

IBM MobileFirst Protect (MaaS360) On Premises



Configuration Guide

Version 3 Release 2.0

IBM MobileFirst Protect (MaaS360) On Premises



Configuration Guide

Version 3 Release 2.0

Note

Before using this information and the product it supports, read the information in "Notices" on page 59.

This edition applies to version 2, release 3, modification level 0 of IBM MobileFirst Protect Devices (program number 5725-R11) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2014, 2015.**

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

Contents

Chapter 1. IBM MobileFirst Protect (MaaS360) Configuration Guide Overview	1
Chapter 2. About IBM MaaS360 Accounts	3
Chapter 3. Step 1: Create an account	5
Chapter 4. Step 2: Customize Your Deployment	9
Chapter 5. Step 3: Configure the Portal Branding	11
Chapter 6. Step 4: Configure iOS MDM Branding	13
Chapter 7. Step 5: Configure Email Settings	15
Chapter 8. Step 6: Enable Web Services	17
Chapter 9. Step 7: Prepare to Manage Apple iOS Devices.	19
Chapter 10. Step 8: Prepare to Manage Windows Phone Devices	25
Upload the AET	26
Chapter 11. About Enterprise Mobile Device Management Agent Apps	29
Chapter 12. Step 9: Download IBM MaaS360 Apps	31
Chapter 13. Step 10: Code Sign iOS MaaS360 Apps	33
Chapter 14. Step 11: Sign IBM MaaS360 Windows Phone Apps	35
Chapter 15. Upload Apps	37
App Upload Setting Options	40
Chapter 16. About the IBM MaaS360 WorkPlace SDK	45
Chapter 17. Use the Apple Device Enrollment Program	47
Chapter 18. About Security Information and Event Management (SIEM) Support With QRadar	53
Chapter 19. About Self-Signed Certificates Support	55
Chapter 20. Next Steps.	57
Notices	59
Programming interface information	61
Trademarks	61
Terms and conditions for product documentation.	62
IBM Online Privacy Statement	63
Safety and environmental notices	63

Chapter 1. IBM MobileFirst Protect (MaaS360) Configuration Guide Overview

The goal of this document is to provide an overview of the steps required to customize your IBM MobileFirst Protect (MaaS360) deployment before you start directing end users to enroll their devices.

Before proceeding, your IBM MobileFirst Protect (MaaS360) instance must be deployed and configured as described in the *IBM MobileFirst Protect (MaaS360) Installation Guide*.

In this guide, the IBM MobileFirst Protect (MaaS360) product will be referred to as *IBM MaaS360*.

Chapter 2. About IBM MaaS360 Accounts

IBM MaaS360 provides four 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™ (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: Create an account

About this task

You can use the account creation portal after your IBM MaaS360 deployment is configured.

Procedure

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

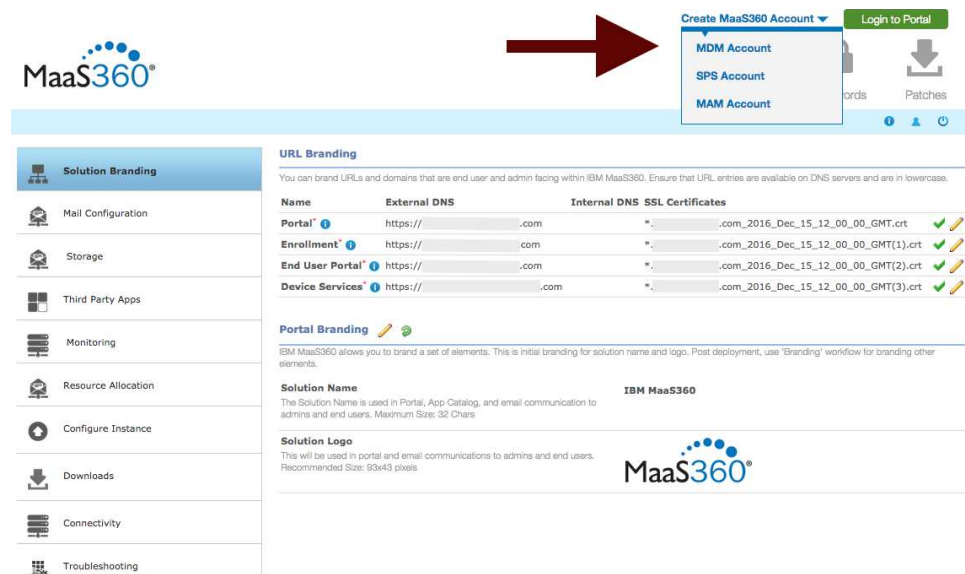
You could also directly open the account creation pages for the account type:

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.



The screenshot displays the IBM MaaS360 account creation portal. On the left is a navigation menu with options like 'Solution Branding', 'Mail Configuration', 'Storage', 'Third Party Apps', 'Monitoring', 'Resource Allocation', 'Configure Instance', 'Downloads', 'Connectivity', and 'Troubleshooting'. The main content area is titled 'URL Branding' and contains a table with columns for 'Name', 'External DNS', 'Internal DNS', and 'SSL Certificates'. Below this is the 'Portal Branding' section, which includes fields for 'Solution Name' and 'Solution Logo'. A dropdown menu is open, showing options for 'MDM Account', 'SPS Account', and 'MAM Account'. A red arrow points to the 'Create MaaS360 Account' dropdown.

Name	External DNS	Internal DNS	SSL Certificates
Portal	https://.com	*	.com_2016_Dec_15_12_00_00_GMT.crt
Enrollment	https://.com	*	.com_2016_Dec_15_12_00_00_GMT(1).crt
End User Portal	https://.com	*	.com_2016_Dec_15_12_00_00_GMT(2).crt
Device Services	https://.com	*	.com_2016_Dec_15_12_00_00_GMT(3).crt

4. Enter the required fields to create your account.

Create a MaaS360 Account

MaaS360 mobile device management offers you On-Premises solution and lets you *simplify the process to install and start managing devices.*

You can create multiple accounts on your instance. We suggest you have separate accounts for staging and testing purposes and a separate account for production environment.

Your Login Details

Email:

Password:

Confirm Password:

Minimum 8 characters. Include both letters and numbers.

Company Name:

Full Name:

Phone Number:

Create Account

Email: Specify the email address used for creating an IBM MaaS360 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.

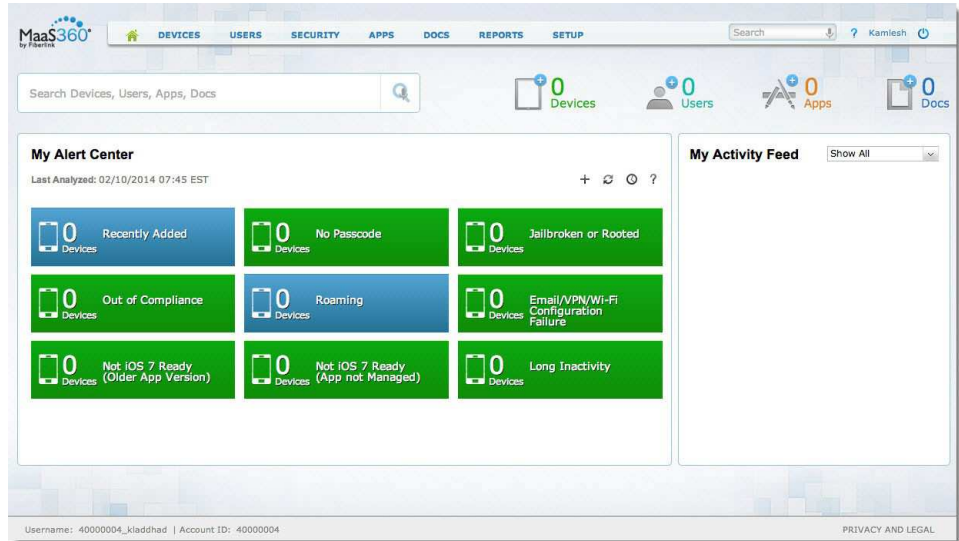
5. Click Create Account.

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.

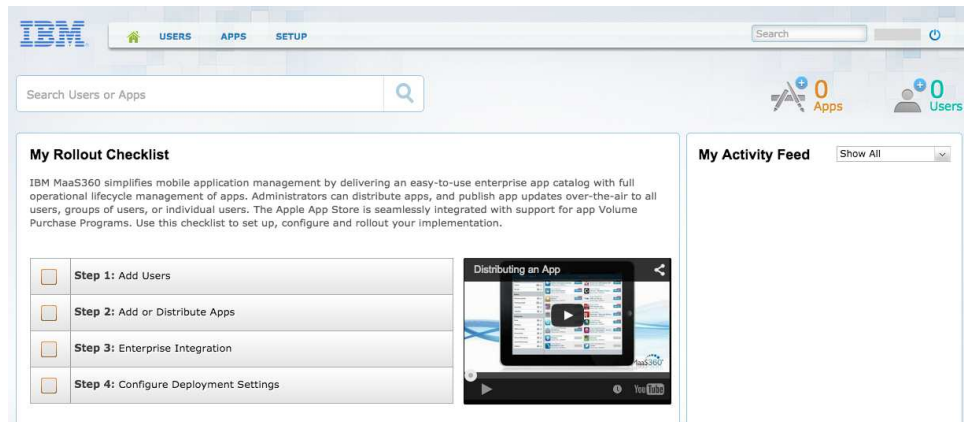
When the Portal is first displayed, some preliminary tips might be displayed.

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: Customize Your Deployment

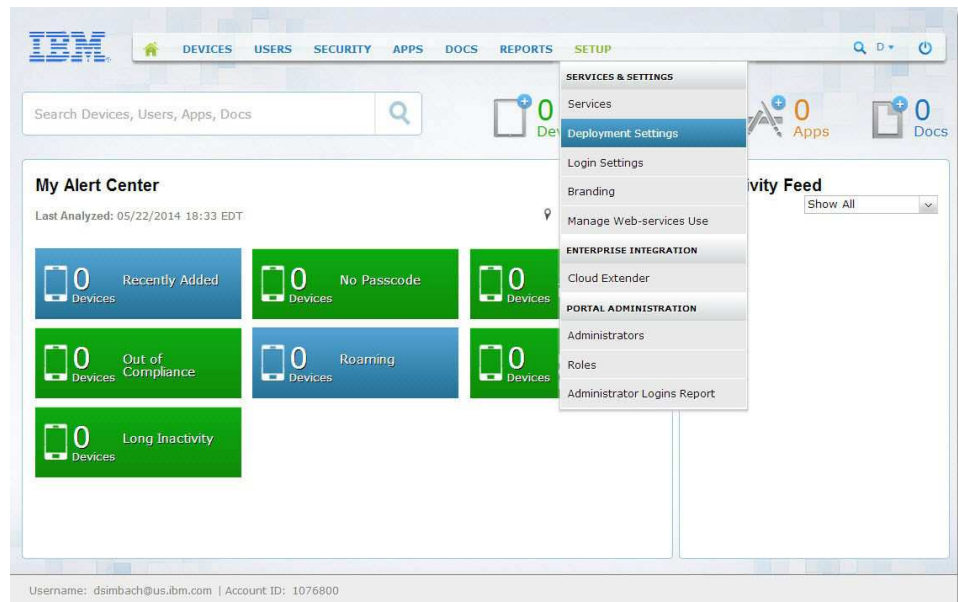
About this task

With an account created, the first step is to make some basic changes to customize your IBM MaaS360 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 Protect console. At the top, there is a navigation bar with tabs for DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. The 'Corporate Identifier' field is highlighted with a red circle and contains the value '1076800'. Below this, there are several sections with checkboxes and radio buttons for configuration options. The 'Corporate Information' section is also highlighted with a red circle 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: Configure the Portal Branding

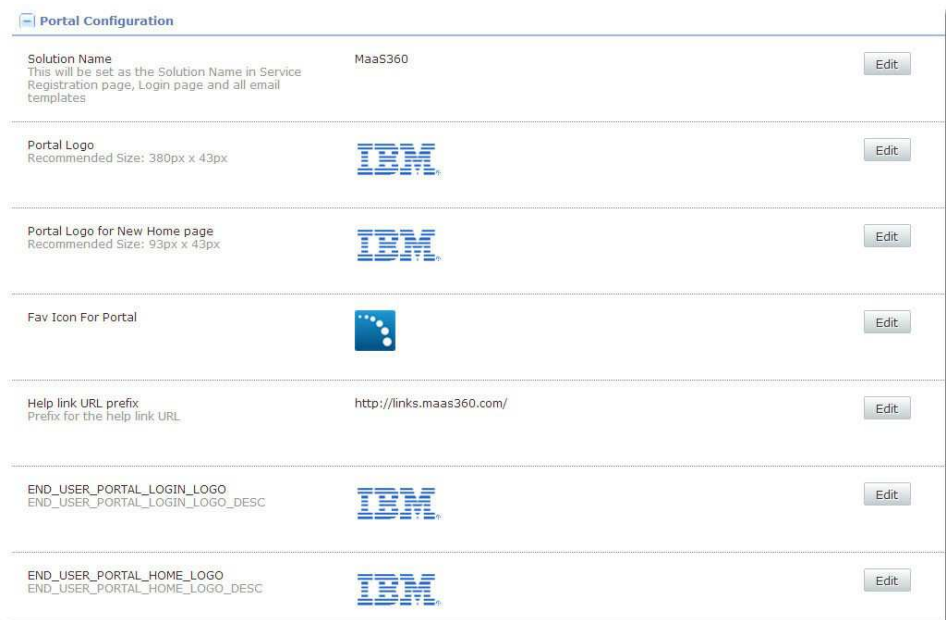
About this task

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 (MaaS360) 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
Solution Name This will be set as the Solution Name in Service Registration page, Login page and all email templates	MaaS360	Edit
Portal Logo Recommended Size: 380px x 43px		Edit
Portal Logo for New Home page Recommended Size: 93px x 43px		Edit
Fav Icon For Portal		Edit
Help link URL prefix Prefix for the help link URL	http://links.maas360.com/	Edit
END_USER_PORTAL_LOGIN_LOGO END_USER_PORTAL_LOGIN_LOGO_DESC		Edit
END_USER_PORTAL_HOME_LOGO 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 MaaS360 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: Configure 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**.

The screenshot displays the 'iOS MDM Configuration' page with the following settings:

Setting Name	Current Value	Action
App Catalog Icon Icon to be displayed on the device		Edit
App Catalog Text Icon text to be displayed on the device	App Catalog	Edit
Splash Image for iPad 2 and below (Portrait Mode) Expected Image Size: 768 x 1004 px		Edit
Splash Image for iPad 2 and below (Landscape Mode) Expected Image Size: 1024 x 748 px		Edit
Splash Image for iPad 3+ (Landscape Mode) Expected Image Size: 2048 x 1496 px		Edit
Splash Image for iPad 3+ (Portrait Mode) Expected Image Size: 1536 x 2008 px		Edit
Splash Image for iPhones 4 and Below Expected Image Size: 320 x 460 px		Edit
Splash Image for iPhones 4G Expected Image Size: 640 x 920 px		Edit

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: Configure 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 (MaaS360) 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) Email Address specified in all emails sent	maas360@fiberlink.com	Edit
Email Sender Display Name Name of the Email sender displayed in all emails sent	MaaS360	Edit
Email Logo Image that will be used in all emails. Recommended Size: 200 x 115 px		Edit
Email Background		Edit
Support Email Support email address specified in emails sent	dsimbach@us.ibm.com	Edit
Support Contact Number Support contact number specified in emails sent	415 555 5555	Edit
Additional Support Information 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
Email Sender	Enter the email address that emails will originate from. This email must be setup on your SMTP server.
Email Sender Display Name	The string entered here determines the name displayed as the email sender. This entry might be overridden by name associated in your SMTP server.
Email Logo	Upload the image used in email communication. The recommended file size is 200x115 pixels.
Email Background	Upload an image to be used in the email header background.
Support Email	The email address entered here is presented as the contact information for support issues.

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

Chapter 8. Step 6: Enable Web Services

About this task

IBM MaaS360 provides a REST style web-service Application Programming Interface (API) for integrating IBM MaaS360 workflows with other applications.

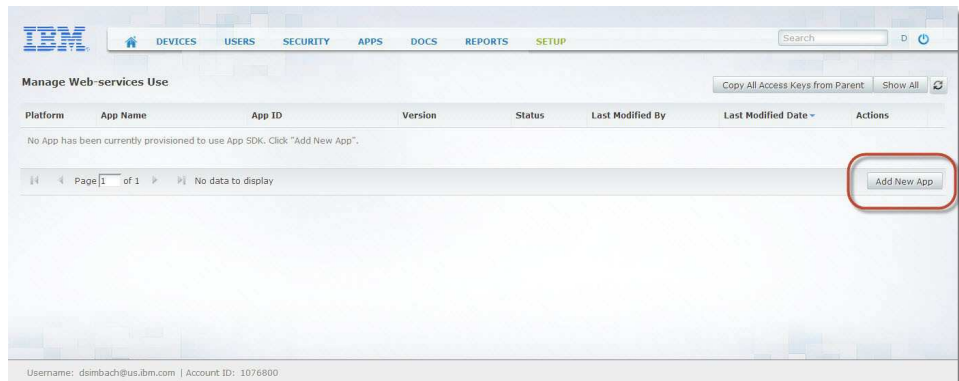
Enabling this API is a requirement for integration with or migration from IBM Endpoint Manager for Mobile Device Management. This is also a requirement for Worklight integration.

To use IBM MaaS360 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
App Name	Name of the application that you are planning to integrate using IBM MaaS360 APIs.
Platform	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.
App ID	Enter an identity for the application you are planning to integrate. For example, com.maas360.mycompany.myapplication.
Version	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

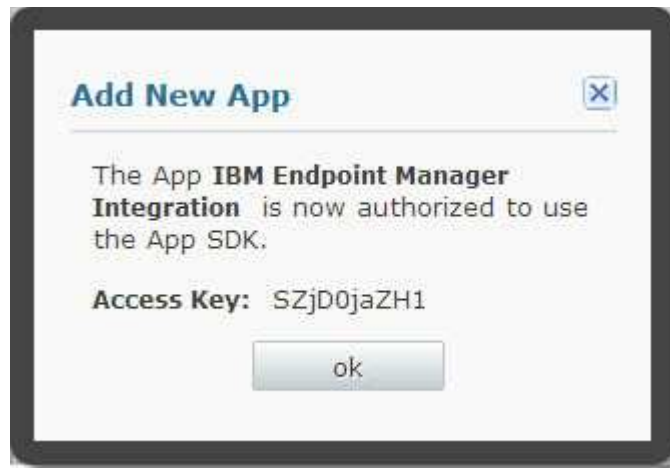
Platform* iOS [v]

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: Prepare to Manage Apple iOS Devices

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

You need three certificates to manage Apple iOS devices. The first and second certificates require you to enroll in the Apple iOS Developer Enterprise Program (<https://developer.apple.com/programs/ios/>). This program has a yearly fee.

Using an iOS Developer Enterprise Program account you can generate an App ID (also known as a Bundle ID), Push Notification Client SSL Certificate, and an iOS App Signing Certificate.

Apple Push Notifications Client SSL certificate

The Apple Push Notifications Client SSL certificate is generated for an application or agent. The Apple Push Notification Client SSL Certificate is required in order to send live notifications to the app from the server.

You need to enroll in the Apple iOS Developer Enterprise Program to obtain this certificate.

iOS Signing Certificate

The iOS Signing Certificate is generated by Apple and given to the developer assigned to the account. This certificate is used to sign the applications in order to push them to devices. This certificate enables iOS Push Notifications for SPS accounts.

You need to enroll in the Apple iOS Developer Enterprise Program to obtain this certificate.

Apple Push Notification Service (APNS) certificate

The APNS certificate is used by IBM MaaS360 Portal (the MDM provider) to communicate with iOS devices through Apple's notification service. The APNS Certificate does not require an Apple Developer ID and creates cryptographic trust between your devices, your IBM MaaS360 instance, and Apple.

Pre-Requisites to Manage Apple Devices

Before creating the certificates for managing Apple devices, you need:

- An Apple ID for the organization
- An Apple Enterprise Developer Account
- A Mac with OSX 10.8+, including:
 - Xcode
 - Xcode Command Line Tools
 - Perl 5.16

About the Apple iOS Developer Enterprise Program

Several components that are necessary to manage iOS devices require enrollment in the Apple iOS Developer Enterprise Program (<https://developer.apple.com/programs/ios/enterprise/>).

There are two items that must be obtained through an Apple iOS Developer Enterprise Program account:

- App ID (also known as a Bundle ID)
- iOS Push Notification Client SSL Certificate

Get an App ID (aka Bundle ID)

About this task

Every iOS App has a unique identifier called an App ID (also known as a Bundle ID) that you choose through the Apple iOS Developer Enterprise Account (<https://developer.apple.com/programs/ios/enterprise/>).

Procedure

With IBM MaaS360, define App IDs for three iOS apps:

Option	Description
IBM MaaS360 App:	The ID must begin with <i>com.fiberlink.maas360.</i> , for example, <i>com.fiberlink.maas360.customer</i> . Be sure to include the required period after <i>com.fiberlink.maas360</i> .
Secure Browser:	The ID must begin with <i>com.fiberlink.browser.</i> , for example, <i>com.fiberlink.browser.customer</i> .
Secure Editor:	The ID must begin with <i>com.fiberlink.editor.</i> , as in <i>com.fiberlink.editor.customer</i> .

These Bundle IDs are also used to code sign the apps before they can be distributed to mobile devices. For more information about signing iOS apps for your deployment, see ““About Signing IBM MaaS360 Apps” on page 33”. For more information about creating an App ID, refer to Apple's documentation (App Distribution Guide).

Get an Apple Push Notification Client SSL Certificate

About this task

You need to generate a Push Notification Client SSL Certificate for IBM MaaS360 MDM app (Bundle ID starting with "com.fiberlink.maas360."). A Push Notification Client SSL Certificate is not required for other two MaaS360 apps.

Procedure

To generate a Push Notification Client SSL Certificate, you first need an App ID defined for the IBM MaaS360 MDM app. Then the Push Notification Client SSL

Certificate is uploaded to your deployment through the Portal.
For more information about generating this certificate, see the Apple documentation (App Distribution Guide).

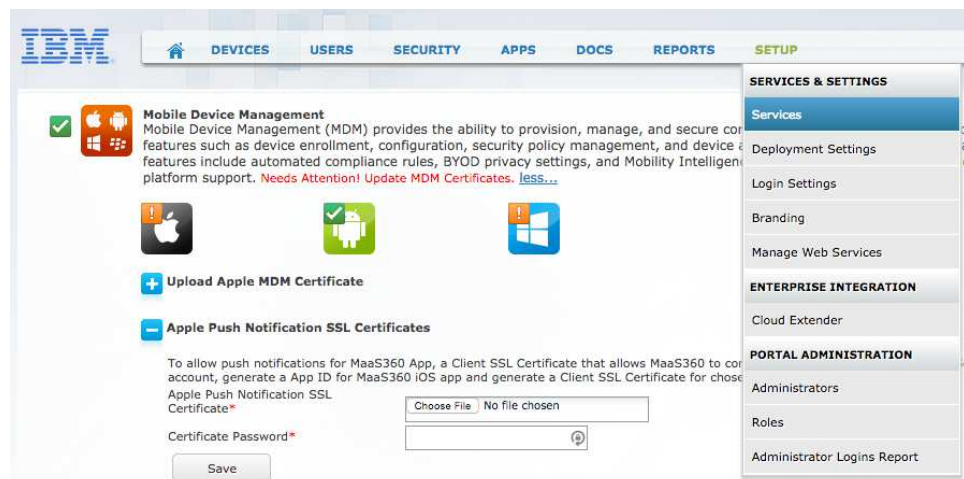
Upload the Apple Push Notification Client SSL Certificate

About this task

An Apple Push Notification Client SSL Certificate that is required to communicate with iOS Apps, and must be uploaded to your IBM MaaS360 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 **Apple Push Notification SSL Certificates**.



4. Click Choose File, and then select the APNS Certificate.

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 your Apple iOS Developer Enterprise Program account.
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 <http://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 MaaS360 deployment.

Upload the APNS Certificate (aka the Apple MDM Certificate)

About this task

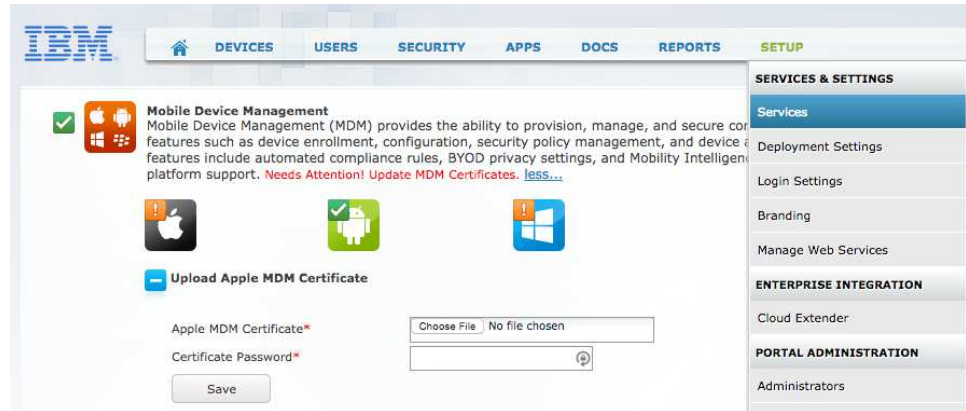
This certificate is required for IBM MaaS360 MDM accounts only, and is not required for SPS and MAM accounts.

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: Prepare 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 IBM MaaS360 Windows Phone Agent is your 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.

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 MaaS360. 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. At the top, there is a navigation bar with tabs for DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. Below this, the 'Services' section is active. Under 'Mobile Device Management', there are three sub-sections: 'Apple MDM Certificate', 'Apple Push Notification SSL Certificates', and 'Windows Phone 8 MDM'. The 'Windows Phone 8 MDM' section is highlighted with a red border. It contains a 'Save' button and a 'Choose File' button next to the 'Application Enterprise Token (AET) *' field. The 'Choose File' button is currently set to 'No file chosen'. The footer of the page displays the username 'dsimbach@us.ibm.com', account ID '1076800', and last login time '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 MaaS360 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 iOS and Windows Phone agents so that they can be transferred to their target devices. The Android agents do not require signing.

Finally, the signed agents must be uploaded to your IBM MaaS360 account so that they are available to devices that begin enrollment.

IBM MaaS360 iOS Apps

Available agent apps for iOS are:

- **IBM MaaS360 for iOS** - IBM MaaS360 MDM Enrollment Agent is installed on iOS devices during enrollment.
- **Secure Browser for iOS** - IBM MaaS360 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 IBM MobileFirst Protect (MaaS360) Secure Productivity Suite.

iOS apps must be code signed with your own App ID, Push Notification Client SSL Certificate, and iOS Code Signing Certificate.

After the apps are signed, they can be uploaded through the Portal so they are available to enrolling devices.

For instructions about uploading signed iOS apps, see “Chapter 15, “Upload Apps,” on page 37”.

IBM MaaS360 Windows Phone Apps

Windows Phone apps for IBM MaaS360 are:

- **IBM MaaS360 Company Hub** - The IBM MaaS360 MDM Agent, or Company Hub, is installed on Windows Phone devices during enrollment.
- **Secure Email for Windows Phone** - This app is the IBM MaaS360 Email client and is part of IBM MobileFirst Protect (MaaS360) Secure Productivity Suite.
- **Secure Browser for Windows Phone** - IBM MaaS360 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 MaaS360 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 14, “Step 11: Sign IBM MaaS360 Windows Phone Apps,” on page 35”.

For instructions about uploading signed Windows Phone apps, see “Chapter 15, “Upload Apps,” on page 37”.

IBM MaaS360 Android Apps

Android agent apps for IBM MaaS360 are:

- **IBM MaaS360 for Android** - This IBM MaaS360 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.
- **IBM MaaS360 for Android Samsung** - This IBM MaaS360 MDM Agent is installed on Android devices manufactured by Samsung.
- **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 IBM MobileFirst Protect (MaaS360) Secure Productivity Suite.
- **Secure Editor for Android** - Secure Editor allows users to edit documents within the IBM MobileFirst Protect (MaaS360) Secure Productivity Suite.
- **Secure Email for Android** - This app is the IBM MaaS360 Email client and is part of IBM MobileFirst Protect (MaaS360) Secure Productivity Suite.
- **Secure Docs for Android** - Secure Docs allows employees to view documents within IBM MaaS360 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 iOS and Windows Phone apps require additional modification.

For instructions about uploading Android apps, see Chapter 15, “Upload Apps,” on page 37.

Chapter 12. Step 9: Download IBM MaaS360 Apps

About this task

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

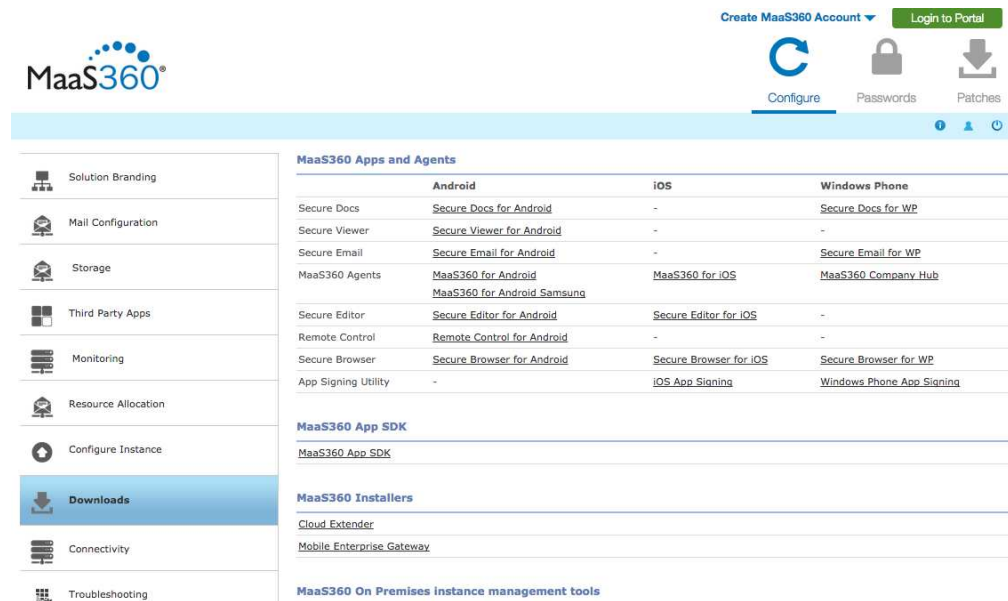
Using any browser, navigate to `http://<Configuration_VM_IP_Address>`.

You might be presented with a warning that the address is untrusted, but this warning can be ignored.

Enter the default username and password and click **Log In**.

Click **Configure** from the upper-right corner, and then click **Downloads**.

Click the desired app or agent link from the MaaS360 Apps and Agents section.



The screenshot displays the MaaS360 Administration Console interface. The top navigation bar includes the MaaS360 logo, a 'Create MaaS360 Account' dropdown, and a 'Login to Portal' button. Below the navigation bar are three icons: 'Configure', 'Passwords', and 'Patches'. The main content area is divided into a left sidebar and a main panel. The sidebar contains a list of menu items: Solution Branding, Mail Configuration, Storage, Third Party Apps, Monitoring, Resource Allocation, Configure Instance, Downloads (highlighted), Connectivity, and Troubleshooting. The main panel is titled 'MaaS360 Apps and Agents' and contains a table with columns for 'Android', 'iOS', and 'Windows Phone'. The table lists various applications and agents, such as Secure Docs, Secure Viewer, Secure Email, MaaS360 Agents, Secure Editor, Remote Control, Secure Browser, and App Signing Utility. Below the table, there are sections for 'MaaS360 App SDK', 'MaaS360 Installers', and 'MaaS360 On Premises instance management tools'.

	Android	iOS	Windows Phone
Secure Docs	Secure Docs for Android	-	Secure Docs for WP
Secure Viewer	Secure Viewer for Android	-	-
Secure Email	Secure Email for Android	-	Secure Email for WP
MaaS360 Agents	MaaS360 for Android MaaS360 for Android Samsung	MaaS360 for iOS	MaaS360 Company Hub
Secure Editor	Secure Editor for Android	Secure Editor for iOS	-
Remote Control	Remote Control for Android	-	-
Secure Browser	Secure Browser for Android	Secure Browser for iOS	Secure Browser for WP
App Signing Utility	-	iOS App Signing	Windows Phone App Signing

Chapter 13. Step 10: Code Sign iOS MaaS360 Apps

About this task

Apple iOS apps cannot be deployed to iOS devices until they are code signed. This process requires an App ID, a Push Notification Client SSL Certificate, and an iOS Code Signing Certificate.

IBM MaaS360 provides a code signing utility for iOS, located on the Downloads page of the Administration Console.

About Signing IBM MaaS360 Apps

After download the desired IBM MaaS360 apps from your deployment, you need to code sign the iOS and Windows Phone apps. The Android apps do not need to be code signed.

Once code signed, these customized apps can be uploaded to your IBM MaaS360 deployment through the Portal. The code signed apps are distributed to end user devices when they enroll in your deployment.

Code signing your apps assures users that they are from a known source and that the app has not been modified since it was signed.

iOS Code Signing Requirements

About this task

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

Procedure

1. Get a computer with OS X v10.8 or later, Xcode, Xcode Command Line Tools, and Perl 5.16 installed.
2. Download the IBM MaaS360 iOS App Signing Utility from the Administration Console.
3. Download the unsigned IBM MaaS360 iOS apps from the Administration Console.
4. Note the enrollment URL for your IBM MaaS360 deployment.
5. Get a iOS Code Signing Certificate in .p12 format and .p12 certificate password, through your Apple iOS Developer Enterprise Program account.
6. Get at least three App IDs (or Bundle IDs), through your Apple iOS Developer Enterprise Program account.

Each app requires a unique Bundle ID. For MaaS360 apps, you need to define these Bundle IDs on the iOS Developer Enterprise Program account:

- **IBM MaaS360 App:** The ID must begin with *com.fiberlink.maas360.*, for example, *com.fiberlink.maas360.customer*. Be sure to include the required period after *com.fiberlink.maas360*.
- **Secure Browser:** The ID must begin with *com.fiberlink.browser.*, for example, *com.fiberlink.browser.customer*.

- **Secure Editor:** The ID must begin with *com.fiberlink.editor.* , as in *com.fiberlink.editor.customer.*
7. Generate a Mobile Provisioning File for each iOS app, through your Apple iOS Developer Enterprise Program account. Each iOS app must bundle a provisioning profile. These profiles tie the Bundle ID with the appropriate Code Signing Certificate. Once the app IDs are created, you must create a provisioning profile for each app using the Code Signing Certificate from the Apple Developer account.

Code Sign the IBM MaaS360 iOS apps

Procedure

1. Download and unzip the IBM MaaS360 iOS App 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 unsigned IBM MaaS360 iOS apps to the Input folder within the unzipped folder structure.
4. Open the MaaS360.properties file and update the following details:
 - The absolute path where the iOS Code Signing Certificate is located.
 - The password for the iOS Code Signing Certificate.
 - The absolute path where the provisioning profile (.mobileprovision file) is located. This parameter should be updated for all IBM MaaS360 apps.
 - Bundle ID for the IBM MaaS360 apps.

The Bundle ID must be in the TEAM_ID.APP_IDENTIFIER format. For example: *YZF67Y7383.com.fiberlink.browser.customer* where the TEAM_ID is *YZF67Y7383* and the APP_IDENTIFIER is *com.fiberlink.browser.customer*

- The Enrollment URL for your IBM MaaS360 deployment.
5. Execute `iOSAppSign.sh`.
If the process is successful, the following message is displayed: *"Successfully generated all signed app files in output folder"*
The signed apps are now available in the Output folder.
Your signed IBM MaaS360 iOS apps can now be uploaded to your deployment through the Portal.

Chapter 14. Step 11: Sign IBM MaaS360 Windows 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 MaaS360 provides a code signing utility, located on the Downloads page of the Administration Console.

In addition to signing your IBM MaaS360 Windows Phone apps, the utility extracts the AET from the Symantec Code Signing Certificate. The AET must be uploaded to your IBM MaaS360 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 MaaS360 deployment.
3. Get the Symantec Code Signing Certificate in .pfx format.
4. Get the IBM MaaS360 Windows Phone App Signing utility from the Administration Console.
5. Get the unsigned IBM MaaS360 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 IBM MaaS360 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 IBM MaaS360 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 MaaS360 account.
 - The enrollment URL for your IBM MaaS360 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 15. Upload Apps

About this task

After the various IBM MaaS360 Agents and apps have been downloaded and signed (if required), the final step is to upload them into the IBM MaaS360 App Catalog.

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

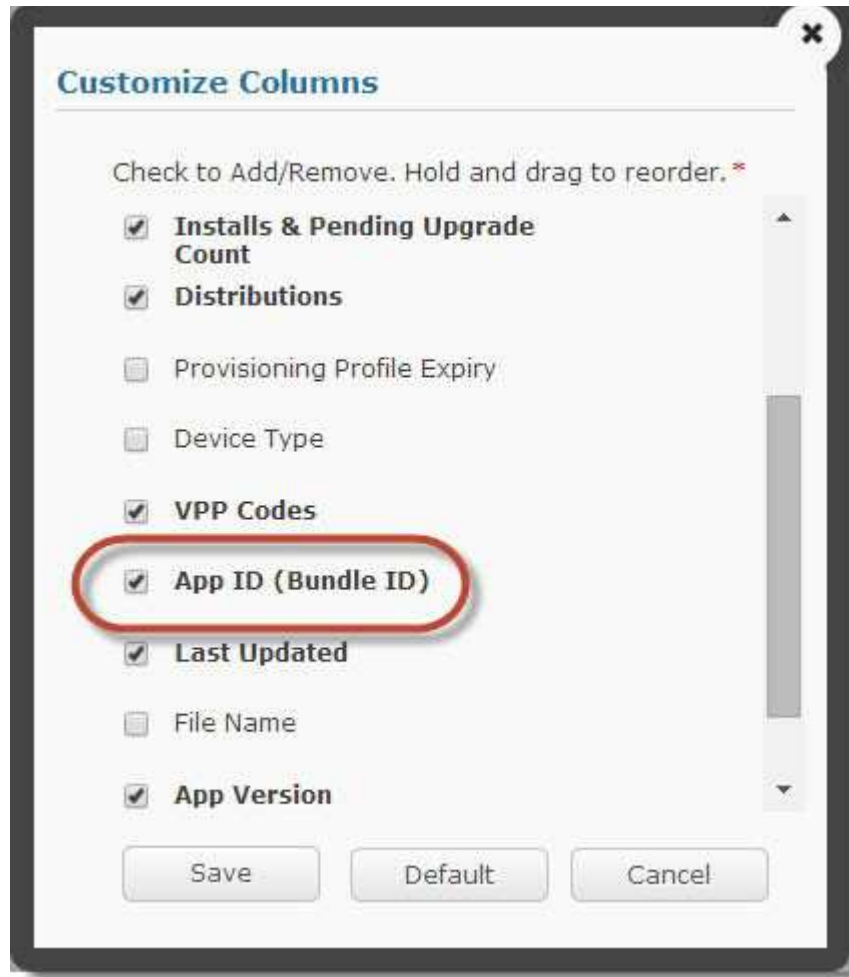
Procedure

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. See the “Options for iOS apps” on page 41 for more information.

6. Configure the settings for Windows Phone apps. See the “Options for Windows Phone apps” on page 41 for more information.

Enterprise App for Windows Phone

App Source ^{*} [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) [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.

7. Configure the settings for Android Enterprise Apps. See the “Options for Android apps” on page 42 for more information.

Enterprise App for Android

App Source ^{*} [Provide URL](#)

Description
Up to 10000 characters.

Category

Screenshot(s) [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.

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

Enterprise App iOS	MaaS360 MDM Agent	Secure Browser
App Source	Signed Agent file - MaaS360 for iOS	Signed Agent file - MaaS360 iOS Secure Browser App
Description	MaaS360 iOS Agent	MaaS360 iOS Secure Browser
Category	MaaS360	MaaS360
Screenshot	NA	NA
Remove App On		
- MDM Control REMOVAL	NA	NA
- SELECTIVE WIPE	Yes (Check)	Yes (Check)
- STOPPING DISTRIBUTION	No	No
Security Policies		
- Restrict data backup to itunes	Yes (Check)	Yes (Check)
Distribute to	All Devices	All Devices

Options for Windows Phone apps

Enterprise App for Windows Phone	Company Hub	PIM (Email App)	Secure Browser	SECURE DOCUMENT Viewer
App Source	Signed Agent file - MaaS360 Company Hub	Signed Agent file - MaaS360 PIM App	Signed Agent file - MaaS360 Secure Browser App	Signed Agent file - MaaS360 Secure Document Viewer App
Description	MaaS360 Company Hub	MaaS360 PIM App	MaaS360 Secure Browser App	MaaS360 Secure Document Viewer
Category	MaaS360	MaaS360	MaaS360	MaaS360
Screenshot	NA	NA	NA	NA
Remove App On				
- MDM Control REMOVAL	NA	NA	NA	NA
- SELECTIVE WIPE	No	No	No	No
- STOPPING DISTRIBUTION	No	No	No	No
INstaLL SETTINGS				
- Instant INSTALL	No	No	No	No
Distribute to	None	None	None	None

Options for Android apps

Enterprise App for Android	MaaS360 for Android	MaaS360 for Android SAMSUNG	Secure EMAIL for Android	SECURE DOCS For Android	Secure Browser for Android	SECUEr VIEWER for Android	Secure EDITOR for Android	REMOTE CONTROL for Android Samsung
App Source	App file - MaaS360 for Android	App file- MaaS360 for Android Samsung	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	App file -Remote Control for Android Samsung
Description	MaaS360 for Android	MaaS360 for Android Samsung	MaaS360 Android Secure Email for Android	MaaS360 Android Secure Docs for Android	MaaS360 Secure Browser for Android	MaaS360 Secure Viewer for Android	MaaS360 Secure Editor for Android	MaaS360 Remote Control for Android Samsung
Category	MaaS360	MaaS360	MaaS360	MaaS360	MaaS360	MaaS360	MaaS360	MaaS360
Screenshots	NA	NA	NA	NA	NA	NA	NA	NA
REview App for RISK Management*	No	No	No	No	No	No	No	No
Remove App On								
- MDM Control Removal	No	No	No	No	No	No	No	No
- Selective Wipe	No	No	No	No	No	No	No	No
- Stopping Distribution	No	No	No	No	No	No	No	No
INSTALL SETTINGS								
- Instant Install	No	No	No	No	No	No	No	No
Security Policies								
- RESTRICT DATA BACKUP to Google PLAY	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
- APPLY workspace policies	No	No	No	No	No	No	No	No

Enterprise App for Android	MaaS360 for Android	MaaS360 for Android SAMSUNG	Secure EMAIL for Android	SECURE DOCS For Android	Secure Browser for Android	SECURE VIEWER for Android	Secure EDITOR for Android	REMOTE CONTROL for Android Samsung
Distribute to	None	None	None	None	None	None	None	None

Chapter 16. About the IBM MaaS360 WorkPlace SDK

The IBM MaaS360 WorkPlace SDK allows you to integrate your app with MaaS360'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 MaaS360 App Security include single sign-on using container PIN, copy/paste restrictions, whitelisting apps for the **Open in...** menu, and per-app VPN.

If you are building a private Enterprise app, and want to integrate with MaaS360 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 MaaS360 Administration Console.

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

The screenshot shows the MaaS360 Administration Console. The left sidebar contains a navigation menu with the following items: Solution Branding, Mail Configuration, Storage, Third Party Apps, Monitoring, Resource Allocation, Configure Instance, Downloads (highlighted), Connectivity, and Troubleshooting. The main content area is titled 'MaaS360 Apps and Agents' and contains a table with columns for Android, iOS, and Windows Phone. Below the table are sections for 'MaaS360 App SDK' and 'MaaS360 Installers'. The 'MaaS360 App SDK' section includes a link for 'MaaS360 App SDK'. The 'MaaS360 Installers' section includes links for 'Cloud Extender' and 'Mobile Enterprise Gateway'. At the bottom of the main content area, there is a section for 'MaaS360 On Premises instance management tools'.

	Android	iOS	Windows Phone
Secure Docs	Secure Docs for Android	-	Secure Docs for WP
Secure Viewer	Secure Viewer for Android	-	-
Secure Email	Secure Email for Android	-	Secure Email for WP
MaaS360 Agents	MaaS360 for Android MaaS360 for Android Samsung	MaaS360 for iOS	MaaS360 Company Hub
Secure Editor	Secure Editor for Android	Secure Editor for iOS	-
Remote Control	Remote Control for Android	-	-
Secure Browser	Secure Browser for Android	Secure Browser for iOS	Secure Browser for WP
App Signing Utility	-	iOS App Signing	Windows Phone App Signing

MaaS360 App SDK

[MaaS360 App SDK](#)

MaaS360 Installers

[Cloud Extender](#)

[Mobile Enterprise Gateway](#)

MaaS360 On Premises instance management tools

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.

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 MaaS360 supports App Wrapping for Android and iOS on the On-Premises offering.

Android App Wrapping

Android App Wrapping is out of the box on IBM MaaS360 On-Premises.

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 MaaS360 On-Premises offering, but you will need additional assistance from IBM support to start using it on your IBM MaaS360 On-Premises setup.

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

Chapter 17. Use 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 MaaS360 On-Premises offering fully supports DEP.

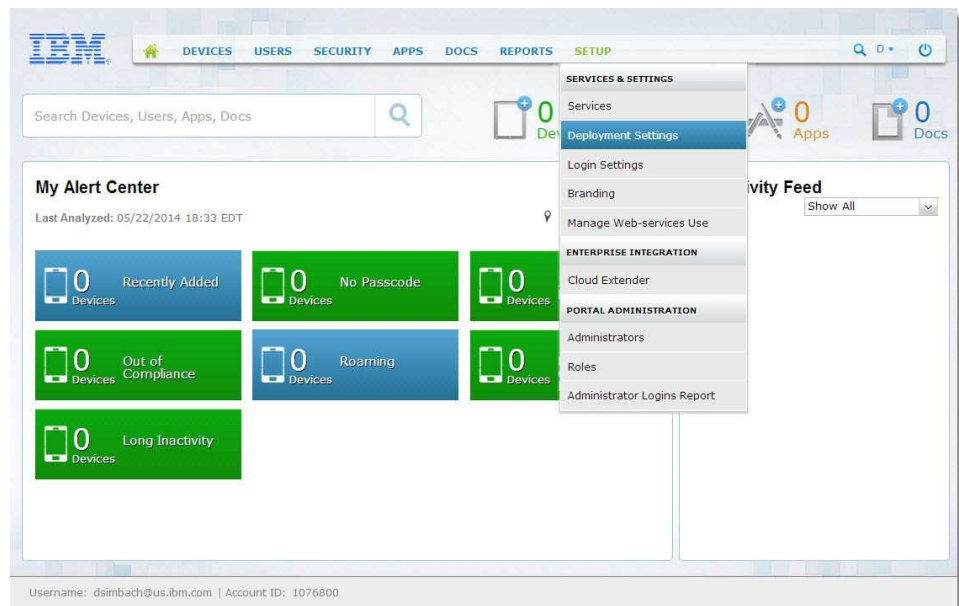
Step 1: Configure the DEP options in the IBM MaaS360 Portal

About this task

To configure the DEP options, perform the following steps:

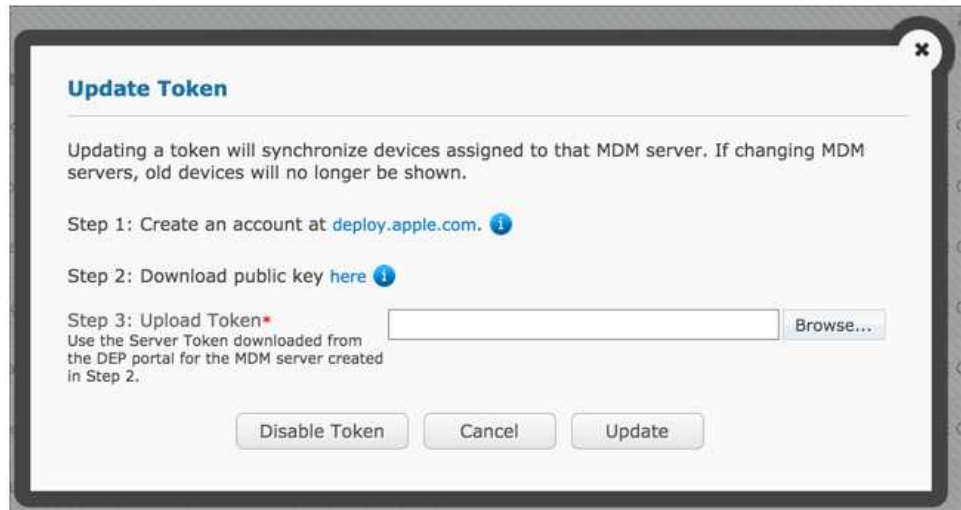
Procedure

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



3. Select **Use Apple's Device Enrollment Program** under **Advanced Management for Corporate iOS Devices**.
4. Enter custom **Authentication Screen Header Text** that will be displayed to the end user when the device is activated.
5. From the the top navigation bar, select **Devices > Enrollments**.
6. On the **Enrollments (Add Device Requests)** screen, click the **Streamlined Enrollment** button.

7. Follow the steps to download and save the IBM MaaS360 public key. This is required for Apple to generate an MDM token to link the MaaS360 MDM server with Apple.
8. Keep this window open. The next set of steps will give you a token that you must upload from this window.



Step 2: Enroll your organization in DEP using the Apple DEP Portal

About this task

Next, perform the following steps in the Apple DEP Portal. This step requires enrollment in the Apple Deployment Program. If you are not enrolled in Apple Deployment Program, see below links for more information. Enrolling takes up to 5 days.

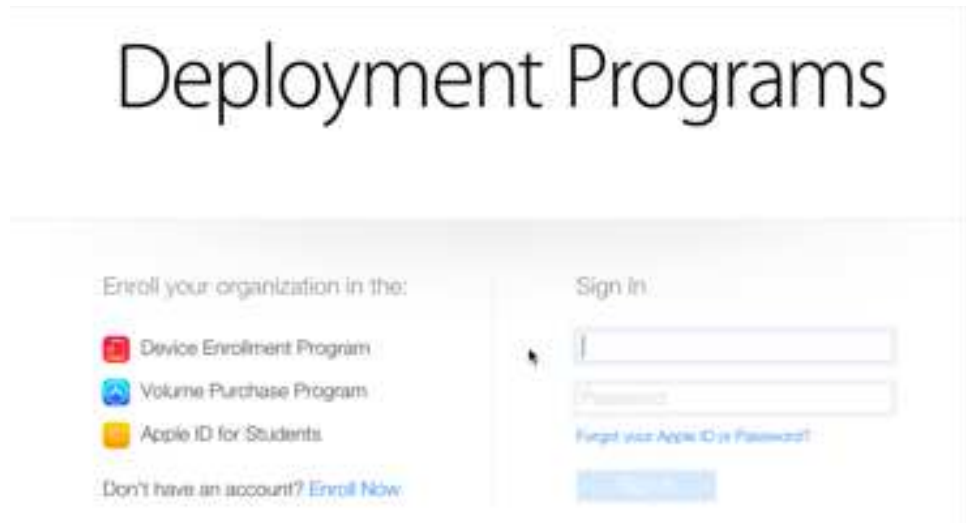
Apple's DEP Home Page: <http://www.apple.com/business/dep/>

Apple's DEP Guide: http://images.apple.com/business/docs/DEP_Guide.pdf

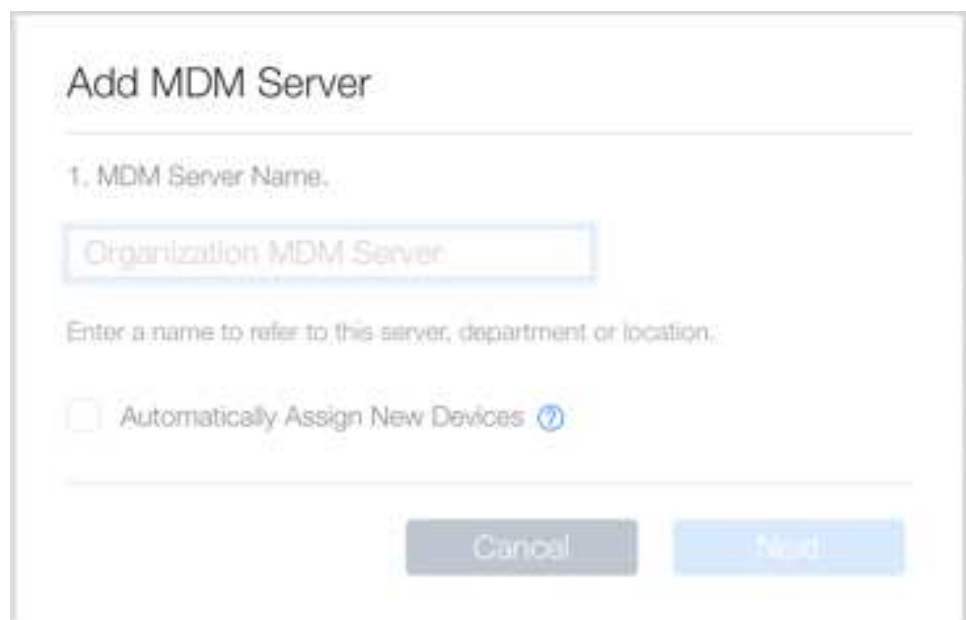
After your enrollment is complete:

Procedure

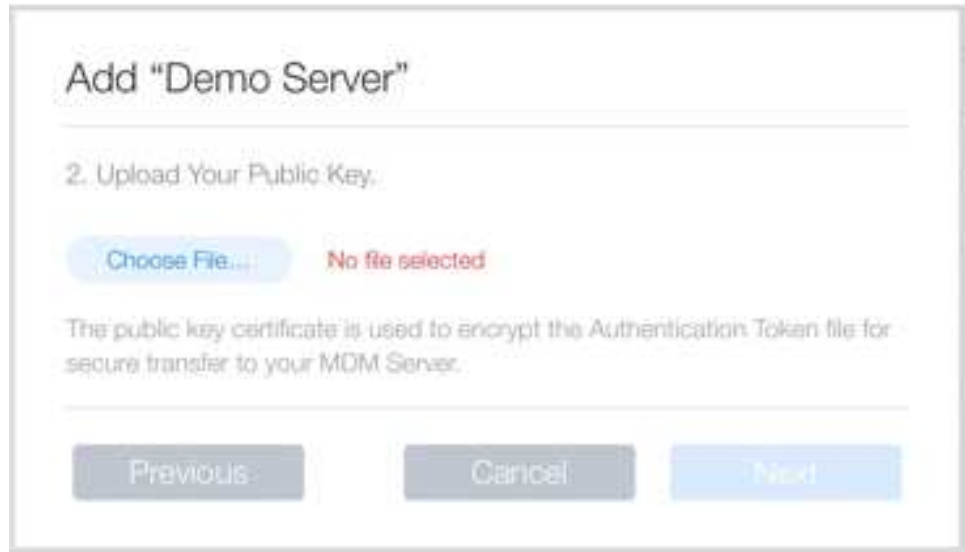
1. Log into the Apple DEP Portal (<http://deploy.apple.com>).



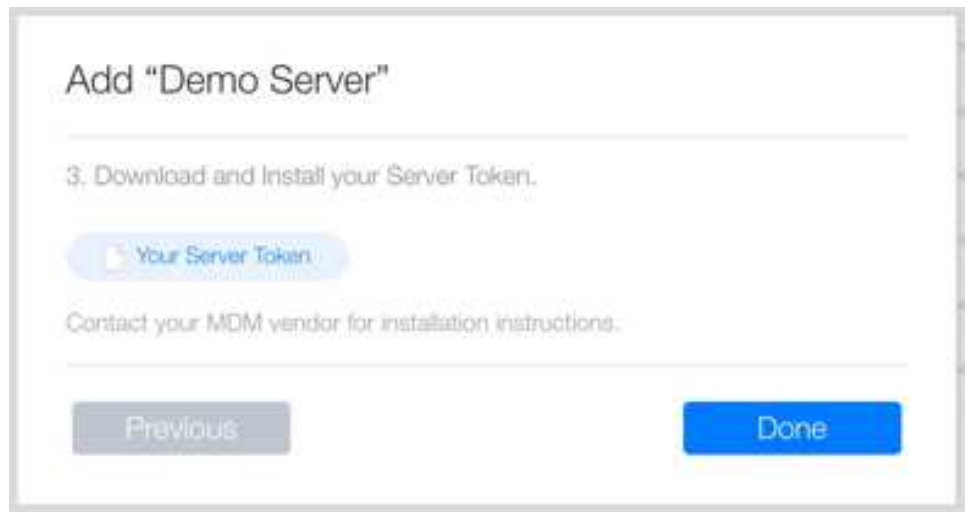
2. On the next screen, select **Add MDM Server** and enter the MDM server name. It is an internal identifier and does not have to be specifically for a particular MDM solution vendor. Click **Next**.



3. Upload MaaS360 Public Key downloaded from the MaaS360 Portal previously. Click **Next**.



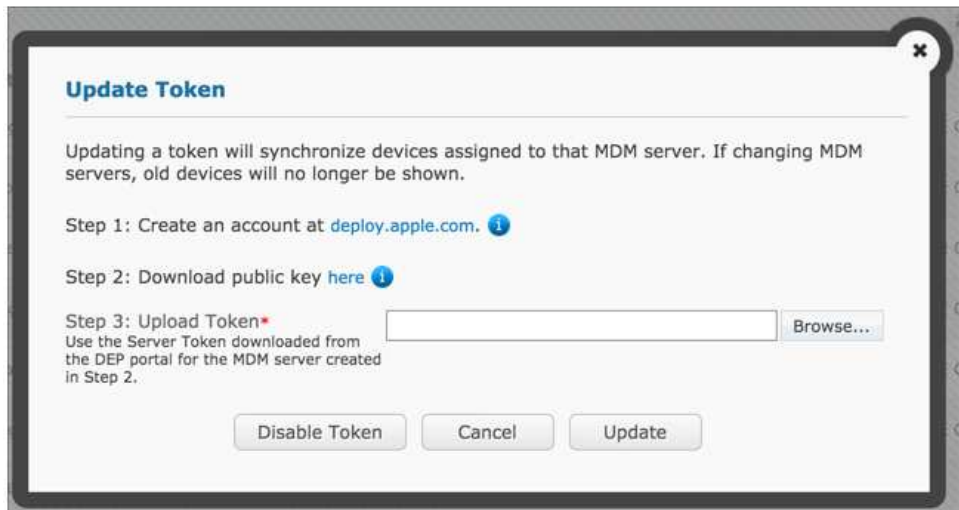
4. Download the MDM Server token and select **Done**.



Step 3: Update the token in the IBM MaaS360 Portal

Procedure

1. Upload the Server token to the deployment from the open window in the IBM MaaS360 Portal.



As soon as the token is uploaded, the deployment uses the token generated in the process and finds all the devices available for DEP. The list of associated device serial numbers is then displayed in the IBM MaaS360 Portal.

Each device has to be assigned a profile which defines the way in which fresh device is setup. IBM MaaS360 refreshes serial numbers automatically every 4 hours, or on demand by using the refresh button.

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

Serial Number	Status
PB4 Assign Profile	Assigned
M5 Assign Profile	Enrolled
FPB4 Assign Profile	Unassigned
FPB4 Assign Profile	Assigned
PB4 Assign Profile	Enrolled
FPB4 Assign Profile	Assigned

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

This profile will allow to define the following based on your requirements, and is also synchronized to Apple's servers.

Profile configuration options:

- **Profile Name:** Display name of the profile
- **Set as Default Profile:** The default profile will override an existing default. New devices and devices without an assigned profile will be assigned this profile.
- **Require MDM Enrollment:** This will require users to enroll their device with MaaS360 during the setup process.
- **Supervise Device:** This will allow you to take advantage of the additional supervised policy options available in MaaS360.
- **Authenticate User:** This will prompt the user to authenticate during devices set up. After the set up they will receive their assigned settings and content, like policies, rules, apps and docs.

NOTE 1: This is only supported on devices running iOS 7.1 or higher

NOTE 2: If using AD/LDAP integration through the Cloud Extender, the username format must be in *domain\username*

- **Allow iTunes Pairing:** This will allow the user to sync their device to iTunes
- **Skip Setup Items:** Skip items such as *Location, Apple ID, Siri, Touch ID, Restore, TOS* and *Diagnostics*.
- **Set a Department Name**
- **Set a Support Phone Number**
- **Set Assignment:** A profile may be assigned to *None, All Devices* or *All unassigned devices*.

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 MaaS360.

You have to license and install IBM QRadar before you can enable the integration with IBM MaaS360.

Refer the following document to configure QRadar for IBM MaaS360:

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 MaaS360 On-Premises instance as configured in Administration Console.

Chapter 19. About Self-Signed Certificates Support

IBM MaaS360 On-Premises 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 MaaS360 On-Premises 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 MaaS360. 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 (MaaS360) On-Premises Installation Guide Version*.

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) Recommended : 2048
Authority Key Identifier		Unique key identifier.
Subject key Identifier		Unique Subject Key Identifier.

ATTRIBUTE	VALUE	REMARKS
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Should exactly match what's given in Value column for device enrollment to work. In Unix based machine you will see "Extended Key Usage" the values should be : 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 : Digital Signature, Key Encipherment Non-Repudiation is an optional value that can exist besides the mandatory values given.
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	In Unix based machine the value for "Basic Constraints" should be: critical CA:FALSE

The IBM MaaS360 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 MaaS360. You can start enrolling devices into your account.

For information related to the administration and use of the main portal, see: *IBM MobileFirst Protect (MaaS360) Portal Administration Guide*.

If you want to integrate your Active Directory, Lotus Traveller, SCEP Server, BES Server, or Exchange ActiveSync deployments with your IBM MaaS360 deployment, install the optional IBM MaaS360 Cloud Extender.

For more information, see: *IBM MobileFirst Protect (MaaS360) 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 MaaS360 Mobile Enterprise Gateway.

For more information, see: *IBM MobileFirst Protect (MaaS360) 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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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. _enter the year or years_. All rights reserved.

Programming interface information

Trademarks

IBM, the IBM logo, and 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.

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.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

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.

IBM Online Privacy Statement

Safety and environmental notices



Product Number: 5725-R11

Printed in USA