



IBM MobileFirst Protect (MaaS360) Mobile Enterprise Gateway Migration Guide

Contents

Chapter 1. Introduction	1	Chapter 2. Migration Steps.	3
-----------------------------------	---	-------------------------------------	---

Chapter 1. Introduction

About this task

IBM MobileFirst Protect (MaaS360) version 2.3.0.1 now includes a newer version of the Mobile Enterprise Gateway (MEG) 2.0 than what was previously released. If your On-Premises version of MaaS360 is an earlier version, you must apply the appropriate fix pack before migrating to MEG 2.0.

For more information about this new version, refer to the *IBM MobileFirst Protect (MaaS360) Mobile Enterprise Gateway Quick Start Guide*.

Procedure

To enable MEG 2.0 for your IBM MaaS360 On-Premises installation, please contact IBM Support.

Chapter 2. Migration Steps

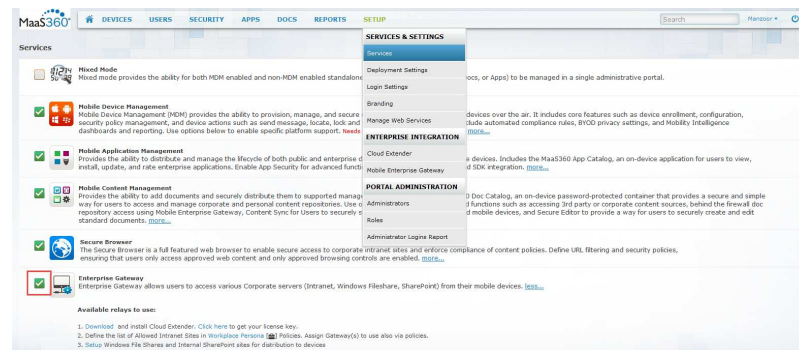
About this task

Customers using the older version of MEG must migrate to MEG 2.0 by performing the following steps:

Procedure

1. Log in to the IBM MaaS360 portal as the customer administrator. Mouse over **Setup** and select **Services**.

The Enterprise Gateway service should be enabled.



2. Follow the instructions in the *Gateway Installation and Basic Set Up* section in the *IBM MEG 2.0 Quick Start Guide* to set up the IBM MaaS360 Cloud Extender and MEG module.
3. If you plan to support SharePoint documents or Windows File Shares with MEG 2.0, perform the following steps:
 - a. Mouse over **Docs** and select **Content Sources**.
 - b. Click the **Add Source** button at the top right side of the screen.
 - c. Select the type of content source (the **Site Display Name**), and then select the MEG 2.0 Gateway's name from the drop-down list.

For SharePoint:

Add SharePoint Site

Site Display Name*
This is what your end user will see.

Site Visibility*
 Internal External

Select Gateway*
Select the Gateway for this File Share

Configure Regional Gateways
Enterprise Gateway to use when devices are connecting from the specified country

Browser URL *
Copy this from the browser where you access a SharePoint folder. To let users add their own SharePoint Sites, provide a URL of type http://mysharepoint.mydomain.com/* (supported on MaaS360 for iOS 2.90+ and MaaS360 Android 5.21+).
E.g. Site Display Name:
http://sp.mydomain.com, Library/Folder:
http://sp.mydomain.com/sub%20site/lists/forms/AllItems.aspx?RootFolder=Folder1/Test

Group Access Permissions
"Select group and set permissions."
"Use Workplace Settings" is supported on iOS App 2.40+ and Android App 5.00+.
 +

Cancel Save

For Windows File Share:

Add Windows File Share

Display Name*
This is what your end user will see.

Select Gateway*
Select the Gateway for this File Share

Configure Regional Gateways
Enterprise Gateway to use when devices are connecting from the specified country

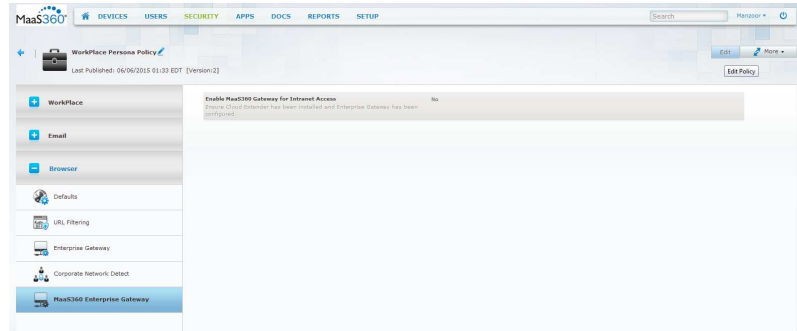
Folder Path

This can be either in the URL format (servername/file_path) or in the UNC naming format (\\server\share\file_path). For ex:
demoserver.corpdomain.local/sales/docs
or \\demoserver\sales\docs . The %username% variable can be used to represent the username provided during enrollment.

Group Access Permissions
Select group and set permissions.
"Use Workplace Settings" is supported on iOS App 2.40+ and Android App 5.00+.
 +

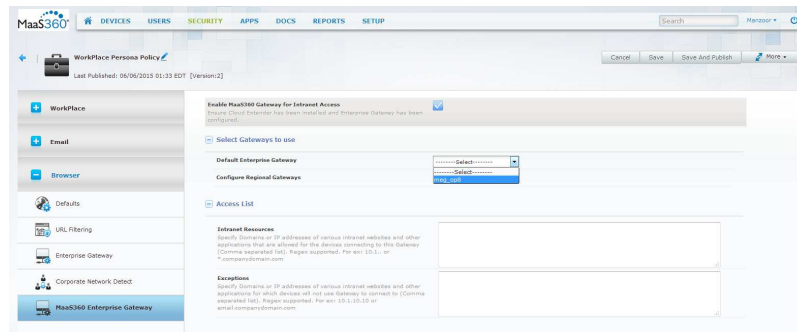
Cancel Save

4. After the MaaS360 Cloud Extender has been set up and the MEG module has been configured, log back in as the customer administrator.
5. Select **Security>Policies** and then find the WorkPlace Persona Policy. Click the **View** link to display the policy.
6. Click the **Browser** tab on the left side to expand the options, and then click **MaaS360 Enterprise Gateway**.
7. Click the **Edit** button at the top of the screen.

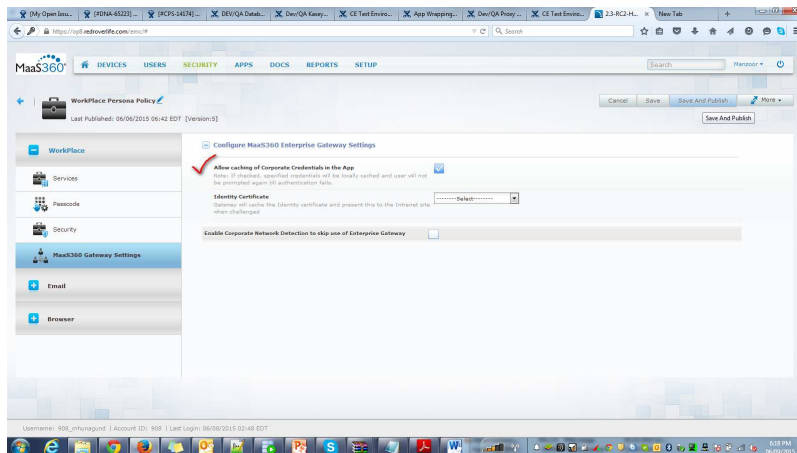


8. Select **Enable MaaS360 Gateway for Intranet Access**. Select the **Default Enterprise Gateway** from the pull-down menu.

For additional details refer to the *IBM MobileFirst Protect (MaaS360) MEG 2.0 Quick Start Guide*.

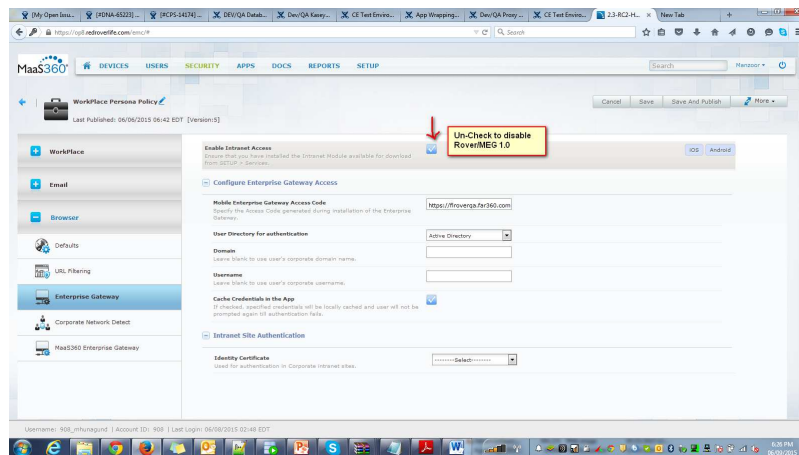


9. Enter the **Intranet Resources** (and more details if necessary).
10. Click **Save and Publish**.
11. You can click the **WorkPlace** tab on the left, and then click **Allow Caching of Corporate Credentials in the App**.



12. After the policy has been saved and published, you can migrate from the previous version of MEG to MEG 2.0. After all the devices are updated with the latest Persona policy, all the requests from the IBM MaaS360 Secure Browser will be routed through the IBM MaaS360 Enterprise Gateway 2.0.
13. If the personal policy has details related to both MEG and MEG 2.0, the MEG 2.0 settings will be used.
 - To disable the older version of MEG in the existing policy, perform the following steps:

- a. Display the existing policy.
 - b. Select the **WorkPlace Persona Policy** tab on the left side of the screen.
 - c. Select **Browser**, and then click **Enterprise Gateway**.
 - d. Clear the **Enable Intranet Access** checkbox.
- To disable the older version of MEG in the new policy, perform the following steps:
 - a. Display the new policy.
 - b. Select the **WorkPlace Persona Policy** tab on the left side of the screen.
 - c. Select **Browser**, and then click **Enterprise Gateway**.
 - d. Clear the **Enable Intranet Access** checkbox.



Note: After successfully migrating all the users from the older version, you can discontinue using it. Contact IBM Support to disable it.