Endpoint Manager for Mobile Devices Setup Guide

Contents

IBM Endpoint Manager for Mobile Devices Setup Guide

The IBM Endpoint Manager for Mobile Devices application manages corporate and employee-owned smartphones and media tablets that access enterprise resources. The application can be used to manage device security, software and hardware inventory, and application management.

This *Setup Guide* provides IT managers and system administrators instruction on how to install and configure the application and how to set up your mobile devices to integrate with the application. Specifically, it includes setup instructions for iOS, Android, Lotus Traveler, and Microsoft Exchange. This guide also includes system requirements for each application component, and provides licensing and installation instructions to enable you to deploy Mobile Devices in your environment.

For information on how to use Endpoint Manager for Mobile Devices, see the *Endpoint Manager for Mobile Devices User's Guide*.

Components

The Mobile Devices application includes the following primary components:

Server – The Endpoint Manager for Mobile Devices server is a database that communicates with the relays and the Tivoli Endpoint Manager console to manage the devices in your deployment.

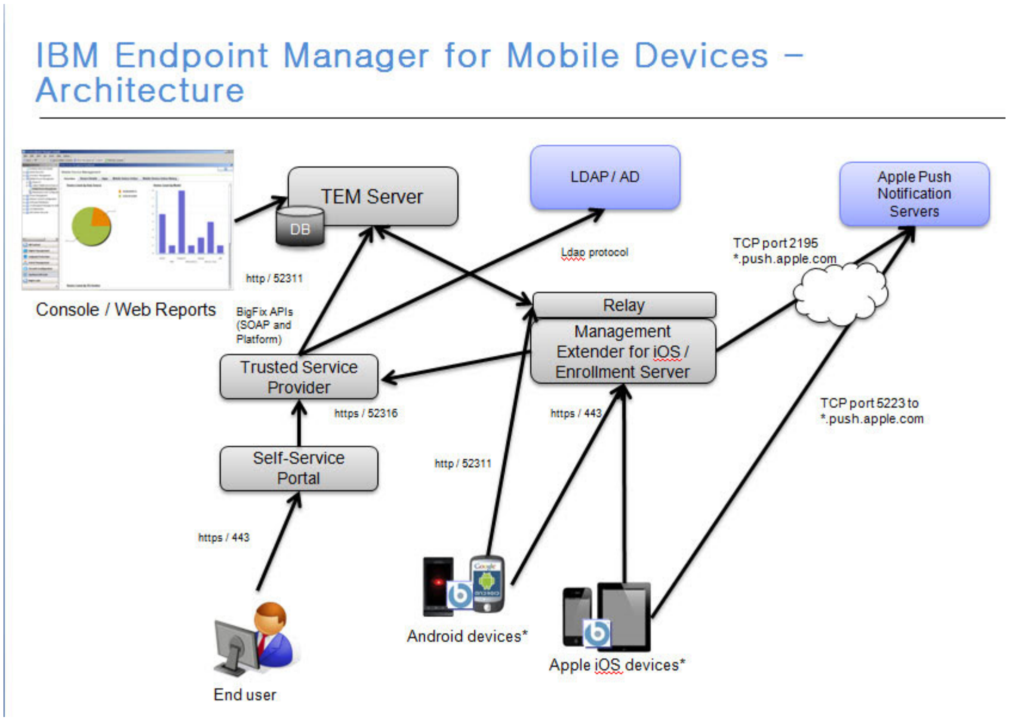
Relay - Relays are network components designed to distribute the download burden from the Tivoli Endpoint Manager server and compile and compress data received from clients. In MDM, the relays process information from your mobile devices and transmit that information to the TEM server.

Management Extenders – Management Extenders allow devices to be managed without an agent on the device.

Email Servers – Includes Lotus Traveler and Microsoft Exchange servers.

Architecture

The diagram below depicts a visual representation of how Mobile Devices is designed to work in your environment.



IBM Endpoint Manager for Mobile Devices – Architecture

Key Features

The following is a list of the most important features of Mobile Devices:

- Integration with Tivoli Endpoint Manager platform
- Ability to import apps from Worklight server
- Support for basic management of devices using email-based management
- Support for advanced management of devices using agent-based management
- Device inventory
- Security and password policy management
- Management commands such as wipe, lock, clear-password, deny email access, push, and data roaming
- App Management
- Authenticated Enrollment for restrictive user access
- Self Service Portal for managing devices without the need for Tivoli Endpoint Manager or Web Reports.
- Android Wi-Fi
- Enterprise access configuration including email, WiFi, and VPN

Note: Support for these features varies by device, OS, and management method.

System Requirements

General

IBM Endpoint Manager for Mobile Devices has the following system requirements.

- IBM Endpoint Manager version 8.2 or above.
- All Management Extenders must be installed on Windows systems.
- An IBM Endpoint Manager relay must already be installed on the system.
- If you are using Mobile Device Management *v*9.1 or above, you must deploy a proxy agent from BES Support before deploying a Management Extender.

IBM Endpoint Manager Management Extenders have the following system requirements. The values apply to both physical and virtualized environments.

- Processor: Quadcore, 64-bit
- Processor Speed: 2 GHz
- Memory: 8 GB RAM
- Storage: 100 GB for server, more as required for backups and logs.

You can have only one Management Extender on each machine.

The number of devices supported by each Mangement Extender (or relay, for Android devices) appears below. The combined total should not excced 5000 endpoints across all Extender types.

System	Endpoints Supported per Management Extender	Notes
iOS	1000	
Android	2000	per relay
MaaS360	5000	
Exchange	5000	
Traveler	5000	
Blackberry	5000	
Divide	5000	

For more specific requirements for each mobile server see the appropriate device section below.

Note: Select an available port for the iOS Management Extender before using the application. The default is 443. If you want to use a different port, specify that port in the Configure Management Extender dashboard.

For Lotus Traveler

See the following requirements for using a Lotus Traveler Server:

- Lotus Traveler Server version 9.0 or earlier.
- Domino server must run the Traveler, DIIOP, and HTTP tasks.
- HTTP must be listening on ports 80, 443, or both. The URL http(s)://<server>/diiop_ior.txt must be publicly accessible.

- DIIOP must be listening on ports 63148, 63149 or both. For configurations using port 63149, the SSL certificate must be valid and current, and a *TrustedCerts.class* file must have been generated in the Domino data folder.
- Create an administrative user. The administrative user must have both *read* and *edit* permissions in the ACL for LotusTraveler.nsf, and must be able to run restricted and unrestricted Domino commands.

See the following requirements for using the Management Extender for Lotus Traveler server:

- The plugin must be able to contact the server in one HTTP and one DIIOP port. If DIIOP listens exclusively on port 63149, the plugin requires the server-specific TrustedCerts.class in its classpath. To do this, include the TrustedCerts.class in a TrustedCerts.jar file and deploy it through the Configure Management Extender dashboard.
- The administrative user must have a username and password. Anonymous connections are not supported.

For Microsoft Exchange

See the following requirements for using Exchange Server:

- Win 2008 Server
- WS-Management protocol
- WinRM
- Exchange Server 2007, 2010, 2013, or Office 365

See the following requirements for using Management Extender for Exchange Server:

- WS-Management protocol and WinRM, or
- Exchange Management Tools (Exchange 2007 and 2010 only)

Note: If you intend to use this Management Extender to connect to a remote 2007 or 2010 Exchange Server, first install Exchange Management Tools on the Management Extender to connect it properly to the remote server.

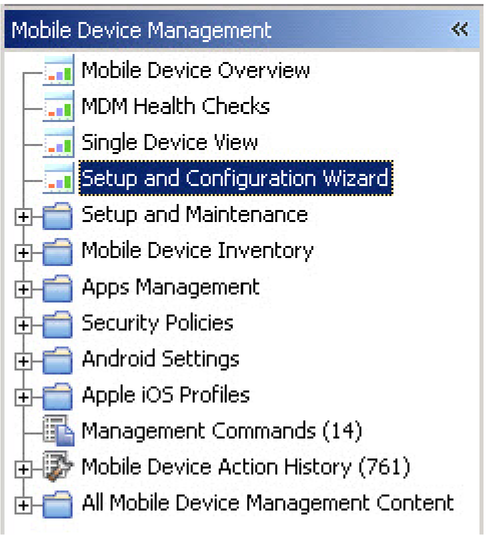
For Android

See the following requirements for Android:

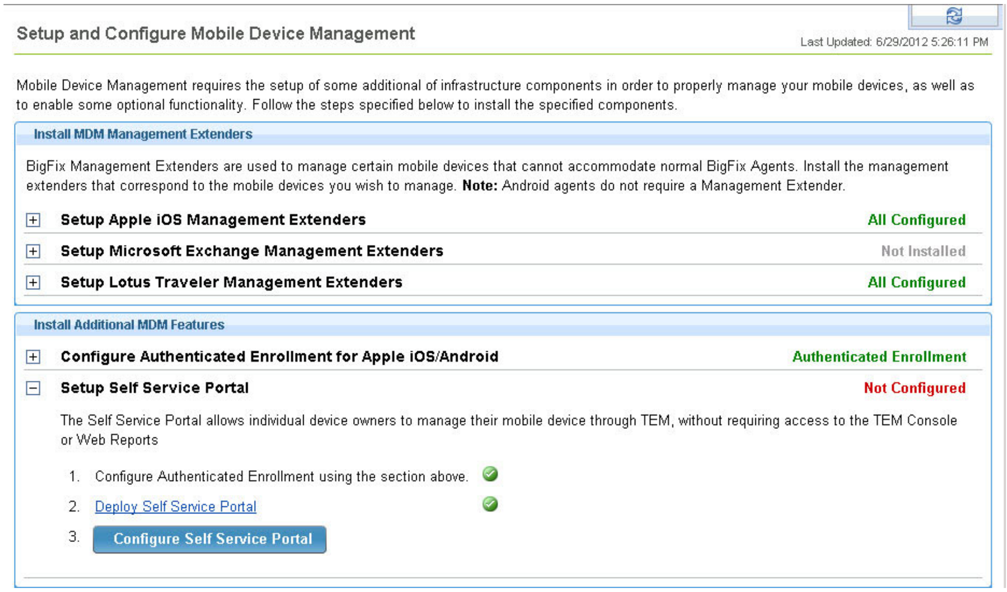
- Android 2.2+ (Froyo) running on ARM processors
- Ability to connect to a Tivoli Endpoint Manager server or relay

Setup and Configuration Wizard

The Setup and Configuration wizard, located at the top of the MDM navigation tree, configures your management extenders to enable them to connect to servers.



From the Setup and Configuration wizard, you can install iOS, Microsoft Exchange, and Lotus Traveler management extenders, as well as additional MDM features, such as Authenticated Enrollment and Self Service Portal.



Setup and Configure Mobile Device Management

Last Updated: 6/29/2012 5:26:11 PM

Mobile Device Management requires the setup of some additional of infrastructure components in order to properly manage your mobile devices, as well as to enable some optional functionality. Follow the steps specified below to install the specified components.

Install MDM Management Extenders

BigFix Management Extenders are used to manage certain mobile devices that cannot accommodate normal BigFix Agents. Install the management extenders that correspond to the mobile devices you wish to manage. **Note:** Android agents do not require a Management Extender.

⊞ **Setup Apple iOS Management Extenders**	All Configured
⊞ **Setup Microsoft Exchange Management Extenders**	Not Installed
⊞ **Setup Lotus Traveler Management Extenders**	All Configured

Install Additional MDM Features

⊞ **Configure Authenticated Enrollment for Apple iOS/Android**	Authenticated Enrollment
⊟ **Setup Self Service Portal**	Not Configured

The Self Service Portal allows individual device owners to manage their mobile device through TEM, without requiring access to the TEM Console or Web Reports

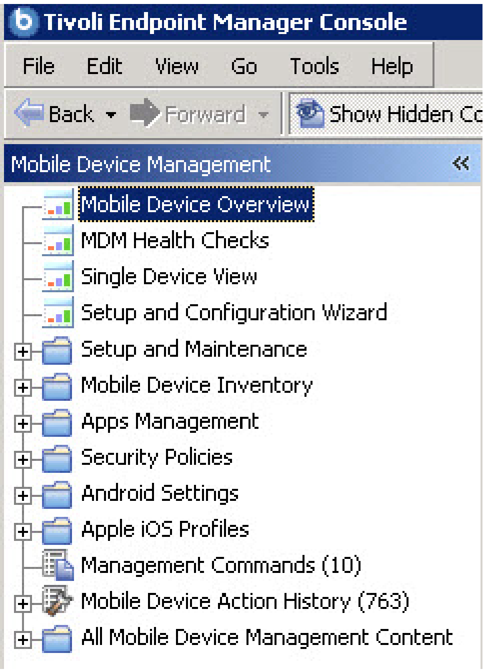
1. Configure Authenticated Enrollment using the section above. ✓
2. Deploy Self Service Portal ✓
3. Configure Self Service Portal

Click the plus sign next to each management extender to expand the options. Then click *Configure*. This will open the Configure Extender window for each type. In the Configure Extender window, you can set parameters for the configuration.

Installing and Configuring

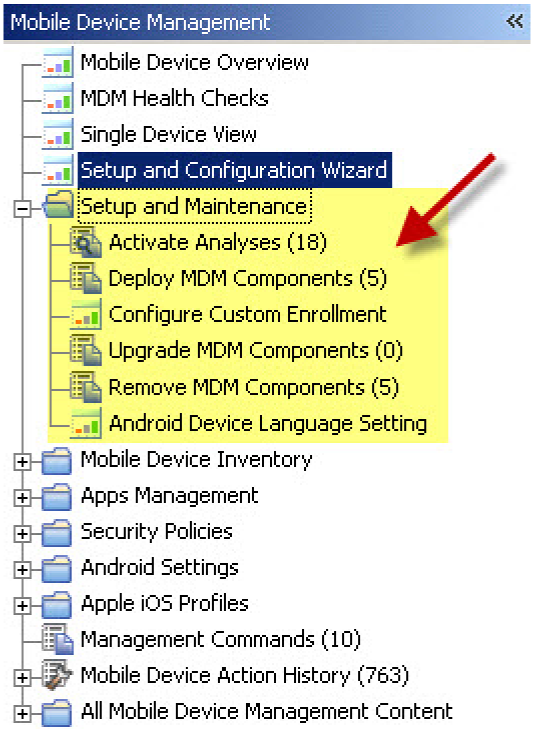
Prior to beginning the installation and setup of Mobile Devices, you should be familiar with the Tivoli Endpoint Manager console and be logged in. For detailed information about the console, see the Tivoli Endpoint Manager Console Operator's Guide.

The Mobile Devices navigation tree in the Tivoli Endpoint Manager console will serve as your central command for all Mobile Devices installation, setup, and management functions. The navigation tree gives you easy access to all reports, wizards, Fixlets, analyses, and tasks related to the management of your devices. The top of the navigation tree contains the four primary dashboards: Mobile Device Overview, MDM Health Checks, Single Device View, and the Setup and Configuration Wizard. The primary MDM content is organized into the following nodes or categories: Setup and Maintenance, Mobile Device Inventory, Apps Management, Security Policies, Android Settings, Apple iOS Profiles, and Mobile Device Action History.



The setup and installation of MDM in your deployment involves using the *Setup and Configuration Wizard* and the *Setup and Maintenance* node in the navigation tree. You used the Setup and Configuration Wizard in the previous section to setup and configure your management extenders. Now you can use the Setup and Maintenance node to activate analyses, deploy or remove components, configure custom enrollment, and set Android device language settings

The Setup and Maintenance node in the navigation tree displays a list of preliminary actions you need to take before using the Mobile Devices application. These include activating analyses, deploying or removing components, configuring custom enrollment, and setting Android device language settings.



The Management Extender provides a mechanism for managing the devices in your deployment by interacting with your existing management process.

Note: You cannot have more than one management extender for each type.

After installing and configuring all MDM components, users can download and install the iOS App from the Apple iTunes store and the Android Agent from Google Play.

Activate Required Analyses

Begin by clicking the Required Analysis node in the navigation tree. Select all analyses in the list, right click to display the drop down menu, and click *Activate*. After all analyses are activated, you can begin deploying your management extenders.

Microsoft Exchange Management Extender

Microsoft Exchange Management Extenders are components within IBM Endpoint Manager for Mobile Devices that allow communication with your Exchange deployment. After it is deployed, a Management Extender is linked to an Exchange Server allowing control over device mail, calendar, contacts, and tasks using Active Sync.

IBM Endpoint Manager for Mobile Devices supports Microsoft Exchange 2007, 2010, 2013, and Office 365.

Microsoft Exchange Management Extenders facilitate communication with all devices that use Active Sync, including BlackBerry 10 and Playbook devices, for example. BlackBerry devices that run BlackBerry OS versions 4.5 through 7.0 are administered by BlackBerry Management Extenders.

Management Extenders must first be deployed, which is the process of installing it on a relay or Microsoft Exchange server. After you deploy an extender, it must be configured. In addition, depending on what version of Microsoft Exchange Server is deployed, and the way it is configured, more steps must be taken to ensure communication between the Exchange Server and the Microsoft Exchange Management Extender.

Microsoft Exchange Configuration

The version of Microsoft Exchange in your deployment and how you choose to communicate with it, dictates various configuration steps that must be taken to ensure that IBM Endpoint Manager for Mobile Devices can communicate to your Exchange deployment.

Exchange 2007

- Exchange Management Tools (EMT) is required to communicate with an Exchange 2007 server. EMT can be installed from your Exchange installation media, or the 32-bit version of the tools can be downloaded from Microsoft here: http://www.microsoft.com/en-us/download/details.aspx?id=11876
- When you use EMT, the computer that is hosting your Microsoft Exchange Management Extender must be a member of the "Exchange Organization Administrators". For more information, see http://technet.microsoft.com/en-us/library/aa996881%28v=exchg.80%29.aspx

Exchange 2010

- Windows Remote Management (WinRM) can be used instead of EMT. WinRM is the recommended default.
- When you use WinRM, you must run the `Enable-PSRemoting` command on your Exchange Server. For more information, see "Exchange Server Configuration" on page 9.
- Exchange Management Tools (EMT) can be used to enable communication between your Management Extender and your Exchange Server. When you use EMT, the computer that is hosting your Microsoft Exchange Management Extender must be a member of the "Exchange Organization Administrators".

Exchange 2013

- Windows Remote Management (WinRM) must be used.
- You must run the `Enable-PSRemoting` command on your Exchange Server. For more information, see "Exchange Server Configuration" on page 9.

Office 365

- Windows Remote Management (WinRM) must be used.
- You must run the `Enable-PSRemoting` command on your Exchange Server. For more information, see "Exchange Server Configuration" on page 9.

Exchange Server Configuration

If your deployment uses Exchange 2013, Office 365, or Exchange 2010 with WinRM, you must set your Exchange Server to receive Windows PowerShell remote commands.

To enable remote PowerShell commands, perform the following steps on the computer that is hosting your Exchange Server:

1. Open an administrator elevated command prompt.
2. Type the command:

```
Enable-PSRemoting
```

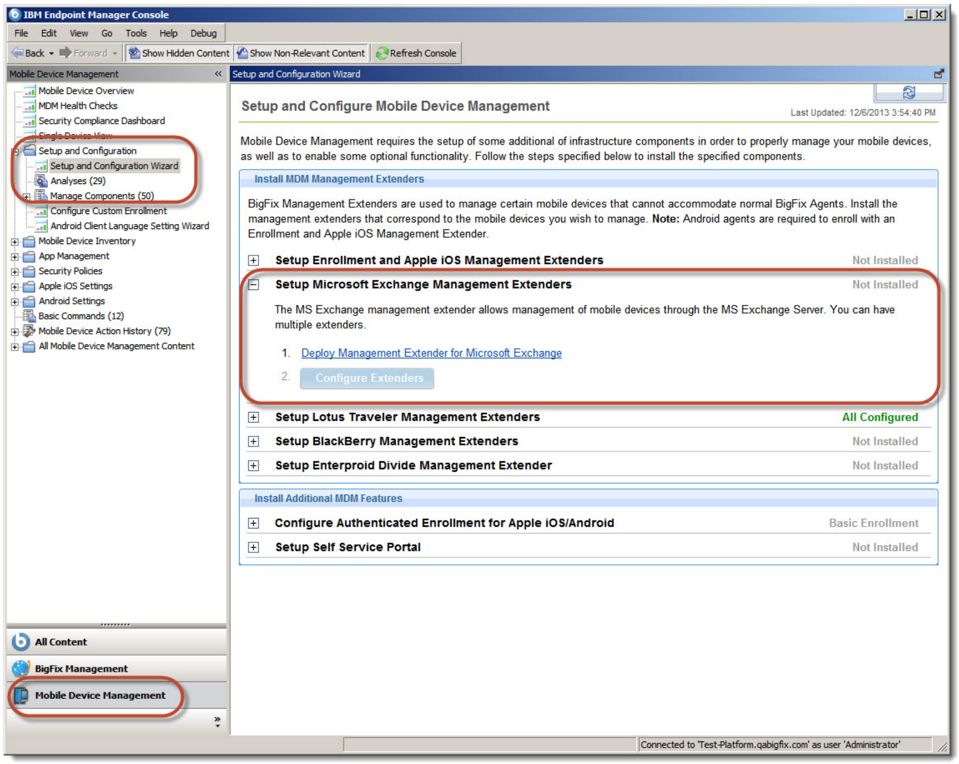
Microsoft Exchange Management Extender Deployment

The first step in setting up a Microsoft Exchange Management Extender is to deploy the Management Extender. Deployment is followed by configuration of the Management Extender.

Note: You cannot install the Exchange Management Extender on a Windows Server Core machine. Server Core computers lack PowerShell, Microsoft's task automation and configuration management framework.

To deploy a Microsoft Exchange Management Extender, complete the following steps:

1. Select the Mobile Device Management Site and navigate to **Setup and Configuration > Setup and Configuration Wizard**. The dashboard displays on the right. You must activate relevant analyses if prompted.
2. From the **Install MDM Management Extenders** field, expand the node **Setup Microsoft Exchange Management Extenders**.


IBM Endpoint Manager Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
Mobile Device Management
Mobile Device Overview
MDM Health Checks
Security Compliance Dashboard
Single Device View
Setup and Configuration
Setup and Configuration Wizard
Analyses (29)
Manage Components (50)
Configure Custom Enrollment
Android Client Language Setting Wizard
Mobile Device Inventory
App Management
Security Policies
Apple iOS Settings
Android Settings
Basic Commands (12)
Mobile Device Action History (79)
All Mobile Device Management Content
All Content
BigFix Management
Mobile Device Management
Setup and Configuration Wizard

Setup and Configure Mobile Device Management

Last Updated: 12/6/2013 3:54:40 PM

Mobile Device Management requires the setup of some additional of infrastructure components in order to properly manage your mobile devices, as well as to enable some optional functionality. Follow the steps specified below to install the specified components.

Install MDM Management Extenders

BigFix Management Extenders are used to manage certain mobile devices that cannot accommodate normal BigFix Agents. Install the management extenders that correspond to the mobile devices you wish to manage. **Note:** Android agents are required to enroll with an Enrollment and Apple iOS Management Extender.

Setup Enrollment and Apple iOS Management Extenders	Not Installed
Setup Microsoft Exchange Management Extenders	Not Installed

The MS Exchange management extender allows management of mobile devices through the MS Exchange Server. You can have multiple extenders.

1. Deploy Management Extender for Microsoft Exchange
2. Configure Extenders

Setup Lotus Traveler Management Extenders	All Configured
Setup BlackBerry Management Extenders	Not Installed
Setup Enterproid Divide Management Extender	Not Installed

Install Additional MDM Features

Configure Authenticated Enrollment for Apple iOS/Android	Basic Enrollment
Setup Self Service Portal	Not Installed

Connected to 'Test-Platform.qabigfix.com' as user 'Administrator'

3. Select option 1, **Deploy Management Extender for Microsoft Exchange**.
   a. With the fixlet task displayed, select **Take Action**.

b. Select the first option, **Click here to deploy...**.

c. Select the computer that you want to deploy the extender to and select **OK**.

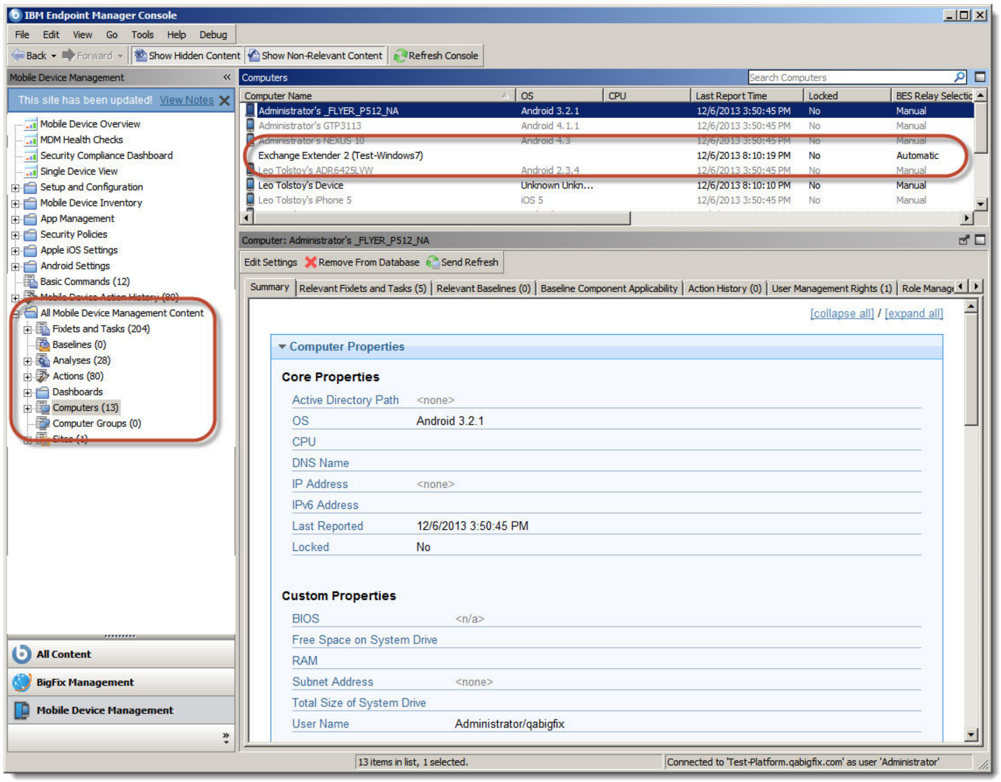
Note: You can install the Microsoft Exchange Management Extender on the same computer that contains your Microsoft Exchange Server.

d. Wait for the task to complete, which might take several minutes.

4. Return to the **Setup and Configuration Wizard** and ensure that the deployment was successful by looking for the **X Deployed** and **X of X Configured** notifications.

Note: When you run tasks, there might be a delay between a task that is listed as "Completed" and all elements of the tasks actually completing on the host computer, such as software installation.

After a Microsoft Exchange Management Extender is deployed, it is listed as an individual computer with the name `Exchange Extender <##> <Relay Name>` where `<##>` is the numerical number of the extender and `<Relay Name>` is the host name of the relay that the extender is installed on.



Computer Name	OS	CPU	Last Report Time	Locked	BES Relay Selectic
Administrator's _FLYER_P512_NA	Android 3.2.1		12/6/2013 3:50:45 PM	No	Manual
Administrator's GTP3113	Android 4.1.1		12/6/2013 3:50:45 PM	No	Manual
Administrator's NEXUS 10	Android 4.3		12/6/2013 3:50:45 PM	No	Manual
Exchange Extender 2 (Test-Windows7)			12/6/2013 8:10:19 PM	No	Automatic
Leo Tolstoy's ADR6425LVW	Android 2.3.4		12/6/2013 3:50:45 PM	No	Manual
Leo Tolstoy's Device	Unknown Unkn...		12/6/2013 8:10:10 PM	No	Manual
Leo Tolstoy's iPhone 5	iOS 5		12/6/2013 3:50:45 PM	No	Manual

Computer: Administrator's _FLYER_P512_NA

Computer Properties

Core Properties

Active Directory Path	<none>
OS	Android 3.2.1
CPU	
DNS Name	
IP Address	<none>
IPv6 Address	
Last Reported	12/6/2013 3:50:45 PM
Locked	No

Custom Properties

BIOS	<n/a>
Free Space on System Drive	
RAM	
Subnet Address	<none>
Total Size of System Drive	
User Name	Administrator/qabigfix

13 items in list, 1 selected.

Connected to 'Test-Platform.qabigfix.com' as user 'Administrator'

Microsoft Exchange Management Extender Configuration

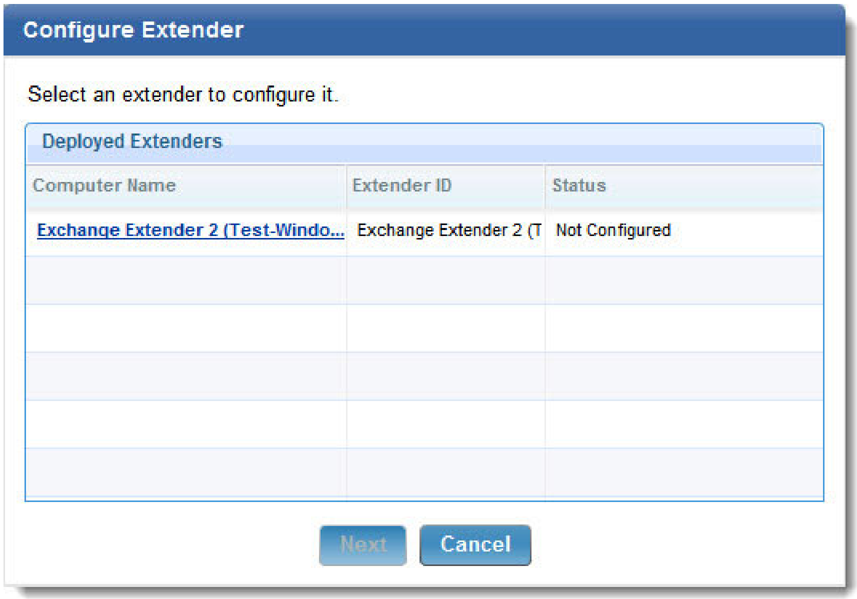
After a Microsoft Exchange Management Extender is deployed, it must be configured. During configuration, you point the Management Extender to an Exchange Server. Actions that are run in the IBM Endpoint Manager Console are directed to the Exchange Server, which passes the commands to devices.

Configuration requires the Exchange Server's Fully Qualified Domain Name (FQDN) and administrator credentials. In addition, after the Management Extender is configured through the IBM Endpoint Manager Console, several commands must be run manually on the computer that hosts the management extender.

To configure a Microsoft Exchange Management Extender, perform the following steps:

1. Navigate to **Mobile Device Management > Setup and Configuration > Setup and Configuration Wizard**.
2. Expand the **Setup Microsoft Exchange Management Extenders** node. This area displays how many of these specific Management Extenders are deployed and how many are configured.
3. Click **Configure Extenders**. In the displayed window, select the row that represents the extender that you want to configure and click **Next**.

Note: If you click the underlined computer name link, the console displays the properties of that computer. Click **Back** to return to the **Configure Extenders** window.



Configure Extender

Select an extender to configure it.

Deployed Extenders

Computer Name	Extender ID	Status
Exchange Extender 2 (Test-Windo...	Exchange Extender 2 (T	Not Configured

The **Configure Extender** window contains several fields that are related to your Microsoft Exchange Server. The settings for these fields must be provided by your administrator. The exception is the **Enrollment Tag for Multitenant Environment** check box, which is used only in multitenant environments.

To continue configuring the Management Extender, perform the following steps:

1. Complete the following fields that pertain to your Microsoft Exchange Server:

   Version

   Set the version of the Exchange Server this management extender is configured for. For more information about the requirements for each version of Exchange Server, see "Microsoft Exchange Configuration" on page 8.

   Refresh Interval

   Set the refresh interval in minutes. This setting dictates how often the Management Extender polls for updated information from the Exchange Server.

   Mailbox Filter

   You can set a mailbox filter with a "regular expression". This feature can be used to limit the management extender to interact with a subset of devices that are based on their mailbox.

Entering `^[A-F]` in this field limits the management extender to devices whose mailbox name begins with an A through F. Regular expressions are case-sensitive.

Use Exchange Management Tools
Depending on your Exchange Server version, this check box might be available. If this check box is not selected, WinRM is used. For more information, see "Microsoft Exchange Configuration" on page 8.

Server Name
If EMT is not used, enter the Exchange Server's fully qualified domain name.

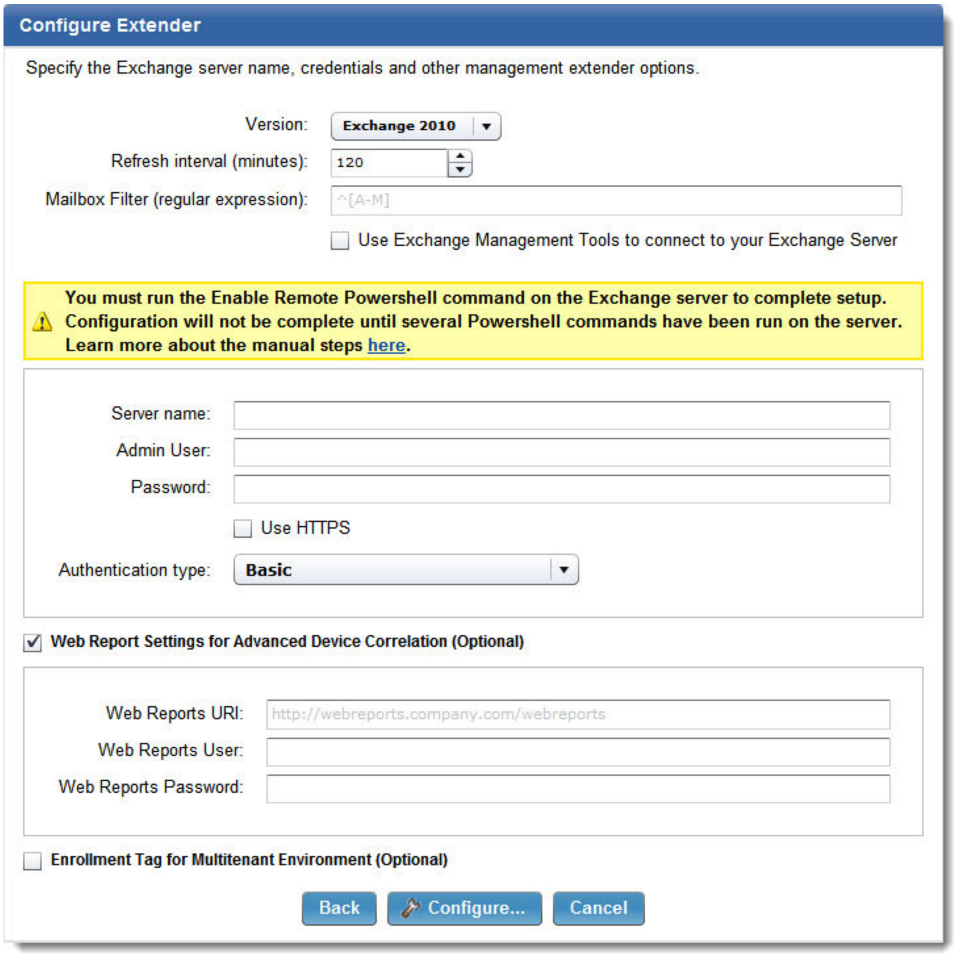
Admin User
If EMT is not used, enter the administrator user name.

Password
If EMT is not sued, enter the administrator password.

Use HTTPS
Select this check box to enable the use of HTTPS. If you are using an Office 365 Server, **HTTPS** must be selected.

Authentication Type
Select the authentication method to use for connection to the Exchange Server. Basic is the default type. Verify with your Exchange Server administrator to determine which **Authentication Type** is correct.

Web Report Settings For Advanced Device Correlation
This feature helps link device entries for individual devices. Devices that are managed by an Exchange Server and run an agent, such as the IBM Endpoint Manager Mobile Client, can have two device entries. This feature attempts to link these entries. This setting allows for greater management options. Enter your Web Reports URL, user name, and password. For more information about this feature, see http://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli%20Endpoint%20Manager/page/Enhanced%20Exchange%20Email%20functionality%20in%20TEM.



Configure Extender

Specify the Exchange server name, credentials and other management extender options.

Version: Exchange 2010

Refresh interval (minutes): 120

Mailbox Filter (regular expression): ^[A-M]

□ Use Exchange Management Tools to connect to your Exchange Server

⚠ You must run the Enable Remote Powershell command on the Exchange server to complete setup. Configuration will not be complete until several Powershell commands have been run on the server. Learn more about the manual steps here.

Server name:

Admin User:

Password:

□ Use HTTPS

Authentication type: Basic

☑ Web Report Settings for Advanced Device Correlation (Optional)

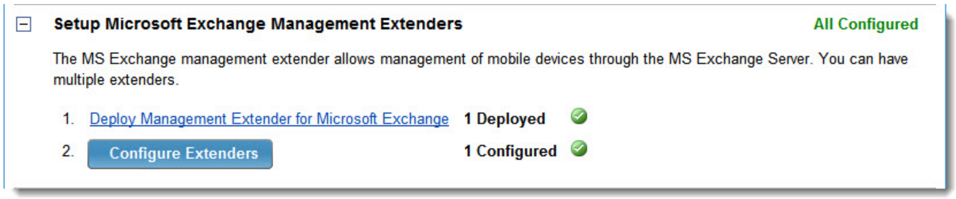
Web Reports URI: http://webreports.company.com/webreports

Web Reports User:

Web Reports Password:

□ Enrollment Tag for Multitenant Environment (Optional)

2. If you manage more than one Exchange Server, check **Enrollment Tag for Multitenant Environments** and enter a tag to assign to this Microsoft Exchange Management Extender. For more information about this option, see “Enrollment Tag for Multitenant Microsoft Exchange” on page 14.
3. Click **Configure**.
4. Select the appropriate Microsoft Exchange Management Extender in the **Computer Name** field and click **OK**.
5. Return to the **Setup and Configuration Wizard** and ensure that a green check mark is displayed to indicate that the Management Extender is configured. This process might take several minutes.



Setup Microsoft Exchange Management Extenders — All Configured

The MS Exchange management extender allows management of mobile devices through the MS Exchange Server. You can have multiple extenders.

1. Deploy Management Extender for Microsoft Exchange — 1 Deployed ✓
2. Configure Extenders — 1 Configured ✓

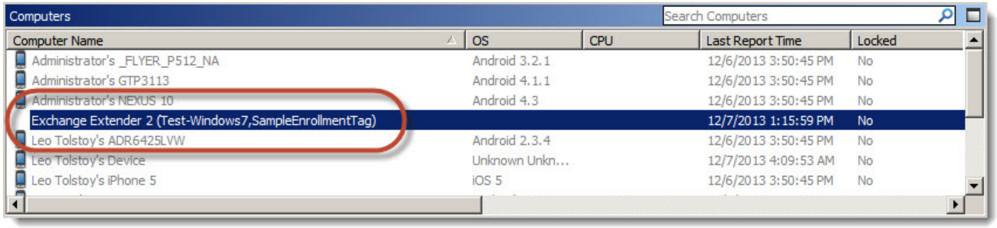
Note: After a Microsoft Exchange Management Extender is installed on a host, that host must be configured to trust the Exchange Server host. For more information, see “Management Extender Trusted Hosts” on page 14.

Enrollment Tag for Multitenant Microsoft Exchange

When you configure a Microsoft Exchange Management Extender, the **Enrollment Tag for Multitenant Environments** check box is used only if you manage multiple Exchange Servers. The Enrollment Tag is used to differentiate this Microsoft Exchange Management Extender from others that are configured for different Exchange Servers in your deployment. Using an Enrollment Tag enables a multitenant environment that allows IBM Endpoint Manager Console operators to target specific devices according to the Exchange Server that manages them.

Select **Enrollment Tag for Multitenant Environments** and enter an Enrollment Tag to assign that Enrollment Tag to the Microsoft Exchange Management Extender that you are configuring. You must deploy and configure a separate Microsoft Exchange Management Extender for each Exchange Server that you want to include in your deployment.

Note: When you configure an Enrollment Tag on a Microsoft Exchange Management Extender, that extender is renamed to include the enrollment tag as part of its name. The naming convention is `Exchange Extender <##> (<RELAY_NAME>, <ENROLLMENT TAG>)`.



Computer Name	OS	CPU	Last Report Time	Locked
Administrator's _FLYER_P512_NA	Android 3.2.1		12/6/2013 3:50:45 PM	No
Administrator's GTP3113	Android 4.1.1		12/6/2013 3:50:45 PM	No
Administrator's NEXUS 10	Android 4.3		12/6/2013 3:50:45 PM	No
Exchange Extender 2 (Test-Windows7,SampleEnrollmentTag)			12/7/2013 1:15:59 PM	No
Leo Tolstoy's ADR6425LVW	Android 2.3.4		12/6/2013 3:50:45 PM	No
Leo Tolstoy's Device	Unknown Unkn...		12/7/2013 4:09:53 AM	No
Leo Tolstoy's iPhone 5	iOS 5		12/6/2013 3:50:45 PM	No

Management Extender Trusted Hosts

The computer that hosts your Exchange Server must be listed as a trusted host on the computer that hosts your Microsoft Exchange Management Extender.

To add the Exchange Server to the trusted hosts of your Microsoft Exchange Management Extender, perform the following steps:

1. Open an administrator elevated command prompt on the computer that hosts your management extender.
2. Type the following command:
   ```
   set-item WSman:\localhost\Client\TrustedHosts –value "<your exchange server FQDN>"
   ```
3. Type the following command:
   ```
   Set-executionpolicy RemoteSigned
   ```

Lotus Traveler Management Extender

IBM Endpoint Manager for Mobile Devices can be used with Lotus Traveler Servers to manage devices. A Lotus Traveler Management Extender acts as the intermediate between IBM Endpoint Manager for Mobile Devices and your Lotus Traveler deployment.

IBM Endpoint Manager for Mobile Devices supports Lotus Traveler version 9.0 and below.

Management Extenders must first be deployed, which is the process of installing it on a computer. After a Lotus Traveler Management Extender is deployed, you must configure it to allow it to communicate with a Lotus Traveler Server in your network. Configuration requires administration details of your Lotus Traveler Server.

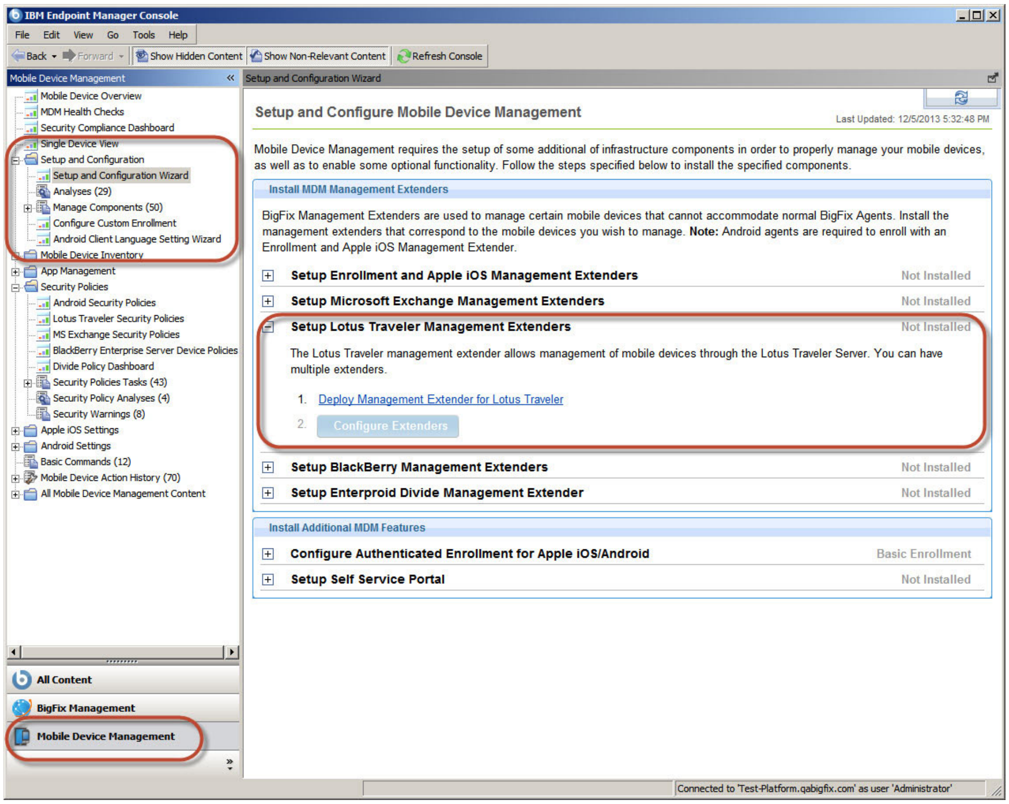
Lotus Traveler Management Extender Deployment

The first step in setting up a Lotus Traveler Management Extender is to deploy the Management Extender. Deployment is followed by configuration of the Management Extender.

To deploy a Lotus Traveler Management Extender, complete the following steps:

1. Select the Mobile Device Management Site and navigate to **Setup and Configuration** > **Setup and Configuration Wizard**. The dashboard displays on the right. You must activate relevant analyses if prompted.
2. From the **Install MDM Management Extenders** field, expand the node **Setup Lotus Traveler Management Extenders**.
3. Select option 1, **Deploy Management Extender for Lotus Traveler**.
   a. With the fixlet task displayed, select **Take Action**.
   b. Select the first option, **Click here to deploy...**.
   c. Select the computer that you want to deploy the extender to and select **OK**.
   d. Wait for the task to complete, which might take several minutes.
4. Return to the **Setup and Configuration Wizard** and ensure that the deployment was successful by looking for the **X Deployed** and **X of X Configured** notifications.

Note: When you run tasks, there might be a delay between a task that is listed as “Completed” and all elements of the tasks actually completing on the host computer, such as software installation.


IBM Endpoint Manager Console
File
Edit
View
Go
Tools
Help
Back
Forward
Show Hidden Content
Show Non-Relevant Content
Refresh Console
Mobile Device Management
Setup and Configuration Wizard
Mobile Device Overview
MDM Health Checks
Security Compliance Dashboard
Single Device View
Setup and Configuration
Setup and Configuration Wizard
Analyses (29)
Manage Components (50)
Configure Custom Enrollment
Android Client Language Setting Wizard
Mobile Device Inventory
App Management
Security Policies
Android Security Policies
Lotus Traveler Security Policies
MS Exchange Security Policies
BlackBerry Enterprise Server Device Policies
Divide Policy Dashboard
Security Policies Tasks (43)
Security Policy Analyses (4)
Security Warnings (8)
Apple iOS Settings
Android Settings
Basic Commands (12)
Mobile Device Action History (70)
All Mobile Device Management Content
All Content
BigFix Management
Mobile Device Management

Setup and Configure Mobile Device Management

Last Updated: 12/5/2013 5:32:48 PM

Mobile Device Management requires the setup of some additional of infrastructure components in order to properly manage your mobile devices, as well as to enable some optional functionality. Follow the steps specified below to install the specified components.

Install MDM Management Extenders

BigFix Management Extenders are used to manage certain mobile devices that cannot accommodate normal BigFix Agents. Install the management extenders that correspond to the mobile devices you wish to manage. **Note:** Android agents are required to enroll with an Enrollment and Apple iOS Management Extender.

⊞ **Setup Enrollment and Apple iOS Management Extenders**	Not Installed
⊞ **Setup Microsoft Exchange Management Extenders**	Not Installed
⊟ **Setup Lotus Traveler Management Extenders**	Not Installed

The Lotus Traveler management extender allows management of mobile devices through the Lotus Traveler Server. You can have multiple extenders.

1. Deploy Management Extender for Lotus Traveler
2. Configure Extenders

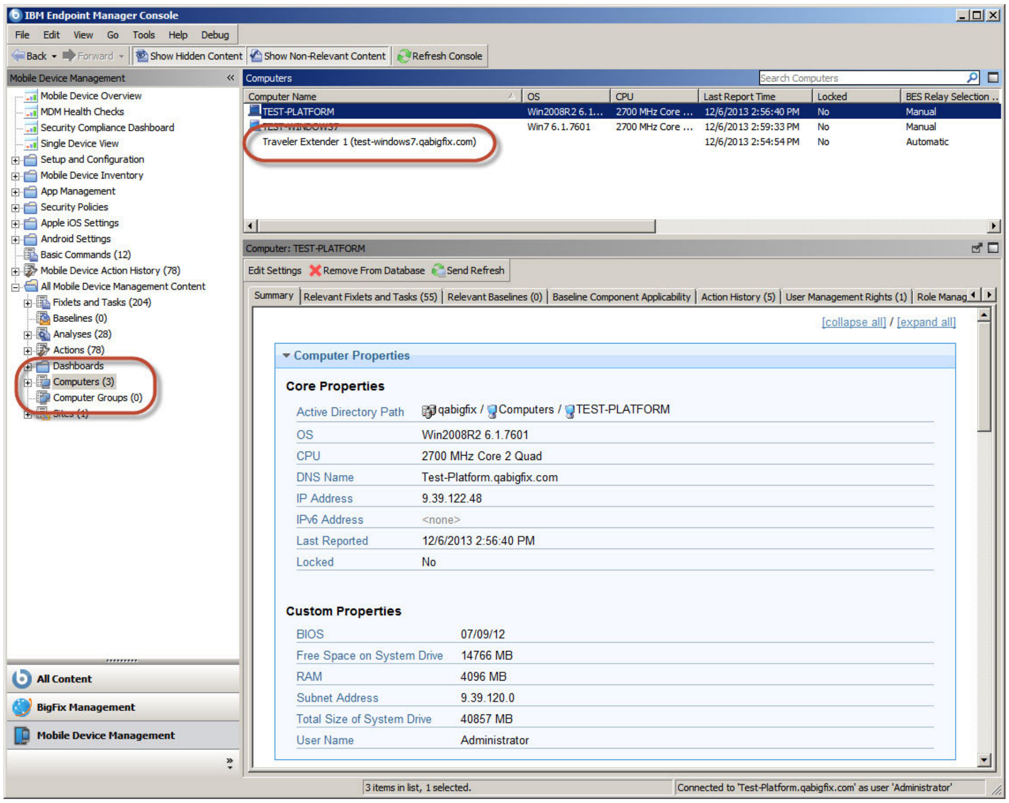
⊞ **Setup BlackBerry Management Extenders**	Not Installed
⊞ **Setup Enterproid Divide Management Extender**	Not Installed

Install Additional MDM Features

⊞ **Configure Authenticated Enrollment for Apple iOS/Android**	Basic Enrollment
⊞ **Setup Self Service Portal**	Not Installed

Connected to 'Test-Platform.qabigfix.com' as user 'Administrator'

After a Lotus Traveler Management Extender is deployed, it is listed as an individual computer with the name `Traveler Extender <##> <Relay Name>` where `<##>` is the numerical number of the extender and `<Relay Name>` is the host name of the relay that the extender is installed on.



Computer Name	OS	CPU	Last Report Time	Locked	BES Relay Selection ..
TEST-PLATFORM	Win2008R2 6.1...	2700 MHz Core ...	12/6/2013 2:56:40 PM	No	Manual
TEST-WINDOWS7	Win7 6.1.7601	2700 MHz Core ...	12/6/2013 2:59:33 PM	No	Manual
Traveler Extender 1 (test-windows7.qabigfix.com)			12/6/2013 2:54:54 PM	No	Automatic

Core Properties

Active Directory Path	qabigfix / Computers / TEST-PLATFORM
OS	Win2008R2 6.1.7601
CPU	2700 MHz Core 2 Quad
DNS Name	Test-Platform.qabigfix.com
IP Address	9.39.122.48
IPv6 Address	<none>
Last Reported	12/6/2013 2:56:40 PM
Locked	No

Custom Properties

BIOS	07/09/12
Free Space on System Drive	14766 MB
RAM	4096 MB
Subnet Address	9.39.120.0
Total Size of System Drive	40857 MB
User Name	Administrator

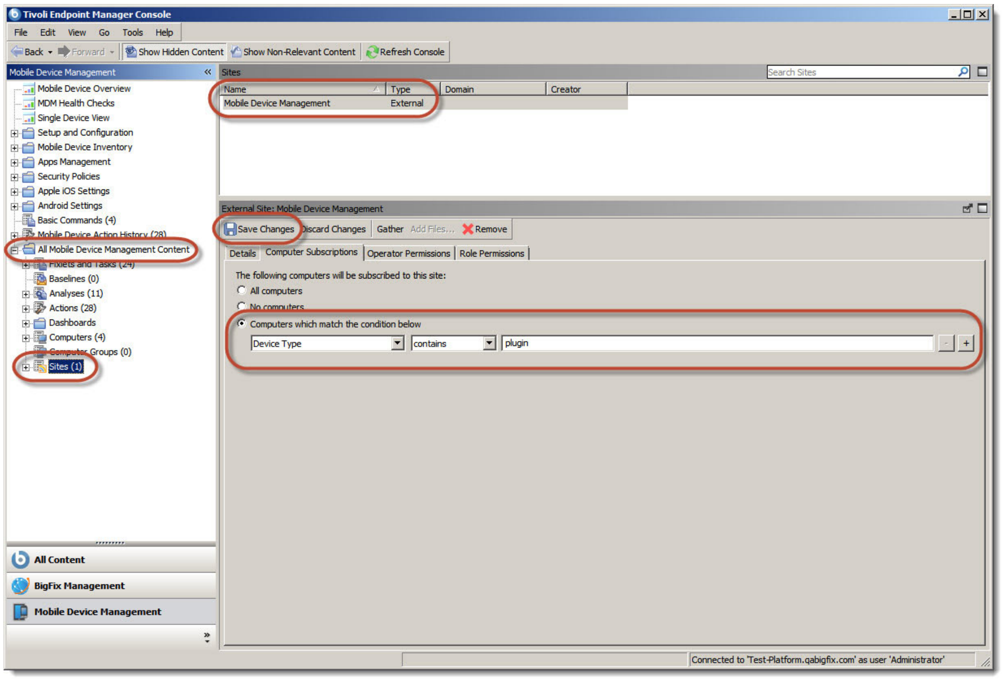
3 items in list, 1 selected.

Connected to 'Test-Platform.qabigfix.com' as user 'Administrator'

Subscribing a Management Extender to Mobile Device Management

Management Extenders must be subscribed to the Mobile Device Management Site to perform management functions. Ensure that new Management Extenders are subscribed to the Mobile Device Management Site by performing the following tasks:

1. Navigate to **Mobile Device Management > All Mobile Device Management Content > Sites**.
2. Select the **Mobile Device Management** Site.
3. Select the **Computer Subscriptions** tab.
   - If **All Computers** is selected, your deployment automatically subscribes new Management Extenders to the site; do not continue with these steps.
   - If you are subscribing sites by defining rules with **Computers which match the conditions below** selected, continue to the next step.
4. Create a rule by entering the following details for the rule:
   - `Device Type | contains | plugin`
5. Click **Save Changes** to save the new rules.



Name	Type	Domain	Creator
Mobile Device Management	External		

External Site: Mobile Device Management

The following computers will be subscribed to this site:

○ All computers

○ No computers

● Computers which match the condition below

Device Type | contains | plugin

Lotus Traveler Management Extender Configuration

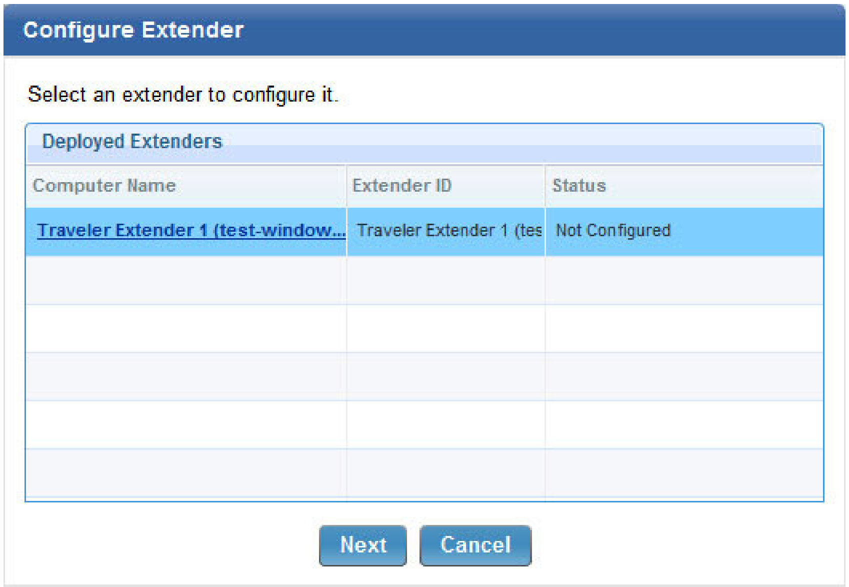
After a Lotus Traveler Management Extender is deployed, it must be configured. During configuration, you point the Management Extender to a Lotus Traveler Server. Actions that are run in the IBM Endpoint Manager Console are directed to the Lotus Traveler Server, which passes the commands to devices.

Configuration requires the server address and administrator credentials. Trusted certificates might also be required if SSL is used, depending on the type of authentication.

To configure a Lotus Traveler Management Extender, perform the following tasks:

1. Navigate to **Mobile Device Management > Setup and Configuration > Setup and Configuration Wizard**.
2. Expand the **Setup Lotus Notes Management Extenders** node. This area displays how many of these specific Management Extenders are deployed and how many are configured.
3. Click **Configure Extenders**. In the displayed window, select the row that represents the extender that you want to configure and click **Next**.

Note: If you click the underlined computer name link, the console displays the properties of that computer. Click **Back** to return to the **Configure Extenders** window.



Configure Extender

Select an extender to configure it.

Deployed Extenders

Computer Name	Extender ID	Status
Traveler Extender 1 (test-window...	Traveler Extender 1 (tes	Not Configured

The **Configure Extender** window contains several fields that are related to your Lotus Traveler Server. The settings for these fields must be provided by your administrator. The exception is the **Enrollment Tag for Multitenant Environment** check box, which is used only in multitenant environments.

To continue configuring the Management Extender, perform the following steps:

1. Complete the following fields that pertain to your Lotus Traveler Server:

   Refresh Interval
   Set the refresh interval in minutes. This field dictates how often IBM Endpoint Manager for Mobile Devices queries the Lotus Traveler server.

   Use Local Connection
   This feature is not currently supported.

   Server Name
   Enter the Lotus Traveler Server location.

   Remove Admin
   Enter the remote admin user name.

   Password
   Enter the remote admin password.

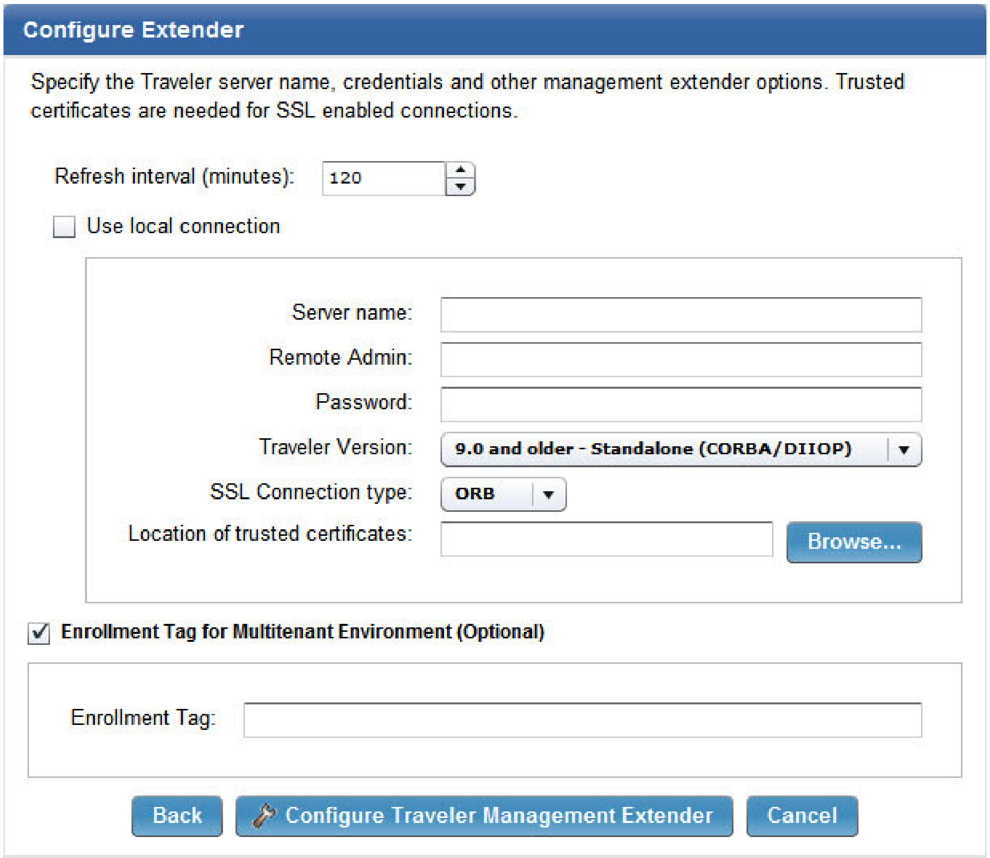
   Traveler Version
   Select the appropriate Lotus Traveler Server version.

   SSL Connection Type
   If you use SSL, select the appropriate protocol, **HTTPS**, **ORB**, or **Both**.

   Location of Trusted Certificates
   If the SSL type is **ORB** or **Both**, you must specify the location of your trusted certificate by selecting **Browse**.

2. If you manage more than one Lotus Traveler Server, check **Enrollment Tag for Multitenant Environments** and enter a tag to assign to this Lotus Traveler Management Extender. For more information about this option, see "Enrollment Tag for Multitenant Lotus Traveler" on page 19.
3. Click **Configure Traveler Management Extender**.
4. Select the appropriate Lotus Traveler Management Extender in the **Computer Name** field and click **OK**.

5. Return to the **Setup and Configuration Wizard** and ensure that a green check mark is displayed to indicate that the Management Extender is configured. This process might take several minutes.



Configure Extender

Specify the Traveler server name, credentials and other management extender options. Trusted certificates are needed for SSL enabled connections.

Refresh interval (minutes): 120

□ Use local connection

Server name:

Remote Admin:

Password:

Traveler Version: 9.0 and older - Standalone (CORBA/DIIOP)

SSL Connection type: ORB

Location of trusted certificates:

☑ Enrollment Tag for Multitenant Environment (Optional)

Enrollment Tag:

Enrollment Tag for Multitenant Lotus Traveler

When you configure a Lotus Traveler Management Extender, the **Enrollment Tag for Multitenant Environments** check box is used only if you manage multiple Lotus Traveler Servers. The Enrollment Tag is used to differentiate this Lotus Traveler Management Extender from others that are configured for different Lotus Traveler Servers in your deployment. Using an Enrollment Tag enables a multitenant environment that allows IBM Endpoint Manager Console operators to target specific devices according to the Lotus Traveler Server that manages them.

Select **Enrollment Tag for Multitenant Environments** and enter an Enrollment Tag to assign that Enrollment Tag to the Lotus Traveler Management Extender that you are configuring. You must deploy and configure a separate Lotus Traveler Management Extender for each Lotus Traveler Server that you want to include in your deployment.

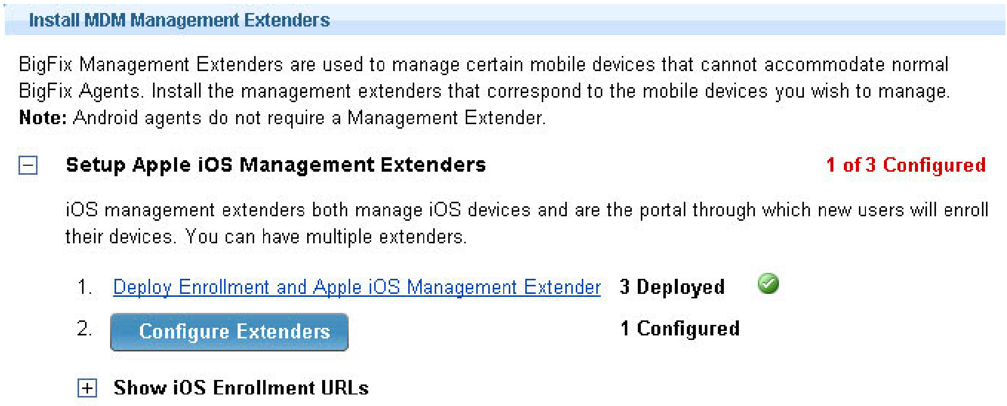
Note: When you configure an Enrollment Tag on a Lotus Traveler Management Extender, that extender is renamed to include the enrollment tag as part of its name. The naming convention is `Traveler Extender <##> <RELAY_NAME>, <ENROLLMENT TAG>`.

Management Extender for iOS

The Management Extender for Apple iOS must be installed on the Tivoli Endpoint Manager server or on a relay. The Management Extender Fixlet is only relevant for computers with a Tivoli Endpoint Manager agent and a relay or server installed.

Note: You need to have an Apple ID to complete this process with a valid email address. Create an account that has a non-personal email address to maintain access to the Push Certificate portal in the event of a departure.

Click the Setup and Configuration wizard from the navigation tree. In the Install MDM Management Extenders section of the wizard, click to expand the *Setup Apple iOS Management Extenders* header.



Install MDM Management Extenders

BigFix Management Extenders are used to manage certain mobile devices that cannot accommodate normal BigFix Agents. Install the management extenders that correspond to the mobile devices you wish to manage.
Note: Android agents do not require a Management Extender.

⊟ **Setup Apple iOS Management Extenders** **1 of 3 Configured**

iOS management extenders both manage iOS devices and are the portal through which new users will enroll their devices. You can have multiple extenders.

1. Deploy Enrollment and Apple iOS Management Extender **3 Deployed** ✓
2. Configure Extenders **1 Configured**

⊞ **Show iOS Enrollment URLs**

Setting up the Apple iOS Management Extender involves the following steps:

1. Deploying the Management Extender Fixlet
2. Obtaining a Certificate
3. Configuring the management Extender

Deploy the Management Extender Fixlet

Click the *Deploy Enrollment and Apple iOS Management Extender* link in the dashboard to deploy the Fixlet.

Back up your Apple Push Notification Private Key.

After you deploy the Fixlet, back up one of the files to a secure location. The file will likely be in the following path on your management extender:

C:\Program Files (x86)\BigFix Enterprise\Management Extender\MDM Provider\private

The file will be called *push_key.pem*.

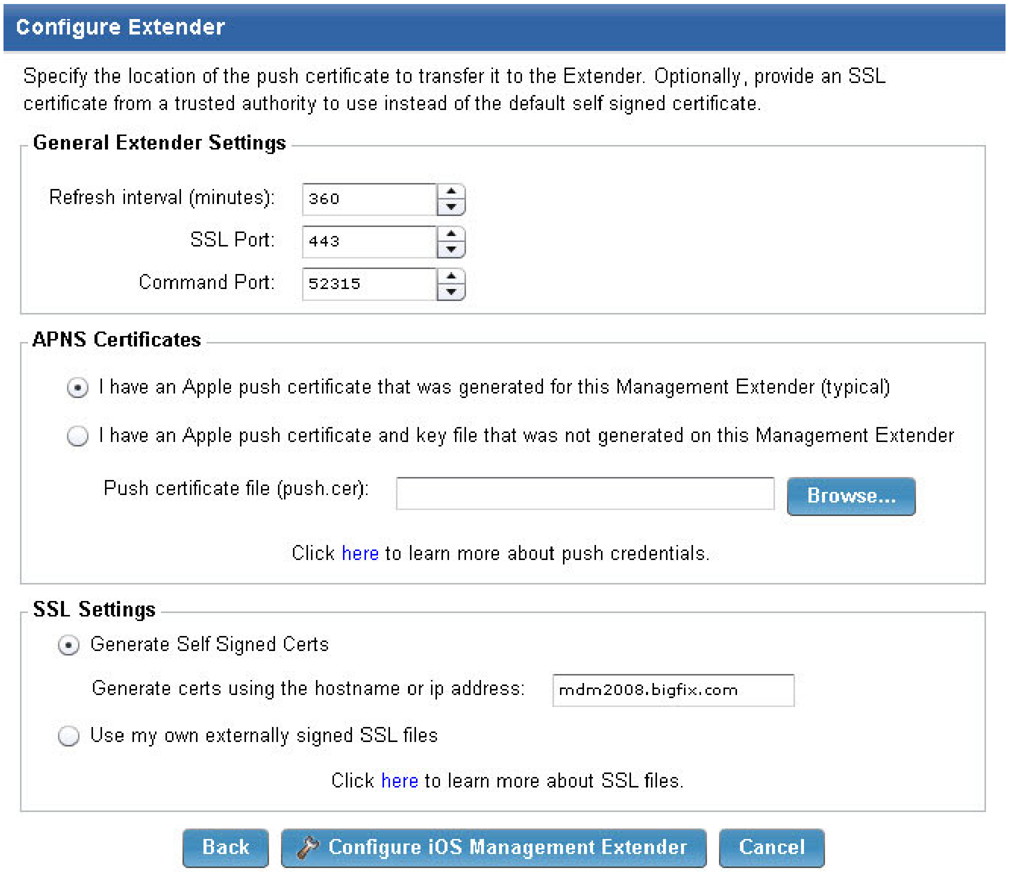
This key is related to your push certificate, in that if you want to deploy multiple extenders with the same certificate, you need to use the same key for each.

Obtain a Certificate

1. Download the CSR file that was generated during the installation by opening https://<dns or IP address>/csr. Save the file.
2. Send an email to iem-mdm-signup@wwpdl.vnet.ibm.com and attach the push.csr file. Type `MDM  APNS CSR <organization name>` in the subject line.
3. IBM will respond via email with a signed certificate request.
4. Go to https://identity.apple.com/pushcert/
5. Log in with your Apple ID. Consider using a non-personal ID so that other members of the organization can use the Apple ID in the future.
6. Select *Create Certificate*.
7. Read and agree to the Terms and Conditions.
8. Follow the instructions to upload the certificate file that you received from IBM.
9. Download the new signed push certificate "MDM_IBM Global Engineering Solutions_Certificate.pem" file.
10. If you open the .pem file in a text editor, you should see a base64 encoded certificate that starts with *BEGIN CERTIFICATE* and has several lines of random characters.
11. Rename the file to *push.cer* and create a backup copy.

Configure Extenders

Click *Configure Extenders* from dashboard.



Configure Extender

Specify the location of the push certificate to transfer it to the Extender. Optionally, provide an SSL certificate from a trusted authority to use instead of the default self signed certificate.

General Extender Settings

Refresh interval (minutes): 360

SSL Port: 443

Command Port: 52315

APNS Certificates

● I have an Apple push certificate that was generated for this Management Extender (typical)

○ I have an Apple push certificate and key file that was not generated on this Management Extender

Push certificate file (push.cer):

Click here to learn more about push credentials.

SSL Settings

● Generate Self Signed Certs

Generate certs using the hostname or ip address: mdm2008.bigfix.com

○ Use my own externally signed SSL files

Click here to learn more about SSL files.

In this window, select configuration options.

It is not common to change the port numbers. The refresh interval controls how often the management extender will send a refresh command to the agents. Using a more frequent refresh interval allows you to see updated information from your devices faster, but potentially causes more data and battery usage on the device.

Select the certificate that you received from Apple in the section above. If you have a push key file (because you generated the CSR and key pair manually), also include that in this section.

If you have an SSL key and certificate from a trusted source, you can include them in this section. This will replace the self-signed SSL certificate and prevent the SSL warnings on the devices.

Your Management Extender for Apple iOS is now ready to manage iOS devices (listening on the port you specified in the previous step). Port 443 is the default port. You can test it by opening your browser and visiting https://<dns or IP address>.

Note: The iOS Management Extender requires direct connection to the Apple Push Notification Server. This interaction occurs over TCP/IP and cannot be proxied via HTTP proxies.

BlackBerry Management Extenders

BlackBerry Management Extenders are components within a Mobile Device Management deployment that manage a subset of BlackBerry devices. BlackBerry devices that run BlackBerry OS versions 4.5, 4.6, 5.0, 6.0, and 7.0 are administered by one or more BlackBerry Enterprise Servers. BlackBerry Management Extenders allow communication between the IBM Endpoint Manager Server and your network's BlackBerry Enterprise Servers. One BlackBerry Management Extender must be deployed and configured for each BlackBerry Enterprise Server in your deployment.

BlackBerry Devices that run BlackBerry 10 or PlayBook are not managed by BlackBerry Management Extenders. Instead, these devices communicate through ActiveSync and are managed by Microsoft Exchange Management Extenders. If your network does not include a BlackBerry Enterprise Server version 4 or 5, then a BlackBerry Management Extender is not needed in your Mobile Device Management deployment.

Management Extenders must first be deployed, which is the process of installing it on a computer. After a BlackBerry Management Extender is deployed, you must configure it to allow it to communicate with a BlackBerry Enterprise Server in your network.

Deploying a BlackBerry Management Extender

To deploy a BlackBerry Management Extender, complete the following steps:

1. Select the Mobile Device Management Site and navigate to **Setup and Configuration > Setup and Configuration Wizard**. The dashboard displays on the right. You must activate relevant analyses if prompted.
2. From the **Install MDM Management Extenders** field, expand the node **Setup BlackBerry Management Extenders**.
3. Select option 1, **Deploy Management Extender for BlackBerry Enterprise Server**.

a. With the Fixlet Task displayed, select **Take Action**.

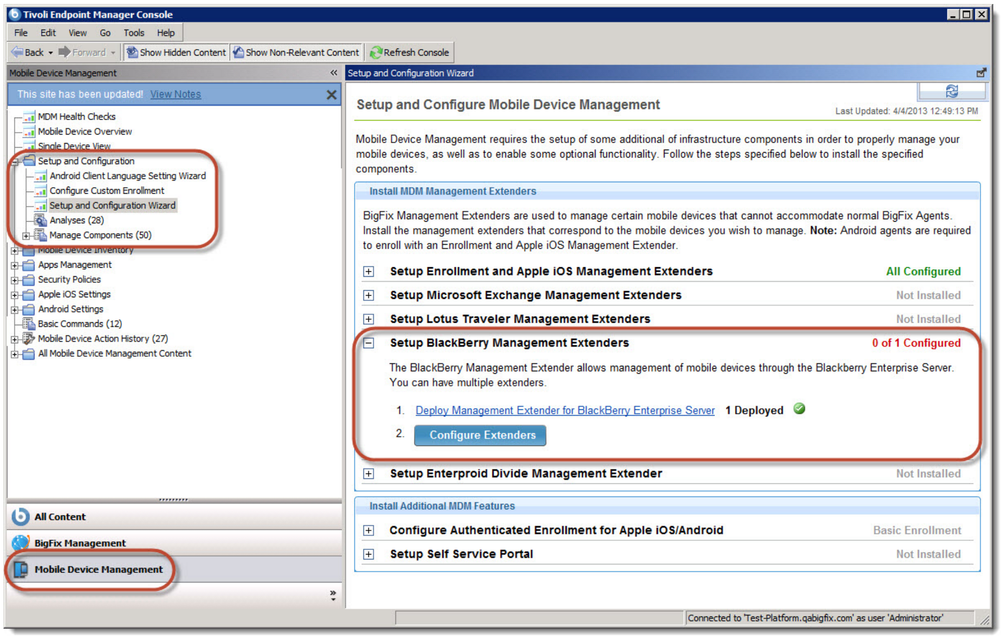
b. Select the first option, **Click here to deploy...**.

c. Select the computer that you want to deploy the extender to and press **OK**.

d. Wait for the task to complete, which might take several minutes.

4. Return to the **Setup and Configuration Wizard** and ensure that the deployment was successful by looking for the **X Deployed** and **X of X Configured** notifications.

Note: When you run tasks, there might be a delay between a task that is listed as "Completed" and all elements of the tasks actually completing on the host computer, such as software installation.



Setup and Configure Mobile Device Management

Last Updated: 4/4/2013 12:49:13 PM

Mobile Device Management requires the setup of some additional of infrastructure components in order to properly manage your mobile devices, as well as to enable some optional functionality. Follow the steps specified below to install the specified components.

Install MDM Management Extenders

BigFix Management Extenders are used to manage certain mobile devices that cannot accommodate normal BigFix Agents. Install the management extenders that correspond to the mobile devices you wish to manage. **Note:** Android agents are required to enroll with an Enrollment and Apple iOS Management Extender.

⊞ **Setup Enrollment and Apple iOS Management Extenders**	All Configured
⊞ **Setup Microsoft Exchange Management Extenders**	Not Installed
⊞ **Setup Lotus Traveler Management Extenders**	Not Installed
⊟ **Setup BlackBerry Management Extenders**	0 of 1 Configured

The BlackBerry Management Extender allows management of mobile devices through the Blackberry Enterprise Server. You can have multiple extenders.

1. Deploy Management Extender for BlackBerry Enterprise Server **1 Deployed** ✓
2. Configure Extenders

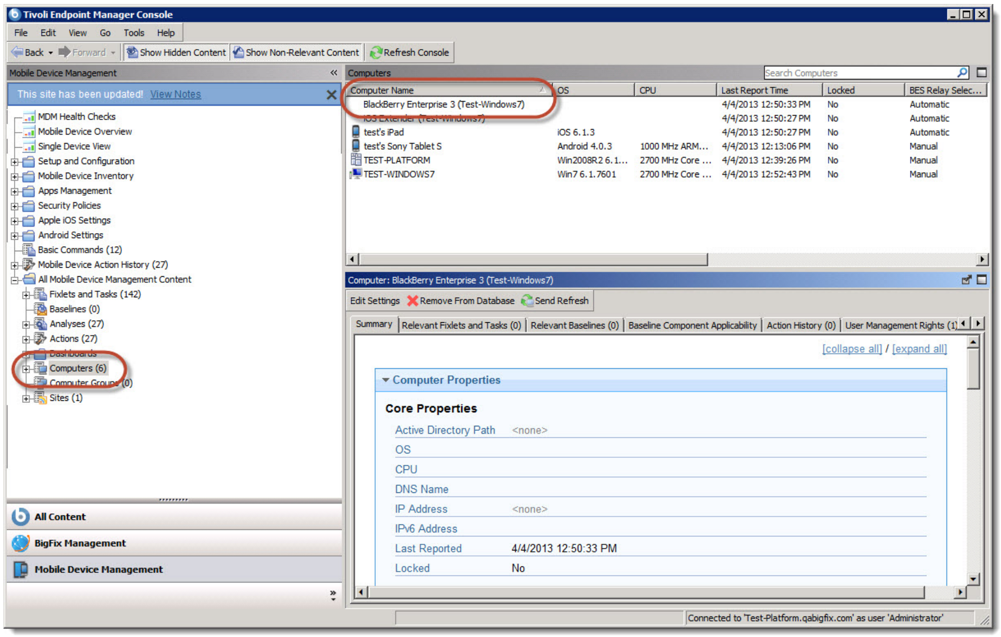
⊞ **Setup Enterproid Divide Management Extender**	Not Installed

Install Additional MDM Features

⊞ **Configure Authenticated Enrollment for Apple iOS/Android**	Basic Enrollment
⊞ **Setup Self Service Portal**	Not Installed

Connected to 'Test-Platform.qabigfix.com' as user 'Administrator'

After a BlackBerry Management Extender is deployed, it is listed as an individual computer with the name `BlackBerry Enterprise <##> <Relay Name>` where `<##>` is the numerical number of the extender and `<Relay Name>` is the hostname of the relay that the extender is installed on. This behavior is different from other management extenders, and allows BlackBerry Management Extenders to be multitenant-capable without further configuration.



Computer Name	OS	CPU	Last Report Time	Locked	BES Relay Selec...
BlackBerry Enterprise 3 (Test-Windows7)			4/4/2013 12:50:33 PM	No	Automatic
iOS Extender (Test-Windows7)			4/4/2013 12:50:27 PM	No	Automatic
test's iPad	iOS 6.1.3		4/4/2013 12:50:27 PM	No	Automatic
test's Sony Tablet S	Android 4.0.3	1000 MHz ARM...	4/4/2013 12:13:06 PM	No	Manual
TEST-PLATFORM	Win2008R2 6.1...	2700 MHz Core ...	4/4/2013 12:39:26 PM	No	Manual
TEST-WINDOWS7	Win7 6.1.7601	2700 MHz Core ...	4/4/2013 12:52:43 PM	No	Manual

Computer: BlackBerry Enterprise 3 (Test-Windows7)

Edit Settings Remove From Database Send Refresh
Summary | Relevant Fixlets and Tasks (0) | Relevant Baselines (0) | Baseline Component Applicability | Action History (0) | User Management Rights (1)
[collapse all] / [expand all]
Computer Properties

Core Properties

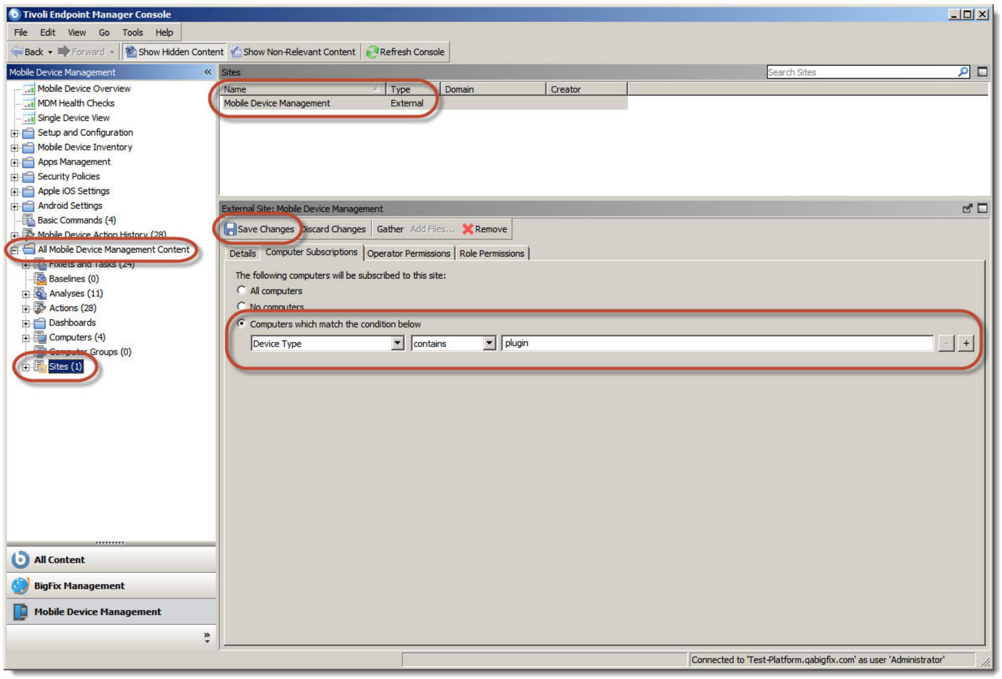
Active Directory Path	<none>
OS	
CPU	
DNS Name	
IP Address	<none>
IPv6 Address	
Last Reported	4/4/2013 12:50:33 PM
Locked	No

Connected to 'Test-Platform.qabigfix.com' as user 'Administrator'

Subscribing a Management Extender to Mobile Device Management

Management Extenders must be subscribed to the Mobile Device Management Site to perform management functions. Ensure that new Management Extenders are subscribed to the Mobile Device Management Site by performing the following tasks:

1. Navigate to **Mobile Device Management** > **All Mobile Device Management Content** > **Sites**.
2. Select the **Mobile Device Management** Site.
3. Select the **Computer Subscriptions** tab.
   - If **All Computers** is selected, your deployment automatically subscribes new Management Extenders to the site; do not continue with these steps.
   - If you are subscribing sites by defining rules with **Computers which match the conditions below** selected, continue to the next step.
4. Create a rule by entering the following details for the rule:
   - `Device Type | contains | plugin`
5. Click **Save Changes** to save the new rules.



Name	Type	Domain	Creator
Mobile Device Management	External		

The following computers will be subscribed to this site:

○ All computers

○ No computers

● Computers which match the condition below

Device Type | contains | plugin

Connected to 'Test-Platform.qabigfix.com' as user 'Administrator'

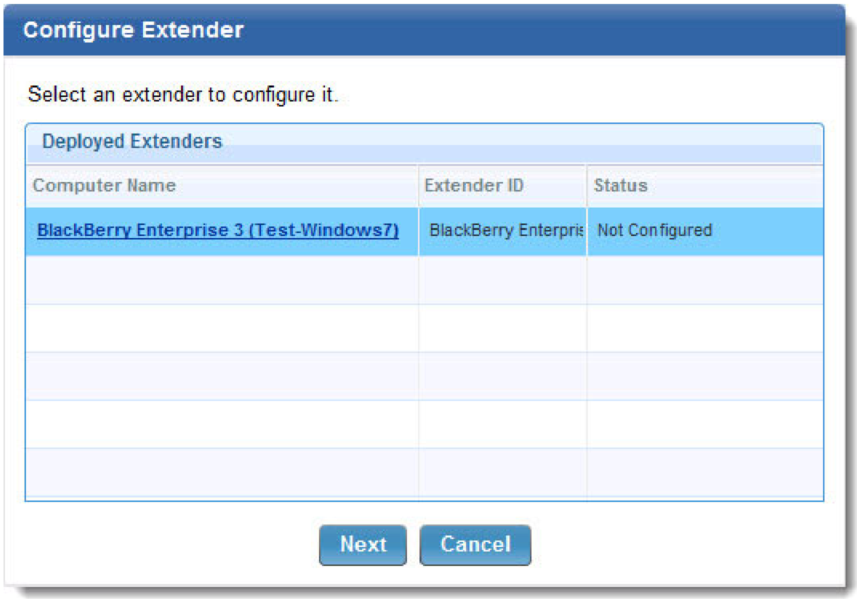
Configuring a BlackBerry Management Extender

After a BlackBerry Management Extender is deployed, it must be configured. Configuration requires settings from your BlackBerry Enterprise Server administrator. During configuration, you point the Management Extender to a BlackBerry Enterprise Server. Actions run in the IBM Endpoint Manager Console are directed to the BlackBerry Enterprise Server, which passes the commands to BlackBerry devices managed by the BlackBerry Enterprise Server.

To configure a BlackBerry Management Extender, perform the following tasks:

1. Navigate to **Mobile Device Management > Setup and Configuration > Setup and Configuration Wizard**.
2. Expand the **Setup BlackBerry Management Extenders** node. This area displays how many of these specific Management Extenders are deployed and how many are configured.
3. Click **Configure Extenders**. In the displayed window, select the row that represents the extender that you want to configure and click **Next**.

Note: If you click the underlined computer name link, the console displays the properties of that computer. Click **Back** to return to the **Configure Extenders** window.



Configure Extender

Select an extender to configure it.

Deployed Extenders

Computer Name	Extender ID	Status
BlackBerry Enterprise 3 (Test-Windows7)	BlackBerry Enterpris	Not Configured

The **Configure Extender** window contains several fields that are related to your BlackBerry Enterprise Server deployment. The settings for these fields must be provided by your BlackBerry administrator. The exception is the **Enrollment Tag for Multitenant Environment** check box, which is used only in multitenant environments.

To continue configuring the Management Extender, perform the following steps:

1. Complete the following fields that pertain to your BlackBerry Enterprise Server:

   Login Method
   Choose the appropriate login method from the drop-down list. The appropriate setting is determined by your BlackBerry Enterprise Server deployment.

   Server Name
   Enter the hostname of the BlackBerry Enterprise Server that you want to associate with this BlackBerry Management Extender.

   Remote Admin
   Enter the username of the administrator account that is used to access the BlackBerry Enterprise Server that is specified in the **Server Name** field.

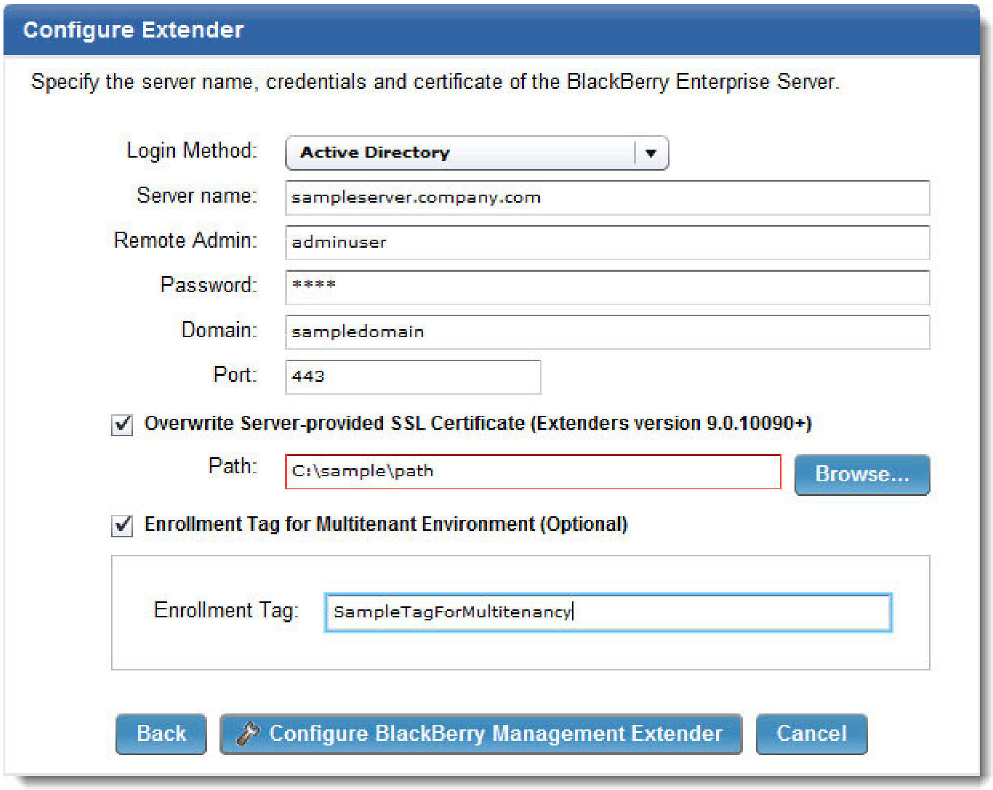
   Password
   The password for the administrator account that is specified in the **Remote Admin** field.

   Domain
   This field is present only if "Active Directory" is the chosen Login Method. Enter the domain for the BlackBerry Enterprise Server.

   Port The port that is used to communicate to the BlackBerry Enterprise Server.

   Overwrite Server-provided SSL Certificate
   By default, the configuration process imports the SSL Certificate for the BlackBerry Enterprise Server. If this option is checked, you can manually provide the appropriate SSL Certificate by entering the file's path name.

2. If you manage more than one BlackBerry Enterprise Server, check **Enrollment Tag for Multitenant Environments** and enter a tag to assign to this BlackBerry Management Extender. For more information about this option, see "Enrollment Tag for Multitenant Environments."
3. Click **Configure BlackBerry Management Extender**.
4. Select the appropriate BlackBerry Management Extender in the **Computer Name** field and click **OK**.
5. Return to the **Setup and Configuration Wizard** and ensure that a green check mark is displayed to indicate that the Management Extender is configured. This process might take several minutes.



Configure Extender

Specify the server name, credentials and certificate of the BlackBerry Enterprise Server.

Login Method: Active Directory

Server name: sampleserver.company.com

Remote Admin: adminuser

Password: ****

Domain: sampledomain

Port: 443

☑ Overwrite Server-provided SSL Certificate (Extenders version 9.0.10090+)

Path: C:\sample\path

☑ Enrollment Tag for Multitenant Environment (Optional)

Enrollment Tag: SampleTagForMultitenancy

Enrollment Tag for Multitenant Environments

When you configure a BlackBerry Management Extender, the **Enrollment Tag for Multitenant Environments** check box is used only if you manage multiple BlackBerry Enterprise Servers. The Enrollment Tag is used to differentiate this BlackBerry Management Extender from others that are configured for different BlackBerry Enterprise Servers in your network. Using an Enrollment Tag enables a multitenant environment that allows IBM Endpoint Manager Console operators to target specific devices according to the BlackBerry Enterprise Server that manages them.

Select **Enrollment Tag for Multitenant Environments** and enter an Enrollment Tag to assign that Enrollment Tag to the BlackBerry Management Extender that you are configuring. You must deploy and configure a separate BlackBerry Management Extender for each BlackBerry Enterprise Server that you want to include in your deployment.

Note: When you configure an Enrollment Tag on a BlackBerry Management Extender, that extender is renamed to include the enrollment tag as part of its name. The naming convention is `BlackBerry Enterprise <##> <RELAY_NAME>, <ENROLLMENT TAG>`.

iOS App Setup

To set the mobile client on your iPhone, use the following steps:

1. From your iPhone, open the App Store.
2. Select *Search* and search for *IBM Mobile.*
3. Select the *IBM Endpoint Manager Mobile Client.*
4. Select *Free* and then *Install App.*
5. At the *Sign In* screen, sign in using your existing Apple ID or create a new Apple ID. This will install the mobile client to your device.
6. Launch the app from your device.
7. Enter server address, work email, and device ownership fields.
8. Select *Enroll.*

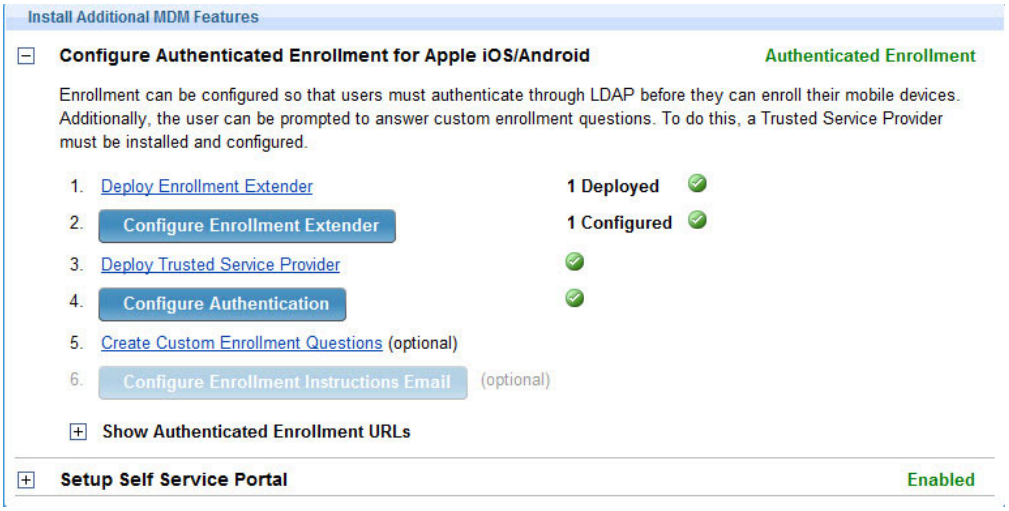
Authenticated Enrollment

By default, devices can be managed by MDM without any authentication. As a new feature, you can now restrict access to your MDM deployment to only authenticated users who log in with a username and password. Authenticated enrollment is an optional feature.

To enable authenticated enrollment, open the Setup and Configuration wizard from the navigation tree, and scroll down to the Configure Authenticated Enrollment section.

Configuring authenticated enrollment involves the following steps:

1. Deploy Enrollment Extender.
2. Configure Enrollment Extender.
3. Deploy Trusted Service Provider.
4. Configure Authentication.
5. (Optional) Create Custom Enrollment Questions.
6. (Optional) Configure Enrollment Instructions Email.



Install Additional MDM Features

⊟ **Configure Authenticated Enrollment for Apple iOS/Android** — Authenticated Enrollment

Enrollment can be configured so that users must authenticate through LDAP before they can enroll their mobile devices. Additionally, the user can be prompted to answer custom enrollment questions. To do this, a Trusted Service Provider must be installed and configured.

1. Deploy Enrollment Extender — 1 Deployed ✓
2. Configure Enrollment Extender — 1 Configured ✓
3. Deploy Trusted Service Provider ✓
4. Configure Authentication ✓
5. Create Custom Enrollment Questions (optional)
6. Configure Enrollment Instructions Email (optional)

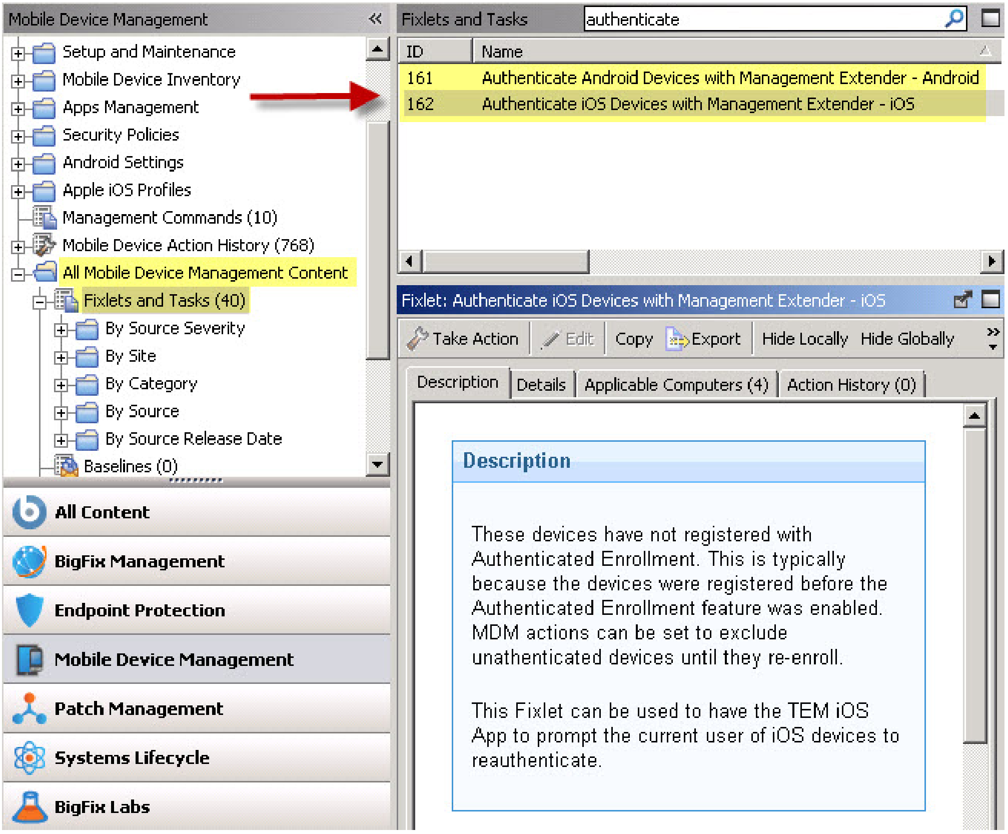
⊞ Show Authenticated Enrollment URLs

⊞ **Setup Self Service Portal** — Enabled

Click each step and follow the prompts to complete the process.

Note: A brief delay follows the completion of each step.

After you setup your enrollment server for authentication, use two enrollment Fixlets to initiate an action to remind users to authenticate or re-authenticate their device. To access these Fixlets, click the All Mobile Device Management Content node at the bottom of the MDM navigation tree. Click to expand the content, then click Fixlets and Tasks and browse to locate Fixlet numbers 161 and 162.



Search: authenticate

ID	Name
161	Authenticate Android Devices with Management Extender - Android
162	Authenticate iOS Devices with Management Extender - iOS

Fixlet: Authenticate iOS Devices with Management Extender - iOS

Description

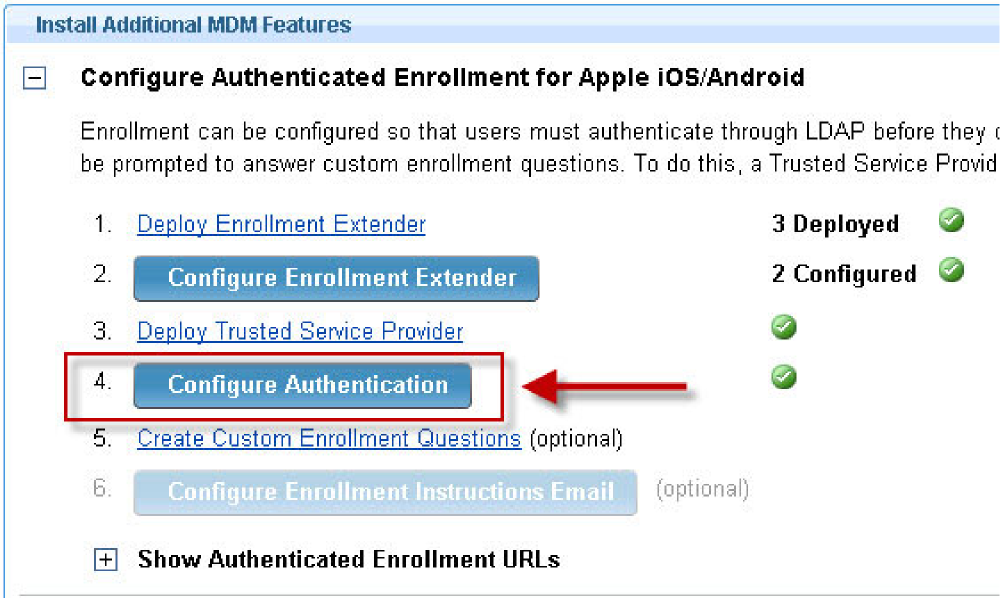
These devices have not registered with Authenticated Enrollment. This is typically because the devices were registered before the Authenticated Enrollment feature was enabled. MDM actions can be set to exclude unathenticated devices until they re-enroll.

This Fixlet can be used to have the TEM iOS App to prompt the current user of iOS devices to reauthenticate.

Restrict Device Enrollment by LDAP Group

Endpoint Manager for Mobile Devices now adds the ability to restrict device enrollment to a specific set of LDAP groups using the Trusted Service Provider (TSP). This optional feature allows system administrators to select only certain groups that are allowed to authenticate into the management extenders. The feature provides additional security and control.

When configuring Authenticated Enrollment on a deployed TSP, enter the LDAP settings. Click the Setup and Configuration Wizard from the navigation tree. Under the Install Additional MDM Features, click Configure Authentication.



Install Additional MDM Features

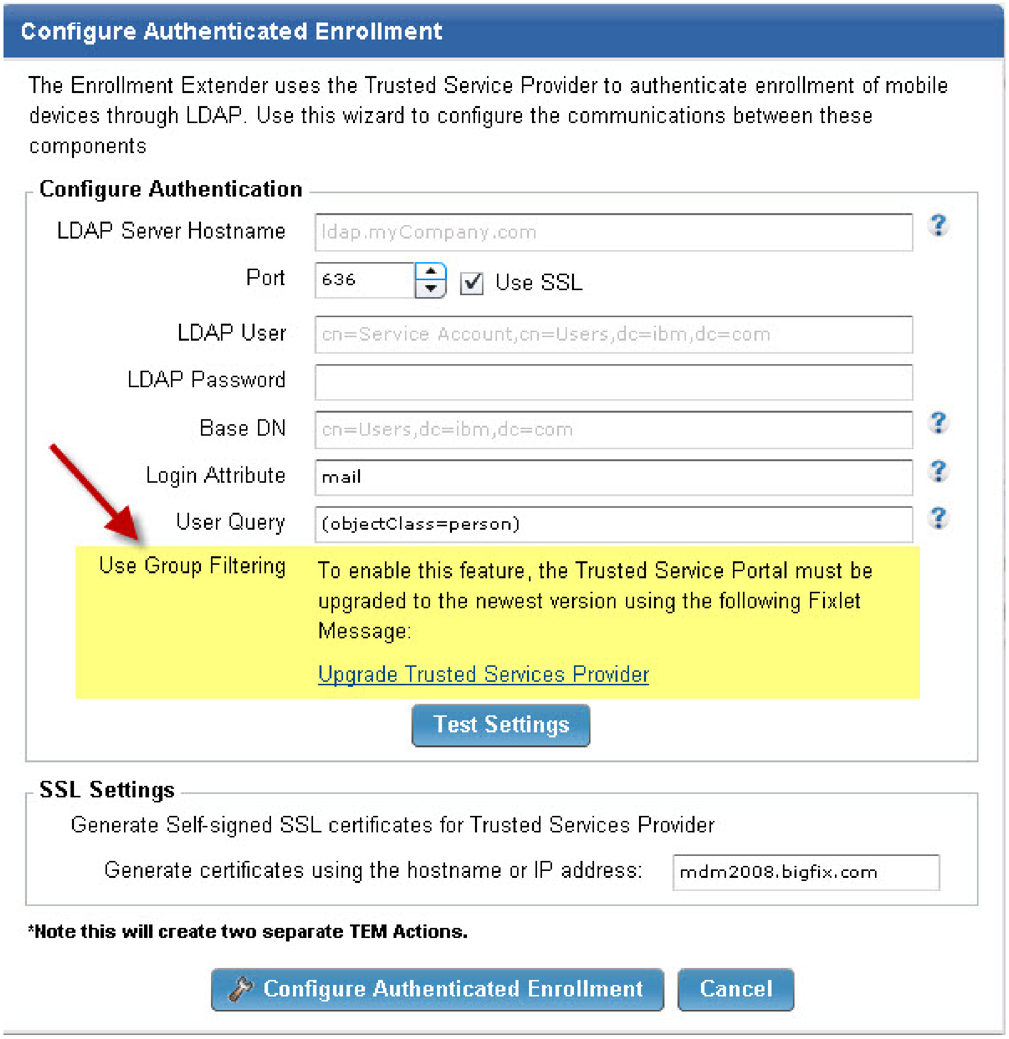
⊟ Configure Authenticated Enrollment for Apple iOS/Android

Enrollment can be configured so that users must authenticate through LDAP before they c be prompted to answer custom enrollment questions. To do this, a Trusted Service Provid

1. Deploy Enrollment Extender — 3 Deployed ✓
2. Configure Enrollment Extender — 2 Configured ✓
3. Deploy Trusted Service Provider ✓
4. Configure Authentication ✓
5. Create Custom Enrollment Questions (optional)
6. Configure Enrollment Instructions Email (optional)

⊞ Show Authenticated Enrollment URLs

If you have a TSP deployed, you can use the Upgrade Trusted Services Provider link to upgrade your TSP to the latest version.



Configure Authenticated Enrollment

The Enrollment Extender uses the Trusted Service Provider to authenticate enrollment of mobile devices through LDAP. Use this wizard to configure the communications between these components

Configure Authentication

LDAP Server Hostname: ldap.myCompany.com

Port: 636 ☑ Use SSL

LDAP User: cn=Service Account,cn=Users,dc=ibm,dc=com

LDAP Password:

Base DN: cn=Users,dc=ibm,dc=com

Login Attribute: mail

User Query: (objectClass=person)

Use Group Filtering: To enable this feature, the Trusted Service Portal must be upgraded to the newest version using the following Fixlet Message:

Upgrade Trusted Services Provider

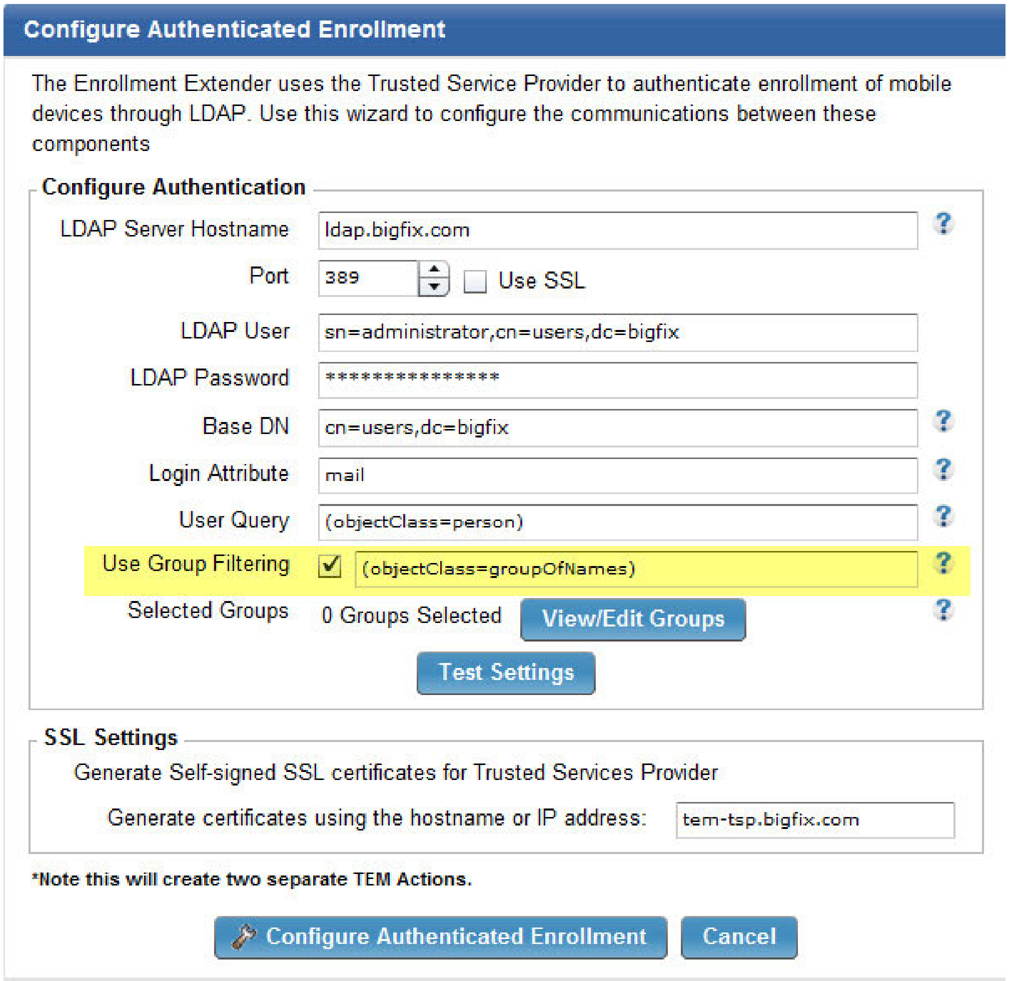
SSL Settings

Generate Self-signed SSL certificates for Trusted Services Provider

Generate certificates using the hostname or IP address: mdm2008.bigfix.com

*Note this will create two separate TEM Actions.

After you have upgraded your TSP, click the checkbox next to Use Group Filtering to enable the View / Edit Groups button.



Configure Authenticated Enrollment

The Enrollment Extender uses the Trusted Service Provider to authenticate enrollment of mobile devices through LDAP. Use this wizard to configure the communications between these components

Configure Authentication

LDAP Server Hostname: ldap.bigfix.com

Port: 389 □ Use SSL

LDAP User: sn=administrator,cn=users,dc=bigfix

LDAP Password: ***************

Base DN: cn=users,dc=bigfix

Login Attribute: mail

User Query: (objectClass=person)

Use Group Filtering: ☑ (objectClass=groupOfNames)

Selected Groups: 0 Groups Selected

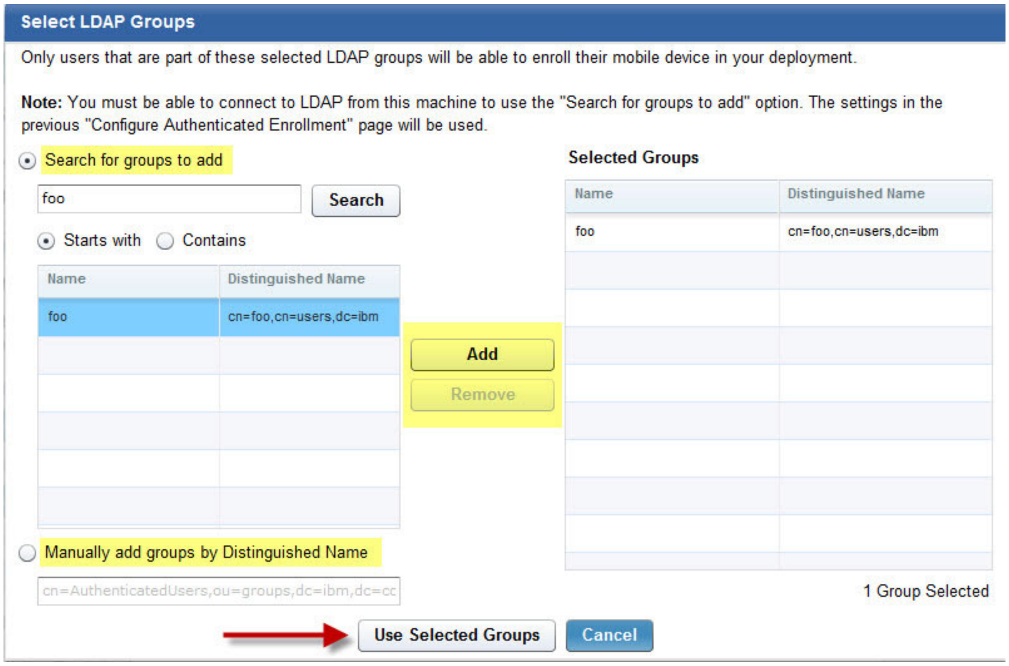
SSL Settings

Generate Self-signed SSL certificates for Trusted Services Provider

Generate certificates using the hostname or IP address: tem-tsp.bigfix.com

*Note this will create two separate TEM Actions.

Next, click View/Edit Groups to open a new "Select LDAP Groups" dialog, where you can search for and select existing LDAP groups or manually enter the distinguished name of LDAP groups. Use the manual option if you cannot establish a connection to the LDAP server.



Select LDAP Groups

Only users that are part of these selected LDAP groups will be able to enroll their mobile device in your deployment.

Note: You must be able to connect to LDAP from this machine to use the "Search for groups to add" option. The settings in the previous "Configure Authenticated Enrollment" page will be used.

● Search for groups to add

foo

● Starts with ○ Contains

Name	Distinguished Name
foo	cn=foo,cn=users,dc=ibm

Selected Groups

Name	Distinguished Name
foo	cn=foo,cn=users,dc=ibm

○ Manually add groups by Distinguished Name

cn=AuthenticatedUsers,ou=groups,dc=ibm,dc=cc

1 Group Selected

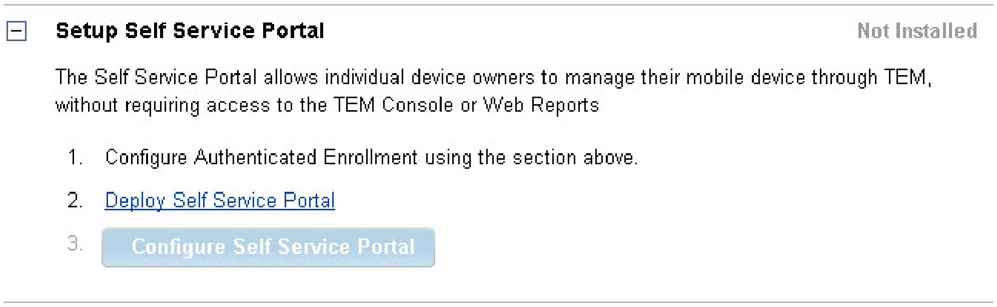
You can search for groups with a common name either starting with or containing a specific string, using the LDAP credentials from the previous dialog. Results are displayed in the Select Groups table. After you locate the specific group, select it in the table and click "Add". This action adds the group to the Selected Groups table on the right. You can also manually enter groups by entering the group's distinguished name in the bottom text box and clicking "Add". To remove a group, select it in the Selected Groups table and click Remove. Click Use Selected Groups to confirm your selections and return to the Configure Authenticated Enrollment dialog.

Self Service Portal

The Self Service Portal allows you to manage devices without the need for Tivoli Endpoint Manager or Web Reports.

To access the Self Service Portal, open the Setup and Configuration wizard from the navigation tree. After configuring Authenticated Enrollment, scroll down to the *Setup Self Service Portal* section of the dashboard.

Deploy the *Self Service Portal* Fixlet, then click the *Configure Self Service Portal* wizard, and follow the required steps.



Setup Self Service Portal Not Installed

The Self Service Portal allows individual device owners to manage their mobile device through TEM, without requiring access to the TEM Console or Web Reports

1. Configure Authenticated Enrollment using the section above.
2. Deploy Self Service Portal
3. Configure Self Service Portal

Mobile Device Management Admin Portal

The Mobile Device Management Admin Portal is a web interface that gives administrators access to view and perform a subset of management tasks on iOS and Android devices that they control. The Admin Portal provides access to managed devices when the IBM Endpoint Manager Console is unavailable, or when the full features of the console are unnecessary. The Admin Portal requires IBM Endpoint Manager version 9.0 or later. In its first release, in Mobile Device Management v2.2, the Admin Portal operates similarly to the Self Service Portal (SSP). The key difference is that the Admin Portal allows administrators to view and control multiple devices. The SSP is designed to give device owners some management capabilities over a single device.

To use an Admin Portal, your Mobile Device Management deployment must contain an Enrollment and Apple iOS Management Extender. In addition, one or more iOS or Android devices must be enrolled through the extender.

Installing an Admin Portal

To install an Admin Portal:

1. Go to Mobile Device Management Site > Setup and Configuration > Manage Components > Deploy MDM Components.
2. Select Fixlet #175 Deploy MDM Admin Portal, and click Take Action.
3. Select a target computer and click OK.

Using an Admin Portal

Access an Admin Portal by browsing to the computer that hosts it. Use one of the following URLs:

- If the computer that is hosting the Admin Portal is also hosting either an Enrollment and Apple iOS Management Extender, or a Self Service Portal, browse to:

  `https://<hostname>/ap`, where `<hostname>` is the computer the Admin Portal is installed on.
- Otherwise, browse to https://<hostname>.

Installing Enterproid Divide Management Extender

IBM Endpoint Manager supports mobile device management for devices that use Divide. Enterproid's Divide software partitions mobile devices into two sections: one for work and one for personal use. Work applications like secure web browsing, corporate email, and contacts are used in one partition, and personal applications installed by the device owner are used in the other. Divide's container solution isolates enterprise information from the rest of the device.

IBM Endpoint Manager uses an Enterproid Divide Management Extender to manage Divide devices. Before deploying and configuring the Extender:

- Ensure that you have an Enterproid contract.
- Be familiar with Divide's capabilities and administration.
- Ensure that all relevant devices have the Divide application installed and are properly enrolled in IBM Endpoint Manager. For further information see www.divide.com.

- For the configuration process you will need the domain name you registered with Enterproid and an access token provided by Enterproid. Obtain these items from your Divide administrator.

Deploying Enterproid Divide Management Extender

To deploy an Enterproid Divide Management Extender:

1. Select the Mobile Device Management Site and navigate to **Setup and Configuration > Setup and Configuration Wizard.** The dashboard displays on the right.

   Note: If prompted, you might need to activate relevant analyses.
2. From the **Install MDM Management Extenders** field, expand the node **Setup Enterproid Divide Management Extender.**
3. Select option 1, **Deploy Management Extender for Enterproid Divide**.
   a. With the Fixlet Task displayed, select **Take Action**.
   b. Select the first option, **Click here to deploy.**
   c. Select the computer you want to deploy the extender to, and press **OK**.
   d. Wait for the task to complete. This might take several minutes.
4. Return to the **Setup and Configuration Wizard** and ensure that the deployment was successful by looking for the **X Deployed** and **X of X Configured** notifications.

Note: When running tasks, there might be a delay between the task listed as “Completed” and all elements of the tasks completing on the host computer, such as software installation.

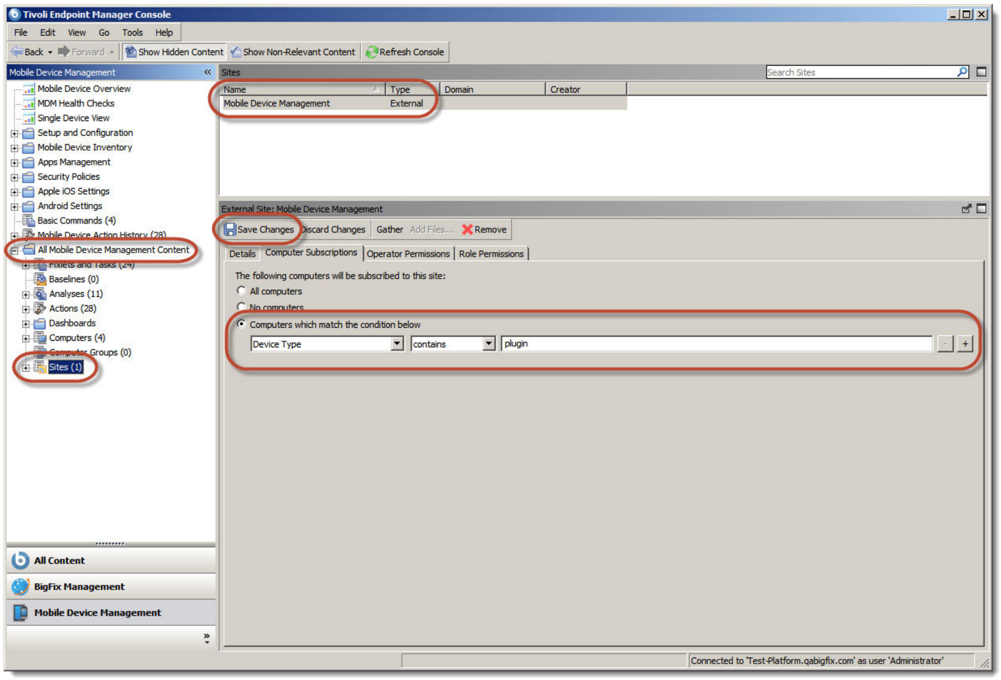
After an Enterproid Divide Management Extender has been deployed it is listed as an individual computer with the name “Divide Container <##> (<Relay_Name>)" where <##> is the number of the extender and <Relay Name> is the host name of the relay that the extender is installed on. This behavior is different from other management extenders, and allows Enterproid Divide Management Extenders to be multitenant-capable without further configuration.

Subscribe a Management Extender to Mobile Device Management

Management Extenders must be subscribed to the Mobile Device Management Site to perform management functions. Ensure that new Management Extenders are subscribed to the Mobile Device Management Site by performing the following tasks:

1. Navigate to **Mobile Device Management > All Mobile Device Management Content > Sites**.
2. Select the **Mobile Device Management** Site.
3. Select the **Computer Subscriptions** tab.
   - If **All Computers** is selected, your deployment automatically subscribes new Management Extenders to the site; do not continue with these steps.
   - If you are subscribing sites by defining rules with **Computers which match the conditions below** selected, continue to the next step.
4. Create a rule by entering the following details for the rule:
   - `Device Type | contains | plugin`

5. Click **Save Changes** to save the new rules.



Name	Type	Domain	Creator
Mobile Device Management	External		

The following computers will be subscribed to this site:

○ All computers

○ No computers

● Computers which match the condition below

Device Type | contains | plugin

Connected to 'Test-Platform.qabigfix.com' as user 'Administrator'

Configuring Enterproid Divide Management Extender

After you deploy an Enterproid Divide Management Extender you must configure it. You will need the domain that you registered with Enterproid and the associated access token. These can be obtained from your Enterproid Divide administrator. To configure an Enterproid Divide Management Extender:

1. Navigate to **Mobile Device Management > Setup and Configuration > Setup and Configuration Wizard.**
2. Expand the **Setup Enterproid Divide Management Extender** node. This area displays how many Management Extenders have been deployed and how many have been configured.
3. Click **Configure Extenders**. In the displayed window, select the extender you want to configure and click **Next**.

   Note: If you click the underlined computer name link, the console displays the properties of that computer. Click **Back** to return to the **Configure Extenders** window.
4. In the **Configure Extender** window, enter:
   a. Domain Name - The domain registered with your Enterproid Enterprise account.
   b. Access Token - The access token provided by Enterproid.
   c. Use Divide Reseller Name (Advanced) - Enterproid accounts can be sold by a third party. If this situation applies to your deployment, check this box and enter the reseller's name.
   d. (Optional) Enrollment Tag for Multitenant Environment - If you are installing multiple Enterproid Divide Management Extenders, check this box and provide an Enrollment Tag to distinguish the management extenders from each other. For more information, see Enrollment Tag for Multitenant Environments, below.

5. Click **Configure Enterproid Divide Management Extender**.
6. Select the appropriate Enterproid Divide Management Extender in the **Computer Name** field and click **OK**.
7. Return to the Setup and Configuration Wizard and ensure that a green check mark is displayed to indicate that the Management Extender is configured. This process might take several minutes.

Enrollment Tag for Multitenant Environments

Select the **Enrollment Tag for Multitenant Environments** check box if you manage multiple management extenders. Using an Enrollment Tag allows IBM Endpoint Manager Console operators to target specific devices according to the management extenders that manage them.

Select the **Enrollment Tag for Multitenant Environments** box and enter an Enrollment Tag to assign it to the management extender you are configuring.

Note: When configuring an Enrollment Tag on an Enterproid Divide Management Extender, that extender is renamed to include the enrollment tag as part of its name. The naming convention is" Divide Container <##> (<RELAY_NAME>, <ENROLLMENT_TAG>".

Android Agent Setup

To set up your Android agent, use the following steps. You will need an internet-facing relay for this process.

1. Launch the Android market app on your device and search for *IBM Endpoint Manager for Mobile Devices.* Select the app and click *download.* Click *Accept and Download.*
2. After the application is installed, select **Open**.
3. Click **Activate**.
4. Enter the TEM Server address (or internet-facing relay) that you obtained from your administrator and enter your work email address. Select one of the two available options to indicate if the device is personal or enterprise. Click **Enroll**.
5. If the connection is successful, the message *Successful set up of the Mobile Client* will display briefly, and service status will indicate that the service is running.

Note: To uninstall the TEM Android agent, clear the Device Administrator option under Settings/Location and Security on the device.

Note: To control your device location privacy, deploy the *Disable GPS Location Properties* Fixlet under Mobile Device Inventory/Data Configuration.

Samsung SAFE

Samsung For Enterprise provides additional device management and security features for compatible Samsung Mobile devices.

After you install and enroll the IBM mobile client, a message automatically prompts you to install the IBM Mobile Client for Samsung from the Google Play Store. After installation you will be promoted to Activate Device Administrator, which subsequently enables Samsung SAFE capabilities on your device.

IBM Endpoint Manager for Mobile Devices supports SAFE up to and including V3.0 (Build Code 5). Later versions are not supported.

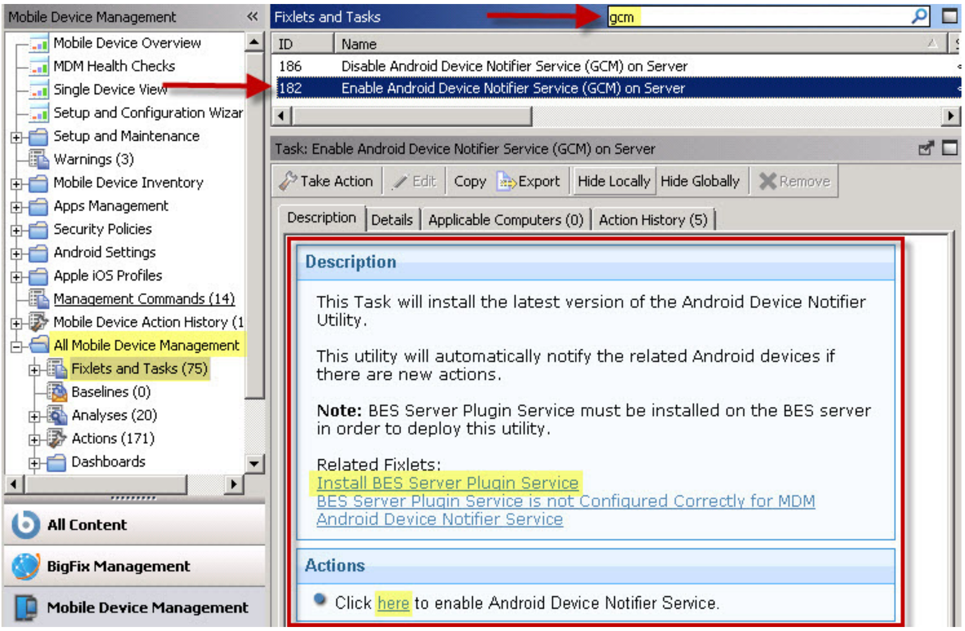
For more information about setting up SAFE on Samsung mobile devices, see the Mobile Device Management Users Guide.

Android Device Notifier Service

The Android Device Notifier Service is the Android equivalent of Google Cloud Messaging. To address slow response times, you can use the Android Device Notifier service to change response times, for example, from five hours to several minutes.

To set up this service on the TEM Server for your Android device, perform the following steps:

1. Install the BES Server Plugin Service on the server. To do this, click the *All Mobile Device Management Content* in the navigation tree and select *Fixlets and Tasks*. In the list, select Enable Android Device Notifier Service. Alternatively, you can type "GCM" in the search box at the top. Click the Install BES Server Plugin Service link in the Description Section to install the service.



ID	Name
186	Disable Android Device Notifier Service (GCM) on Server
182	Enable Android Device Notifier Service (GCM) on Server

Task: Enable Android Device Notifier Service (GCM) on Server

Description

This Task will install the latest version of the Android Device Notifier Utility.

This utility will automatically notify the related Android devices if there are new actions.

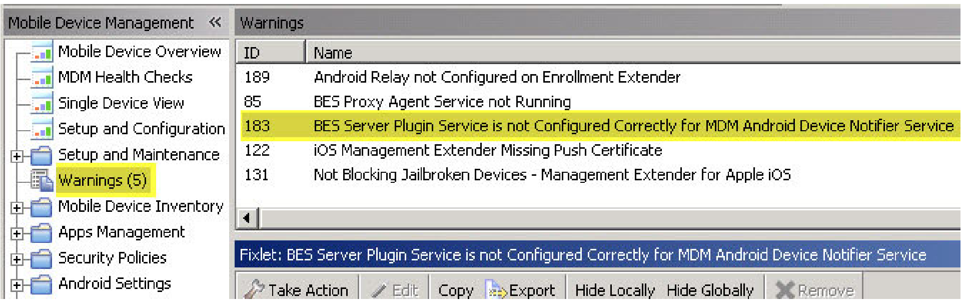
Note: BES Server Plugin Service must be installed on the BES server in order to deploy this utility.

Related Fixlets:
Install BES Server Plugin Service
BES Server Plugin Service is not Configured Correctly for MDM Android Device Notifier Service

Actions

- Click here to enable Android Device Notifier Service.

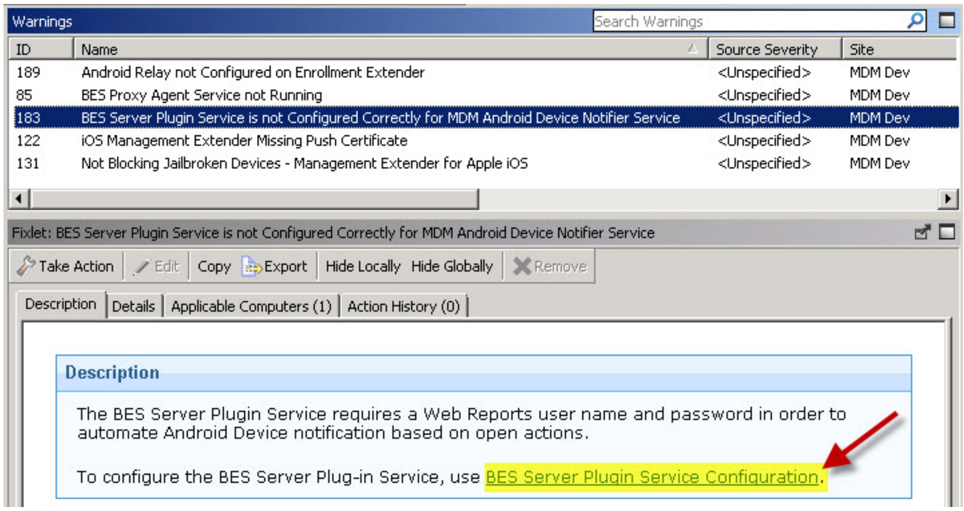
2. Use the BES Server Plugin Service Configuration to configure the BES Server Plugin service. Click Warnings in the navigation tree and select BES Server Plugin Service Configuration.



ID	Name
189	Android Relay not Configured on Enrollment Extender
85	BES Proxy Agent Service not Running
183	BES Server Plugin Service is not Configured Correctly for MDM Android Device Notifier Service
122	iOS Management Extender Missing Push Certificate
131	Not Blocking Jailbroken Devices - Management Extender for Apple iOS

Fixlet: BES Server Plugin Service is not Configured Correctly for MDM Android Device Notifier Service

In the Fixlet window, click the BES Server Plugin Service Configuration link.



ID	Name	Source Severity	Site
189	Android Relay not Configured on Enrollment Extender	<Unspecified>	MDM Dev
85	BES Proxy Agent Service not Running	<Unspecified>	MDM Dev
183	BES Server Plugin Service is not Configured Correctly for MDM Android Device Notifier Service	<Unspecified>	MDM Dev
122	iOS Management Extender Missing Push Certificate	<Unspecified>	MDM Dev
131	Not Blocking Jailbroken Devices - Management Extender for Apple iOS	<Unspecified>	MDM Dev

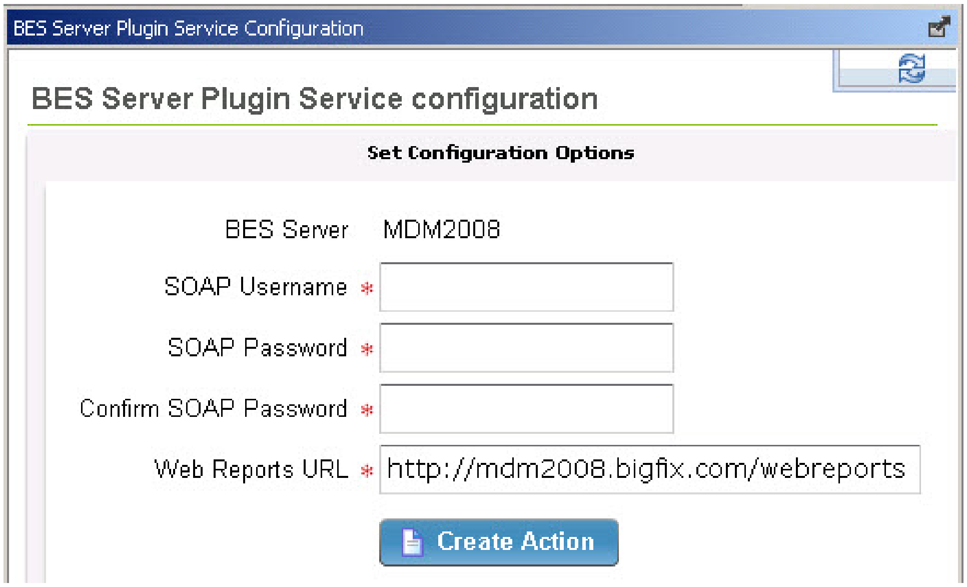
Fixlet: BES Server Plugin Service is not Configured Correctly for MDM Android Device Notifier Service

Description

The BES Server Plugin Service requires a Web Reports user name and password in order to automate Android Device notification based on open actions.

To configure the BES Server Plug-in Service, use BES Server Plugin Service Configuration.

Set configuration options by entering your Web Reports (SOAP) username and password in the fields provided. Then click *Create Action*.



BES Server Plugin Service configuration

Set Configuration Options

BES Server MDM2008

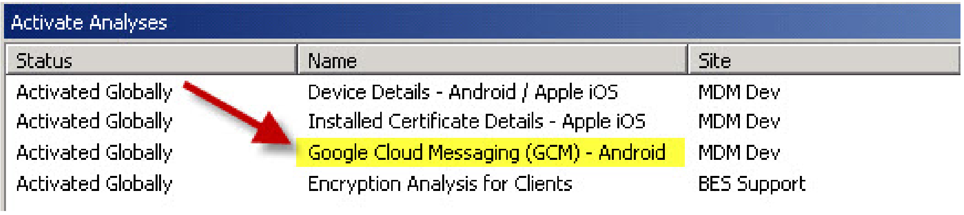
SOAP Username *

SOAP Password *

Confirm SOAP Password *

Web Reports URL * http://mdm2008.bigfix.com/webreports

3. Enable the Android Device Notifier Service (GCM) on the Server. To do this, go back to the All Mobile Device Management Content in the navigation tree and select Fixlets and Tasks. In the list, select Enable Android Device Notifier Service. Click the link in the Actions box to enable the Android Device Notifier Servicet.
4. Activate the *Google Cloud Messaging (GCM) - Android* analysis. To do this, click the Setup and Maintenance node in the navigation tree and select Activate Analyses. Select the Google Cloud Messaging analysis, right-click, and select Activate.



Status	Name	Site
Activated Globally	Device Details - Android / Apple iOS	MDM Dev
Activated Globally	Installed Certificate Details - Apple iOS	MDM Dev
Activated Globally	Google Cloud Messaging (GCM) - Android	MDM Dev
Activated Globally	Encryption Analysis for Clients	BES Support

When sending Notification messages, you could experience a delay in delivery to the target Android application running on the device, depending on message volume and how messages are queued.

Note: The Android Device Notifier Service notifies ALL Android devices if there is a new action that does not target specific devices. It then notifies the targeted devices if the action is targeted by computer IDs.

MaaS360 Integration for Unified Reporting

Customers who are using or migrating to IBM MaaS360 software can now integrate MaaS360 device data into their IBM Endpoint Manager deployments. In an Integrated deployment MaaS360 device data is visible in the MaaS360 Single Device View dashboard, the "All Computers" listings, and the IBM Endpoint Manager Reports and database feeds. You can also use the Single Device View to perform basic tasks on MaaS360-managed devices: Device Wipe, Lock Device, Send Message to User, and Selective Wipe MaaS360 Data.

Install the MaaS360 Management Extender to perform the integration. The process is similar to those used for other Mobile Device Management Extenders. For a list of endpoints supported per Management Extender, see General System Requirements.

System Requirements

- You must have Administrative permissions sufficient to manage plugins (Management Extenders).
- Management Extenders can be deployed only on computers that have a relay installed (*v*8.2 or higher).
- If you have one MaaS360 billing account deploy and configure one MaaS360 Management Extender. If you have multiple MaaS360 billing accounts, deploy an Extender for each account.
  - Customers with multitenant systems might want to deploy all their Extenders and have individual operators configure their own. This will allow individual tenants to access their own configuration settings and data, but not anyone else's. Deploy each Extender in multitenant mode.
- During installation, you might be prompted to authorize various Analysis tasks. Click **Activate** if this occurs.

Web Service Access

During configuration you will be prompted for the following values:

- MaaS360 user name
- MaaS360 password
- Billing ID
- Application Version
- MaaS360 Root URL
- Application ID
- Platform ID
- Application Access Key (API Key)

The MaaS360 Management Extender uses this information to access IBM Fiberlink Web Services. Together they constitute the Extender's Web Services credentials. If you have the MaaS360 SaaS option, use the method below to obtain your credentials. If you have the MaaS360 On Premises option, see the *IBM MaaS360 On-Premises Configuration Guide* for instructions.

MaaS360 SaaS customers: you have the first two items in the list: MaaS360 user name and password. Billing ID is your MaaS360 account number. The remaining values must be obtained from IBM Fiberlink Customer Services:

- Application version
- MaaS360 Root URL
- Application ID
- Platform ID
- Application Access Key (API Key)

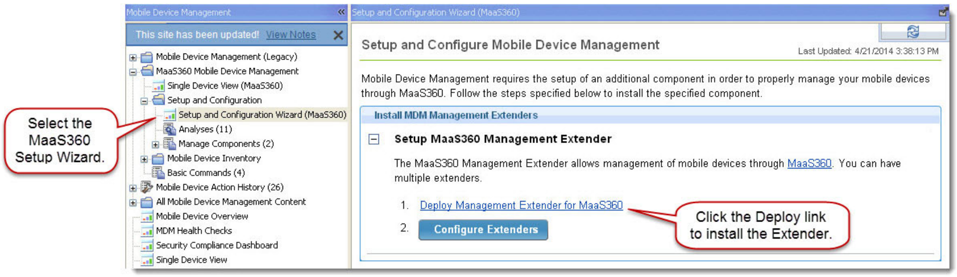
IBM Fiberlink will establish these credentials at your request; contact their Customer Services department at the number below. Tell them you are integrating your IBM Mobile Device Management and MaaS360 deployments and want access to Fiberlink Web Services. Estimated completion time for this task is one week.

IBM Fiberlink Customer Services

- 1-855-622-7360 (1-855-MAAS360).
- Email: ops@fiberlink.com.

MaaS360 Integration Procedure

1. From the IBM Endpoint Manager Console, open the Mobile Device Management node.
2. Subscribe to the MaaS360 Mobile Device Management site.
   - If you use rules to manage Extender subscriptions in your deployment, add a rule using the formula:
     - `device type | contains | plugin.`
3. From the Setup and Configuration node, select **Setup and Configuration Wizard (MaaS360)**.
4. Click **Deploy Management Extender for MaaS360** to run the Fixlet that installs the Extender.


Mobile Device Management
This site has been updated! View Notes
Mobile Device Management (Legacy)
MaaS360 Mobile Device Management
Single Device View (MaaS360)
Setup and Configuration
Setup and Configuration Wizard (MaaS360)
Analyses (11)
Manage Components (2)
Mobile Device Inventory
Basic Commands (4)
Mobile Device Action History (26)
All Mobile Device Management Content
Mobile Device Overview
MDM Health Checks
Security Compliance Dashboard
Single Device View
Setup and Configuration Wizard (MaaS360)
Install MDM Management Extenders
Configure Extenders

Setup and Configure Mobile Device Management

Last Updated: 4/21/2014 3:38:13 PM

Mobile Device Management requires the setup of an additional component in order to properly manage your mobile devices through MaaS360. Follow the steps specified below to install the specified component.

Setup MaaS360 Management Extender

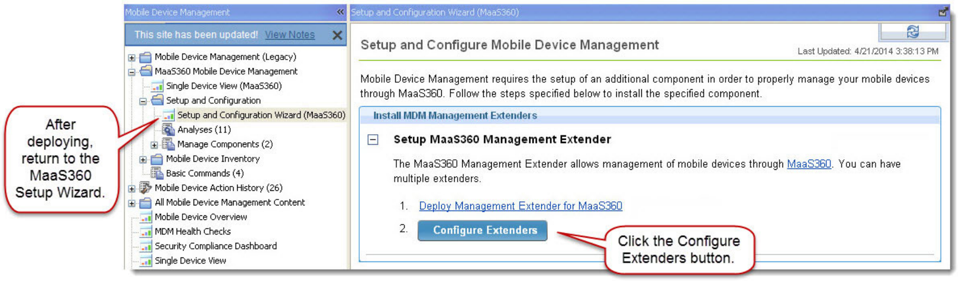
The MaaS360 Management Extender allows management of mobile devices through MaaS360. You can have multiple extenders.

1. Deploy Management Extender for MaaS360
2. Configure Extenders

Select the MaaS360 Setup Wizard.

Click the Deploy link to install the Extender.

5. When the Fixlet action completes return to the Setup and Configuration Wizard and refresh the screen.
6. Click **Configure Extenders**. Configuration establishes communications between the Extender and the IBM MaaS360 Server.


Mobile Device Management
This site has been updated! View Notes
Mobile Device Management (Legacy)
MaaS360 Mobile Device Management
Single Device View (MaaS360)
Setup and Configuration
Setup and Configuration Wizard (MaaS360)
Analyses (11)
Manage Components (2)
Mobile Device Inventory
Basic Commands (4)
Mobile Device Action History (26)
All Mobile Device Management Content
Mobile Device Overview
MDM Health Checks
Security Compliance Dashboard
Single Device View
Setup and Configuration Wizard (MaaS360)
Configure Extenders

Setup and Configure Mobile Device Management

Last Updated: 4/21/2014 3:38:13 PM

Mobile Device Management requires the setup of an additional component in order to properly manage your mobile devices through MaaS360. Follow the steps specified below to install the specified component.

Install MDM Management Extenders

Setup MaaS360 Management Extender

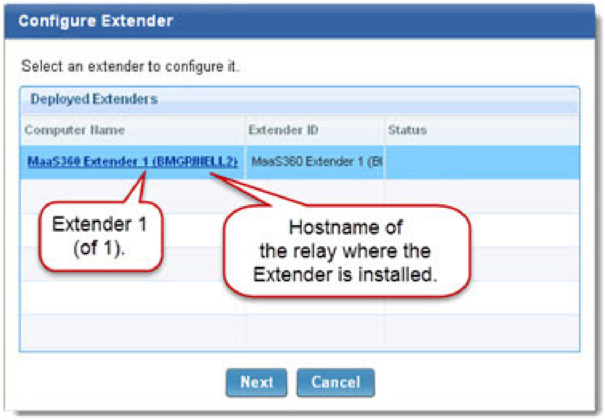
The MaaS360 Management Extender allows management of mobile devices through MaaS360. You can have multiple extenders.

1. Deploy Management Extender for MaaS360
2. Configure Extenders

After deploying, return to the MaaS360 Setup Wizard.

Click the Configure Extenders button.

7. Select the MaaS360 Management Extender that you want to configure and click **Next**.



Select an extender to configure it.

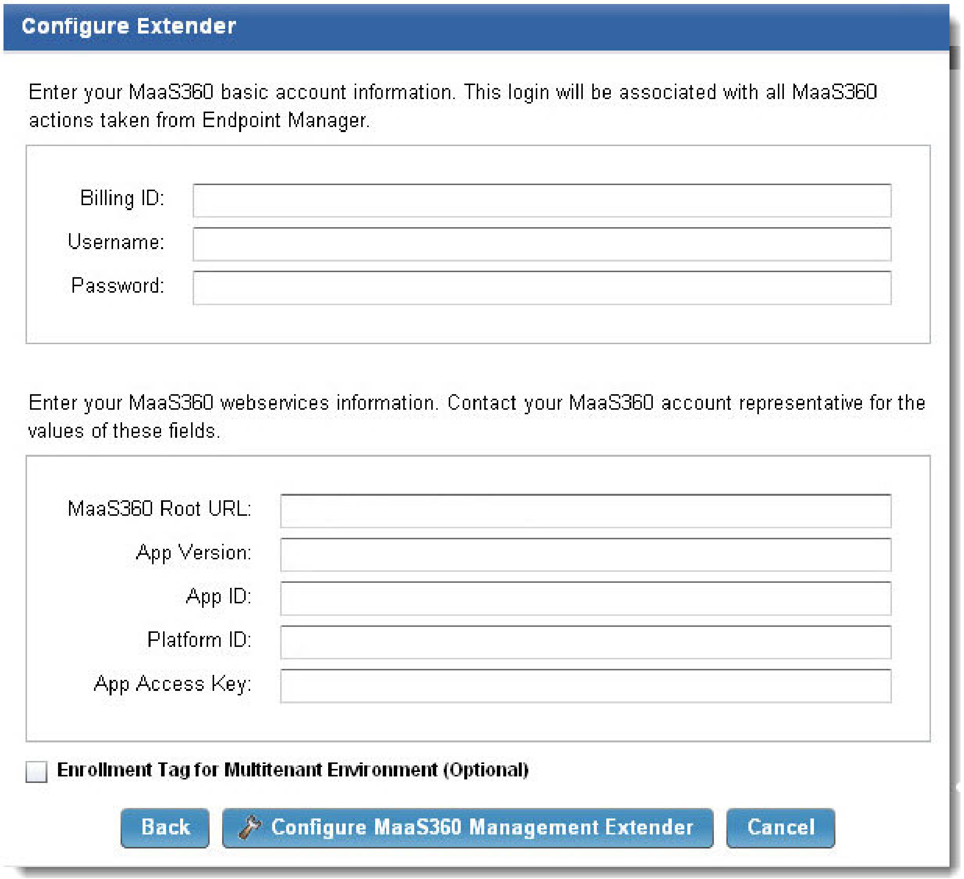
Deployed Extenders

Computer Name	Extender ID	Status
MaaS360 Extender 1 (BMGRIHELL2)	MaaS360 Extender 1 (B(	

Extender 1 (of 1).

Hostname of the relay where the Extender is installed.

8. Enter your MaaS360 account information and Web Services credentials.
   - If you use the MaaS360 SaaS option: use the MaaS360 Root URL provided (https://services.fiberlink.com).
   - If you use the MaaS360 On Premises option: enter the URL of the primary V-app (virtual appliance) hosting the Web Services.
   - If you operate a multitenant environment check the **Enrollment Tag** box to enter an organization-specific identifier for the selected Extender and the devices that report through it. If you do not use multitenant functions leave the box cleared.



Configure Extender

Enter your MaaS360 basic account information. This login will be associated with all MaaS360 actions taken from Endpoint Manager.

Billing ID:

Username:

Password:

Enter your MaaS360 webservices information. Contact your MaaS360 account representative for the values of these fields.

MaaS360 Root URL:

App Version:

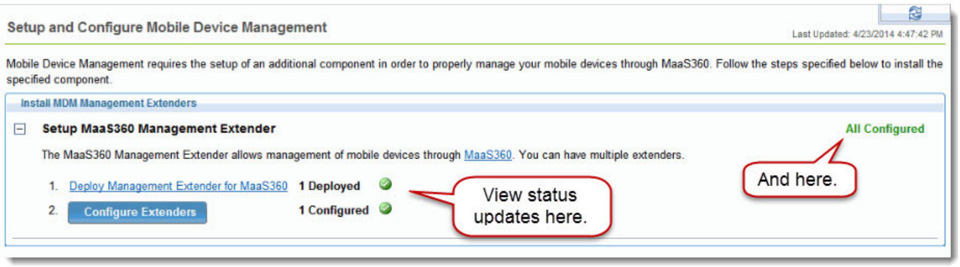
App ID:

Platform ID:

App Access Key:

□ Enrollment Tag for Multitenant Environment (Optional)

9. Click **Configure MaaS360 Mangment Extender** to start configuration processing and complete the integration procedure.



Setup and Configure Mobile Device Management

Last Updated: 4/23/2014 4:47:42 PM

Mobile Device Management requires the setup of an additional component in order to properly manage your mobile devices through MaaS360. Follow the steps specified below to install the specified component.

Install MDM Management Extenders

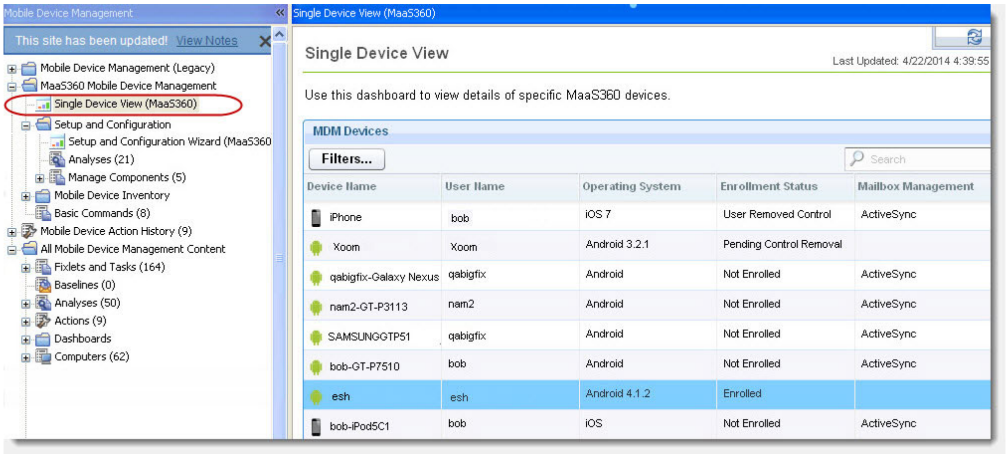
Setup MaaS360 Management Extender All Configured

The MaaS360 Management Extender allows management of mobile devices through MaaS360. You can have multiple extenders.

1. Deploy Management Extender for MaaS360 **1 Deployed**
2. Configure Extenders **1 Configured**

Working in an Integrated Environment

MaaS360-manged devices will now start reporting in to your IBM Endpoint Manager deployment. You will see them in the MaaS360 Single Device View. Click a specific device to see its details.


Mobile Device Management
This site has been updated! View Notes
Single Device View (MaaS360)

- Mobile Device Management (Legacy)
- MaaS360 Mobile Device Management
  - Single Device View (MaaS360)
  - Setup and Configuration
    - Setup and Configuration Wizard (MaaS360
    - Analyses (21)
    - Manage Components (5)
  - Mobile Device Inventory
  - Basic Commands (8)
- Mobile Device Action History (9)
- All Mobile Device Management Content
  - Fixlets and Tasks (164)
  - Baselines (0)
  - Analyses (50)
  - Actions (9)
  - Dashboards
  - Computers (62)

Single Device View

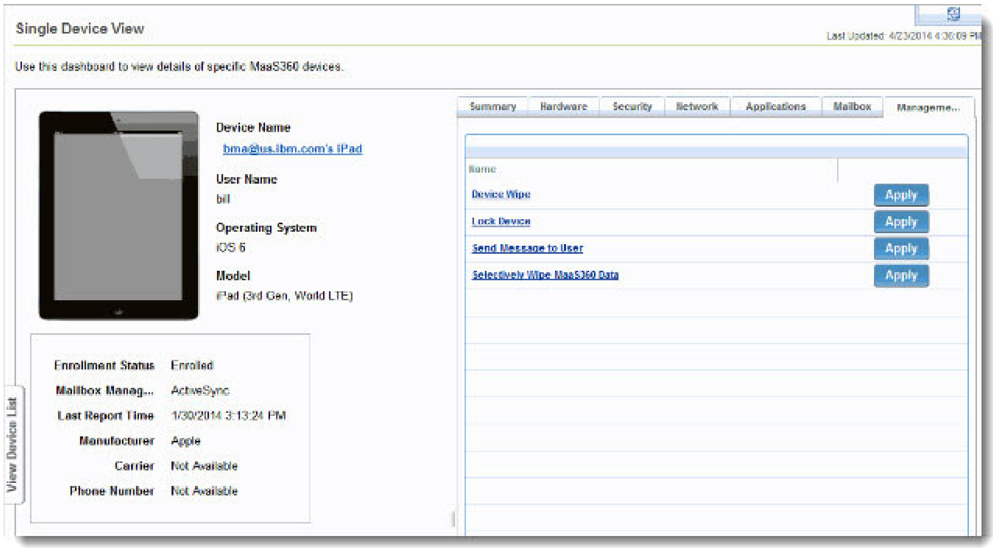
Last Updated: 4/22/2014 4:39:55

Use this dashboard to view details of specific MaaS360 devices.

MDM Devices

Device Name	User Name	Operating System	Enrollment Status	Mailbox Management
iPhone	bob	iOS 7	User Removed Control	ActiveSync
Xoom	Xoom	Android 3.2.1	Pending Control Removal	
qabigfix-Galaxy Nexus	qabigfix	Android	Not Enrolled	ActiveSync
nam2-GT-P3113	nam2	Android	Not Enrolled	ActiveSync
SAMSUNGGTP51	qabigfix	Android	Not Enrolled	ActiveSync
bob-GT-P7510	bob	Android	Not Enrolled	ActiveSync
esh	esh	Android 4.1.2	Enrolled	
bob-iPod5C1	bob	iOS	Not Enrolled	ActiveSync

Perform basic management tasks on MaaS360 devices on the Device Details screen: Device Wipe, Lock Device, Send Message to User, and Selective Wipe MaaS360 Data. Click the **Management Command** tab to see a list of available options for a specific device.



Single Device View

Last Updated: 4/23/2014 4:36:09 PM

Use this dashboard to view details of specific MaaS360 devices.

Device Name
bma@us.ibm.com's iPad

User Name
bill

Operating System
iOS 6

Model
iPad (3rd Gen, World LTE)

Enrollment Status	Enrolled
Mailbox Manag...	ActiveSync
Last Report Time	1/30/2014 3:13:24 PM
Manufacturer	Apple
Carrier	Not Available
Phone Number	Not Available

Name	
Device Wipe	Apply
Lock Device	Apply
Send Message to User	Apply
Selectively Wipe MaaS360 Data	Apply

Device Wipe

Returns a device to its factory default settings. Warning: deletes all the data on the device. You will no longer be able to manage it. After the Device Wipe, the device's MaaS360 enrollment state will be "control removed." If the targeted mobile device cannot be contacted, its MaaS360 enrollment state will be "pending control removal." MaaS360 will wipe the device at the next available opportunity.

Lock Device

Locks device with the existing passcode.

Send Message to User

Send an unsecured message to the device through the installed application. Note: Do not send confidential information or passwords using this method. The message will be clearly visible in both the MaaS360 ActionSite and MaaS360 Action History.

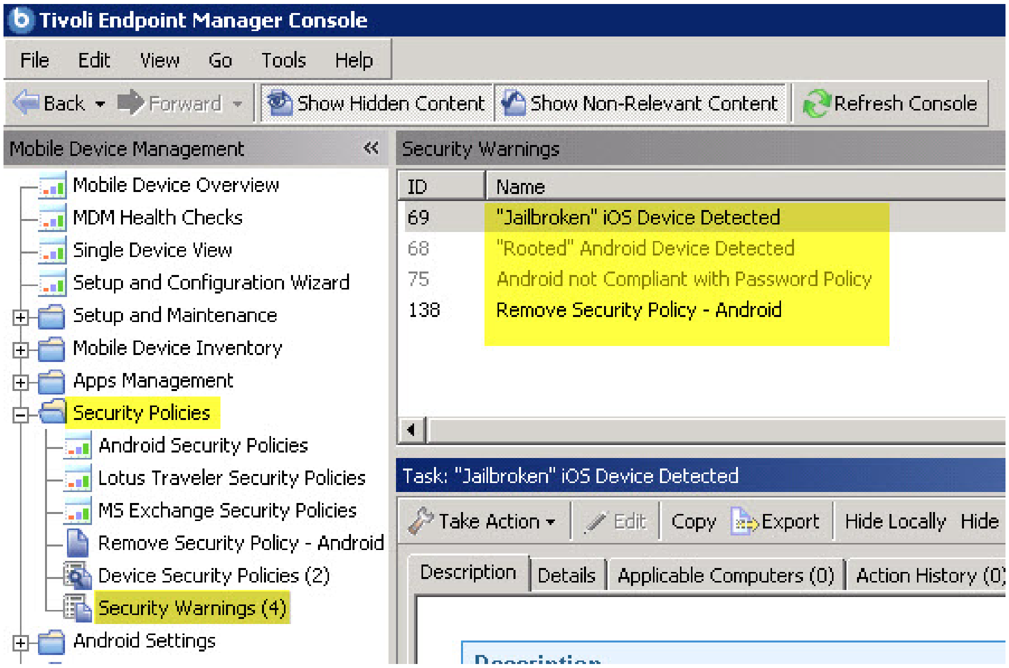
Selectively Wipe MaaS360 Data

Removes company data stored on the device, including distributed applications and documents. The device holder's personal data will not be removed. Warning: deletes all company data on the device. You will no longer be able to manage it. The device will continue to report into MaaS360 as an Enrolled device. Selective Wipe information will be displayed in the MaaS360 Security and Compliance Devices Analysis.

Warnings

Four possible warning messages display in the Warnings list panel if they are relevant to your deployment:

- "Jailbroken" iOS Device Detected
- "Rooted" Android Device Detected
- Android not compliant with Password Policy
- Remove Security Policy - Android



ID	Name
69	"Jailbroken" iOS Device Detected
68	"Rooted" Android Device Detected
75	Android not Compliant with Password Policy
138	Remove Security Policy - Android

Task: "Jailbroken" iOS Device Detected

To determine warnings that may be relevant to your deployment, access them through the Security Policies node in the navigation tree.

Click on each individual warning, and deploy it by clicking the link in the Actions section of the Fixlet window.

Frequently Asked Questions

Use the following list of Frequently Asked Questions for general MDM setup support:

What is the relationship between Management Extender for iOS and Authenticated Enrollment?

The iOS extender is also the enrollment server that acts as the gateway for devices that want to enroll in Mobile Device Management. It performs all of the backend calls to LDAP to verify that a user is allowed or authenticated to enroll. For iOS, it downloads the Mobile Device Management profile that gets installed on the iOS device that configures the phone to be managed by the Mobile Device Management server. For Android, it uses a relay to perform the rest of the enrollment process.

Can two management extenders be installed on one relay?

Yes. You can have two different management extenders on the same relay, but they cannot be the same type of extender. For example, you could have iOS and Lotus Traveler extenders on the same relay, but not two iOS extenders.

What credentials do I need to set to use Mobile Device Management?

LDAP, Web Reports, and credentials for accessing the Tivoli Endpoint Manager console.

What ports should I enable to use Mobile Device Management?

You must have ports 52315 and 52316 enabled on one computer.

Does the version of my Mobile Device Management Server need to match the version of my apps?

As a best practice, yes. In addition, MDM Server 1.1 displays as version 8.2.20000.0, and MDM Server 1.0 displays as 8.2.10000.0.

Where in my network should I place TSP (Trusted Service Provider) and SSP (Self Service Portal)?

Place the TSP in the internal network where it has access to LDAP, Tivoli Endpoint Manager, and Web Reports. It also needs to be accessible by the iOS extender. TSP exists to protect sensitive operations that the iOS/SSP performs internally. SSP can be placed externally or internally, depending on whether you want to enforce users be on VPN to access it or allowing usage from home as well.

How do I upgrade to the latest version of Mobile Device Management?

To upgrade server components, click *Upgrade MDM Components* from the Setup and Maintenance node in the navigation tree. After upgrading, use the Setup and Configuration Wizard to ensure that all components are properly configured. To upgrade an iOS app, go to the Apple iTunes Store from your device. To upgrade an Android app, go to Google Play from your Android device.

How many computers can an iOS Management Extender support?

iOS Management Extenders may support up to 2,000 devices. This number is dependent on the specs of the computer the extender is installed on.

How do I enable or disable data usage tracking on iOS devices?

You can use Fixlets 195 and 196 to enable or disable data usage tracking by creating a client setting on a targeted iOS device. To access these Fixlets, click *All Mobile Device Management Content* from the navigation tree, click *Fixlets and Tasks*, and type the Fixlet number in the search box on the right. Note: if you disable location tracking on an iOS App, it will also disable the data tracking, which means that the iOS App will not track any data usage.

How do I enable or disable device location tracking?

Enabling device location tracking requires opt-in from both the device user and the TEM Administrator. The device user must toggle the appropriate setting in the device application settings. The TEM Administrator must run the "Enable GPS Location Properties" task under Setup and Configuration/Configure MDM Components in the navigation tree, and activate the "Location Information - Android / Apple iOS" analysis under Setup and Configuration/Activate Analyses. To disable location tracking, the device user can turn the setting off in the device application settings. The TEM Administrator can deactivate the analysis, or run the "Disable GPS Location Properties" task listed in Configure MDM Components if the device has been previously enabled. For privacy reasons, the device user opt-in setting cannot be overwritten by the TEM Administrator.

Why does the name of the install application on my Android device show up as unreadable characters?

The Android Agent (IBM Mobile Client app) will have no knowledge of the code page (language) of the Tivoli Endpoint Manager deployment, even after it is enrolled. The current IANA client setting on Android devices defaults to English (Windows-1252), unless it is configured. If this setting is not the same as the Tivoli Endpoint Manager deployment, data sent from the Android devices might be unreadable even if the devices have the same code page (language) as the Tivoli Endpoint Manager deployment.

To set the IANA Client setting automatically for all Android devices upon enrollment, create a policy action from the Android Device Language Setting wizard. Click *Create Policy Action*.

The list below highlights the currently supported languages/IANA settings:

- ENU - windows-1252
- CHS - gh2312
- JPN - Shift_JIS
- ESN - windows-1252
- ITA - windows-1252
- FRA - windows-1252
- DEU - windows-1252
- CHT - big5
- KOR - ks_c_5601-1987

Support

For more information about this product, see the following resources:

- http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base

- Forums and Communities

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.

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.

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.

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.

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.

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.

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.

NitroDesk Touchdown Legal Notices

If a customer chooses to use IBM Endpoint Manager for Mobile Devices to configure and manage NitroDesk TouchDown software, IBM Endpoint Manager for Mobile Devices will use the NitroDesk TouchDown APIs to communicate with the NitroDesk TouchDown product. Customers are responsible for independently purchasing NitroDesk TouchDown software by working directly with NitroDesk, Inc.

The NitroDesk TouchDown APIs are used under license from NitroDesk, Inc. IBM may update the NitroDesk Touchdown APIs from time to time at its sole discretion. NitroDesk may change the NitroDesk Touchdown software or APIs in such a way that the changes cause management of NitroDesk TouchDown via IBM Endpoint Manager for Mobile Devices to cease working. IBM shall have no obligation to support NitroDesk TouchDown software or APIs even if the capability ceases to function.

The NitroDesk Touchdown APIs and use of the APIs are provided AS-IS. SUBJECT TO ANY STATUTORY WARRANTIES THAT CANNOT BE EXCLUDED, IBM MAKES NO WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, REGARDING THE NITRODESK APIS OR SUPPORT, IF ANY, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND TITLE, AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO LICENSEE. IN THAT EVENT, SUCH WARRANTIES ARE LIMITED IN DURATION TO THE MINIMUM PERIOD REQUIRED BY LAW. NO WARRANTIES APPLY AFTER THAT PERIOD. SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE. LICENSEE MAY HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE OR JURISDICTION TO JURISDICTION.