use the MaaS360 apps in the Apple App Store, you need one certificate from IBM support to manage iOS devices. For more information about getting this certificate, see the IBM MobileFirst Protect On-Premise Installation Guide.

### Apple Push Notification Service (APNS) certificate

The APNS certificate is used by IBM MobileFirst Protect On-Premise Portal (the MDM provider) to communicate with iOS devices through Apple's notification service. The APNS Certificate requires an Apple ID for your organization, and it creates cryptographic trust between your devices, your IBM MobileFirst Protect instance, and Apple.

---

## Prerequisites to Manage Apple Devices

If your IBM MobileFirst Protect On-Premise (v2.4 or later) Instance manages the devices using apps from the Apple App Store, you need:

- An Apple ID for the organization
- A Mac with OSX 10.8+
- Contact with your organization's primary administrator
- Contact with IBM MobileFirst Protect Support
- Firewall rules to allow the Apple push notification requests, originating from IBM MobileFirst Protect VMs, to Apple Servers (typically hosted in the IP range 17.0.0.0/8) at port 2195 to go out to the internet.
- Firewall and/or proxy rule whitelisting <https://gateway.push.apple.com:2195>.

---

## Get an APNS Certificate (aka an Apple MDM Certificate)

### About this task

An Apple Push Notification (APNS) SSL Certificate is required to allow communication to Apple iOS devices. The certificate is sometimes referred to simply as the Apple MDM Certificate.

You need to contact IBM Support to obtain an APNS Certificate requires IBM Support. Contact IBM Support and reference the following documentation:

<https://www-01.ibm.com/support/docview.wss?uid=swg21674105>

**Note:** The APNS Certificate must be renewed on a yearly basis.

When you renew the certificate, you must use the same Apple ID that was used to originally generate the certificate. Using a different Apple ID changes the APNS Certificate, which results in communication issues within your deployed devices.

For this reason, use an Apple ID owned by your organization, and not an individual. Be sure to record which Apple ID is used to create your APNS Certificate.

## Procedure

1. Generate a Certificate Signing Request (CSR) with the Internet Information Services Manager (IIS) on a Windows host.

For more information, see <http://technet.microsoft.com/en-us/library/cc730929.aspx>.

The CSR must be created with the following parameters provided:

| Parameter      | Description  |
|----------------|--|
| Common Name    | Enter the name that is associated with the Apple ID account for your organization. |
| Organization   | Your company name.   |
| City/Locality  | The city in which your company is located.   |
| State/Province | The state or province in which your company is located.                            |
| Country/Region | The country or region in which your company is located.                            |

2. Send your new CSR to IBM Support. IBM Support signs the CSR and returns it to you.
3. Use the newly signed CSR to generate an APNS Certificate using Apple Inc.'s web site.  
To begin the process, see <https://identity.apple.com/> .  
This process ties the APNS certificate to an Apple ID. Use an organization Apple ID that can be used to renew the certificate on a yearly basis. Do not use a personal Apple ID.
4. After you finish the process with Apple, download the final APNS Certificate. The APNS Certificate from Apple site is in .pem format, and the file must be converted into .p12 format by using a private key and password.
5. Import the .pem file on the same computer where you generated the CSR before sending to IBM support.
6. Upload the final APNS Certificate to your IBM MobileFirst Protect deployment.

---

## Upload the APNS Certificate (aka the Apple MDM Certificate)

### About this task

This certificate is required for IBM MobileFirst Protect MDM accounts only, and is not required for SPS and MAM accounts.

Your APNS Certificate, sometimes referred to simply as the Apple MDM Certificate, must be uploaded within the Portal to allow communication with iOS devices.

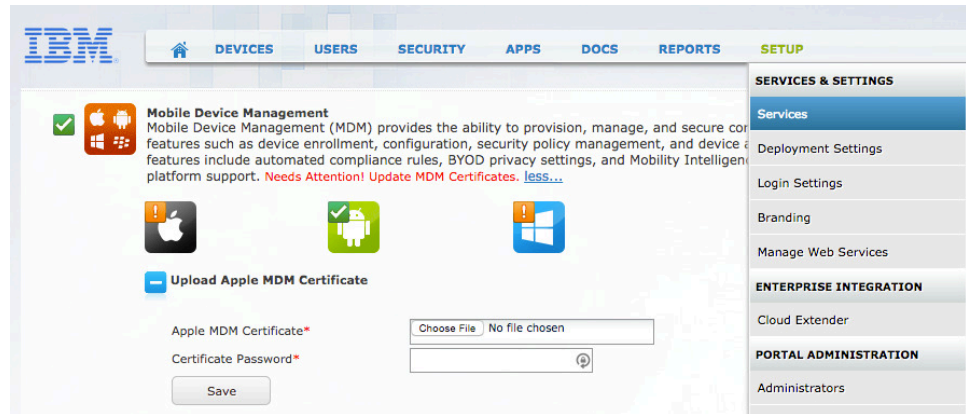
Complete the following steps to upload the certificate:

### Procedure

1. Log in to the main portal page, and navigate to **Setup > Services**.



2. Click the **Mobile Device Management** check box, and then click **more...** to expand the settings.
3. Click **Upload Apple MDM Certificate**.



4. Click **Choose File**, and then select your APNS Certificate.
5. Enter the Certificate Password and click **Save**.



---

## Chapter 10. Step 8: Preparing to Manage Windows Phone Devices

### About this task

Windows Phone enables companies to publish and distribute Windows Phone apps directly to their employees or other users, bypassing the Windows Phone Store.

Users can install apps published by their company only after they enroll their phones for app distribution from their company. Windows Phone uses the term *Company Hub* to refer to Windows Phone agents. The MaaS360 for Windows Phone Agent is your MaaS360 Company Hub.

To distribute apps to Windows Phone devices, you must:

### Procedure

1. Get a Windows Phone Developer account.  
This account requires a yearly fee.
2. Get a Symantec Code Signing Certificate.  
Symantec charges a yearly fee for each certificate.
3. Extract an Application Enrollment Token (AET) from the Symantec Code Signing Certificate.
4. Upload the AET to your deployment Portal.
5. Whitelist the following URLs in your firewall and/or proxy server:
  - [http://\\*.notify.live.net](http://*.notify.live.net)
  - [http://\\*.notify.windows.com](http://*.notify.windows.com)
  - <https://www.windowsphone.com>
  - <https://www.microsoft.com>

---

## Get a Windows Phone Developer Account

### About this task

Getting a Windows Phone Developer Account is the first step in the process of managing Windows Phone devices.

From the developer account, get your Publisher ID. The Publisher ID is used to validate your company with Symantec.

### Procedure

1. Establish a company account on Windows Phone Dev Center. For more information, see the Windows documentation at <https://dev.windows.com/en-US/>.
2. After registration is complete, your Publisher ID can be found on the Dev Center account summary page.

---

## Get a Symantec Code Signing Certificate

### About this task

After you get a Windows Phone Developer Account, you can purchase the Code Signing Certificate from Symantec.

### Procedure

1. Navigate to the following URL to purchase a Symantec Code Signing Certificate: <https://products.websecurity.symantec.com/orders/enrollment/microsoftCert.do>
2. Enter your Publisher ID from Windows Dev Center and the email address associated with your Windows Phone Developer account.
3. Symantec sends an email with instructions on how to import your new certificate into your computer's local certificate store (certmgr.msc).

Three certificates should be imported into the computer's local certificate store: one certificate for your organization and two other Symantec/Microsoft certificates.

To export the certificate from your certificate store, so the AET can be extracted, it is important that each of the steps in the Symantec email be executed properly.

---

## Export the Code Signing Certificate

### About this task

You use the Windows certificate manager to export the code signing certificate as a PFX file.

### Procedure

1. Open your computer's certificate manager by running *certmgr.msc* from the Windows Start menu.
2. Expand the Personal folder and select your new certificate.
3. Select **Actions > All Tasks > Export**. The Certificate Export Wizard launches.
4. Select the following options as part of the export:
  - Yes, export the private key.
  - Include all certificates in the certification path if possible.
  - Export all extended properties.
5. You are prompted for a password to encrypt the certificate's private key.
6. You will need this password to upload the certificate to IBM MobileFirst Protect. The password should not contain special characters like ;, \, " = ( ) + | % &.
7. Choose a destination for the finished certificate file.

---

## Upload the AET

### About this task

After your Application Enterprise Token (AET) is extracted from your Symantec Code Signing Certificate, it must be uploaded to your deployment through the Portal.

## Procedure

1. Log in to the main portal page, and navigate to **Setup > Services**.
2. Click the **Mobile Device Management** check box, and then click **more...** to expand the settings.
3. Click **Windows Phone 8 MDM**.

The screenshot shows the IBM MaaS360 Services page. The top navigation bar includes 'DEVICES', 'USERS', 'SECURITY', 'APPS', 'DOCS', 'REPORTS', and 'SETUP'. The 'Services' section is expanded to show 'Mobile Device Management' with a checked checkbox. Below this, there are three device icons: Apple, Android, and Windows. The 'Apple MDM Certificate' section has a 'Choose File' button with 'APNS (Phani).p12' selected and a 'Certificate Password' field. The 'Apple Push Notification SSL Certificates' section has a 'Choose File' button with 'No file chosen' and a 'Certificate Password' field. The 'Import iPhone Configuration Utility settings' checkbox is unchecked. The 'Windows Phone 8 MDM' section is highlighted with a red box and has a checked checkbox. It includes a description: 'The Windows Phone 8 Company Hub certificate allows for the distribution of applications, real-time actions, and location services. To take advantage of these features, the certificate must be installed prior to enrolling your Windows Phone 8 devices.' Below this is an 'Application Enterprise Token (AET)' field with a 'Choose File' button and 'No file chosen' selected, and a 'Save' button. The footer shows 'Username: dsimbach@us.ibm.com | Account ID: 1076800 | Last Login: 05/22/2014 18:33 EDT'.

4. Select **Choose File**, and then select your AET file.
5. Click **Save**.



---

## Chapter 11. About Enterprise Mobile Device Management Agent Apps

Before managing iOS, Android, or Windows Phone devices, IBM MobileFirst Protect Agent Apps must be uploaded to your account for each platform.

When devices are enrolled in your environment, the appropriate agent app is sent to the device.

The first step of this process is to obtain the various agent apps. The agent apps are available on the Services VM within your deployment.

The next step is to code sign the Windows Phone agents so that they can be transferred to their target devices. The iOS App Store apps and Android agents do not require signing.

Finally, the signed agents must be uploaded to your IBM MobileFirst Protect account so that they are available to devices that begin enrollment.

---

### MaaS360 iOS Apps

The following agent apps for iOS are available on Apple iOS App Store:

- **MaaS360 for iOS** -MaaS360 MDM Enrollment Agent is installed on iOS devices during enrollment.
- **Secure Browser for iOS** -Secure Browser helps you track and block websites visited by the user on the device.
- **Secure Editor for iOS** - Secure Editor allows users to edit documents inside the MaaS360 Secure Productivity Suite.

For instructions about uploading iOS apps, see “Chapter 14, “Uploading Apps,” on page 31”.

---

### MaaS360 Windows Phone Apps

Windows Phone apps for IBM MobileFirst Protect are:

- - The is an MDM agent that is installed on Windows Phone devices during enrollment.
- **Secure Email for Windows Phone** - This app is the IBM MobileFirst Protect Email client and is part of IBM MobileFirst Protect Secure Productivity Suite.
- **Secure Browser for Windows Phone** – IBM MobileFirst Protect Secure Browser helps you track and block websites visited by the user on the device.
- **Secure Docs for Windows Phone** - Secure Docs allows employees to view documents within IBM MobileFirst Protect content management system.

Windows Phone apps must be code signed with your Symantec Code Signing Certificate. After the apps are signed, they can be uploaded through the Portal so they are available to enrolling devices. For more information, see “Chapter 13, “Step 10: Signing MaaS360 for Windows Phone Phone Apps,” on page 29”.

For instructions about uploading signed Windows Phone apps, see “Chapter 14, “Uploading Apps,” on page 31”.

---

## IBM MobileFirst Protect Android Apps

Android agent apps for IBM MobileFirst Protect are:

- **MaaS360 for Android** - This MDM Agent is installed on Android devices during enrollment. This agent is installed on all Android devices that are not manufactured by Samsung and are running at least Android version 4.0, which is also known as Ice Cream Sandwich.
- **MaaS360 for Android Samsung** - This MDM Agent is installed on Android devices manufactured by Samsung.
- **MaaS360 for Android LG** - This MDM agent is optional and can be installed on Android devices manufactured by LG. If you need special administrative features for LG devices, contact IBM Customer Support. By default, MaaS360 for Android agent works on LG devices
- **Secure Browser for Android** – Secure Browser helps you track and block websites visited by the user on the device.
- **Secure Viewer for Android** - Secure Viewer allows users to view documents within the MaaS360 Secure Productivity Suite.
- **Secure Editor for Android** - Secure Editor allows users to edit documents within the MaaS360 Secure Productivity Suite.
- **Secure Email for Android** - This app is the Secure Email client and is part of the MaaS360 Secure Productivity Suite.
- **Secure Docs for Android** - Secure Docs allows employees to view documents within IBM MobileFirst Protect content management system.
- **Remote Control Agent for Samsung** - This add-on agent allows IT help desk to sign into enrolled user's device and remotely help troubleshoot any issues user may be experiencing. Permission must be given to IT before they are able to control the device.
- **Android Kiosk Agent**- This agent runs the Android device in “kiosk mode” preventing users from reconfiguring the device.
- All Android apps are signed, and do not require a separate signing process. Only Windows Phone apps require additional modification.

For instructions about uploading Android apps, see Chapter 14, “Uploading Apps,” on page 31.



---

## Chapter 12. Step 9: Downloading IBM MobileFirst Protect Apps

### About this task

The apps and agents are available to download through the Administration Console that is hosted on the Configuration VM.

### Procedure

1. Using any browser, navigate to [http://Configuration\\_VM\\_IP\\_Address](http://Configuration_VM_IP_Address).  
You might be presented with a warning that the address is untrusted, but this warning can be ignored.
2. Enter the default username and password and click **Log In**.
3. Click **Configure** from the upper-right corner, and then click **Downloads**.
4. Click the desired app or agent link from the IBM MobileFirst Protect Apps and Agents section.

| MaaS360 Apps and Agents         |  |   |   |
|---------------------------------|--|---|---|
|                                 | Android  | iOS                                       | Windows Phone   |
| Secure Docs                     | <a href="#">Secure Docs for Android</a>  | -   | <a href="#">Secure Docs for WP</a>  |
| Secure Viewer                   | <a href="#">Secure Viewer for Android</a>  | -   | -   |
| Secure Email                    | <a href="#">Secure Email for Android</a>   | -   | <a href="#">Secure Email for WP 8.0</a><br><a href="#">Secure Email for WP 8.1+</a> |
| MaaS360 Agents                  | <a href="#">MaaS360 for Android</a><br><a href="#">MaaS360 for Android Samsung</a><br><a href="#">MaaS360 for Android LG</a> | <a href="#">Apple iTunes AppStore app</a> | <a href="#">MaaS360 Company Hub</a>   |
| Secure Editor                   | <a href="#">Secure Editor for Android</a>  | <a href="#">Apple iTunes AppStore app</a> | -   |
| Remote Control                  | <a href="#">Remote Control for Android</a>   | -   | -   |
| Secure Browser                  | <a href="#">Secure Browser for Android</a>   | <a href="#">Apple iTunes AppStore app</a> | <a href="#">Secure Browser for WP</a>   |
| App Signing Utility             | -  | <a href="#">Apple iTunes AppStore app</a> | <a href="#">Windows Phone App Signing</a>   |
| <b>MaaS360 App SDK</b>          |  |   |   |
| <a href="#">MaaS360 App SDK</a> |  |   |   |
| <b>MaaS360 Installers</b>       |  |   |   |
| <a href="#">Cloud Extender</a>  |  |   |   |



---

## Chapter 13. Step 10: Signing MaaS360 for Windows Phone Phone Apps

### About this task

Windows Phone apps cannot be deployed to end user devices until they are code signed. This process requires a Symantec Code Signing Certificate.

IBM MobileFirst Protect provides a code signing utility, located on the Downloads page of the Administration Console.

In addition to signing your MaaS360 for Windows Phone apps, the utility extracts the AET from the Symantec Code Signing Certificate. The AET must be uploaded to your IBM MobileFirst Protect deployment through the Portal if you haven't already done so.

---

### Windows Phone Code Signing Requirements

Before code signing, prepare by gathering the following hardware, software, and account access:

1. Get a computer or VM with Windows 8 and the Windows Phone 8 SDK installed.
2. Note the Enrollment URL for your IBM MobileFirst Protect deployment.
3. Get the Symantec Code Signing Certificate in .pfx format.
4. Get the IBM MobileFirst Protect Windows Phone App Signing utility from the Administration Console.
5. Get the unsigned IBM MobileFirst Protect Windows Phone apps

---

### Windows Phone App Signing Procedure

#### About this task

Complete this procedure for all the Windows Phone apps you want to deploy.

#### Procedure

1. Download and unzip the MaaS360 for Windows Phone Code Signing Utility from the Administration Console.
2. Copy the complete folder structure to the signing machine, in a location of your choice.
3. Copy the Symantec Code Signing Certificate to this machine, in a location of your choice.
4. Copy the unsigned MaaS360 for Windows Phone apps to the config folder within the unzipped folder structure.
5. Open the `companyhub.properties` file in the config folder and update the following details:
  - The absolute path where the Symantec Code Signing Certificate is located.
  - The certificate password.
  - The relative path for the app file (`config\MaaS360_WindowsPhoneApp.xap`).

- The Billing ID of your IBM MobileFirst Protect account.
  - The enrollment URL for your IBM MobileFirst Protect deployment.
6. Navigate to the bin folder and execute run.bat. The following success messages should be displayed:
- Successfully validated all the properties.*
- Successfully generated signed app file.*
- Successfully generated AET file.*
- Your newly signed app and AET will be generated and copied to the output folder.

---

## Chapter 14. Uploading Apps

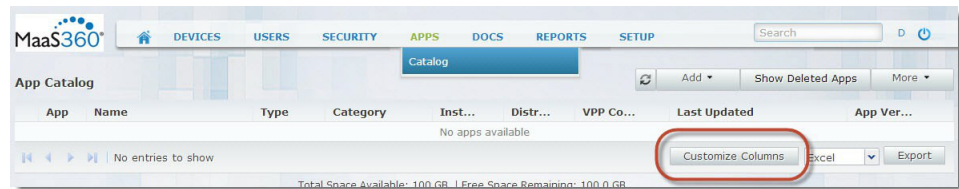
### About this task

After the various IBM MobileFirst Protect Agents and apps have been downloaded and signed (if required), the final step is to upload them into the IBM MobileFirst Protect App Catalog.

After the apps are uploaded, they are available to end user devices during enrollment.

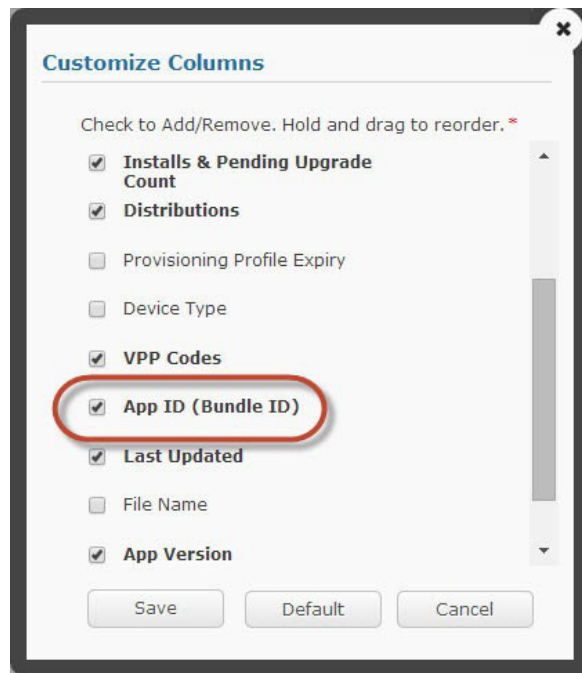
### Procedure

1. Log in to the main portal page, and navigate to **Apps > Catalog**.
2. Click **Customize Columns** in the lower-right corner.

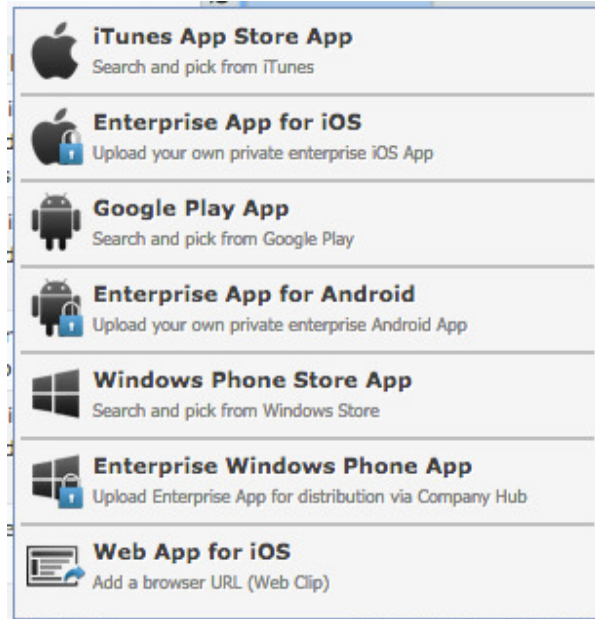


The Customize Columns window is displayed.

3. Check **App ID (Bundle ID)** and click **Save**.



4. Click **Add** in the upper-right corner and select the desired platform.



You might not see option to add Enterprise Windows Phone App if the AET is not uploaded.

5. Configure the settings for iOS apps.

For more information, see the Options for iOS apps.

If you are using Apple's App Store, choose **iTunes App Store App** then **MaaS360 for iOS**, **MaaS360 Browser** and **MaaS360 Editor** into App Catalog.

6. Configure the settings for Windows Phone apps.

For more information, see the Options for Windows Phone apps.

If your devices consist only of Windows Phone 8.1 and Windows 10 Mobile, you upload the latest versions of the apps in "Downloads" section. If your devices consist of Windows Phone 8.0 devices, see Adding Multiple Versions of Windows Apps.

**Enterprise App for Windows Phone**

App Source \*  \* [Browse...](#) [Provide URL](#)

NOTE: This App will need to be signed by the same Symantec Code signing certificate as what has been uploaded to MaaS360 for signing the Company Hub.

Description  
Up to 10000 characters.

Category

Screenshot(s)  [Browse...](#) [Attach More](#)

Remove App on  MDM Control Removal  Selective Wipe  
 Stopping Distribution

Install Settings  Instant Install

Distribute to  
Select 'None' if you wish to wait for security ratings to be available before the app is distributed  ▾

[Cancel](#) [Add](#)

- Configure the settings for Android Enterprise Apps.  
For more information, see the Options for Android apps for more information.

**Enterprise App for Android**

App Source \*  \* [Browse...](#) [Provide URL](#)

Description  
Up to 10000 characters.

Category

Screenshot(s)  [Browse...](#) [Attach More](#)

Review App for Risk Management

Remove App on Supported on Samsung SAFE devices only.  MDM Control Removal  Selective Wipe  
 Stopping Distribution

Install Settings  Instant Install

Security Policies  
Define app policies and behavior. Supported on Android 4.0 to 4.4 only.  Restrict Data Backup to Google Play  Apply Workplace Policies

Distribute to  
Select 'None' if you wish to wait for security ratings to be available before the app is distributed  ▾

[Cancel](#) [Add](#)

## App Upload Setting Options

When you upload apps for distribution, you designate certain settings that determine how the app appears and how it interacts with other features and security policies.

## Options for iOS apps

Remove "signed agent file" from all columns and use "MaaS360 for iOS" iTunes App, "MaaS360 Browser" iTunes App, "MaaS360 Secure Editor" iTunes App

| Apple iOS App Store              | MaaS360 for iOS           | Secure Browser                              | Secure Editor              |
|----------------------------------|---------------------------|---|----------------------------|
| App Source                       | MaaS360 for iOS app       | Secure Browser app                          | Secure Editor app          |
| Description                      | Base iOS management agent | Additional browser for organization gateway | Document viewer and editor |
| Category                         | Business                  | Business                                    | Business                   |
| Screenshot                       | NA                        | NA  | NA                         |
| Remove App On                    |                           |   |                            |
| - MDM Control REMOVAL            | NA                        | NA  | NA                         |
| - SELECTIVE WIPE                 | Yes (Check)               | Yes (Check)                                 | Yes (Check)                |
| - STOPPING DISTRIBUTION          | No                        | No  | No                         |
| Security Policies                |                           |   |                            |
| - Restrict data backup to iTunes | Yes (Check)               | Yes (Check)                                 | Yes (Check)                |
| Distribute to                    | All Devices               | All Devices                                 | All Devices                |

## Options for Android apps

| Enterprise App for Android      | MaaS360 for Android          | MaaS360 for Android Samsung          | MaaS360 for Android LG          | Remote Control for Android Samsung          |
|---------------------------------|------------------------------|--------------------------------------|---------------------------------|---|
| App Source                      | App file-MaaS360 for Android | App file-MaaS360 for Android Samsung | App file-MaaS360 for Android LG | App file-Remote Control for Android Samsung |
| Description                     | MDM agent for Android        | MDM agent for Android Samsung        | MDM agent for Android LG        | Remote Control for Android Samsung          |
| Category                        | MaaS360                      | MaaS360                              | MaaS360                         | MaaS360                                     |
| Review App for Risk Management* | No                           | No                                   | No                              | No  |
| Remove App On                   |                              |                                      |                                 |   |
| - MDM Control Removal           | No                           | No                                   | No                              | No  |
| - Selective Wipe                | No                           | No                                   | No                              | No  |
| - Stopping Distribution         | No                           | No                                   | No                              | No  |
| INSTALL SETTINGS                |                              |                                      |                                 |   |



| Enterprise App for Android            | MaaS360 for Android | MaaS360 for Android Samsung | MaaS360 for Android LG | Remote Control for Android Samsung |
|---------------------------------------|---------------------|-----------------------------|------------------------|------------------------------------|
| - Instant Install                     | No                  | No                          | No                     | No                                 |
| Security Policies                     |                     |                             |                        |                                    |
| - RESTRICT DATA BACKUP to Google Play | Yes                 | Yes                         | Yes                    | Yes                                |
| - Apply workspace policies            | No                  | No                          | No                     | No                                 |
| Distribute to                         | None                | None                        | None                   | None                               |

| Enterprise App for Android            | Secure Email for Android           | Secure Docs For Android           | Secure Browser for Android           | Secure Viewer for Android           | Secure Editor for Android           |
|---------------------------------------|------------------------------------|-----------------------------------|--------------------------------------|-------------------------------------|-------------------------------------|
| App Source                            | App file– Secure Email for Android | App file– Secure Docs for Android | App file– Secure Browser for Android | App file– Secure Viewer for Android | App file– Secure Editor for Android |
| Description                           | Secure email client                | Secure storage access             | Secure browser via gateway           | Document viewer                     | Document editor                     |
| Category                              | MaaS360                            | MaaS360                           | MaaS360                              | MaaS360                             | MaaS360                             |
| Review App for Risk Management*       | No                                 | No                                | No                                   | No                                  | No                                  |
| Remove App On                         |                                    |                                   |                                      |                                     |                                     |
| - MDM Control Removal                 | No                                 | No                                | No                                   | No                                  | No                                  |
| - Selective Wipe                      | No                                 | No                                | No                                   | No                                  | No                                  |
| - Stopping Distribution               | No                                 | No                                | No                                   | No                                  | No                                  |
| INSTALL SETTINGS                      |                                    |                                   |                                      |                                     |                                     |
| - Instant Install                     | No                                 | No                                | No                                   | No                                  | No                                  |
| Security Policies                     |                                    |                                   |                                      |                                     |                                     |
| - RESTRICT DATA BACKUP to Google PLAY | Yes                                | Yes                               | Yes                                  | Yes                                 | Yes                                 |
| - Apply workspace policies            | No                                 | No                                | No                                   | No                                  | No                                  |
| Distribute to                         | None                               | None                              | None                                 | None                                | None                                |



---

## Chapter 15. About the IBM MobileFirst Protect WorkPlace SDK

The IBM MobileFirst Protect WorkPlace SDK allows you to integrate your app with IBM MobileFirst Protect's Enterprise Mobility Management platform for App Security.

The SDK provides containerization controls for apps, so that IT administrators can manage corporate data on any devices, including personally owned Bring Your Own Device (BYOD) devices without fear of data loss. Key features of IBM MobileFirst Protect App Security include single sign-on using container PIN, copy/paste restrictions, whitelisting apps for open-in controls, and per-app VPN.

If you are building a private Enterprise app, and want to integrate with IBM MobileFirst Protect for security policies, this SDK with should be bundled with your enterprise app to allow administrators to layer on additional security controls on your app using the IBM MobileFirst Protect Administration Console.

Download the SDK from Downloads section on Administration Console of your deployment.

| MaaS360 Apps and Agents         |  |   |   |
|---------------------------------|--|---|---|
|                                 | Android  | iOS                                       | Windows Phone   |
| Secure Docs                     | <a href="#">Secure Docs for Android</a>  | -   | <a href="#">Secure Docs for WP</a>  |
| Secure Viewer                   | <a href="#">Secure Viewer for Android</a>  | -   | -   |
| Secure Email                    | <a href="#">Secure Email for Android</a>   | -   | <a href="#">Secure Email for WP 8.0</a><br><a href="#">Secure Email for WP 8.1+</a> |
| MaaS360 Agents                  | <a href="#">MaaS360 for Android</a><br><a href="#">MaaS360 for Android Samsung</a><br><a href="#">MaaS360 for Android LG</a> | <a href="#">Apple iTunes AppStore app</a> | <a href="#">MaaS360 Company Hub</a>   |
| Secure Editor                   | <a href="#">Secure Editor for Android</a>  | <a href="#">Apple iTunes AppStore app</a> | -   |
| Remote Control                  | <a href="#">Remote Control for Android</a>   | -   | -   |
| Secure Browser                  | <a href="#">Secure Browser for Android</a>   | <a href="#">Apple iTunes AppStore app</a> | <a href="#">Secure Browser for WP</a>   |
| App Signing Utility             | -  | <a href="#">Apple iTunes AppStore app</a> | <a href="#">Windows Phone App Signing</a>   |
| <b>MaaS360 App SDK</b>          |  |   |   |
| <a href="#">MaaS360 App SDK</a> |  |   |   |
| <b>MaaS360 Installers</b>       |  |   |   |
| <a href="#">Cloud Extender</a>  |  |   |   |

The SDK package downloaded from Administration console is a .zip file having SDK files for iOS & Android platforms, documentation on usage of the SDK, sample apps created using App SDK.

Get a developer ID and license key from IBM Support to integrate your software with IBM MobileFirst Protect. Make sure to obtain the email address of your organization's primary administrator and obtain the app ID of the app you are developing.

### About App Wrapping

App wrapping is the process of applying a management layer to a mobile app without requiring any changes to the underlying mobile application.

App wrapping allows a mobile application management administrator to set specific policy elements that can be applied to an application or group of applications. Policy elements can include such things, as whether or not user

authentication is required for a specific app, whether or not data associated with the app can be stored on the device and whether or not specific APIs such as copy and paste or file sharing will be allowed.

In the enterprise, app wrapping allows an administrator to take an application, associate extra security and management features with it and re-deploy it as a single containerized program in an enterprise app store.

IBM MobileFirst Protect supports App Wrapping for Android and iOS on the On-Premise offering.

## **Android App Wrapping**

Android App Wrapping is out of the box on IBM MobileFirst Protect On-Premise.

You can upload any enterprise Android app via App Catalog from the portal and choose to include security policies on the app.

## **iOS App Wrapping**

iOS App wrapping is supported on IBM MobileFirst Protect On-Premise offering, but you will need additional assistance from IBM support to start using it on your IBM MobileFirst Protect On-Premise setup.

Please get in touch with you IBM contact person to know more.

---

## Chapter 16. Configuring for the Apple Device Enrollment Program

### About this task

The Apple Device Enrollment Program (DEP) provides a fast, streamlined way to deploy your corporate-owned Mac or iOS devices, whether purchased directly from Apple or through participating Apple Authorized Resellers.

For more information, please visit <http://www.apple.com/business/dep/>

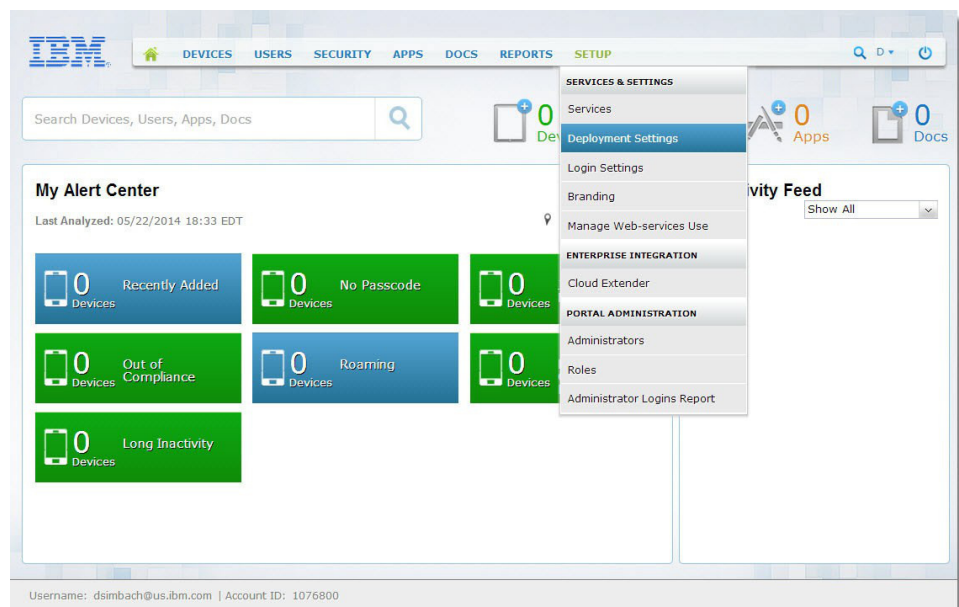
IBM MobileFirst Protect On-Premise offering fully supports DEP.

---

## Configuring the DEP options with the IBM MobileFirst Protect On-Premise Portal

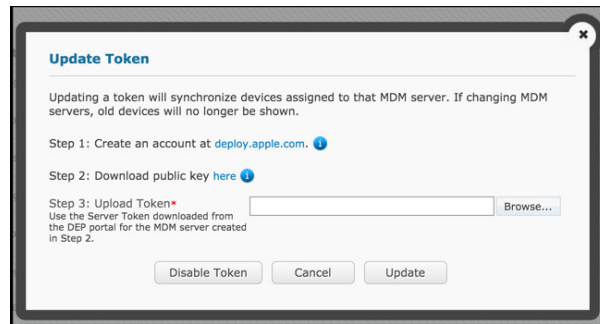
### Procedure

1. Log in to the main portal.
2. From the top navigation bar, go to **Setup > Deployment Settings**.



3. Select **Use Apple's Device Enrollment Program** under **Advanced Management for Corporate iOS Devices**.
4. If desired, enter custom Authentication Screen Header Text. The enrollment screen shows the header text to the user during activation.
5. From the navigation bar, select **Devices > Enrollments**.
6. On the **Enrollments (Add Device Requests)** screen, click **Streamlined Enrollment**.
7. Follow the steps to download and save the IBM MobileFirst Protect public key. Apple uses the public key to generate an MDM token to link the IBM MobileFirst Protect MDM server with Apple.

8. Keep this window open.



The next set of steps gives you a token that you upload via this window.

---

## Downloading an MDM token from the Apple DEP Portal

### Before you begin

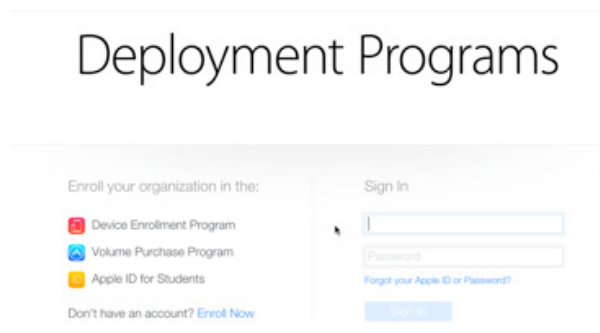
This step requires enrollment in the Apple Deployment Program. If you are not enrolled in Apple Deployment Program, see Apple's DEP home page, and Apple's DEP Guide. Enrolling takes up to 5 days.

### About this task

Perform the following steps in the Apple DEP Portal at <https://deploy.apple.com>.

### Procedure

1. Log in to the Apple DEP Portal.



2. On the next screen, select **Add MDM Server** and enter the MDM server name. The name is an internal identifier and does not have to be specifically for a particular MDM solution vendor. Click **Next**.

Add MDM Server

1. MDM Server Name.

Organization MDM Server

Enter a name to refer to this server, department or location.

Automatically Assign New Devices ⓘ

Cancel Next

3. Upload IBM MobileFirst Protect Public Key downloaded from the IBM MobileFirst Protect Administration Portal previously. Click **Next**.

Add "Demo Server"

2. Upload Your Public Key.

Choose File... No file selected

The public key certificate is used to encrypt the Authentication Token file for secure transfer to your MDM Server.

Previous Cancel Next

4. Download the MDM Server token and select **Done**.

Add "Demo Server"

3. Download and Install your Server Token.

Your Server Token

Contact your MDM vendor for installation instructions.

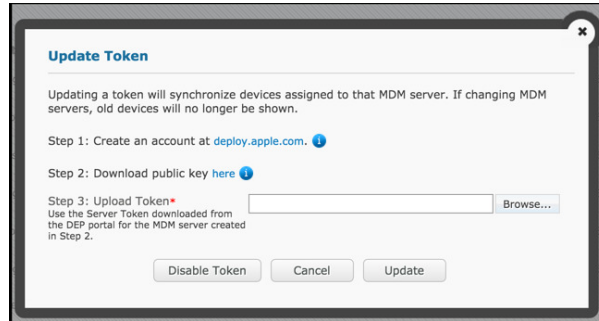
Previous Done

---

## Uploading the token to the IBM MobileFirst Protect On-Premise Portal

### Procedure

1. Upload the Server token to the deployment from the open window of the IBM MobileFirst Protect On-Premise Portal.



As soon as you upload the token, the deployment uses the token to find all the devices available for DEP. The IBM MobileFirst Protect On-Premise Portal displays a list of associated device serial numbers. IBM MobileFirst Protect refreshes serial numbers automatically every 4 hours, or on demand by clicking refresh.

You need to assign a profile to each device, which defines the initial setup experience.

2. To assign a DEP profile to a device manually, click **Assign Profile**.

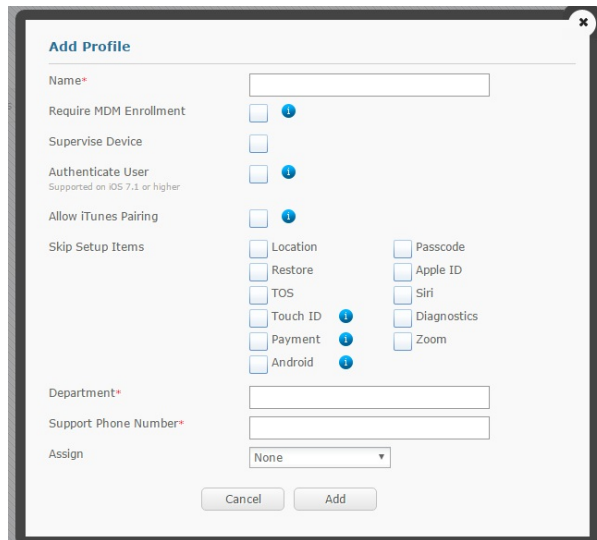
| Serial Number                          | Status     |
|--|------------|
| P84<br><a href="#">Assign Profile</a>  | Assigned   |
| M5<br><a href="#">Assign Profile</a>   | Enrolled   |
| P84<br><a href="#">Assign Profile</a>  | Unassigned |
| FP84<br><a href="#">Assign Profile</a> | Assigned   |
| P84<br><a href="#">Assign Profile</a>  | Enrolled   |
| P84<br><a href="#">Assign Profile</a>  | Assigned   |

Displaying 1 - 6 of 6 Records

3. To create a profile for the streamlined enrollment, click the **Profiles** option, and then **Add Profile**.

This profile becomes the default, and is synchronized to Apple's servers.

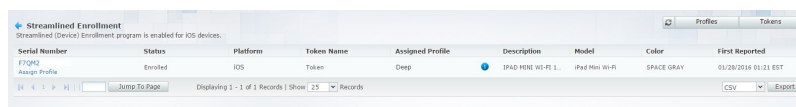




To see information about an option and the operating system it supports, put the mouse pointer over the option's information graphic.

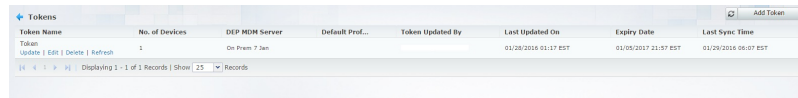
| Option                                       | Description  |
|--|--|
| <b>Profile Name.</b>                         | Display name of the profile.   |
| <b>Set as Default Profile.</b>               | The default profile overrides an existing default. New devices and devices without an assigned profile get this profile.   |
| <b>Require MDM Enrollment.</b>               | This option requires users to enroll their device with IBM MobileFirst Protect during setup.   |
| <b>Supervise Device.</b>                     | This option enables supervised policy options available in IBM MobileFirst Protect. When this option is enabled, you can prevent the device users from removing the MDM profile.   |
| <b>Authenticate User (iOS 7.1 or later).</b> | This option prompts the user to authenticate during setup. After setup, they receive their assigned settings and content, like policies, rules, apps, and docs.<br><b>Note:</b> If you enable AD/LDAP integration through the Cloud Extender, the user name format is <i>domain\username</i> . |
| <b>Allow iTunes Pairing.</b>                 | This option allows the user to sync their device to iTunes.  |
| <b>Skip Setup Items.</b>                     | Skip items such as Location, Apple ID, Siri, Touch ID, Restore, TOS, and Diagnostics.  |
| <b>Set Assignment.</b>                       | A profile can be assigned to <b>None</b> , <b>All Devices</b> , or <b>All unassigned devices</b> .   |

4. Set a Department name and a support phone number, then click **Add**.
5. To change profiles for streamlined enrollments, click **Profiles**.



- To update, edit, delete, or replace tokens, click **Tokens**, then click **Update**, **Edit**, **Delete**, or **Refresh**.

You might have to enlarge the **Token Name** column to see all the options.



| Token Name                                | No. of Devices | DEP MDM Server | Default Prof... | Tokens Updated By | Last Updated On      | Expiry Date          | Last Sync Time       |
|---|----------------|----------------|-----------------|-------------------|----------------------|----------------------|----------------------|
| Token<br>Update   Edit   Delete   Refresh | 1              | On Prem 7 Jan  |                 |                   | 01/28/2016 01:17 EST | 01/05/2017 21:57 EST | 01/29/2016 06:07 EST |

- To add more tokens, click **Tokens**, then **Add Token**.

---

## Chapter 17. Configuring IBM MobileFirst Protect for the Android for Work Program

You use IBM MobileFirst Protect and Android for Work to allow separate personal and work data from each other. Android for Work offers support for all Android apps across the ecosystem and support of security controls built into the Android OS.

---

### Making sure that your IBM MobileFirst Protect and Google Accounts are ready

#### Before you begin

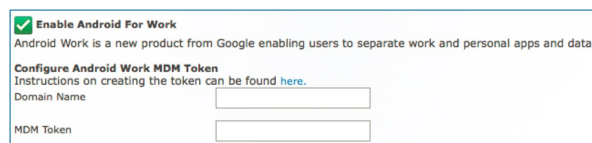
Before you can use Android for Work, you must have accounts set up in both IBM MobileFirst Protect and Google for Work.

Your company must have a Google for Work account to use Android for Work. This account manages the apps available in the Work Play app, and to distribute apps to your users silently.

If you do not have an account, go to [https://www.google.com/a/signup/u/0/?enterprise\\_product=ANDROID\\_WORK](https://www.google.com/a/signup/u/0/?enterprise_product=ANDROID_WORK) and create one.

#### Procedure

1. Access the IBM MobileFirst Protect Administration Portal.
2. Mouse over **Setup** at the top of the screen to display the menu, and then click **Services**.
3. Find **Mobile Device Management**, and then click the **More** link.
4. Select **Enable Android For Work**. If it is not selected, contact IBM Customer Support.



**Enable Android For Work**  
Android Work is a new product from Google enabling users to separate work and personal apps and data.

**Configure Android Work MDM Token**  
Instructions on creating the token can be found [here](#).

Domain Name

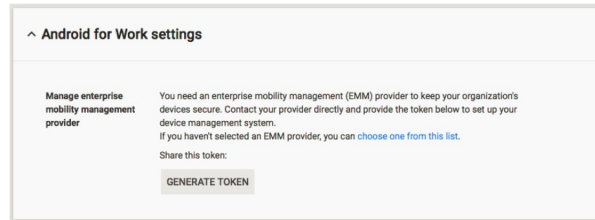
MDM Token

---

### Configuring Android for Work in your Google for Work account

#### Procedure

1. Log in to the Google administration console.
2. Click **Security**, then click **Show more**.
3. Find **Android for Work settings** and click it.



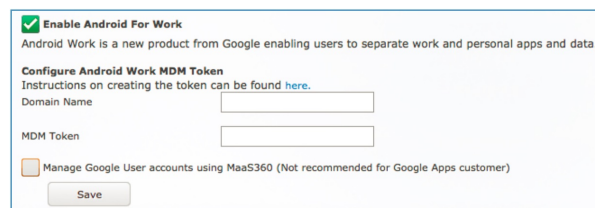
You can create a new token or use the currently available one.

4. Generate a new token, or save the existing one.

You need to enter this token to the IBM MobileFirst Protect Administration Portal.

**Note:** If the token is bound to another MDM vendor, you must unbind it in that vendor's console before you create a new one.

5. In the IBM MobileFirst Protect Administration Portal, select **Setup > Services**. Find **Mobile Device Management** and click **more...**
6. Enter the domain name for your Google account, and then paste the MDM Token that you copied previously.



Do not use IBM MobileFirst Protect to manage the Google user accounts (clear the check box).

**Note:** If you are an existing Google Apps customer, the user accounts are probably managed elsewhere already (for example, the Google Directory Sync tool).

7. Click **Save**.

## What to do next

Contact IBM Customer Support with your organization's email domain, MDM token, Service Account email ID (configured in the IBM MobileFirst Protect Configuration UI) to complete your integration for Android for Work.

---

## Creating Google accounts for your users

### Before you begin

Each user who activates a device with Android for Work needs a Google Account created inside your company account. Create the Google Accounts before continuing.

### Procedure

1. Return to the Home screen by clicking the back arrow, and then click the **Users** icon.



2. Click the Add ( + ) icon to start adding users.

You can assign them temporary passwords, which they can change during first enrollment on their devices.

**Important:** Users must enroll with IBM MobileFirst Protect with these user names and domains, so they need to be saved for device enrollment. The user account that you create in the Google console must match the information that the user enters when they enroll into IBM MobileFirst Protect.

---

## Enrolling users with IBM MobileFirst Protect and Android for Work

### About this task

You set up the Android for Work profile on the device, encrypt the device, and then load the user's corporate Google account.

**Important:** Activating Android for Work and the prior Device Admin approach are mutually exclusive. During enrollment, users enroll with one or the other.

### Procedure

1. To enable or disable Android for Work, select the new check box that appears in the manual **Add Device** workflow when it sends out enrollment requests.

2. Check **Use Android Work** to trigger Android for Work enrollment on capable devices.
3. To control how self-enrolled devices (when users browse to the enrollment URL and authenticate with their credentials) are activated, select **Setup > Deployment Settings**, and then select **Use of Android Work container**.

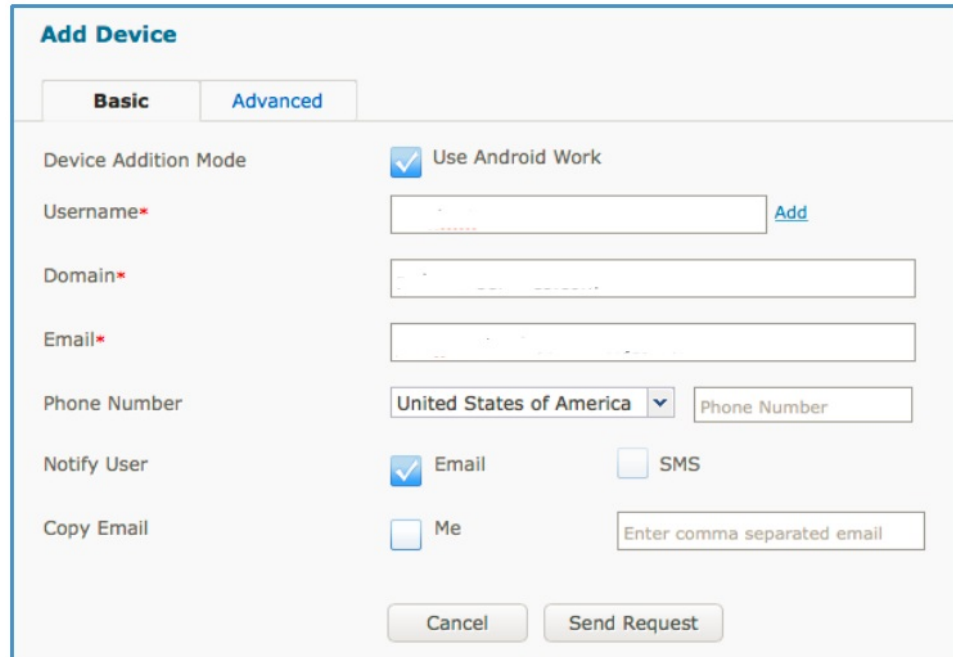
**Important:** Before you enable Android for Work company-wide, contact IBM MobileFirst Protect Customer Support.

## Enrolling your first Android for Work device

Make sure that you have a device that supports Android for Work Native, which is a limited subset of Android L devices. Contact IBM Customer Support for the complete list.

### Procedure

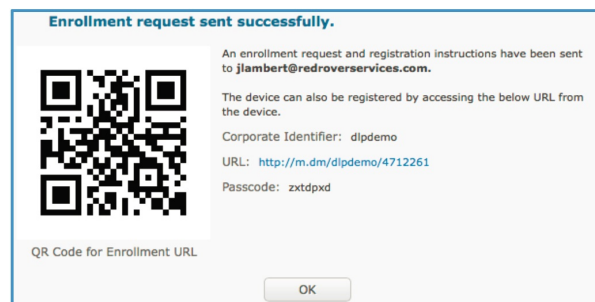
1. Create a new enrollment request by selecting **Devices > Enrollments**, and then clicking **Add Device**.
2. To enable Device Addition Mode, check **Use Android Work**.



The credentials should match both the corporate credentials and the Google account.

3. If you need to assign a specific policy to the device rather than using the default, click the **Advanced** tab.

You see a dialog with the passcode and corporate identifier the user needs to enroll. Since the user probably doesn't have access to the Google accounts mail, copy this information and deliver it with another method.



4. On the user device, download a profile.
  - a. Open Chrome and browse to the specified URL.
  - b. Download the MaaS360 for Android app from Google Play.
  - c. Install the app and open it.

- d. Enter the corporate ID and email address from the enrollment request. Tap **Continue**.
  - e. Enter the user credentials and accept the Terms and Conditions.  
The user is prompted to set up a profile.
  - f. If the device is not encrypted, the user must encrypt it now. When the encryption process is finished, the Android for Work profile is created, and a Google account must be set.
5. Click **OK** to continue and then enter the Google account and password that was set up earlier.
  6. When it asks for payment information, the click **Remind me later**, and then tap **Next**.

The user's device is now enrolled, and it has an Android for Work profile.

Icons with the orange briefcase are part of the Work profile, and are separated from the personally installed apps on the device by the Android Operating System. The restrictions that are configured in IBM MobileFirst Protect policies are applied to these apps.

---

## Managing Apps for Android for Work

### Authorizing Apps

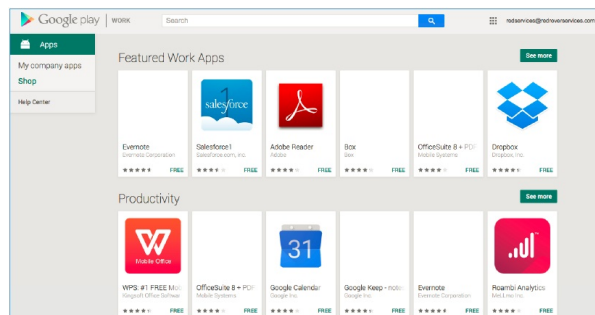
#### About this task

Android for Work offers IT administrators and enterprises the ability to distribute apps into the Android for Work profile silently and over the air, including apps downloaded directly from Google Play.

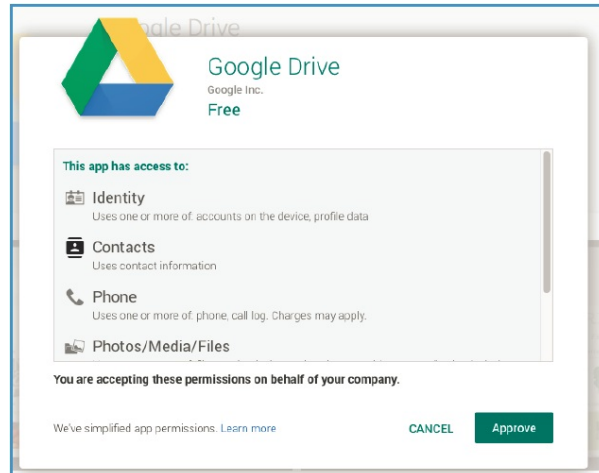
For an app to be authorized to be installed in the Work profile, you agree to its permissions in the Google Play Store first.

#### Procedure

1. In a browser, navigate to <https://play.google.com/work>.
2. Authenticate with the same Google administrator account you used earlier to create the users.
3. Browse the store and authorize apps to be deployed to your users in the Android for Work profile.



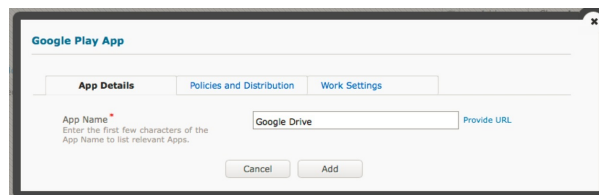
4. Set an app's permissions by selecting an app and clicking **Approve**.
5. Review the permissions and click **Approve**.



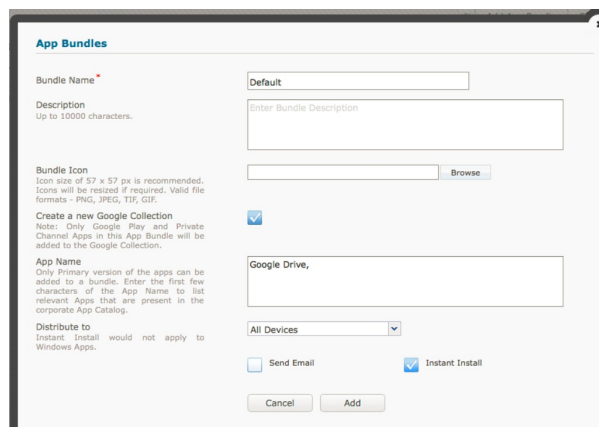
The app is now authorized and able to be deployed using IBM MobileFirst Protect.

## Deploying Apps Procedure

1. To deploy an app to your users, access the IBM MobileFirst Protect Administration Portal. Select **Apps > Catalog**.
2. Click **Add**, and then click **Google Play App**.
3. In the *App Name* field, enter the name of the app you approved in Google Play. Click **Add**.



4. Create a collection of apps for your users. Select **Apps > Bundles** and then click **Add App Bundle**.
5. Give the bundle a name. Click **Create a new Google Collection** to allow this app to be displayed in the Google Play Store.



6. In the *App Name* field, type the name of the app you added earlier and it automatically completes.



7. If you would like to the app bundle to be deployed silently, select **Instant Install**. If you want to deploy the bundle to a particular group, use **Distribute**.
8. Click **Add**.

It can take up to an hour for the changes you made to propagate through the Google Play store.

For apps distributed with Instant Install, users need to open the Google Play Store to start the installations.

## Managing Policies

### About this task

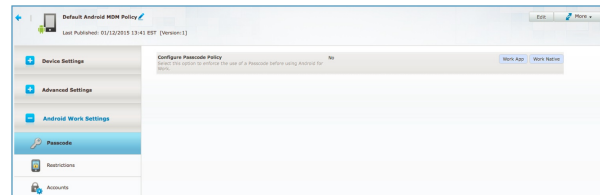
Android for Work and IBM MobileFirst Protect offer a variety of controls to manage how users interact with the Android for Work profile, and what options they have available to them. These settings appear in the standard IBM MobileFirst Protect Android policy.

**Important:** Create a separate policy to use when you test Android for Work.

### Procedure

To view the policy options, select **Security > Policies**.

Android for Work settings are found in the Android Work tab at the left side of the screen.



Procedures for managing and controlling Android for Work policies are the same as for standard Android policies.



---

## Chapter 18. About Security Information and Event Management (SIEM) Support With QRadar

IBM QRadar Security Intelligence Platform can be used to collect event logs from IBM MobileFirst Protect On-Premise.

You have to license and install IBM QRadar before you can enable the integration with IBM MobileFirst Protect.

Refer the following document to configure QRadar for IBM MobileFirst Protect:

[http://public.dhe.ibm.com/software/security/products/qradar/documents/iTeam\\_addendum/IBM\\_Fibrelink\\_MAAS.pdf](http://public.dhe.ibm.com/software/security/products/qradar/documents/iTeam_addendum/IBM_Fibrelink_MAAS.pdf)

**Note:** The Login URL should be the Services URL of IBM MobileFirst Protect On-Premise instance as configured in Administration Console.



---

## Chapter 19. Managing Certificates

---

### Managing SCEP Certificates

The SCEP (Simple Certificate Enrollment Protocol) certificates built in to IBM MobileFirst Protect On-Premise need to be updated and replaced every two years.

#### About this task

The IBM MobileFirst Protect On-Premise version 2.4.0.3 and later bundle the scripts to help you renew the internal SCEP certificate.

For uninterrupted security, renew the certificate within 60 days of expiry.

The scripts need to be executed manually during a downtime window of 30 minutes.

### Checking SCEP Certificate Expiry

#### About this task

You can find out how many days you have left before expiry without interrupting service.

#### Procedure

1. Log in to the Configuration VM from VSphere Client Console as the root user.
2. Switch to the automation\_prod user. `$ su - automation_prod`
3. Navigate to /home/automation\_prod/fabric/onprem `$ cd /home/automation_prod/fabric/onprem`
4. Run the expiry script. `$ fab check_ejbca_cert_expiry`

The output is the number of days left until the certificates expire and the expiry date.

### Renewing the SCEP Certificate

#### Before you begin

The administrator needs to back up all the Virtual Machines and databases before attempting this task.

#### About this task

Before the certificates expire, you need to renew the SCEP certificate in the Services 1-0 VM.

**Important:** This task results in service downtime.

#### Procedure

1. Log in to the Services VM 1-0 from VSphere Client Console as the root user.
2. Switch to the tomcat user. `$ su - tomcat`
3. Navigate to /u001/ `$ cd /u001/`
4. Unzip the renewal scripts `$ unzip renew-superadmin.zip`

5. Give execution and write privileges to the tomcat user for all the unzipped files and directories. `$ chmod u=rwx -R /u001/renew-superadmin`  
The output is the number of days left until the certificates expire and the expiry date.
6. Make sure the JBOSS process is running. `$ ps -aux | grep jboss`
7. Create a backup directory. `$ mkdir /u001/backup-superadmin`
8. Navigate to `/u001/renew-superadmin/` and run the scripts.  
`$ cd /u001/renew-superadmin`  
`$ ./renew/renew_certificate.sh -j /u001/jboss-5.1.0.GA/ -s /u001/ejbca/ -b /u001/backup-superadmin`
9. When it's finished, save the output.

**Note:** The full backup directory path of the output is for rollback, if required.

10. Stop the JBOSS process. `$ /etc/init.d/jboss-5.1.0.GA stop`
11. Monitor JBOSS server log to ensure a clean shutdown. `$ tailf /u001/jboss-5.1.0.GA/server/default/log/server.log`
12. Restart the JBOSS process. `$ /etc/init.d/jboss-5.1.0.GA start` This usually takes 2 to 3 minutes.
13. Monitor JBOSS server log to ensure it starts up. `$ tailf /u001/jboss-5.1.0.GA/server/default/log/server.log`
14. Validate SCEP using the provided script.  
`$ cd /u001/renew-superadmin`  
`$ ./generic-validation/validate.sh`

## Renewing the SCEP Certificate in HA (High Availability) Environments

### Before you begin

Complete the steps to renew the certificate as explained in “Renewing the SCEP Certificate” on page 55.

### About this task

**Important:** This task is for HA instances only. Non-HA instances do not use this task.

### Procedure

1. Copy the `/u001/ejbca/p12/superadmin.p12` certificate that was generated from the renewal script from the master node to the remote slave node server.  
`$ scp /u001/ejbca/p12/superadmin.p12 tomcat@op1svcap1-1:/tmp/`
2. Copy and unzip the renewal scripts in the Services VM path `/u001/` as the tomcat user. `$ unzip renew-superadmin.zip`
3. Confirm execution privileges of the renewal scripts. Make sure that `/tmp/superadmin.p12` has appropriate privileges for it to be accessed by the tomcat user.
4. Make sure the JBOSS process is running. `$ ps -aux | grep jboss`
5. Create a backup directory. `$ mkdir /u001/backup-superadmin`
6. Navigate to `/u001/renew-superadmin/` and run the scripts.  
`$ cd /u001/renew-superadmin`  
`$ ./renew/renew_certificate_slave.sh -j /u001/jboss-5.1.0.GA/ -s /tmp/superadmin.p12 -b /u001/backup-superadmin`
7. Stop the JBOSS process. `$ /etc/init.d/jboss-5.1.0.GA stop`

8. Monitor JBOSS server log to ensure a clean shutdown. `$ tailf /u001/jboss-5.1.0.GA/server/default/log/server.log`
9. Restart the JBOSS process. `$ /etc/init.d/jboss-5.1.0.GA start` This usually takes 2 to 3 minutes.
10. Validate SCEP using the provided script.
 

```
$ cd /u001/renew-superadmin
$ ./generic-validation/validate.sh
```

## Roll Back SCEP Certificate Renewal

### Before you begin

You need to have the backup directory that was created during the renewal process. This can be found in the output of the renewal scripts, and this task refers to the backup directory as *BACKUP\_FILEPATH*.

### About this task

If validation fails and devices can't successfully enroll, you should roll back the certificate changes in Services1-0 (and Services1-1, if applicable).

### Procedure

1. Log in to the Services VM 1-0 from VSphere Client Console as the root user.
2. Switch to the tomcat user. `$ su - tomcat`
3. Stop the JBOSS process. `$ /etc/init.d/jboss-5.1.0.GA stop`
4. Monitor JBOSS server log to ensure a clean shutdown. `$ tailf /u001/jboss-5.1.0.GA/server/default/log/server.log`
5. Navigate to `/u001/renew-superadmin/` and run the rollback script.
 

```
$ cd /u001/renew-superadmin
$ ./rollback/rollback_certificate.sh -j /u001/jboss-5.1.0.GA/ -s /u001/ejbca -b /BACKUP_FILEPATH
```
6. Restart the JBOSS process. `$ /etc/init.d/jboss-5.1.0.GA start` This usually takes 2 to 3 minutes.
7. Monitor JBOSS server log to ensure it starts up. `$ tailf /u001/jboss-5.1.0.GA/server/default/log/server.log`
8. Validate SCEP using the provided script.
 

```
$ cd /u001/renew-superadmin
$ ./generic-validation/validate.sh
```

---

## About Self-Signed Certificates Support

IBM MobileFirst Protect On-Premise allows usage of self-signed certificates or certificates issued from an internal Certificate Authority (not public CA), for the domain SSL certificates needed to configure the instance.

If you use Mobile Enterprise Gateway with your IBM MaS360 On-Premise deployment, then you have to use trusted domain SSL certificates for the instance configuration. Self-signed certificates are not supported.

**Important:** The Root Certificate of the domain SSL certificates have to be added to the devices that will enroll into IBM MobileFirst Protect. Make sure this is completed before enrolling the devices.

You can find more information about the SSL certificates in **Certificate Requirements** section of IBM MobileFirst Protect On-Premise Installation Guide.

The SSL certificates should have the following mandatory attributes and values.

**Note:** Wherever values are left blank it implies they have to be set to an appropriate value by customers or have to be set by the certificate generation tool.

| ATTRIBUTE                | VALUE  | REMARKS  |
|--------------------------|--|--|
| Version                  | V3   | X509 certificate version   |
| Serial Number            | △  | Unique Serial Number of the certificate.   |
| Signature Algorithm      | sha512RSA  | Encryption algorithm, sha512 or higher.  |
| Signature Hash Algorithm | sha512   | Hashing algorithm, sha512 or higher  |
| Issuer                   |  | Certificate issuer details.  |
| Valid From               |  | Date depicting since when the certificate is valid.  |
| Valid To                 |  | Date depicting till when the certificate is valid.   |
| Subject                  |  | Certificate's subject.   |
| Public Key               |  | RSA (1024 or higher)<br>Recommended : 2048   |
| Authority Key Identifier |  | Unique key identifier.   |
| Subject key Identifier   |  | Unique Subject Key Identifier.   |
| Enhanced Key Usage       | Server Authentication<br>(1.3.6.1.5.5.7.3.1)<br><br>Client Authentication<br>(1.3.6.1.5.5.7.3.2) | Should exactly match what's given in Value column for device enrollment to work.<br><br>In Unix based machine you will see "Extended Key Usage" the values should be :<br><br>TLS Web Server Authentication, TLS Web Client Authentication |
| Key Usage                | Digital Signature, Key Encipherment (e0)   | In Unix based machine the value for "Key Usage" should be :<br><br>Digital Signature,<br><br>Key Encipherment<br><br>Non-Repudiation is an optional value that can exist besides the mandatory values given.                               |
| Basic Constraints        | Subject Type=End Entity<br><br>Path Length<br>Constraint=None                                    | In Unix based machine the value for "Basic Constraints" should be:<br><br>critical CA:FALSE  |



The IBM MobileFirst Protect virtual appliance has a seeded self-signed certificate that can be used for **test instances only**.

This certificate should not be used in **production** instances.

To download this certificate from the Configuration VM:

1. Login to op1infra1-0.op1.sysint.local as **maas** user
2. Elevate to **root** user using: su -
3. Navigate to the following folder: cd /u001/apache/conf/keys/default
4. Download the files: default.crt, default.key, default\_chain.crt



---

## Chapter 20. Next Steps

You have finished the configuration required for IBM MobileFirst Protect. You can start enrolling devices into your account.

For information related to the administration and use of the main portal, see: *IBM MobileFirst Protect On-Premise Portal Administration Guide*.

If you want to integrate your Active Directory, Lotus Traveller, SCEP Server, BES Server, or Exchange ActiveSync deployments with your IBM MobileFirst Protect deployment, install the optional IBM MobileFirst Protect Cloud Extender®.

For more information, see: *IBM MobileFirst Protect Cloud Extender Installation Guide*.

If you want to provide secure access to behind-the-firewall resources such as SharePoint, Windows File Share content, and Intranet sites on Mobile devices without a VPN connection, install the optional IBM MobileFirst Protect Mobile Enterprise Gateway.

For more information, see the *IBM MobileFirst Protect Mobile Enterprise Gateway 2.0 Quick Start Guide*.



---

## Notices

This information was developed for products and services that are offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
United States of America*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. 2016. All rights reserved.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® and device, MaaS360 PRO™, MCM360™, MDM360™, MI360™, Mobile Context Management™, Mobile NAC®, Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360®, and We do IT in the Cloud.™ and device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM Company.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.



Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

---

## Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

## **Applicability**

These terms and conditions are in addition to any terms of use for the IBM website.

## **Personal use**

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

## **Commercial use**

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

## **Rights**

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.







Product Number: 5725-R11

Printed in USA