Product Guide

McAfee Enterprise Mobility Management 11.0 Software

For use with ePolicy Orchestrator 4.6.5-5.0 Software
COPYRIGHT
Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
# Contents

## Preface
- About this guide .................................. 5
- Audience .................................. 5
- Conventions ................................. 5
- Find product documentation ................. 6

## 1 Introducing McAfee Enterprise Mobility Management
- ePolicy Orchestrator features customized for McAfee EMM .................. 7
- McAfee EMM components ............................... 8
  - Server components .................................. 8
  - Client components ............................... 9

## 2 Getting started
- Customize the company profile ......................... 11
- Update the default administrator account ................ 12
- Create a service record ................................ 12
- Configure an authorization directory ................... 12
- Add GCM settings for upgrades ......................... 13
- Configure an SMTP server and default notification settings .......... 14
- Customize certificate expiration notifications ............... 14
- Using permission sets with McAfee EMM ................... 15

## 3 Authorizing users
- Manage provisioning tokens ............................. 17
  - Require provisioning tokens .......................... 17
  - Update provisioning tokens ........................... 18
- Authorize users .................................. 19
  - Bulk-authorize and notify LDAP or ActiveSync users ............... 19
  - Authorize select LDAP users .......................... 20
  - Authorize select ActiveSync users .................. 21
  - Authorize LDAP or ActiveSync users based on a list ................. 21
- Unlock users ................................... 22
- Managing Android Device ID Mapping ......................... 22
  - Activate manual Device ID Mapping ................... 23
  - Manually approve Device ID Mapping .................. 23

## 4 Configuring devices
- Device configuration requirements ........................... 25
- Communicating with users .............................. 26
- Configure devices ................................. 26
  - Configure iOS devices ................................ 27
  - Configure Android devices ............................ 27
  - Configure Windows Phones ........................... 28
- Updating devices .................................. 29
  - Update devices ...................................... 29
Preface

Contents

About this guide
Find product documentation

About this guide

This information describes the guide’s target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- Administrators — People who implement and enforce the company’s security program.

Conventions

This guide uses these typographical conventions and icons.

- **Book title, term, emphasis**
  - Title of a book, chapter, or topic; a new term; emphasis.

- **Bold**
  - Text that is strongly emphasized.

- **User input, code, message**
  - Commands and other text that the user types; a code sample; a displayed message.

- **Interface text**
  - Words from the product interface like options, menus, buttons, and dialog boxes.

- **Hypertext blue**
  - A link to a topic or to an external website.

  **Note:** Additional information, like an alternate method of accessing an option.

  **Tip:** Suggestions and recommendations.

  **Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.

  **Warning:** Critical advice to prevent bodily harm when using a hardware product.
Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task


2. Under Self Service, access the type of information you need:

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User documentation</td>
<td>1. Click Product Documentation.</td>
</tr>
<tr>
<td></td>
<td>2. Select a product, then select a version.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click Search the KnowledgeBase for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click Browse the KnowledgeBase for articles listed by product and version.</td>
</tr>
</tbody>
</table>
Introducing McAfee Enterprise Mobility Management

McAfee® Enterprise Mobility Management (McAfee EMM™) provides management and security for mobile devices in enterprise environments.

McAfee EMM 11.0 leverages McAfee® ePolicy Orchestrator® to deliver management and security for iOS and Android devices, and Windows Phones. With McAfee EMM, enterprises smoothly integrate mobile data protection into their existing infrastructure.

McAfee EMM can be used to:

- Enforce authentication, authorization, and encryption
- Define security and use policies
- Block jailbroken or rooted devices
- Remotely lock or wipe lost devices
- Segregate corporate email, contacts, and calendars
- Monitor and report on the mobile enterprise

McAfee EMM offers a comprehensive, scalable solution for the rapidly expanding bring-your-own-device (BYOD) market and for traditional enterprise-driven environments, providing a unified solution for complete mobile security.

Contents

- ePolicy Orchestrator features customized for McAfee EMM
- McAfee EMM components

---

### ePolicy Orchestrator features customized for McAfee EMM

McAfee EMM 11.0 is managed exclusively by ePolicy Orchestrator. Understanding how these products’ features interact helps you navigate and use the system effectively.

<table>
<thead>
<tr>
<th>For this ePolicy Orchestrator feature</th>
<th>McAfee EMM adds...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboards</td>
<td>Predefined, mobile-specific dashboards and monitors.</td>
</tr>
<tr>
<td>Permission Sets</td>
<td>McAfee Enterprise Mobility Management policy permission group and Mobile Actions permission group in each permission set.</td>
</tr>
<tr>
<td>Policy Catalog</td>
<td>Android, iOS, and Windows Phone policy categories in the Enterprise Mobility Management 11.0.0 product group.</td>
</tr>
<tr>
<td>For this ePolicy Orchestrator feature</td>
<td>McAfee EMM adds...</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| Queries & Reports                    | • Predefined, mobile-specific queries.  
• Custom query property groups: EMM Properties, Device Details, Device Properties, Mobile Applications, and Telecommunication Properties. |
| Server Settings                      | EMM Server Settings with access to System Settings, Package Management, and User Notifications. |
| Server Tasks                         | EMM Certificates Notification server task. |
| System Information                   | • Mobile Properties window.  
• Mobile actions: Lock, MDM Uninstall, Unlock, Wipe, and Wipe Corporate Data. |
| User Management                      | Locked Users page. |

**McAfee EMM components**

The McAfee EMM system includes server-side and client-side components that are managed through ePolicy Orchestrator.

McAfee EMM for ePolicy Orchestrator automatically installs Mobile ePolicy Orchestrator, a lightweight extension that allows ePolicy Orchestrator to communicate with mobile devices. McAfee EMM 11.0 can be used with ePolicy Orchestrator 4.6.5 and later.

**Server components**

These components are installed on enterprise servers to administer McAfee EMM.

![Typical configuration of McAfee EMM server components](image)

**Figure 1-1  Typical configuration of McAfee EMM server components**

For basic configuration on a single server, see the *McAfee EMM Installation Guide*. 
<table>
<thead>
<tr>
<th>McAfee EMM server component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub</td>
<td>Manages communication between components. The Hub allows secure communication across the firewall (between the DMZ and the internal network) and eliminates the need to open custom firewall ports. SSL communication is established between the components. Using a custom installation, the Hub can also communicate with the DMZ components through an HTTP (non-secure) connection.</td>
</tr>
<tr>
<td>Portal</td>
<td>Allows device users to initiate wipe requests in the event their device is lost or stolen. Users access the Portal from a browser on a PC or mobile device. We recommend installing the Portal in the DMZ.</td>
</tr>
<tr>
<td>Proxy</td>
<td>Proxies ActiveSync traffic to the email servers. This IIS (Internet Information Services) application controls access to enterprise resources on the DMZ server before reaching the internal network. We recommend installing the Proxy in the DMZ.</td>
</tr>
<tr>
<td>Push Notifier</td>
<td>Sends push notifications to mobile devices. The Push Notifier is a required component that communicates with Apple and Google push notification services. We recommend installing the Push Notifier in the DMZ.</td>
</tr>
</tbody>
</table>

**Client components**

These components are installed on mobile devices that are registered on the enterprise network. They help configure the device and communicate with the McAfee EMM server.

<table>
<thead>
<tr>
<th>McAfee EMM client component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee EMM app</td>
<td>Free app for iOS or Android that enables easy configuration by the user, and allows push notifications to deliver profile and security policy changes.</td>
</tr>
<tr>
<td>McAfee® Secure Container app (Android devices)</td>
<td>Free app that encrypts, passcode-secures, and segregates enterprise email, contacts, and calendars.</td>
</tr>
</tbody>
</table>
Introducing McAfee Enterprise Mobility Management

McAfee EMM components
Getting started

Get up-and-running quickly by completing these preliminary tasks.

Contents

- Customize the company profile
- Update the default administrator account
- Create a service record
- Configure an authorization directory
- Add GCM settings for upgrades
- Configure an SMTP server and default notification settings
- Customize certificate expiration notifications
- Using permission sets with McAfee EMM

Customize the company profile

Customize the company name and use agreement that appears on user devices.

Task


2. Modify the fields as needed, then click Save.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Company name as it appears on user devices.</td>
</tr>
<tr>
<td>User Agreement</td>
<td>Use agreement that is pushed to devices during configuration.</td>
</tr>
</tbody>
</table>
**Update the default administrator account**

Secure the connection between the McAfee EMM Hub and the ePolicy Orchestrator server by changing the default system administrator logon credentials.

**Task**

1. Select **Menu** | **Configuration** | **Server Settings** | **EMM Server Settings** | **System Settings** | **Console Access**.

2. Click **Add**, complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Type</td>
<td>Local User</td>
</tr>
<tr>
<td>Role</td>
<td>System Administrator</td>
</tr>
<tr>
<td>Username</td>
<td>User name for the connection to the McAfee EMM server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the connection to the McAfee EMM server.</td>
</tr>
</tbody>
</table>

3. Select the default account, then click **Delete**.

**Create a service record**

A service (SRV) record automatically directs user devices to the McAfee EMM Portal so users don't need to enter the server name during device configuration.

**Task**

1. Create an SRV record with this format:

   `_activation._tcp.<domainname>. 86400 IN SRV 0 1 443 <EMMportalhostname>`

   • `<domainname>` is the domain name used in company email addresses.
   • `<EMMportalhostname>` is the fully qualified domain name of the McAfee EMM portal.

   An SRV record for Acme, Corp. would look like this:

   `_activation._tcp.acme.com. 86400 IN SRV 0 1 443 emm.acme.com`

2. Publish the SRV record to a device-accessible Domain Name System (DNS) server.

**Configure an authorization directory**

To authorize users, specify an authorization directory. You can use LDAP or ActiveSync Protocol for user authentication.

**Task**

1. Select **Menu** | **Configuration** | **Server Settings** | **EMM Server Settings** | **System Settings** | **Auth Directories**.

2. Do one of the following:
   - To add a directory, click **Add**.
   - To edit a directory, select the directory from the list, then click **Edit**.

---

**Getting started**

**Update the default administrator account**

Secure the connection between the McAfee EMM Hub and the ePolicy Orchestrator server by changing the default system administrator logon credentials.

**Task**

1. Select **Menu** | **Configuration** | **Server Settings** | **EMM Server Settings** | **System Settings** | **Console Access**.

2. Click **Add**, complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Type</td>
<td>Local User</td>
</tr>
<tr>
<td>Role</td>
<td>System Administrator</td>
</tr>
<tr>
<td>Username</td>
<td>User name for the connection to the McAfee EMM server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the connection to the McAfee EMM server.</td>
</tr>
</tbody>
</table>

3. Select the default account, then click **Delete**.

**Create a service record**

A service (SRV) record automatically directs user devices to the McAfee EMM Portal so users don't need to enter the server name during device configuration.

**Task**

1. Create an SRV record with this format:

   `_activation._tcp.<domainname>. 86400 IN SRV 0 1 443 <EMMportalhostname>`

   • `<domainname>` is the domain name used in company email addresses.
   • `<EMMportalhostname>` is the fully qualified domain name of the McAfee EMM portal.

   An SRV record for Acme, Corp. would look like this:

   `_activation._tcp.acme.com. 86400 IN SRV 0 1 443 emm.acme.com`

2. Publish the SRV record to a device-accessible Domain Name System (DNS) server.

**Configure an authorization directory**

To authorize users, specify an authorization directory. You can use LDAP or ActiveSync Protocol for user authentication.

*Email policy settings override authorization directory settings.*

**Task**

1. Select **Menu** | **Configuration** | **Server Settings** | **EMM Server Settings** | **System Settings** | **Auth Directories**.

2. Do one of the following:
   - To add a directory, click **Add**.
   - To edit a directory, select the directory from the list, then click **Edit**.
3  Complete or modify the fields based on your authentication type, then click **Save**.

User authentication options vary depending on the LDAP server settings specified during installation.

- **For LDAP user authentication:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Type</strong></td>
<td>• AD&lt;br&gt;• Domino</td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>Fully qualified domain name of the LDAP server.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>This field populates when <strong>FQDN</strong> is completed.</td>
</tr>
<tr>
<td><strong>DN</strong></td>
<td>Domain distinguished name of the LDAP. &lt;br&gt;• AD — This field populates when <strong>FQDN</strong> is completed.&lt;br&gt;• Domino — Leave this field blank.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>User name for the connection to the server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password for the connection to the server.</td>
</tr>
<tr>
<td><strong>External EMM Proxy Server Address</strong></td>
<td>Fully qualified domain name of the McAfee EMM Proxy. Devices connect to this McAfee EMM Proxy address for ActiveSync.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>This option is selected by default and can't be changed.</td>
</tr>
</tbody>
</table>

- **For ActiveSync Protocol user authentication:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ActiveSync Authentication Address</strong></td>
<td>IP address or fully qualified domain name of the ActiveSync server.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Domain name of the ActiveSync server.</td>
</tr>
<tr>
<td><strong>Verification Username</strong></td>
<td>User name for the connection to the server.</td>
</tr>
<tr>
<td><strong>Verification Password</strong></td>
<td>Password for the connection to the server.</td>
</tr>
<tr>
<td><strong>ActiveSync External DNS</strong></td>
<td>External DNS or IP address of the server that connects to the McAfee EMM Proxy.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>This option is selected by default and can't be changed.</td>
</tr>
</tbody>
</table>

---

**Add GCM settings for upgrades**

If you upgraded from McAfee EMM 10.2 and reused an existing database, manually add Google Cloud Messaging (GCM) settings. For new installations, the installer prompts for these settings.

**Before you begin**

Set up a **Google API project** and obtain a token and **Sender ID**, or project number, from Google. See **KB77397** for details.

To use GCM push notifications, Android devices must be upgraded to the McAfee EMM Android app version 2.5 or later. Earlier versions of the app are functional with McAfee EMM 11.0, but they rely on the deprecated Google Cloud to Device Messaging (C2DM) framework. See **Upgrade Android devices**.
Configure an SMTP server and default notification settings

Before sending user notifications, configure an SMTP server. You can also specify default notification settings to speed the bulk-authorization process.

**Task**


2. Click Update, complete the fields, then click Save.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender ID</td>
<td>Project number of your Google API project.</td>
</tr>
<tr>
<td>Token</td>
<td>API key value of your Google API project.</td>
</tr>
</tbody>
</table>

3. (Optional) To send a test text message, click Send Test SMS.

**See also**

*Upgrade Android devices on page 30*

**Customize certificate expiration notifications**

Automatically receive notification when portal, push, or mobile device management (MDM) certificates near expiration by customizing the default EMM Certificates Notification server task. The server task can be viewed, edited, or disabled, but it can't be deleted.

**Before you begin**

An email server must be configured in ePolicy Orchestrator. For details, see the ePolicy Orchestrator documentation.
Task
For option definitions, click ? in the interface.

1. Select Menu | Automation | Server Tasks.
2. In the EMM Certificates Notification row, click Edit.
3. Use the Server Task Builder to customize the server task.

Using permission sets with McAfee EMM

McAfee EMM adds two permission groups to each ePolicy Orchestrator permission set. These permission sets define rights for policies and actions performed on mobile devices.

McAfee EMM adds these permission groups:

- McAfee Enterprise Mobility Management — Defines permissions for mobile policies.
- Mobile Actions — Defines permissions for actions performed on mobile devices.

ePolicy Orchestrator grants all permissions for all products and features to global administrators, who in turn assign user roles to existing permission sets or create new permission sets. For users not assigned a global administrator user role, both of the McAfee EMM permission groups grant No Permissions by default. Permissions must be granted for mobile policies to appear in the Policy Catalog, and for mobile actions to appear on the Actions menu in the System Tree.

Permissions assigned to ePolicy Orchestrator features might affect users' ability to perform certain McAfee EMM functions. For example, to access mobile actions, users must also have permission to view the System Tree.

For details on managing permission sets, see the ePolicy Orchestrator documentation.
Getting started
Using permission sets with McAfee EMM
Authorizing users

Grant users access to your network from their mobile devices based on LDAP or ActiveSync credentials. You can set temporary passwords, or provisioning tokens, unlock users with failed password attempts, and (optionally) manage Device ID Mapping for certain Android devices.

Contents
- Manage provisioning tokens
- Authorize users
- Unlock users
- Managing Android Device ID Mapping

Manage provisioning tokens
Provisioning tokens provide an optional, extra measure of security when users configure their devices.

You can use provisioning tokens only with iOS and Android devices. Windows Phones can't be configured successfully if users are assigned provisioning tokens.

Tasks
- **Require provisioning tokens on page 17**
  Turn on the provisioning token requirement so that you can create and send provisioning tokens as you authorize users.
- **Update provisioning tokens on page 18**
  Update a user’s provisioning token manually when a token expires, or when a user needs to configure another device.

Require provisioning tokens
Turn on the provisioning token requirement so that you can create and send provisioning tokens as you authorize users.

Selecting the provisioning token option doesn’t affect users who have already configured their devices.

If you require provisioning tokens:
• When you bulk-authorize users, a default token and expiration are added to the notification message. See Bulk-authorize and notify LDAP or ActiveSync users.

• When you authorize select users, you're prompted to specify provisioning token options. See Authorize select LDAP users.

Task
1 Select Menu | Configuration | Server Settings | EMM Server Settings | System Settings | Authorized Users.

2 Select Allow Only Authorized Users and Require Provisioning Token, specify the default Token Length and Hours Valid, then click Save.

See also
Bulk-authorize and notify LDAP or ActiveSync users on page 19
Authorize select LDAP users on page 20

Update provisioning tokens
Update a user’s provisioning token manually when a token expires, or when a user needs to configure another device.

Before you begin
The user must be on the Authorized Users list. See Authorize users.
(Optional) To send the updated provisioning token to users in a text message or email, an SMTP server must be configured in Mail Settings. See Configure an SMTP server and default notification settings.

Task
1 Select Menu | Configuration | Server Settings | EMM Server Settings | System Settings | Authorized Users.

2 Click Update Token, then select a user or group.

3 Specify options for the provisioning token, then click Save.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Token</td>
<td>Temporary password.</td>
</tr>
<tr>
<td>Hours Valid</td>
<td>Number of hours the temporary password is valid. This value overrides the default value set on the Authorized Users screen.</td>
</tr>
<tr>
<td>Delivery Action</td>
<td>Select how the user receives the temporary password:</td>
</tr>
<tr>
<td></td>
<td>• No Action</td>
</tr>
<tr>
<td></td>
<td>• Send SMS — Opens the Provisioning SMS screen. Enter the Recipient’s Phone Number, Carrier, Subject, and Message, then click Send SMS.</td>
</tr>
<tr>
<td></td>
<td>• Send E-mail — Opens an email to the user containing the temporary password. Click Send to deliver the email.</td>
</tr>
</tbody>
</table>

See also
Authorize users on page 19
Configure an SMTP server and default notification settings on page 14
Authorize users

Choose an authorization method based on the type of user authentication in use on your system and the number of users you need to authorize.

Tasks

- **Bulk-authorize and notify LDAP or ActiveSync users on page 19**
  Authorize many users at once and automatically send them emails or text messages with configuration details. You can bulk-authorize users based on LDAP groups or by importing a list in comma separated value (CSV) format. This is the recommended authorization method if you require provisioning tokens.

- **Authorize select LDAP users on page 20**
  By default, all users with valid Active Directory or Domino credentials can configure their devices. For greater security, specify which LDAP users or groups can configure devices.

- **Authorize select ActiveSync users on page 21**
  Allow selected users to configure their devices by manually specifying their ActiveSync credentials.

- **Authorize LDAP or ActiveSync users based on a list on page 21**
  Allow a list of users to configure their devices using LDAP or ActiveSync credentials.

Bulk-authorize and notify LDAP or ActiveSync users

Authorize many users at once and automatically send them emails or text messages with configuration details. You can bulk-authorize users based on LDAP groups or by importing a list in comma separated value (CSV) format. This is the recommended authorization method if you require provisioning tokens.

Before you begin

An SMTP server must be configured in Mail Settings. See Configure an SMTP server and default notification settings.

(Optional) To automatically assign temporary passwords as you authorize users, change your settings to require provisioning tokens. See Require provisioning tokens.

(Optional) To authorize users based on a CSV list, create a list. For details on formatting, see CSV format for list-based user authorization.

Task


2. Click Provision Users, complete the fields, then click Next.

- **Search LDAP (LDAP authentication)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Search LDAP</td>
</tr>
<tr>
<td>Location</td>
<td>Domain of the LDAP server.</td>
</tr>
<tr>
<td>User/Group</td>
<td>Select the users or groups to add as authorized users. Entering a user or group name populates the Search Results.</td>
</tr>
<tr>
<td>Search Results</td>
<td>Select users from this list and use the arrows to move them to the list of Users to Provision.</td>
</tr>
</tbody>
</table>
• Import CSV (LDAP or ActiveSync Protocol authentication)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Import CSV</td>
</tr>
<tr>
<td>Location</td>
<td>Domain of the LDAP or ActiveSync server.</td>
</tr>
<tr>
<td>CSV File Path</td>
<td>Browse to select the CSV file.</td>
</tr>
</tbody>
</table>

3 On the second Provision Users screen, complete the fields, then click Send Email or Send SMS.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Delivery Method | Email  

SMS — This option is available only with CSV import.  

Notification Message | Enter the message you want to send to users.  

• If you select Email as the Delivery Method, the default notification text specified in Mail Settings appears. You can edit the message before sending.  

• If you select SMS as the Delivery Method, your notification message can't exceed 140 characters.  

If your system settings require a provisioning token, a default token and expiration are added to your notification message in the format OTPToken: %OTPToken%
Token Expiration: %OTPTokenExpiration. Don't delete this text.

Targeted Users | Confirm the list of users to authorize.  

See also  
Configure an SMTP server and default notification settings on page 14  
Require provisioning tokens on page 17  
CSV format for list-based user authorization on page 22

Authorize select LDAP users  
By default, all users with valid Active Directory or Domino credentials can configure their devices. For greater security, specify which LDAP users or groups can configure devices.

Before you begin  
(Optional) To create and send temporary passwords as you authorize users, change your settings to require provisioning tokens. See Require provisioning tokens.

Task  
1 Select Menu | Configuration | Server Settings | EMM Server Settings | System Settings | Authorized Users.  
2 Select Allow Only Authorized Users.  
3 Click Add, then complete the fields to search for a user or group:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Search LDAP</td>
</tr>
<tr>
<td>Location</td>
<td>Domain of the LDAP server.</td>
</tr>
<tr>
<td>User/Group</td>
<td>Enter at least the first three characters of the user or group to add.</td>
</tr>
</tbody>
</table>

4 Do one of the following, based on whether your settings require provisioning tokens:  

• Provisioning tokens — Select the user or group to add, specify additional options, then click Save.
Option | Definition
---|---
Provisioning Token | Temporary password.
Hours Valid | Number of hours the temporary password is valid. This value overrides the default value set on the Authorized Users screen.
Delivery Action | Select how the user receives the temporary password:
  • **No Action**
  • **Send SMS** — Opens the Provisioning SMS screen. Enter the **Recipient’s Phone Number**, **Carrier**, **Subject**, and **Message**, then click **Send SMS**.
  • **Send E-mail** — Opens an email to the user containing the temporary password. Click **Send** to deliver the email.

**No provisioning tokens** — Select the user or group to add, click **Save** to add them to the list of authorized users, then click **Save** again.

**See also**
*Require provisioning tokens on page 17*

**Authorize select ActiveSync users**
Allow selected users to configure their devices by manually specifying their ActiveSync credentials.

**Task**
1. Select **Menu** | **Configuration** | **Server Settings** | **EMM Server Settings** | **System Settings** | **Authorized Users**.
2. Click **Add**, complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Manually Define User</td>
</tr>
<tr>
<td>Location</td>
<td>Domain of the ActiveSync server.</td>
</tr>
<tr>
<td>Username</td>
<td>User name of the individual to authorize.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Email address of the individual to authorize.</td>
</tr>
<tr>
<td>First Name</td>
<td>First name of the individual to authorize.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Last name of the individual to authorize.</td>
</tr>
</tbody>
</table>

**Authorize LDAP or ActiveSync users based on a list**
Allow a list of users to configure their devices using LDAP or ActiveSync credentials.

**Before you begin**
Create a CSV list of authorized users. For details on formatting, see *CSV format for list-based user authorization*. 
Task
2. Select Allow Only Authorized Users.
3. Click Add, complete the fields, then click Save.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Import CSV</td>
</tr>
<tr>
<td>Location</td>
<td>Domain of the LDAP or ActiveSync server.</td>
</tr>
<tr>
<td>CSV File Path</td>
<td>Browse to select the CSV file.</td>
</tr>
</tbody>
</table>

See also
CSV format for list-based user authorization on page 22

CSV format for list-based user authorization
Use these guidelines to format a CSV file for importing authorized users.

Format your CSV file with a file name on row one of your spreadsheet, column headings on row two, and user data beginning on row three. Column headings must read exactly as shown here.

<table>
<thead>
<tr>
<th>[File Name]</th>
<th>UserName</th>
<th>Email</th>
<th>FirstName</th>
<th>LastName</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserXyz</td>
<td><a href="mailto:userxyz@company.com">userxyz@company.com</a></td>
<td>User</td>
<td>Xyz</td>
<td>123-456-7890</td>
<td></td>
</tr>
</tbody>
</table>

Unlock users
When users exceed the allowed attempts to enter their credentials during device configuration, their account must be unlocked by an administrator.

Task
For option definitions, click ? in the interface.
1. Select Menu | User Management | Locked Users.
2. Select the checkbox next to the users to unlock, then click Actions | Unlock.

The user is removed from the Locked Users list.

Managing Android Device ID Mapping
The Device ID Mapping feature in McAfee EMM resolves duplicate System Tree entries for certain Android devices. Device IDs are paired automatically by default, but you can opt to manually pair Device IDs.

Some Android devices that were provisioned with ActiveSync for email report two separate Device IDs to the McAfee EMM server. Device ID Mapping pairs the duplicate IDs so that the device appears only once in the System Tree.
By default, Device ID Mapping is set to Automatic. This is the recommended setting, but you can choose to manually approve Device ID pairings for increased security and assurance of user and device identity. Manual Device ID Mapping requires action by both the McAfee EMM administrator and the device user.

When manual Device ID Mapping is activated:

- The Device Status for unpaired devices appears as Pending Approval until an administrator approves the Device ID pairing.
- Android users with a Device ID Mapping discrepancy must respond to a confirmation notification during email provisioning.
- Users can’t sync email until the Device ID pairing is resolved.

For details on provisioning Android devices with manual Device ID Mapping activated, see *Manually configure email for Android devices*.

See also
*Manually configure email for Android devices on page 28*

**Activate manual Device ID Mapping**
To manually approve Android Device ID pairings, activate manual Device ID Mapping. McAfee EMM automatically maps Device IDs by default.

**Task**
1. Select *Menu* | *Configuration* | *Server Settings* | *EMM Server Settings* | *System Settings* | *Device ID Mapping*.
2. Select Manual, then click *Save*.

**Manually approve Device ID Mapping**
If you activated manual ID mapping for Android devices, you must approve each duplicate Device ID pairing when users configure their devices.

**Task**
1. Select *Menu* | *Configuration* | *Server Settings* | *EMM Server Settings* | *System Settings* | *Device ID Mapping*.
2. Select the device to approve, then click *Approve*.

The McAfee EMM server sends the user a confirmation notification. After the user confirms, the Device Status on the System Information page (Mobile Properties | Device Details) changes from Pending Approval to Available and the device begins syncing.
Authorizing users
Managing Android Device ID Mapping
Configuring devices

After configuring the server-side McAfee EMM components, mobile devices can be configured with the McAfee EMM app and McAfee Secure Container. Configuration secures the device and provides access to corporate email, contacts, and calendars. Configuration must be done on the device.

Since device configuration involves entering user credentials, we recommend sharing the configuration instructions with users to allow them to configure their own devices.

Device configuration requirements

Before configuring mobile devices, verify these requirements for your McAfee EMM installation and the devices on your network.

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>• Configure ActiveSync to use the same LDAP server as McAfee EMM for authentication.</td>
</tr>
<tr>
<td></td>
<td>• Grant these server permissions:</td>
</tr>
<tr>
<td></td>
<td><strong>Grant this permission...</strong> To the LDAP account used to...</td>
</tr>
<tr>
<td></td>
<td>Local administrator rights on the McAfee EMM Hub server.</td>
</tr>
<tr>
<td></td>
<td>Read-only access to the LDAP Directory server.</td>
</tr>
<tr>
<td></td>
<td>Access the database.</td>
</tr>
<tr>
<td></td>
<td>Query the database for user and group searches.</td>
</tr>
<tr>
<td>Authorization</td>
<td>• Configure an authorization directory. See <em>Configure an authorization directory</em>.</td>
</tr>
<tr>
<td></td>
<td>• If your system selectively authorizes users, add users to the Authorized Users list.</td>
</tr>
<tr>
<td></td>
<td>• If you set provisioning tokens for authorized users, send users their tokens.</td>
</tr>
<tr>
<td></td>
<td>Use the User Notifications feature to bulk-authorize users and send their provisioning tokens at the same time. See <em>Bulk authorize and notify LDAP or ActiveSync users</em>.</td>
</tr>
<tr>
<td>SRV record</td>
<td>If you want devices to automatically detect the McAfee EMM Portal, create an SRV record. See <em>Create a service record</em>.</td>
</tr>
</tbody>
</table>
## Configuring devices

**Communicating with users**

Facilitate a smooth onboarding process by communicating with mobile device users about configuration steps and planned changes or restrictions to their devices.

User Notifications allow you to authorize many users at once and automatically send an email with configuration steps and provisioning tokens. For guidance on sending User Notifications, see *Bulk-authorize and notify LDAP or ActiveSync users*.

After configuring their devices, users might notice some changes in functionality. In many cases, the only difference is that users must enter a passcode to access their device. In other cases, your security policy might limit access to applications. To reduce support calls, make users aware of anticipated changes in advance.

**See also**

*Bulk-authorize and notify LDAP or ActiveSync users* on page 19

## Configure devices

Mobile devices must be configured on the device itself. Configuration methods vary by device type.

**Tasks**

- *Configure iOS devices on page 27*
  Use the McAfee EMM app to configure iOS devices.

- *Configure Android devices on page 27*
  Use the McAfee EMM app to configure Android devices. The app walks you through installing McAfee Secure Container. If you don't install McAfee Secure Container, manually configure email for Android devices.

- *Configure Windows Phones on page 28*
  Use Exchange ActiveSync to manually configure email for Windows Phone 7 or Windows Phone 8.
Configure iOS devices
Use the McAfee EMM app to configure iOS devices.

Task
1. Download the McAfee EMM app from the Apple App Store.
2. Launch the McAfee EMM app, enter your email address and password, then tap Sign In.
   - If prompted, enter the server address provided by your administrator, then tap Sign In.
   - If prompted, enter the provisioning token provided by your administrator, then tap OK.
3. Review and accept the terms of the license agreement, then tap Next.
4. Tap Install, then confirm by tapping Install Now.
   - If prompted, enter the device passcode, then tap Done.
5. Tap Install to allow your administrator to remotely manage your device, then tap Done.

Configure Android devices
Use the McAfee EMM app to configure Android devices. The app walks you through installing McAfee Secure Container. If you don't install McAfee Secure Container, manually configure email for Android devices.

These instructions provide general guidance to configure an Android device. Specific screens might vary by device manufacturer.

Tasks
- Configure Android devices using the McAfee EMM app on page 27
  Configuring with the McAfee EMM app secures the device and optionally installs McAfee Secure Container for enterprise email, contacts, and calendars.
- Manually configure email for Android devices on page 28
  If you don't install McAfee Secure Container, use Exchange ActiveSync to configure email.

Configure Android devices using the McAfee EMM app
Configuring with the McAfee EMM app secures the device and optionally installs McAfee Secure Container for enterprise email, contacts, and calendars.

Task
1. Download the McAfee EMM app from Google Play and confirm the download, then tap Install.
2. Launch the McAfee EMM app, enter your email address and password, then tap Sign In.
   - If prompted, enter the server address provided by your administrator, then tap Sign In.
   - If prompted, enter the provisioning token provided by your administrator, then tap OK.
3. Review and accept the terms of the license agreement, then tap Next.
4. Tap Activate to activate Device Administrator.
5. If you're redirected to your device's encryptions settings page, tap to encrypt your device.
6. Set a passcode for your device, then tap OK.
7. Do one of the following, based on whether your organization requires McAfee Secure Container:
If McAfee Secure Container is...

<table>
<thead>
<tr>
<th>Required</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>Tap OK to go to Google Play to install the app.</td>
</tr>
<tr>
<td>Recommended</td>
<td>Tap Yes to go to Google Play to install the app.</td>
</tr>
<tr>
<td>Recommended</td>
<td>Tap No to set up email using Exchange ActiveSync. See <em>Manually configure email for Android devices</em>.</td>
</tr>
</tbody>
</table>

8 If you installed McAfee Secure Container in the previous step, enter your email password and set a passcode for McAfee Secure Container.

See also

_Manually configure email for Android devices on page 28_

**Manually configure email for Android devices**

If you don't install McAfee Secure Container, use Exchange ActiveSync to configure email.

**Task**

1. Tap **Applications** | **Settings** | **Accounts and sync** | **Add Account** | **Microsoft Exchange ActiveSync**.

2. Enter your email address, password, domain\user name, and proxy server address, then tap **Done**.
   - If you receive an error message, when a notification appears in the notification area, open it and tap **OK** to confirm email setup.
   - It might take a few minutes for the McAfee EMM server to send a notification to your device.

   • If you receive a second error message, contact your system administrator for resolution. When the administrator resolves the issue, a second notification appears in the notification area. Open it and tap **OK** to complete the email setup.

3. If prompted, tap **OK** to allow remote security administration.

**Configure Windows Phones**

Use Exchange ActiveSync to manually configure email for Windows Phone 7 or Windows Phone 8.

This task provides general guidance to configure a Windows Phone. Specific screens might vary by device manufacturer.

**Task**

1. Tap **Settings** | **Email & Accounts** | **Add an Account** | **Outlook**.

2. Enter your email address and password, then tap **Sign In**.
   - The message "Your settings could not be found..." appears.

3. Enter the domain, then tap **Sign In**.
   - The message "Your settings could not be found..." appears.

4. Tap **OK**, then tap **Advanced**.

5. Enter the server address of the McAfee EMM Proxy, then tap **Sign In**.
# Updating devices

iOS and Android devices configured for McAfee EMM 10.2 or earlier must be updated for version 11.0. Updating iOS and Android devices applies the updated policy framework of McAfee EMM 11.0. This allows you to change individual policy settings without reapplying the entire policy.

The update requirements vary by platform.

## iOS

To configure iOS devices for McAfee EMM 11.0, update the device. This is a one-click process with minimal impact on users. See Update devices.

## Android

To configure Android devices for McAfee EMM 11.0, you have two options:

- **Update devices** — This is a one-click process with minimal impact on users. See Update devices.

- **Upgrade devices** — This process involves upgrading to the McAfee EMM Android app version 2.5 or later, then re-entering user credentials. Upgrading applies the updated policy framework of version 11.0 and migrates Android devices to the GCM push service. Earlier versions of the app are functional with McAfee EMM 11.0, but they rely on a deprecated push notification framework. See Upgrade Android devices.

> Upgrade is recommended at the first opportunity for Android devices.

## Windows Phone

Windows Phones don’t require an update to move to McAfee EMM 11.0.

See also

- Update devices on page 29
- Upgrade Android devices on page 30

# Update devices

Updating iOS and Android devices applies the updated policy framework of McAfee EMM 11.0. This allows you to change individual policy settings without reapplying the entire policy.

**Task**

1. On iOS devices, tap **Settings | General | Profiles**, select the **Mobile Device Management Profile**, then tap **Remove**.

2. On iOS and Android devices, open the McAfee EMM app and tap **Update Configuration**.

Devices check in and receive updated McAfee EMM configuration and policy profiles.
Upgrade Android devices
Upgrading Android devices to the McAfee EMM Android app version 2.5 or later activates GCM push services. Upgrade is recommended at the first opportunity for Android devices since the previous Android push service is deprecated.

Before you begin
If you upgraded from McAfee EMM 10.2 and reused an existing database, manually add GCM settings. See Add GCM settings for upgrades. GCM settings are added during setup for new installations.

Task
1. Tap Google Play | My Apps, locate the McAfee EMM app, then tap Update.
2. Launch the McAfee EMM app, enter your email address and password, then tap Sign In.
   - If prompted, enter the server address provided by your administrator, then tap Sign In.
   - If prompted, enter the provisioning token provided by your administrator, then tap OK.
3. Review and accept the terms of the license agreement, then tap Next.

See also
Add GCM settings for upgrades on page 13
Managing devices

McAfee EMM provides day-to-day management of mobile devices in your network. You can view device details and perform actions on mobile devices, distribute apps and files using packages, and manage volume licenses for iOS apps.

Contents

- Organizing mobile devices in the System Tree
- Viewing mobile properties
- Performing mobile actions
- Updating mobile devices
- Blacklisting apps
- Distributing apps and files
- Managing volume licenses for iOS apps

Organizing mobile devices in the System Tree

The ePolicy Orchestrator System Tree lets you organize and manage mobile devices in your network. The organizational structure that you put in place in the System Tree affects how security policies are inherited and enforced throughout your environment. For details on setting up your System Tree, see the ePolicy Orchestrator documentation.

Make your McAfee EMM extension easier to manage by following these guidelines for setting up your System Tree:

- Tag devices as corporate-owned or personal so you can perform targeted actions and queries.
- Tag devices that have blacklisted apps so you can apply policies accordingly. To automate tagging of blacklisted apps, see Blacklisting apps.

To differentiate mobile devices from other systems in your System Tree, add columns for Product Version (EMM) or Management Type.

See also

Blacklisting apps on page 33

Viewing mobile properties

Mobile properties provide in-depth data about the devices in your network.

You can view details about mobile devices by clicking a device to open the System Information page, then selecting the Mobile Properties window. The System Information page is accessible from the System Tree and from other areas of ePolicy Orchestrator that let you drill down to specific devices.
Mobile properties are grouped into these categories on separate tabs of the Mobile Properties window:

- Device Properties
- Pending Actions
- Telecommunication Properties
- Certificates
- Device Details
- Configuration Profiles
- Mobile Applications
- Provisioning Profiles

For details on mobile properties, see Mobile properties.

The properties that are reported to ePolicy Orchestrator vary by mobile operating system. Mobile properties appear only for devices where they apply. For example, iOS devices display the ActiveSync ID property, but not the Android-specific Device ID property. Similarly, the categories on the Mobile Properties window, like Pending Actions, appear only if they apply, and the Mobile Properties window itself is only displayed for mobile devices.

To view compliance status for mobile devices at a glance, customize the Summary pane on the System Information page to display EMM Managed Devices Compliant Status.

Compliance status for other McAfee products, like the McAfee Agent, don't provide an accurate compliance summary for mobile devices.

See also
Mobile properties on page 4

## Performing mobile actions

Remotely control access to mobile devices with lock and passcode controls, and protect corporate data with targeted wipe functions.

McAfee EMM adds these mobile actions to the Actions menu in ePolicy Orchestrator, accessible from the System Tree or by selecting a device to open the System Information page. Users must be granted permission to the Mobile Actions permission group for these actions to appear on the Actions menu.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Useful when...</th>
<th>Platform support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock</td>
<td>Activates the device passcode. This action doesn't prevent the user from unlocking the device if they know the passcode.</td>
<td>Users are temporarily away from their unlocked device.</td>
<td>X X</td>
</tr>
<tr>
<td>MDM Uninstall</td>
<td>Removes the MDM profile and other profiles installed by McAfee EMM, like email, Wi-Fi, and VPN profiles.</td>
<td>Users leave the company in a BYOD environment, taking their enterprise-enabled personal device with them.</td>
<td>X X</td>
</tr>
</tbody>
</table>
| Unlock       | • iOS — Temporarily deactivates the passcode so the user can open the device without entering a passcode.  
               • Android — Generates a new, temporary passcode. | Users forget their device passcode.                                           | X X             |
### Action Description Useful when... Platform support

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>iOS</th>
<th>Android</th>
<th>Windows Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wipe</td>
<td>Restores the device to factory settings.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wipe Corporate Data</td>
<td>Deletes company email, contacts, and calendars, but does not remove software, profiles, or applications.</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

- **Wipe**: Restores the device to factory settings. Useful when devices are lost or stolen, or need to be redeployed to a new user.
- **Wipe Corporate Data**: Deletes company email, contacts, and calendars, but does not remove software, profiles, or applications. Useful when users no longer want to perform company functions on their devices, but you still want to manage the device with McAfee EMM.

In addition to mobile-specific actions, you can use many of the standard ePolicy Orchestrator actions to organize mobile devices in the System Tree, like applying tags and moving or deleting systems. However, since mobile devices don't have a traditional McAfee Agent, some options in the Actions menu don't have any effect on mobile devices. For a complete list of actions that don't apply to mobile devices, see KB77599.

### Updating mobile devices

Devices check in automatically every 24 hours for MDM, or every 15 minutes for ActiveSync. At check-in, pending actions and policy updates are pushed to the device, and device properties are updated in ePolicy Orchestrator.

You can force an update immediately by clicking Wake Up Agents in the System Information page for any device. The device has successfully updated when Pending Actions are cleared and the Last check-in property in the Device Details tab is updated.

### Blacklisting apps

To specify blacklisted apps, and tag devices that contain those apps, complete these tasks in order.

**Before you begin**
Create a blacklisted apps tag. For information on creating and using tags, see the ePolicy Orchestrator documentation.

Consider setting up blacklisting separately for iOS and Android devices to allow more flexibility for scheduling blacklist checks, applying policies, and managing devices in the System Tree.

**Tasks**
- **Create a blacklisted apps query on page 33**
  Customize a query to search for specific apps to blacklist.
- **Create a blacklisted apps server task on page 34**
  Customize a server task to tag mobile devices that include blacklisted apps. Once tagged, you can group devices with blacklisted apps in the System Tree, or perform other actions as needed.

**Create a blacklisted apps query**
Customize a query to search for specific apps to blacklist.
**Task**

For option definitions, click ? in the interface.

1. Select Menu | Reporting | Queries & Reports, then click Actions | New.

2. From the System Management Feature Group, select Managed Systems, then click Next.

3. Select to display results as a Table, then click Next.

4. From the Available Columns list, select to display System Name and, from the Mobile Applications properties group, Identifier and Name, then click Next.

Your table mock-up should look like this:

<table>
<thead>
<tr>
<th>System Name</th>
<th>Identifier</th>
<th>Name</th>
</tr>
</thead>
</table>

5. From the Available Properties list in the Mobile Applications properties group, select at least one of these properties:
   - **Identifier** — Use to filter based on the app's bundle ID (iOS) or package name (Android).

   Identifiers for installed apps are listed for each device on the System Information page under Mobile Properties | Mobile Applications. The bundle ID for iOS apps also appears in the .plist file of the app after "com." The package name for Android apps is shown in the Google Play URL of the app between "id=" and "&feature".

   - **Name** — Use to filter based on the name of the app.

6. Specify criteria for the properties you selected in the previous step, then click Save.

7. Enter a name for the query, like Blacklisted Apps, then click Save.

**Create a blacklisted apps server task**

Customize a server task to tag mobile devices that include blacklisted apps. Once tagged, you can group devices with blacklisted apps in the System Tree, or perform other actions as needed.

**Before you begin**

Create a blacklisted apps query. See Create a blacklisted apps query.

To ensure that blacklisted apps tags are updated on a continual basis, configure the server task to perform two actions. The first action clears the existing blacklisted apps tag, and the second action applies — or reapplies — the blacklisted apps tag based on the latest blacklisted apps query.

**Task**

For option definitions, click ? in the interface.

1. Select Menu | Automation | Server Tasks, then click New Task.

2. Enter a name for the server task, like Blacklisted Apps, then click Next.
Specify options to clear existing blacklisted apps tags, then click + to add a second Action.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Actions | System Search — ePolicy Orchestrator 4.6.5  
          | System Search by Tag or Group — ePolicy Orchestrator 5.0 |
| By Tag  | Select the custom blacklisted apps tag to search for. |
| Sub-Actions | Clear Tag |
| Tag     | Select the custom blacklisted apps tag to clear.  
          | ![Caution: Don't check Clear All. This option clears all tags applied to devices.](image)

Specify options to apply the blacklisted apps tag based on the blacklisted apps query, then click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Run Query</td>
</tr>
<tr>
<td>Query</td>
<td>Select the custom blacklisted apps query.</td>
</tr>
<tr>
<td>Sub-Actions</td>
<td>Apply Tag</td>
</tr>
<tr>
<td>Tag</td>
<td>Select the custom blacklisted apps tag.</td>
</tr>
</tbody>
</table>

Specify scheduling options for the server task, then click Next.

Review the server task summary, then click Save.

The server task is added to the Server Tasks list, and runs as specified. For details, select Menu | Automation | Server Task Log.

See also

Create a blacklisted apps query on page 33

### Distributing apps and files

**Packages** allow you to distribute and install applications remotely on user devices. With packages, you can give employees the apps they need without the hassle of searching for apps individually.

Create customized packages for iOS or Android devices, then assign and push packages to devices based on users or groups.

Packages can include these types of files:

**iOS**

- Enterprise apps
- Apple App Store apps
- Configuration profiles, or `mobileconfig` files

**Android**

- Enterprise apps
- Google Play apps
Create or modify packages

McAfee EMM provides two default packages, one for iOS and one for Android. You can modify files in the default package, or you can create, name, and modify new packages.

Task

1 Select Menu | Configuration | Server Settings | EMM Server Settings | Package Management.

2 To create a new package, click Create New, select a mobile platform, provide a name for the package, then click Save.

3 Select the package to modify, then do one of the following:
   • To add a file to the package, click Add, specify details about the file, then click Add File. For option definitions, see Package options.
   • To change the installation order of files, click Reorder, use the arrows to set the installation order of files, then click Save.
   • To remove files from the package, select the file to delete, then click Remove.

See also

Package options on page 37
Package options
Use these option definitions to specify apps and files to add to packages.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Enterprise Application</th>
<th>App Store Application or Marketplace Application</th>
<th>MobileConfig</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS</td>
<td>• IPA Path — Browse to select the app.</td>
<td>• Application Name — Name of the app.</td>
<td>• File Name — Browse to select the file.</td>
</tr>
<tr>
<td></td>
<td>• Icon Path — Browse to select an optional icon.</td>
<td>• Application Link — Link to the app.</td>
<td>• Version — Version of the file.</td>
</tr>
<tr>
<td></td>
<td>• Install application when provisioning, reprovisioning, or pushing the package — Select to install the app each time:</td>
<td>• Icon Path — Browse to select an optional icon.</td>
<td>• Notes — Optional description.</td>
</tr>
<tr>
<td></td>
<td>• The device is configured.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The user clicks Update Configuration in the McAfee EMM app.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A McAfee EMM administrator pushes applications to the device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Delete application and application data at MDM uninstall — Select to delete the app and app data when:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A user uninstalls the MDM profile from the device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A McAfee EMM administrator performs an MDM Uninstall action on the device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• App data can't be recovered after uninstalling.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Prevent the backup of application data to iTunes and iCloud — Select to prevent cloud backup of app data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>• Application Name — Name of the app.</td>
<td>• Application Name — Name of the app.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Version — Version of the app.</td>
<td>• Application Link — Link to the app.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• APK Path — Browse to select the app.</td>
<td>• Icon Path — Browse to select an optional icon.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Icon Path — Browse to select an optional icon.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assign and push packages
Specify which users or groups receive a package, and push the package to user devices.

For iOS packages, click Push Applications on the Applications & Files tab to update assigned iOS devices with changes immediately. This option can be helpful if a user doesn't see a particular app on their device, or if they accidentally deleted it.

Task
2. Select the package to assign, click the Assigned Devices tab, then use the drop-down menus in the Filters table to select users or groups.
   You can have only one user and one group filter per package.
3  Push the package to devices.
   • For Android packages, click Save.
   • For iOS packages, click Save & Push Applications.

Users must open the McAfee EMM app, then tap Recommended Apps to download package apps.

Managing volume licenses for iOS apps

For paid iOS apps, you can purchase volume licenses from Apple and manage them with the package feature in McAfee EMM.

The Apple Volume Purchase Program (VPP) lets you bulk-purchase licenses for user devices. For details, see the Apple Volume Purchase Program site.

Volume licenses are provided in a spreadsheet, which you can generate as a CSV file and upload to any iOS package that contains the licensed app. See Add or update volume licenses for iOS package apps.

Volume licensing is handled differently depending on iOS version. When you push a package that contains a volume-licensed app:

• iOS 5 and later — The user is prompted to install the app. They don’t have to pay for the app directly, and the license count is updated automatically in McAfee EMM.

• iOS 4 — Users must open the McAfee EMM app, then tap Recommended Apps to download the volume-licensed app. The volume license key is not automatically supplied. We recommend providing license keys to users of iOS 4 and earlier by phone, email, or text, then manually marking the license Redeemed. See Manually redeem or delete volume licenses.

If you push a licensed app to a user device that already has it installed, the license status is updated from Redeemed to Available the next time the device reports its status to the McAfee EMM server. This can take up to 24 hours.

If you purchase additional licenses for an app, or if you want to verify license count or status, download an updated license spreadsheet from Apple, then use the spreadsheet to generate a CSV file to upload to the McAfee EMM package.

See also
Add or update volume licenses for iOS package apps on page 38
Manually redeem or delete volume licenses on page 39

Add or update volume licenses for iOS package apps

Distribute paid iOS apps to users by adding a VPP license to the app in an iOS package.

Before you begin
A VPP-eligible app must exist in an iOS package. See Create or modify packages.

Task
1  Download the license spreadsheet for the VPP app from Apple, then use Save As to generate a CSV file.
   ! Changing the file extension instead of regenerating the file doesn’t work.

2  Select Menu | Configuration | Server Settings | EMM Server Settings | Package Management.
3. Select an iOS package, then select the VPP-eligible app.

4. Click the Volume Licenses tab, then click Add.

5. If prompted, click OK to confirm that you’re uploading the latest version.

6. Browse to select the VPP CSV file, then click Save.

**See also**
*Create or modify packages on page 36*

**Manually redeem or delete volume licenses**
To keep your list of licenses up-to-date, manually mark licenses redeemed or delete them entirely as needed.

**Before you begin**
A VPP license must be associated with an app in an iOS package. See *Add or update volume licenses for iOS package apps*.

Rewinding and deleting licenses in McAfee EMM has no impact on users.

**Task**
1. Select **Menu | Configuration | Server Settings | EMM Server Settings | Package Management**.

2. Select an iOS package, then select the VPP app to redeem or delete licenses from.

3. Click the Volume Licenses tab, select one or more licenses, then click Redeem or Delete.

**See also**
*Add or update volume licenses for iOS package apps on page 38*
Configuring policies

McAfee EMM policies define and enforce requirements for mobile devices in enterprise environments.

Contents

- Using McAfee EMM policies in ePolicy Orchestrator
- Configure policies

Using McAfee EMM policies in ePolicy Orchestrator

McAfee EMM adds policy categories for mobile devices to the ePolicy Orchestrator Policy Catalog. Policies are collections of settings that you create, configure, apply, and then enforce. Mobile polices are applied when devices are initially configured, and at the next device check-in or agent wake-up call when there's a change to the existing policy.

For mobile devices, policies are applied to devices using profiles. Each policy setting corresponds to a single profile, except VPN, Wi-Fi, and Web Clips, which trigger different profiles for each configuration you add to the policy. This approach allows you to apply and update settings independently of each other.

For details on assigning policies, see the ePolicy Orchestrator documentation.

McAfee EMM adds policy categories for Android, iOS, and Windows Phone to the Policy Catalog. The settings available in each policy category vary. For details on policy settings, see Policy Settings.

Users must be granted permission to the McAfee Enterprise Mobility Management permission group for mobile policies to appear in the Policy Catalog.

Customizing policies

In each category, McAfee EMM provides predefined McAfee Default and My Default policies. Initially, the settings for both the McAfee Default and My Default policies are the same. You can use predefined policies as is, edit the My Default predefined policies, or create new policies.

Table 6-1  McAfee EMM predefined policies

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Default</td>
<td>Defines the out-of-the-box policy that takes effect if no other policy is applied. You can duplicate, but not delete or modify, this policy.</td>
</tr>
<tr>
<td>My Default</td>
<td>Defines the customizable default policy for your environment.</td>
</tr>
</tbody>
</table>

Modify this policy to create your own customized default.
Comparing policies

In ePolicy Orchestrator 5.0 and later, you can compare policies within the same McAfee EMM policy category (iOS, Android, or Windows Phone) using Policy Comparison. McAfee EMM lets you compare all settings available within each policy category, except VPN, Wi-Fi, and Web Clips.

See also

Policy settings on page 4

Configure policies

Fine-tune requirements for mobile devices in your enterprise environment by configuring policies to assign in the System Tree.

Task

For option definitions, click ? in the interface.

1. Select Menu | Policy | Policy Catalog, then from the Product list, select Enterprise Mobility Management 11.0.0.

2. Click the name of an editable policy.

   ![Tip]

   You can edit the My Default policies, or any policies you create. The McAfee Default policies aren’t editable.

3. Configure the settings on each tab, then click Save.
Monitoring devices

McAfee EMM provides tools for monitoring mobile devices in your environment. Make the most of your software by setting up dashboards with McAfee EMM monitors, and query the system to create customized reports as needed.

Contents

- Using dashboards and monitors with McAfee EMM
- Using queries and reports with McAfee EMM

Using dashboards and monitors with McAfee EMM

Keep watch on the mobile devices in your environment by adding McAfee EMM monitors to your customizable dashboard.

Dashboards are collections of monitors that track activity in your ePolicy Orchestrator environment. Use dashboards to get a global and graphical overview of McAfee EMM mobile properties reported for devices.

These are the predefined monitors available on the McAfee EMM dashboard.

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Endpoints by OS</td>
<td>Displays the operating system of all devices and systems in your network. This includes mobile devices as well as traditional client systems, like desktops.</td>
</tr>
<tr>
<td>EMM Devices by OS</td>
<td>Displays the operating system of all mobile devices in your network.</td>
</tr>
<tr>
<td>EMM Devices by Model</td>
<td>Displays the device model of all mobile devices in your network.</td>
</tr>
<tr>
<td>EMM Devices by Android OS Version</td>
<td>Displays the operating system version of all Android devices in your network.</td>
</tr>
<tr>
<td>EMM Devices by iOS Version</td>
<td>Displays the operating system version of all iOS devices in your network.</td>
</tr>
</tbody>
</table>
## Monitor and Description

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMM Devices by Status</td>
<td>Displays the current status of all mobile devices in your network. Statuses include:</td>
</tr>
<tr>
<td></td>
<td>• Available — Device is configured and communicating with network servers.</td>
</tr>
<tr>
<td></td>
<td>• Pending Approval — Android Device ID mapping must be manually approved.</td>
</tr>
<tr>
<td></td>
<td>• Uninstall Initialized — Admin-initiated MDM Uninstall action is pending.</td>
</tr>
<tr>
<td></td>
<td>• Uninstall Completed — Admin-initiated MDM Uninstall action is complete.</td>
</tr>
<tr>
<td></td>
<td>• User Uninstalled — User uninstalled the MDM profile on the device.</td>
</tr>
<tr>
<td></td>
<td>• Wipe Initialized — Admin-initiated Wipe action is pending.</td>
</tr>
<tr>
<td></td>
<td>• Wipe In Progress — Admin-initiated Wipe action is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Wipe Completed — Admin-initiated Wipe action is complete.</td>
</tr>
<tr>
<td></td>
<td>• Delete Corporate Data Initialized — Admin-initiated Wipe Corporate Data action is pending.</td>
</tr>
<tr>
<td></td>
<td>• Delete Corporate Data Completed — Admin-initiated Wipe Corporate Data action is complete.</td>
</tr>
<tr>
<td></td>
<td>• Pending Deletion — Admin-initiated Delete action (Actions</td>
</tr>
<tr>
<td></td>
<td>The device statuses listed here appear as combined if multiple actions are selected for a device. For example, successful MDM Uninstall and Wipe actions results in the device status Uninstall Completed &amp; Wipe Completed.</td>
</tr>
<tr>
<td>EMM Devices by Compliance Status</td>
<td>Displays the compliance status of all mobile devices in your network. Devices are Compliant or Non-Compliant according to the policy applied to them.</td>
</tr>
<tr>
<td>EMM Devices with No Check-in for 7 Days</td>
<td>Displays the number of mobile devices that didn't check in to the McAfee EMM server within the past seven calendar days. The most common cause is that the device doesn't have a network connection, or the MDM profile was uninstalled from iOS devices.</td>
</tr>
<tr>
<td>EMM Devices with No Check-in for 30 Days</td>
<td>Displays the number of mobile devices that didn't check in to the McAfee EMM server within the past 30 calendar days. The most common cause is that the device doesn't have a network connection, or the MDM profile was uninstalled from iOS devices.</td>
</tr>
</tbody>
</table>

You can use predefined dashboards as is, modify predefined dashboards to add or remove monitors, or create new dashboards.

For information on creating and using dashboards, see the ePolicy Orchestrator documentation.

---

## Using queries and reports with McAfee EMM

Use ePolicy Orchestrator queries to retrieve detailed information about the mobile devices in your network. You can export, download, combine queries into reports, and use most queries as dashboard monitors.

You can view query data only for resources that you have permissions to. For example, if your permissions grant access to the System Tree location "Athens," your queries return data only for that location.
McAfee EMM provides predefined queries in the Mobile Management query group. You can use predefined queries as is, edit predefined queries, or create custom queries from properties in the ePolicy Orchestrator database. To create custom queries, your assigned permission set must include the ability to create and edit private queries.

You can restrict access to reports using groups and permission sets in the same way you restrict access to queries. Reports and queries can use the same groups, which allows for consistent access control.

For information on creating and using queries and reports, see the ePolicy Orchestrator documentation.

### McAfee EMM predefined queries

- Managed Endpoints by OS
- EMM Devices by OS
- EMM Devices by Model
- EMM Devices by Android OS Version
- EMM Devices by Android OS Version
- EMM Devices by Status
- EMM Devices by Compliance Status
- EMM Devices with No Check-in for 7 Days
- EMM Devices with No Check-in for 30 Days

### Custom queries

McAfee EMM adds mobile-specific properties to the System Management feature group, in the Managed Systems result type. You can use these properties to create custom queries about mobile devices in your network.

<table>
<thead>
<tr>
<th>Property Group</th>
<th>Property (Column)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMM Properties</td>
<td>Product Version (EMM)</td>
</tr>
<tr>
<td>Mobile Applications</td>
<td>EMM deployed</td>
</tr>
<tr>
<td></td>
<td>Identifier</td>
</tr>
<tr>
<td></td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Short version</td>
</tr>
<tr>
<td></td>
<td>Version</td>
</tr>
<tr>
<td>Device Properties</td>
<td>BlueTooth MAC</td>
</tr>
<tr>
<td></td>
<td>Model</td>
</tr>
<tr>
<td></td>
<td>Model Version</td>
</tr>
<tr>
<td></td>
<td>Vendor</td>
</tr>
<tr>
<td></td>
<td>WIFI MAC</td>
</tr>
<tr>
<td>Device Details</td>
<td>ActiveSync ID</td>
</tr>
<tr>
<td></td>
<td>Agent version</td>
</tr>
<tr>
<td></td>
<td>Compliant</td>
</tr>
<tr>
<td></td>
<td>Device encryption enabled/supported</td>
</tr>
<tr>
<td></td>
<td>Device status</td>
</tr>
<tr>
<td></td>
<td>Hardware encryption enabled</td>
</tr>
<tr>
<td></td>
<td>Jailbroken/Rooted</td>
</tr>
<tr>
<td></td>
<td>Last check-in</td>
</tr>
<tr>
<td></td>
<td>Last jailbreak/root check</td>
</tr>
<tr>
<td>Property Group</td>
<td>Property (Column)</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Property Group</td>
<td>MDM profile version</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Passcode compliant</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Passcode enabled</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Passcode profile compliant</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Registration</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Supervised</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Unique Device Identifier (UDID)</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Uses McAfee Secure Container</td>
</tr>
<tr>
<td>Telecommunication Properties</td>
<td>IMEI/MEID/ESN</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Mobile Country Code</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Mobile Network Code</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Network Operator</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Network Type</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Phone Number</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Phone Type</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>SIM Country Code</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>SIM Operator</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>SIM Operator Name</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>SIM Serial Number</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>SIM State</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Software</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Software Version</td>
</tr>
<tr>
<td>Property (Column)</td>
<td>Subscriber ID</td>
</tr>
</tbody>
</table>
Performing system maintenance

Perform these maintenance tasks as needed to ensure that the McAfee EMM server-side components continue to operate smoothly.

Contents
- Edit the McAfee EMM registered server
- Update portal, MDM, and push certificates
- Update the device catalog
- Back up your McAfee EMM installation
- Viewing McAfee EMM log files

Edit the McAfee EMM registered server

Registering the McAfee EMM server allows ePolicy Orchestrator to communicate with the McAfee EMM database. This connection is established during installation, but you can update your connection settings any time.

To change the host name or IP address of the McAfee EMM Hub, delete the existing registered server and add a new entry with the updated address. See the McAfee EMM Installation Guide for details.

Task
For option definitions, click ? in the interface.

1. Select Menu | Configuration | Registered Servers.
2. Select the McAfee EMM server from the Registered Servers sidebar, then click Actions | Edit.
3. Use the Registered Server Builder to edit the Description and Details for the server.

Update portal, MDM, and push certificates

Portal, MDM, and push certificates must be updated periodically to maintain continual secure communication with mobile devices.

- **Portal certificate** — Expiration varies. Contact your certificate authority (CA) to obtain updates.
- **MDM certificate** — Expires annually. Renew before expiration to avoid reconfiguring all iOS devices. See KB73382 for details on obtaining updates from Apple.
- **iOS Agent Push Notification certificate** — Expires annually. Visit the McAfee Downloads site and enter a valid McAfee EMM grant number to obtain updates.

Configure the EMM Certificates Notification server task to email reminders when certificates near expiration. See Customize certificate expiration notifications.
**Task**

1. Select **Menu | Configuration | Server Settings | EMM Server Settings | System Settings | Certificates**.
2. Select a certificate, then click **Update**.
3. Browse to select the certificate, enter the password for the certificate, then click **Save**.
4. If you updated the portal certificate, reset IIS.

**See also**

*Customize certificate expiration notifications on page 14*

---

**Update the device catalog**

The device catalog contains information on supported mobile devices. It’s automatically added during installation, but should be updated monthly or whenever new device types are approved for your network.

**Before you begin**

Obtain an updated device catalog .zip file by visiting the [McAfee Downloads site](https://www.mcafee.com) and entering a valid McAfee EMM grant number.

**Task**

1. Select **Menu | Configuration | Server Settings | EMM Server Settings | System Settings | Device Catalog**.
2. Click **Add**, then browse to select the device catalog .zip file.
3. Click **Install**.

---

**Back up your McAfee EMM installation**

Save a copy of your McAfee EMM database and export an encryption key to prevent loss due to system or network failure.

**Task**

1. Select **Menu | Configuration | Server Settings | EMM Server Settings | System Settings**.
2. Click **Export Encryption Key**.
3. Enter a **Key Password**, then click **Export**.
4. Save a copy of the database by copying the database file from the SQL Server.

Repeat this step regularly so that you have a recent copy of the database if you need to restore. You can reuse the same encryption key.
**Viewing McAfee EMM log files**

McAfee EMM log files can help you troubleshoot issues with your installation.

Use the Windows Event Viewer to review McAfee EMM log files when your system doesn't behave as expected. McAfee EMM log files are located under Application and Services Logs in the Event Viewer console tree.

McAfee EMM generates separate log entries for each server component. For dual server installations, the DMZ server logs events for the McAfee EMM Portal, Proxy, and Push Notifier, while the internal server logs events for McAfee EMM Hub. For single server installations, all logs entries can be found in the Event Viewer of the McAfee EMM server.

To review events, select a log entry, then use the General or Details tabs to view server messages. The Source column indicates which McAfee EMM server component generated the event.

By default, the Event Viewer logs McAfee EMM events with a severity level of Warning or Error. For more detailed logging, change the level value for the log4net root to All.

```
<level value="ALL" />
```

The McAfee EMM log4net configurations are located in these locations:

- **Hub** — `<installation path of McAfee EMM>\EMMPlatform\EMMHub\web.config`
- **Portal** — `<installation path of McAfee EMM>\EMMPlatform\EMMPortal\web.config`
- **Proxy** — `<installation path of McAfee EMM>\EMMPlatform\EAS Filter\filter.config`
- **Push Notifier** — `<installation path of McAfee EMM>\EMMPlatform\EAS Filter \TrustDigital-Server-ActiveSync\web.config`
# Troubleshooting

Use these troubleshooting tips to work through issues encountered while using McAfee EMM.

<table>
<thead>
<tr>
<th>Task</th>
<th>Issue</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring devices</td>
<td>Installation profile is not signed error when configuring iOS devices.</td>
<td>Check for these issues with the portal certificate:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Incorrect password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Invalid, missing, or empty certificate file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Expired dates for the certificate file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No certificate chain in the certificate file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Invalid or missing certificate authority in the certificate chain of the certificate file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• None of the certificates in the certificate chain are marked as certificate authority certificates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The portal certificate installed on the McAfee EMM Proxy server doesn't match the portal certificate specified in the software (Menu</td>
</tr>
<tr>
<td></td>
<td>Timeout error in Safari when configuring iOS devices.</td>
<td>See KB71248.</td>
</tr>
<tr>
<td></td>
<td>Error configuring Android devices using ActiveSync.</td>
<td>Verify the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The device can connect to the internet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The McAfee EMM Portal is accessible from the device and from other devices or workstations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If no access issues are found, manually specify the McAfee EMM server name on the device:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Tap the McAfee EMM app, then click Properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Select EMM Settings, then check to enable the server field.</td>
</tr>
<tr>
<td></td>
<td>Cannot connect to server error when configuring a device.</td>
<td>If the issue still isn't resolved, check the IIS log on the McAfee EMM Proxy server for errors connecting to the device.</td>
</tr>
</tbody>
</table>

You can verify the SRV record by navigating in a browser to https://<domainname>/emmportal.
<table>
<thead>
<tr>
<th>Task</th>
<th>Issue</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unexpected exception</td>
<td>indicating an overall failure when configuring a device.</td>
<td>Make sure that the McAfee EMM Portal is configured correctly by verifying the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The portal certificate installed on the McAfee EMM Proxy server matches the portal certificate specified in the software (Menu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In IIS on the McAfee EMM Proxy server, the correct portal certificate is selected for the site hosting the DMZ components. If you make any changes, restart IIS.</td>
</tr>
<tr>
<td>Communicating with</td>
<td>Devices can't sync mail.</td>
<td>Make sure that the McAfee EMM Proxy is configured correctly by verifying the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In IIS on the McAfee EMM Proxy server, the TrustDigital-Server-ActiveSync component is installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In the Proxy web.config file, located at C:\Program Files (x86)\McAfee\EMMPlatform\EAS Filter \trustdigital-server-activesync\web.config, the Exchange server address is correct.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In the &lt;easFilter&gt; tag, check the value for the BaseUri attribute.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the back end Exchange server is 2003, make sure the BaseUri attribute specifies http, not https.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• On the McAfee EMM Proxy server, the McAfee EMM Hub is accessible at <a href="https://HubhostMachine/EMMHub/">https://HubhostMachine/EMMHub/</a>.</td>
</tr>
<tr>
<td>Devices aren't</td>
<td>checking in or receiving policy updates.</td>
<td>Make sure that the McAfee EMM Push Notifier is configured correctly by verifying the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Router and firewall access is configured correctly for servers and devices. For details on network requirements, see the McAfee EMM Installation Guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All Push Notifiers have a green status checkmark and a recent Last Update Time in McAfee EMM Certificates settings (Menu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If any Push Notifier components have a red X, log in to the DMZ server and check the Event Viewer for errors from the McAfee EMM Push Notifier. See Viewing McAfee EMM log files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• On the System Information page for a device, clicking Wake Up Agents adds a push notification action to the Pending Actions tab. Refresh the screen and wait for the pending push notification action to be processed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the action remains, log in to the DMZ server and check the Event Viewer for errors from the McAfee EMM Push Notifier. See Viewing McAfee EMM log files.</td>
</tr>
<tr>
<td>Task</td>
<td>Issue</td>
<td>Resolution</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Connecting to McAfee EMM | Error connecting to McAfee EMM Server Settings through ePolicy Orchestrator. | Verify the following:  
  - A valid McAfee EMM server appears in the list of ePolicy Orchestrator Registered Servers (Menu | Configuration | Registered Servers).  
  - The host name or IP address of the McAfee EMM registered server must be network accessible and should not specify localhost.  
  - Router and firewall access is configured correctly for servers and devices. For details on network requirements, see the McAfee EMM Installation Guide. |
| Failed EMM Certificates  | Notification server task.                                            | Verify the following:  
  - A valid McAfee EMM server appears in the list of ePolicy Orchestrator Registered Servers (Menu | Configuration | Registered Servers).  
  - The host name or IP address of the McAfee EMM registered server must be network accessible and should not specify localhost.  
  - An SMTP server is configured in McAfee EMM Mail Settings (Menu | Configuration | Server Settings | EMM Server Settings | System Settings | Mail Settings).  
  - A valid email address appears in the server task. |
| Authorizing users        | When authorizing select LDAP users, Invalid: No Email appears in the Status column, and the user can't provision. | In the Active Directory server, select Active Directory Users and Computers | User Properties | General and enter an email address for the user in the format username@domain. The email does not have to be active, but the field must be populated. |
| Working with policies    | Unenforced passcode requirements on devices.                         | On the System Information page for the device, click Wake Up Agents to force an immediate policy update.  
  If the issue still isn't resolved, verify that the device is assigned a policy that enforces passcode requirements as expected. For example, policy assignment rules in ePolicy Orchestrator can cause lower priority policies to be overridden.  
  Users aren't prompted to set up a new passcode after a policy update if their existing passcode meets all policy requirements.  
  Blank white icon on iOS devices where policy-based web clips used to appear.  
  Restart the device, or delete the blank web clip manually by touching and holding the icon until it shakes, then tapping the x over the icon to delete it. |

See also
Viewing McAfee EMM log files on page 49
Policy settings

These are the policy settings by mobile platform.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Used to...</th>
<th>Policy categories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>i</strong>OS</td>
</tr>
<tr>
<td>APN</td>
<td>Configure APN (access point name) settings to force devices</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>to connect to a specific mobile network.</td>
<td>X</td>
</tr>
<tr>
<td>Compliance</td>
<td>Determine which devices are</td>
<td>Policy</td>
</tr>
<tr>
<td></td>
<td>allowed to sync corporate data</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>based on these parameters:</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Configure whether devices get email through the default EMM proxy, a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>different proxy, or directly from an Exchange, Domino, or other server.</td>
<td>X</td>
</tr>
<tr>
<td>Passcode</td>
<td>Specify passcode requirements, including passcode length,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>composition, expiration, history, fail action, and auto-lock period.</td>
<td>X</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Select features and functionality to block.</td>
<td>Camera</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iTunes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iTunes explicit content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Installing iTunes applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In-App Purchases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safari</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voice dialing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Screen capture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multiplayer gaming</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Roaming</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automatic sync while roaming</td>
</tr>
<tr>
<td></td>
<td></td>
<td>YouTube</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iTunes store access without password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iCloud backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iCloud document sync</td>
</tr>
<tr>
<td>Setting</td>
<td>Used to...</td>
<td>Policy categories</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td>iCloud key-value sync</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Photo Stream</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Untrusted TLS certificates</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Siri (voice assistant)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Sending diagnostic data</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Moving, forwarding, or replying to corporate email using other email accounts</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Sending corporate email from third-party apps</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Passbook when device is locked</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Shared Photo Stream</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Secure Container</td>
<td>Specify passcode, syncing, and other requirements for McAfee</td>
<td>X</td>
</tr>
<tr>
<td>Supervised Devices</td>
<td>Specify a proxy server or set specialized restrictions for iOS devices that are supervised by the Apple Configurator</td>
<td>X</td>
</tr>
<tr>
<td>VPN</td>
<td>Configure VPN (virtual private network) profiles.</td>
<td>X</td>
</tr>
<tr>
<td>Web Clips</td>
<td>Send shortcuts to specific webpages, like your enterprise homepage.</td>
<td>X</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Configure Wi-Fi profiles.</td>
<td>X</td>
</tr>
</tbody>
</table>

Policy settings
Mobile properties

These are the mobile properties shown in the ePolicy Orchestrator System Tree.

Mobile properties are updated automatically when devices check in (every 24 hours for MDM, or every 15 minutes for ActiveSync). You can force an update immediately by clicking Wake Up Agents in the System Information page for any device.

### Device Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td>Manufacturer of the device.</td>
</tr>
<tr>
<td>Model</td>
<td>Model name of the device as reported by the OS, like iPhone 4S or Samsung Galaxy Nexus.</td>
</tr>
<tr>
<td>Model Version</td>
<td>Model number of the device.</td>
</tr>
<tr>
<td>WIFI MAC</td>
<td>MAC address for Wi-Fi connection. This is a unique address that can be used to identify the device.</td>
</tr>
<tr>
<td>BlueTooth MAC</td>
<td>MAC address for Bluetooth connection.</td>
</tr>
</tbody>
</table>

### Telecommunication Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Type</td>
<td>Type of radio signal used to transmit voice calls, including CDMA, GSM, SIP, or NONE.</td>
</tr>
<tr>
<td>Software</td>
<td>Original equipment manufacturer (OEM) software.</td>
</tr>
<tr>
<td>Software Version</td>
<td>OEM software version for GSM phones.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Phone number as reported by the operating system.</td>
</tr>
<tr>
<td>Mobile Country Code</td>
<td>Mobile country code where the device is currently connected.</td>
</tr>
<tr>
<td>Mobile Network Code</td>
<td>Mobile network code of the mobile service provider that the device is currently connected to.</td>
</tr>
<tr>
<td>IMEI/MEID/ESN</td>
<td>Mobile equipment identifier. For GSM phones, the ID is supplied as an International Mobile Equipment Identity (IMEI). For CDMA phones, the ID is supplied as a Mobile Equipment Identifier (MEID) or Electronic Serial Number (ESN).</td>
</tr>
<tr>
<td>Network Operator</td>
<td>Friendly carrier name, like Verizon, AT&amp;T, or T-Mobile.</td>
</tr>
<tr>
<td>Network Type</td>
<td>Radio technology used on the device for data transmission, including CDMA, EDGE, eHRPD, EVDO0, EVDOA, EVDOB, GPRS, HSDPA, HSPA, HSPAP, HSUPA, IDEN, LTE, UMTS, or UNKNOWN.</td>
</tr>
<tr>
<td>SIM Country Code</td>
<td>Mobile country code of the SIM card manufacturer.</td>
</tr>
<tr>
<td>SIM Operator Name</td>
<td>Mobile network code of the SIM card manufacturer.</td>
</tr>
<tr>
<td>SIM Operator</td>
<td>Friendly SIM operator name, like Verizon, AT&amp;T, or T-Mobile.</td>
</tr>
<tr>
<td>Property</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIM Serial Number</td>
<td>Serial number, or Subscriber Identity Module, of the SIM card.</td>
</tr>
<tr>
<td>SIM State</td>
<td>Status of the device's SIM card, including ABSENT, PINREQUIRED, PUKREQUIRED, LOCKED, READY, or UNKNOWN.</td>
</tr>
<tr>
<td>Subscriber ID</td>
<td>International mobile subscriber identity for GSM phones.</td>
</tr>
</tbody>
</table>

**Device Details**

<table>
<thead>
<tr>
<th>Property</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveSync ID</td>
<td>Unique ID for ActiveSync traffic.</td>
</tr>
<tr>
<td>Device ID</td>
<td>Unique ID for Android devices.</td>
</tr>
<tr>
<td>Unique Device Identifier (UDID)</td>
<td>Unique ID for iOS devices.</td>
</tr>
<tr>
<td>Agent version</td>
<td>Version of the McAfee EMM app installed on the device.</td>
</tr>
<tr>
<td>MDM profile version</td>
<td>Version of the MDM profile.</td>
</tr>
<tr>
<td>Registration</td>
<td>Date and time that the device was configured.</td>
</tr>
<tr>
<td>Last check-in</td>
<td>Date and time of last device check-in. Check-in happens automatically by default every 24 hours for MDM devices, or every 15 minutes for ActiveSync devices. You can manually force a device to check in by clicking Wake Up Agents.</td>
</tr>
<tr>
<td>Device status</td>
<td>Current status off the device. Statuses include:</td>
</tr>
<tr>
<td></td>
<td>• Available — Device is configured and communicating with network servers.</td>
</tr>
<tr>
<td></td>
<td>• Pending Approval — Android Device ID mapping must be manually approved.</td>
</tr>
<tr>
<td></td>
<td>• Uninstall Initialized — Admin-initiated MDM Uninstall action is pending.</td>
</tr>
<tr>
<td></td>
<td>• Uninstall Completed — Admin-initiated MDM Uninstall action is complete.</td>
</tr>
<tr>
<td></td>
<td>• User Uninstalled — User uninstalled the MDM profile on the device.</td>
</tr>
<tr>
<td></td>
<td>• Wipe Initialized — Admin-initiated Wipe action is pending.</td>
</tr>
<tr>
<td></td>
<td>• Wipe In Progress — Admin-initiated Wipe action is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Wipe Completed — Admin-initiated Wipe action is complete.</td>
</tr>
<tr>
<td></td>
<td>• Delete Corporate Data Initialized — Admin-initiated Wipe Corporate Data action is pending.</td>
</tr>
<tr>
<td></td>
<td>• Delete Corporate Data Completed — Admin-initiated Wipe Corporate Data action is complete.</td>
</tr>
<tr>
<td></td>
<td>• Pending Deletion — Admin-initiated Delete action (Actions</td>
</tr>
</tbody>
</table>

The device statuses listed here appear as combined if multiple actions are selected for a device. For example, successful MDM Uninstall and Wipe actions results in the device status Uninstall Completed & Wipe Completed.

<table>
<thead>
<tr>
<th>Supervised</th>
<th>Yes for iOS devices that are Supervised by the Apple Configurator.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant</td>
<td>Yes if the device meets compliance parameters specified in its assigned policy.</td>
</tr>
<tr>
<td>Uses McAfee Secure Container</td>
<td>Yes if McAfee Secure Container is installed on the Android device.</td>
</tr>
<tr>
<td>Jailbroken Rooted</td>
<td>Yes if the device is jailbroken (iOS) or rooted (Android). Unverified indicates the device hasn't responded after the maximum number of jailbreak verification attempts.</td>
</tr>
</tbody>
</table>
### Property | Definition
--- | ---
Last jailbreak check | Date and time of the last jailbreak (iOS) or root (Android) status check, as specified by the compliance policy.
Last root check |  
Device encryption enabled | Yes for encrypted devices, including:
- iOS devices later than 3GS, which are encrypted by default.
- Android versions 3 and later with optional encryption enabled.
Device encryption supported | **Windows Phones don’t report whether encryption is enabled. Yes for Windows Phones indicates only that encryption is supported on the device.**
Hardware encryption enabled | Type of encryption enabled on the device:
- Hardware encryption — Block-level encryption.
- File encryption — File-level encryption.
- Hardware encryption and passcode — Block-level encryption plus a passcode to unlock the device.
Passcode enabled | Yes if a passcode must be entered to unlock the device.
Passcode compliant | Yes if the user’s passcode is compliant with requirements set on the device, for example, for email and other accounts.
Passcode profile compliant | Yes if the user’s passcode is compliant with requirements set by profiles on the device, including the McAfee EMM passcode profile.

### Mobile Applications
This tab lists all apps installed on the device. The app Name, Identifier, and Version are provided. The EMM deployed column indicates whether the app was distributed in a McAfee EMM package.

### Pending Actions
This tab lists any pending actions for the device, and the date the action was created. This can be used to troubleshoot problems with devices.

### Certificates
This tab lists all certificates installed on the device. This includes certificates installed by McAfee EMM, like the MDM and portal certificate, as well as user- and app-installed certificates.

### Configuration Profiles
This tab lists all profiles installed on the device. McAfee EMM policies are applied to devices with configuration profiles.

### Provisioning Profiles
This tab lists profiles for in-development iOS apps installed on the device.
Mobile properties
Index

A
about this guide 5
actions, mobile
  locking, unlocking, wiping, and uninstalling remotely 32
  pending 57
  permissions 15
  pushing to devices 33
ActiveSync authorization
  bulk 19
  configuring directories 12
  list-based 21
  mobile device check-in intervals 33
  mobile device configuration requirements 25
  selected users 21
administrative accounts
  granting permissions, ePO 15
  updating default logon credentials, EMM 12
Agent, EMM, See app, EMM
Android devices
  app identifiers 33
  configuring email with ActiveSync 28
  configuring EMM app and Secure Container 27
  Device ID Mapping 22
  EMM app description 9
  Secure Container description 9
  supported policy settings 55
  updating for version 11.0 29
  upgrading for version 11.0 30
API project, Google Cloud Messaging (GCM) 13
.apk file, package options 37
APN (access point name), policy settings 55
app, EMM
  configuring Android devices 27
  configuring iOS devices 27
  description 9
  version, mobile properties 57
Apple App Store
  configuring iOS devices 27
  package options 37
  restrictions 55
apps
  blacklisting 33
  finding identifiers 33
  installed on user devices 57
apps (continued)
  package management 36
  package options 37
  pushing to users or groups 37
authorization, See user authorization
authorization directories
  configuring 12
  mobile device configuration requirements 25
B
backups, EMM database 48
blacklisted apps 33
bulk authorization
  deployment planning 26
  LDAP or ActiveSync 19
bundle IDs, iOS app identifier 33
C
camera, restrictions 55
catalog, device 48
categories, mobile properties 57
certificate authority (CA), portal certificate updates 47
certificates
  expiration notifications 14
  mobile properties 57
  untrusted, restrictions 55
  updating 47
Certificates Notification server task
  configuring 14
  troubleshooting 51
check-in, devices
  default intervals 33
  last check-in, mobile properties 57
Cloud to Device Messaging (C2DM), deprecated 13
comma separated value (CSV) file
  bulk LDAP or ActiveSync authorization 19
  formatting for user authorization 22
  list-based LDAP or ActiveSync authorization 21
  volume-licensed apps 38
communication
  between server components 8
  with users, deployment planning 26
company profile, customizing 11
Index

compliance
  policy settings 55
  status summary 31
components
  client-side 9
  server-side 8
configuration
  Android devices 27
  iOS devices 27
  troubleshooting 51
  Windows Phones 28
configuration profiles, mobile properties 57
conventions and icons used in this guide 5
corporate data, wipe 32

D
  dashboards, EMM 43
  database, EMM
    backups 48
    communication with ePO 47
    permissions 25
device catalog
  mobile device configuration requirements 25
  updating 48
device details, mobile properties 57
Device ID Mapping
  about 22
  configuring Android devices 28
  manual pairings, activating 23
  manual pairings, approving 23
device properties, mobile 57
device statuses
  Android Device ID Mapping 22
  definitions 57
devices, See mobile devices
diagnostic data, restrictions 55
DMZ
  configuration 8
  viewing log files 49
documentation
  audience for this guide 5
  product-specific, finding 6
typographical conventions and icons 5
documentation, EMM Installation Guide, adding a registered server 47
documentation, ePO Product Guide
  dashboards, creating and using 43
  email servers, configuring 14
  permission sets, managing 15
  policies, assigning 41
  queries, creating 44
  System Tree, managing 31
tags, creating and using 33
documentation, McAfee KnowledgeBase
  actions that don’t apply to mobile devices, KB77599 32
documentation, McAfee KnowledgeBase (continued)
  GCM credentials, obtaining, KB77397 13
  MDM certificate renewal, KB73382 47
  Safari timeout error, KB71248 51
domain name system (DNS) server
  mobile device configuration requirements 25
  publishing an SRV record 12
E
  email
    authorization directories 12
    bulk authorization notifications 19
    configuring Android devices with ActiveSync 28
    policy settings 55
    restrictions 55
    SMTP server configuration 14
    updated provisioning token notifications 18
  EMM
    actions 32
    dashboards and monitors 43
    features added to ePO 7
    mobile properties 31
    permission sets 15
    policies 41
    queries and reports 44
    registered servers 47
    server tasks 14
    System Tree 31
  encryption
    policy compliance 55
    status, mobile properties 57
    Windows Phones, limitation 57
  encryption key, exporting 48
  enterprise apps, package options 37
  Event Viewer, viewing log files 49
  expiration, certificates 14

F
  factory settings, restoring remotely on user devices 32
  figures, configuration 8

G
  Google Cloud Messaging (GCM)
    adding server settings for upgrades 13
    upgrading Android devices 29
  Google Play
    configuring Android devices 27
    package options 37
    upgrading Android devices 30

H
  Hub, EMM
    description 8
Hub, EMM (continued)
   viewing log files 49

I
iCloud
   package options, preventing app backup 37
   restrictions 55
icons, specifying for package apps 37
identifiers
   apps 33
   mobile devices 57
In-App Purchases, restrictions 55
Installation Guide, EMM, adding a registered server 47
iOS devices
   app identifiers 33
   configuring 27
   EMM app description 9
   supported policy settings 55
   updating for version 11.0 29
   volume-licensed apps 38
.ipa file, package options 37
iPad, See iOS devices
iPhone, See iOS devices
iPod, See iOS devices
iTunes
   package options, preventing app backup 37
   restrictions 55

J
jailbroken devices
   policy compliance 55
   status, mobile properties 57

K
KnowledgeBase (KB), McAfee, See documentation, McAfee KnowledgeBase

L
LDAP authorization
   bulk 19
   configuring directories 12
   list-based 21
   mobile device configuration requirements 25
   selected users 20
lock, mobile actions 32
Locked Users page 22
log files, viewing 49

M
McAfee Downloads
   device catalog updates 48
   iOS Agent Push Notification certificate updates 47
McAfee ServicePortal, accessing 6
mobile actions
   locking, unlocking, wiping, and uninstalling remotely 32
   permissions 15
mobile applications, mobile properties 57
Mobile Device Management (MDM)
   certificate updates 47
   mobile device check-in intervals 33
   package options, deleting apps 37
   version, mobile properties 57
MDM uninstall, mobile actions 32
mobile devices
   check-in intervals 33
   configuration requirements 25
   differentiating in the System Tree 31
   identifiers, mobile properties 57
   locking, unlocking, wiping, and uninstalling remotely 32
   policy settings 55
   properties 57
   supported operating systems 25
   troubleshooting connectivity 51
   updating vs. upgrading for version 11.0 29
Mobile ePO (MePO) extension, automatic installation with EMM 8
mobile properties
   definitions 57
   viewing 31
mobileconfig file, package options 37
monitors, EMM 43
multiplayer gaming, restrictions 55

N
network details, mobile properties 57
notifications to users
   deployment planning 26
   setting the default message 14

O
operating system, policy compliance 55
ownership, mobile devices 31

P
package names, Android app identifier 33
packages
   about 35
   adding volume licenses 38
   assigning to users or groups 37
   creating and modifying 36
   installing recommended apps 37
   options 37
Passbook, restrictions 55
passcodes
   compliance, mobile properties 57
   controlling remotely on user devices 32
   policy settings 55
passcodes (continued)  
troubleshooting policy application 51  
passwords, temporary, See provisioning tokens  
pending actions  
mobile properties 57  
pushing to devices 33  
pending approval, device status 22  
permission sets, EMM  
about 15  
mobile actions 32  
policies 41  
queries and reports 44  
permissions, database, EMM 25  
phone details, mobile properties 57  
phone number, mobile properties 57  
Photo Stream, restrictions 55  
policies, EMM  
about 41  
configuring 42  
pushing to devices 33  
settings 55  
Policy Comparison, EMM 41  
portal certificates, updating 47  
Portal, EMM  
automatic detection by mobile devices 12  
description 8  
verifying configuration 51  
viewing log files 49  
ports, mobile device access rules 25  
Product Guide, ePO  
dashboards, creating and using 43  
email servers, configuring 14  
permission sets, managing 15  
policies, assigning 41  
queries, creating 44  
System Tree, managing 31  
tags, creating and using 33  
profiles  
mobile properties 57  
policy application for mobile devices 41  
policy settings 55  
properties, EMM  
definitions 57  
queries 44  
provisioning profiles, mobile properties 57  
provisioning tokens  
configuring Android devices 27  
configuring iOS devices 27  
generating, bulk authorization 19  
generating, selected LDAP user authorization 20  
specifying requirements 17  
supported for iOS and Android devices only 17  
updating 18  
Proxy, EMM  
description 8  
Proxy, EMM (continued)  
verifying configuration 51  
viewing log files 49  
Push Notifier, EMM  
description 8  
verifying configuration 51  
viewing log files 49  
push technology, certificate updates 47  
Q  
queries, EMM  
blacklisted apps 33  
custom and predefined 44  
R  
recommended apps 37  
registered servers, EMM  
editing 47  
troubleshooting connectivity 51  
reports, EMM, creating from queries 44  
requirements  
mobile device configuration 25  
updating mobile devices for version 11.0 29  
restrictions, policy settings 55  
roaming, restrictions 55  
rooted devices  
policy compliance 55  
status, mobile properties 57  
S  
Safari, restrictions 55  
screen capture, restrictions 55  
Secure Container  
configuring Android devices 27  
description 9  
policy settings 55  
status, mobile properties 57  
Sender ID, Google Cloud Messaging (GCM) 13  
Server Settings, EMM, accessing select features 7  
server tasks, EMM  
blacklisted apps 34  
certificate expiration notifications 14  
service (SRV) record  
creating 12  
mobile device configuration requirements 25  
ServicePortal, finding product documentation 6  
shortcuts, distributing to mobile devices 55  
SIM details, mobile properties 57  
Siri, restrictions 55  
SMS messages, See text messages  
SMTP server, specifying 14  
SSL certificates, See portal certificates  
statuses, mobile properties 57