Product Guide

McAfee Enterprise Mobility Management 10.1
COPYRIGHT
Copyright © 2012 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 .............................. 7
About this guide .................................. 7
Audience .................................. 7
Conventions .................................. 7
Find product documentation ......................... 8

1 Introduction ................................ 9
McAfee EMM features ................................ 9
McAfee EMM components .............................. 11
Server components .................................. 11
Client components .................................. 12
Navigating the EMM Console ......................... 13

Configuring your McAfee EMM software

2 Console access ................................ 17
View role permissions ................................ 17
Log on for the first time ............................... 17
Create administrative accounts ....................... 18
Create administrative accounts based on LDAP groups ................ 18
Create a local administrative account ................ 19
Delete an administrative account .................... 19

3 Basic settings .................................. 21
Manage your company profile and licenses ............... 21
About device compliance ................................ 21
Enable or disable compliance enforcement ............... 22
Specify an SMTP server ................................ 22
Update portal, push, and MDM security certificates ............ 23
Update the device catalog .............................. 23
Enrollment Agents for PKI environments ................. 23
Edit an Enrollment Agent ................................ 24
Delete an Enrollment Agent ........................... 24
View installed auxiliary components ................. 24
View your BES Agent .................................. 24
View your Push Notifier ............................. 24

4 User authorization .............................. 27
Manage authorization directories ....................... 27
Add or edit an authorization directory .................. 27
Delete an authorization directory ..................... 28
Authorize users .................................. 28
Authorize all LDAP users ................................ 29
Authorize selected users ................................ 29
Authorize users based on a list ......................... 30
Delete a package ................................................................. 62
Download recommended apps to a device ........................................ 62

Monitoring network activity

8 Reports ............................................................. 65
View reports ................................................................. 65
Export reports .............................................................. 65
Types of reports ............................................................ 65

A Finding bundle identifiers (iOS) and package names (Android) ............... 67
Find package names for Android ............................................. 67
Find bundle identifiers for iOS ................................................ 67

B Policy settings for mobile devices ........................................ 69

Index ........................................................................... 75
Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

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.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses the following typographical conventions and icons.

- **Book title or Emphasis**: Title of a book, chapter, or topic; introduction of a new term; emphasis.
- **Bold**: Text that is strongly emphasized.
- **User input or Path**: Commands and other text that the user types; the path of a folder or program.
- **Code**: A code sample.
- **User interface**: Words in the user interface including options, menus, buttons, and dialog boxes.
- **Hypertext blue**: A live link to a topic or to a 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>
Introduction

Get familiar with the features and components of your McAfee® EMM™ software.
McAfee EMM combines secure mobile application access, strong authentication, a scalable architecture, and compliance reporting in a seamless system. Integration with McAfee® ePolicy Orchestrator® enables IT to implement persistent policies and ease compliance management while protecting devices and the corporate network. (For more information on integrating McAfee EMM with ePolicy Orchestrator, see the McAfee Enterprise Mobility Management Extension for ePolicy Orchestrator Product Guide.) McAfee EMM helps drive down support costs and total cost of ownership by leveraging the enterprise's existing data center infrastructure and IT network.

Contents

- McAfee EMM features
- McAfee EMM components
- Navigating the EMM Console

McAfee EMM features

McAfee EMM offers the following features:

- **Network security** — All devices must authenticate, register, and pass policy-based compliance verification before accessing your network. ActiveSync traffic is routed to filter servers, ensuring devices can't bypass compliance services.

- **Strong authentication with public key infrastructure (PKI) features** — The optional PKI Agent offers strong authentication with provisioning tokens and certificate-based authentication.

- **Simplified policy and device management** — The web-based McAfee EMM Console manages your security policies and mobile devices. Policies can be assigned based on LDAP groups and device ownership (personal or corporate-owned). You can control how devices work by setting parameters for allowed resources, password criteria, and more. Security policies are pushed to devices through the Console, ensuring devices remain compliant.

- **Secure and easy provisioning of user devices** — McAfee EMM provides secure and easy provisioning using the McAfee EMM app or the EMM Portal. The McAfee EMM system interacts with Microsoft Active Directory (AD) or Domino to validate authorized device users. iOS and Android users can download a free McAfee EMM app, which streamlines provisioning and adds functionality to deliver security policies as needed.

- **MDM and C2DM support** — You can install McAfee EMM using Mobile Device Management (MDM) for iOS versions 4 and later, and Cloud to Device Message (C2DM) for Android. MDM/C2DM allows policy updates without user intervention and provides enhanced Helpdesk capabilities, including remote lock, passcode unlock, cleaner selective wipe, and uninstall. You can also collect details about devices, including contacts, installed apps, certificates, profiles, restrictions, policy compliance, IMEI number, and WAPMACA address.
• **Android support** — McAfee EMM for Android manages compliance enforcement, remote lock/unlock, remote uninstall, passcodes, Wi-Fi, and for some Android devices, remote wipe and VPN configurations. The optional Secure Container for Android sandboxes enterprise email, contacts, and calendar.

• **iOS (iPhone, iPod Touch, and iPad) support** — McAfee EMM for iOS manages compliance enforcement, reporting, jailbreak detection, Wi-Fi and VPN configurations, and more. Data loss protection is provided through endpoint security with password policies across all iOS devices. Remote wipe and on-the-fly policy updates can be pushed to iOS devices.

• **iCloud key-value data storage** — Apps that store preferences or small amounts of non-critical configuration data can use the iCloud key-value data store to do so. The key-value data store is similar to the local user default database used to store app preferences, but keys stored in the iCloud are shared by all instances of the app running on the user's devices. Key-value updates are shared across all devices.

• **Encrypted connections** — McAfee EMM servers use encrypted SSL (HTTPS) connections so that all data transmitted between mobile devices and servers is encrypted. iOS devices that don't have native encryption (prior to the iPhone 3GS) can be blocked from accessing your network.

• **Windows native encryption** — McAfee EMM relies on Windows native encryption for data on the main memory and removable storage media of Windows Mobile devices (Windows Mobile 6.0 and later, excluding Windows Phone 7). This allows faster access to email and personal information management (PIM) data. When data is saved and resides on the device, it is automatically encrypted.

• **Email server support** — McAfee EMM supports the email servers Exchange 2003, 2007, 2010, and Domino 8.5.1 and 8.5.2. (The Domino environment must have a Traveler server in place.)

• **Secure device check-in** — The device check-in process ensures the devices in your network maintain the most current policy settings. When a device checks in, information about that device appears in the Console. Only compliant devices can access your enterprise resources.

• **Integrated Helpdesk** — McAfee EMM contains an integrated Helpdesk to troubleshoot and support your mobile device users. The Helpdesk features include remote wipe, removal of email and PIM data, remote policy removal, and compliance override capabilities.

• **McAfee EMM Portal** — The McAfee EMM Portal provides a website for users to provision their own mobile devices and perform basic Helpdesk functions. Users can troubleshoot some device issues on their own, and don't have to rely on Helpdesk personnel for assistance.

• **Reports** — McAfee EMM provides a suite of status reports on your mobile environment. Reports contain details about your devices and users, including device ID, make and model, operating system, assigned security policies, and Active Directory or LDAP membership. A complete system audit log tracks all Console activity, and all reports can be exported to Microsoft Excel format.

• **Integration with ePolicy Orchestrator** — McAfee EMM software can be installed as an extension to ePolicy Orchestrator. You can view reports and create a McAfee EMM dashboard in ePolicy Orchestrator.

• **Extended functionality with representation state transfer (REST) services** — You can access certain McAfee EMM functions with REST services, allowing you to manage devices and users with the same functionality in the McAfee EMM Console.
McAfee EMM components

The McAfee EMM system is based on a client-server architecture with server-side and client-side components.

Server components

These components are installed on enterprise servers and are used in the administration of the McAfee EMM system.

**McAfee EMM Enhanced Security Mode**

<table>
<thead>
<tr>
<th>EMM server component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hub</strong></td>
<td>The McAfee EMM Hub (Hub) manages communication between McAfee EMM components. It 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><strong>Console</strong></td>
<td>The McAfee EMM Console (Console) is the application that manages the McAfee EMM system. It is an Internet Information Services (IIS) application accessible with Internet Explorer or Firefox web browsers with Microsoft Silverlight installed. Through the Console, administrative users can configure system settings, change policies, manage devices and users, administer McAfee EMM roles, perform Helpdesk functions, and view reports.</td>
</tr>
<tr>
<td><strong>Portal</strong></td>
<td>The McAfee EMM Portal (Portal) is an Internet-facing component that allows device users to initiate requests for software downloads, and to perform limited Helpdesk functions. Users access the Portal from a browser on a PC or mobile device. The Portal typically resides on a McAfee EMM server installed in the DMZ.</td>
</tr>
<tr>
<td>EMM server component</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Device Management Gateway</td>
<td>The McAfee Device Management Gateway (DMG) is an Internet-facing component that manages the server-side communication with legacy Windows Mobile devices. It controls policy, software, and configuration updates for mobile devices.</td>
</tr>
<tr>
<td>ActiveSync Proxy and Compliance Filter</td>
<td>The McAfee ActiveSync Proxy is an Internet-facing component that proxies ActiveSync traffic to the email servers. It is an IIS application that resides in the DMZ and enables McAfee EMM to control access to enterprise resources on the DMZ server before reaching the internal network. The McAfee Compliance Filter is installed on the filter/proxy server that is placed in the DMZ (or for basic security deployments, on the internal McAfee EMM server).</td>
</tr>
<tr>
<td>Push Notifier</td>
<td>The McAfee Push Notifier is an Internet-facing component that sends push notifications to mobile devices. The Push Notifier is a required component that is usually installed in the DMZ so it can communicate with Apple and Android push notification services.</td>
</tr>
<tr>
<td>BES Agent (optional)</td>
<td>The McAfee BES Agent is an optional component that synchronizes the BlackBerry Enterprise Server to McAfee EMM and performs select device actions. We recommend installing the BES Agent on the internal server.</td>
</tr>
<tr>
<td>PKI Agent (optional)</td>
<td>The McAfee PKI Agent is an optional component that dynamically retrieves certificates from a Microsoft certificate authority in PKI environments. It is usually installed on an internal server.</td>
</tr>
</tbody>
</table>

### Client components

These components are installed on mobile devices that are registered on the enterprise network. They help provision user devices and communicate with the server.

<table>
<thead>
<tr>
<th>EMM Client Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee EMM app (iOS devices)</td>
<td>McAfee EMM is a free iOS app that enables easy provisioning by the user, and allows push notifications to deliver profile and security policy changes.</td>
</tr>
<tr>
<td>McAfee EMM app (Android devices)</td>
<td>McAfee EMM is a free Android app that enables easy provisioning by the user, and allows push notifications to deliver profile and security policy changes.</td>
</tr>
<tr>
<td>McAfee EMM Secure Container app (Android devices)</td>
<td>The McAfee EMM Secure Container app is a free app, currently for Android only, that sandboxes enterprise email, contacts, and calendars.</td>
</tr>
<tr>
<td>Download Manager (Windows Mobile)</td>
<td>The Download Manager is the communication module installed on Windows Mobile devices. It provides device-side communication with the McAfee EMM server.</td>
</tr>
<tr>
<td>PDA Secure (Windows Mobile)</td>
<td>PDA Secure is the security module installed on Windows Mobile devices. It enforces security based on policies that are created in the McAfee EMM Console. Except for the password screen, there is no user interface for PDA Secure, and it can’t be modified by the user. An administrative unlock code is required to remove PDA Secure from the device.</td>
</tr>
</tbody>
</table>
## Navigating the EMM Console

Icons at the bottom of the Console access the main functions of the McAfee EMM software. Clicking an icon opens a window for that function with additional options listed at right.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td><strong>System Settings</strong>&lt;br&gt;Create and manage Console accounts, set global compliance enforcement, change the license key, update company information and the use agreement, manage authorization servers, manage authorized users, update security certificates, update the device catalog, view and edit Enrollment Agents, configure and send text messages, and view BES Agents and Push Notifiers.</td>
</tr>
<tr>
<td>![Icon]</td>
<td><strong>Policies</strong>&lt;br&gt;Create, manage, and publish security policies. Select device settings, assign policies to groups, and specify policies for device compliance, email, passwords, resource restrictions, Secure Container, VPN, APN, Wi-Fi, blacklisting, and certificate authorities.</td>
</tr>
<tr>
<td>![Icon]</td>
<td><strong>User Notifications</strong>&lt;br&gt;Bulk-authorize users and automatically send them emails or text messages with provisioning details. You can bulk-authorize users based on LDAP group or by importing a list.</td>
</tr>
<tr>
<td>![Icon]</td>
<td><strong>Reports</strong>&lt;br&gt;View and export reports, including audit logs, compliance status, package deployment, pending actions, registered users, software status, and unregistered devices.</td>
</tr>
<tr>
<td>![Icon]</td>
<td><strong>Helpdesk</strong>&lt;br&gt;Troubleshoot issues on mobile devices, including wiping the device, deleting email and PIM data (for iOS devices), uninstalling software, locking and unlocking the device, resetting passwords, and overriding compliance. View device information, including applications, certificates, configuration profiles, pending actions, provisioning profiles, and security details.</td>
</tr>
<tr>
<td>![Icon]</td>
<td><strong>Packages</strong>&lt;br&gt;Create and distribute packages containing third-party files or applications for installation on user devices.</td>
</tr>
</tbody>
</table>
Configuring your McAfee EMM software

To get started with your McAfee EMM software, configure access to the EMM Console, review basic settings, and authorize device users.

Chapter 2  Console access
Chapter 3  Basic settings
Chapter 4  User authorization
Console access

The Console is the control center for your McAfee EMM system.
To manage the Console, set up administrative accounts and assign them one of the four default access roles:

- System Administrator
- Policy Administrator
- Helpdesk Administrator
- Reports Viewer

Contents
- View role permissions
- Log on for the first time
- Create administrative accounts
- Delete an administrative account

View role permissions

You can view permissions settings from the Console Access window.

Task
1. Click System Settings | Console Access.
2. In the Console Access window, click Show Details to open the Role Permission screen.
3. From the drop-down list at the top right, select a role.

Log on for the first time

The first time you log on to the Console, use the default administrative account. You can create additional accounts at any time after your first logon.

Task
1. Launch the Console using one of these methods:
   - If you are logged on to the computer where the Console is installed: from the Windows Start menu, select All Programs | McAfee EMM | McAfee EMM Console.
   - Open a web browser and enter the URL for your EMM Console, for example https://<yourhostname>/EMMConsole.
2  On the logon screen, complete the fields, then click Login.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>TDadmin*</td>
</tr>
<tr>
<td>Domain</td>
<td>Local</td>
</tr>
</tbody>
</table>

### Create administrative accounts

Create an administrative account for each user needing access to the Console. This allows you to see which users are logged on to the Console in the audit log report. You can set up individual accounts using LDAP groups (recommended) or by creating a local account.

**Tasks**

- **Create administrative accounts based on LDAP groups on page 18**
  Use LDAP groups to create most administrative accounts. When an LDAP group is added to a role in the McAfee EMM Console, all members of the group have the permissions assigned to that role.

- **Create a local administrative account on page 19**
  You can create a local administrative account to provide access to the McAfee EMM Console without using LDAP groups. This can be useful if you outsource the Helpdesk or management of the Console.

#### Create administrative accounts based on LDAP groups

Use LDAP groups to create most administrative accounts. When an LDAP group is added to a role in the McAfee EMM Console, all members of the group have the permissions assigned to that role.

**Before you begin**

- In Active Directory, set the group property to **Security Group**. In Domino, set the group as a **Multi-purpose Group**.
- Log on to the Console with the system administrator account.

**Task**

1. Click **System Settings | Console Access**.
2. In the **Console Access** window, click **Add**.
3. On the **Add Access** screen, complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Type</td>
<td>LDAP Group</td>
</tr>
<tr>
<td>Role</td>
<td>• System Administrator</td>
</tr>
<tr>
<td></td>
<td>• Policy Administrator</td>
</tr>
<tr>
<td></td>
<td>• Helpdesk Administrator</td>
</tr>
<tr>
<td></td>
<td>• Reports Viewer</td>
</tr>
<tr>
<td>Location</td>
<td>Authorization server domain.</td>
</tr>
<tr>
<td>Group Name</td>
<td>AD or Domino group name.</td>
</tr>
</tbody>
</table>
Once an administrative LDAP account is created, users log on by entering their user name and password, then selecting their domain.

**Create a local administrative account**
You can create a local administrative account to provide access to the McAfee EMM Console without using LDAP groups. This can be useful if you outsource the Helpdesk or management of the Console.

Once a local Console account is created, it can't be edited. If you want to change something on a local account, you must delete it and re-create the account.

**Task**
1. Click **System Settings | Console Access**.
2. In the **Console Access** window, click **Add**.
3. On the **Add Access** screen, complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</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></td>
<td>• Policy Administrator</td>
</tr>
<tr>
<td></td>
<td>• Helpdesk Administrator</td>
</tr>
<tr>
<td></td>
<td>• Reports Viewer</td>
</tr>
<tr>
<td>Username</td>
<td>User name for the account.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the account.</td>
</tr>
</tbody>
</table>

Once a local administrative account is created, the user logs on by entering user name and password, then selecting the local domain.

**Delete an administrative account**
Delete a user's administrative account if you want to remove their access to the Console. Deleting an LDAP-based administrative account removes the group's access to the Console, but does not delete the group from the LDAP server.

**Task**
1. Click **System Settings | Console Access**.
2. In the **Console Access** window, select the account you want to delete, then click **Delete**.
3. Click **OK** to delete the account.
Console access
Delete an administrative account
Basic settings

Configuring these basic settings allows you to perform related management tasks.

Contents
- Manage your company profile and licenses
- About device compliance
- Specify an SMTP server
- Update portal, push, and MDM security certificates
- Update the device catalog
- Enrollment Agents for PKI environments
- View installed auxiliary components

Manage your company profile and licenses
Manage your company name, use agreement, serial number, and device registrations with Activation Settings.

Activation Settings appear when you log on, instead of the Helpdesk, if your available licenses fall below ten percent of your total number of licenses. The screen shows the status of the license and a link to request additional licenses.

Task
1. Click System Settings | General Settings.
2. Modify the fields as needed, then click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Your company name as it appears on user devices.</td>
</tr>
<tr>
<td>Use Agreement</td>
<td>The agreement that appears on devices during provisioning. The updated use agreement is pushed only to devices that have not yet provisioned.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Your McAfee EMM serial number. To add more devices, enter a new serial number.</td>
</tr>
</tbody>
</table>

About device compliance
Device compliance is determined based on the following predefined parameters.
A device is considered compliant if the following is true:
- The device has the current version of the McAfee EMM software installed.
- The device has the current security policy installed.
• If encryption is required by your security policies, the device reports its encrypted status as enabled.
• The iOS device has the correct device certificate that was issued during provisioning.

A device is considered noncompliant if one or more of the following is true:
• The security policy has been updated and the device does not yet have the new policy.
• The device has not checked in since the software or security policy was last updated.
• The device has been hard-reset because of a company policy, and the device no longer contains the McAfee EMM software.
• The device has been jailbroken (iOS) or rooted (Android).
• The device does not support encryption, encryption is disabled, or the device isn't reporting its encrypted status to the EMM server (for example, if the iOS device was provisioned with the McAfee EMM Portal and your EMM software was installed without MDM).

**Enable or disable compliance enforcement**

You can turn compliance enforcement on or off and set a time limit on a single compliance check-in.

**Task**

1. Click **System Settings | General Settings**.
2. Modify the fields as needed, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
</table>
| Compliance Enforcement | • **Enabled** — Only devices that have the current security policy can sync.  
                         | • **Disabled** — Any provisioned device can sync, regardless of its security policy. |
| Compliance Duration (min) | The amount of time (in minutes) a compliance check-in is valid. After this period, the device is considered noncompliant. |

**Specify an SMTP server**

You must configure an SMTP server before sending text messages to user devices.

**Task**

1. Click **System Settings | Mail Settings**.
2. On the **Mail Settings** screen, update the information as you want it to appear in messages to devices, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message From Address</td>
<td>Email address you want to send the text message from.</td>
</tr>
<tr>
<td>Message Subject</td>
<td>Subject line of the text message.</td>
</tr>
<tr>
<td>EMM Portal Message</td>
<td>Provisioning message.</td>
</tr>
<tr>
<td>SMTP Relay Server</td>
<td>IP address or DNS name of an SMTP relay server.</td>
</tr>
</tbody>
</table>

3. (Optional) To send a test SMS message, click **Send Test SMS message**.
Update portal, push, and MDM security certificates

Use certificate settings to update portal, push, and MDM security certificates.

Each time the portal certificate is updated, the EMM profile is removed from all iOS devices and the device must be re-provisioned. Consider obtaining a multi-year portal certificate to minimize this occurrence.

**Task**

1. Click **System Settings | Certificates**.
2. Select a certificate, then click **Update**.
3. On the **Update Certificate** screen, browse to select the certificate, enter your password, then click **Save**.
4. (Optional) If you updated your portal certificate, reset Internet Information Services (IIS) for the changes to take effect.

Update the device catalog

The device catalog contains information on supported mobile devices. It is automatically added when McAfee EMM installs, but you should update the device catalog monthly after installation.

**Task**

1. Click **System Settings | Device Catalog**.
2. On the **Device Catalog** screen, click **Add**.
3. Browse to select the file SFI.nnnn.zip, where, "nnnn" is the build number.
4. On the **Add Device Catalog** screen, click **Install**.

Enrollment Agents for PKI environments

If you are operating in a PKI environment, you enabled an Enrollment Agent during installation. You can edit or delete the Enrollment Agent from the Console after installation.

**Tasks**

- **Edit an Enrollment Agent on page 24**
  You can edit your Enrollment Agent if you have a new certificate, or if you want to update certificate details.
- **Delete an Enrollment Agent on page 24**
  You can delete an Enrollment Agent if it is not being used by an active policy.
Edit an Enrollment Agent
You can edit your Enrollment Agent if you have a new certificate, or if you want to update certificate details.

**Task**
1. Click **System Settings | Enrollment Agents**.
2. On the **Enrollment Agents** screen, select a connection, then click **Edit**.
3. On the **Edit Enrollment Agent** screen, complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Name of the certificate authority server.</td>
</tr>
<tr>
<td>Server URL</td>
<td>Name or FQDN of the server where the Enrollment Agent is installed.</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>FQDN of the certificate authority in the format CA-server\CA-name.</td>
</tr>
<tr>
<td>Signer Certificate</td>
<td>Enrollment Agent certificate installed in the service user's local certificate store.</td>
</tr>
</tbody>
</table>

Delete an Enrollment Agent
You can delete an Enrollment Agent if it is not being used by an active policy.

**Task**
1. Click **System Settings | Enrollment Agents**.
2. On the **Enrollment Agent** screen, select a connection, then click **Delete**.

View installed auxiliary components
View details, such as the host/server name and last update time, for auxiliary components installed on your system.

**Tasks**
- **View your BES Agent on page 24**
  The BES Agent is an optional component that connects to a BlackBerry Enterprise Server. Your BES Agent collects data and writes it to the McAfee EMM Database. You can view the BES Agents installed on your system from the Console.
- **View your Push Notifier on page 25**
  The Push Notifier retrieves device details and allows push notifications to be sent to both MDM and non-MDM devices for policy updates. You can view the Push Notifier installed on your system from the Console.

View your BES Agent
The BES Agent is an optional component that connects to a BlackBerry Enterprise Server. Your BES Agent collects data and writes it to the McAfee EMM Database. You can view the BES Agents installed on your system from the Console.

**Task**
- Click **System Settings | BES Agents**.
**View your Push Notifier**

The Push Notifier retrieves device details and allows push notifications to be sent to both MDM and non-MDM devices for policy updates. You can view the Push Notifier installed on your system from the Console.

**Task**

- Click **System Settings | Push Notifiers**.
Basic settings
View installed auxiliary components
You must authorize users in the McAfee EMM Console before they can provision a device.

Contents

- Manage authorization directories
- Authorize users
- Create a provisioning token
- Delete users

Manage authorization directories

In order to authorize users, you must specify an authorization directory. You can add, edit, or delete servers from the Auth Directories screen.

Tasks

- Add or edit an authorization directory on page 27
  You can add authorization directories or edit the settings on existing directories.
- Delete an authorization directory on page 28
  You may want to delete authorization directories that are no longer in use. If you delete a directory that is in use, all users and devices provisioned to the server will be deleted from the system.

Add or edit an authorization directory

You can add authorization directories or edit the settings on existing directories.

Email policy settings override authorization directory settings.

Task

1. Click System Settings | Authorization Directories.

2. On the Auth Directories screen, 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. On the Add or Edit Auth Directory screen, complete or modify the fields, then click Save.
   - For LDAP user authentication:
### Field | Value
---|---
**Server Type** | • AD  
  • Domino  
**FQDN** | Fully qualified domain name of the AD or Domino server. This field may auto-populate.  
**Domain** | This field populates when FQDN is completed.  
**DN** | The name of the server to be used for authentication:  
  • AD — This field populates when FQDN is completed.  
  • Domino — Leave this field blank.  
**User Name** | User name to connect to the directory service.  
**Password** | Password to connect to the directory service.  
**External EMM Proxy Server Address** | External DNS or IP address of the server that connects to the McAfee EMM Proxy.  
**Use SLL** | This field is checked by default and can't be changed.  

- For ActiveSync Protocol user authentication:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
</table>
| ActiveSync Authentication Address | ActiveSync server.  
| Domain | Domain name of the ActiveSync server. If you are adding a Domino server, enter `servername/servlet/traveler`.  
| Verification Username | Exchange ActiveSync user name.  
| Verification Password | Exchange ActiveSync password.  
| ActiveSync External DNS | External DNS or IP address of the server that connects to the McAfee EMM Proxy.  
| Use SLL | This field is checked by default and can't be changed.  

---

**Delete an authorization directory**

You may want to delete authorization directories that are no longer in use. If you delete a directory that is in use, all users and devices provisioned to the server will be deleted from the system.

**Task**

1. Click **System Settings | Authorization Servers**.

2. On the **Authorization Servers** screen, select the server you want to delete, then click **Delete**.

3. Click **OK** to confirm deletion.

---

**Authorize users**

There are multiple methods for authorizing users. Choose an authorization method based on the type of user authentication in use on your system and the number of users.

**i** If your system uses ActiveSync Protocol for user authentication, you can only authorize users based on a list or manually.
Tasks

- **Authorize all LDAP users on page 29**
  Allow any user to provision using their Active Directory or Domino credentials.

- **Authorize selected users on page 29**
  Allow selected users or groups to provision using Active Directory or Domino credentials.

- **Authorize users based on a list on page 30**
  Allow a list of users to provision using AD or Domino credentials, or using ActiveSync Protocol. Your list of authorized users must be in comma-separated value (CSV) format.

- **Authorize users manually on page 30**
  If you use ActiveSync Protocol for user authentication, you can manually authorize users with their user name and email address.

- **Bulk-authorize and notify users on page 30**
  User Notifications allow you to bulk-authorize many users at once and automatically send them emails or text messages with provisioning details. You can bulk-authorize users based on LDAP groups or by importing a list in comma-separated value (CSV) format.

Authorize all LDAP users

Allow any user to provision using their Active Directory or Domino credentials.

**Task**

1. Click **System Settings | Authorized Users**.
2. On the **Authorized Users** screen under **User Registration**, select **Allow All Users**.
3. Click **Save**.

Authorize selected users

Allow selected users or groups to provision using Active Directory or Domino credentials.

**Task**

1. Click **System Settings | Authorized Users**.
2. On the **Authorized Users** screen under **User Registration**, select **Allow Only Authorized Users**.
3. Click **Add**.
4. On the **Add Authorized User(s)** screen, complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Search LDAP</td>
</tr>
<tr>
<td>Location</td>
<td>Domain</td>
</tr>
<tr>
<td>User/Group</td>
<td>Users or groups to add as authorized users.</td>
</tr>
</tbody>
</table>

If the status No Email appears in the email column, the user can't provision. In your 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.
Authorize users based on a list

Allow a list of users to provision using AD or Domino credentials, or using ActiveSync Protocol. Your list of authorized users must be in comma-separated value (CSV) format.

**Task**
1. Click **System Settings | Authorized Users**.
2. On the **Authorized Users** screen under **User Registration**, select **Allow Only Authorized Users**.
3. Click **Add**.
4. On the **Add Authorized User(s)** screen from the **Source** field, select **Import CSV**.
5. Complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Domain.</td>
</tr>
<tr>
<td>CSV File Path</td>
<td>Select the CSV file.</td>
</tr>
</tbody>
</table>

**See also**

*CSV format for list-based user authorization on page 31*

Authorize users manually

If you use ActiveSync Protocol for user authentication, you can manually authorize users with their user name and email address.

**Task**
1. Click **System Settings | Authorized Users**.
2. On the **Authorized Users** screen, click **Add**.
3. On the **Add Authorized User(s)** screen from the **Source** field, select **Manually Define User**.
4. Complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Domain.</td>
</tr>
<tr>
<td>Username</td>
<td>User's user name.</td>
</tr>
<tr>
<td>E-mail</td>
<td>User's email address.</td>
</tr>
<tr>
<td>First Name</td>
<td>User's first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>User's last name.</td>
</tr>
</tbody>
</table>

Bulk-authorize and notify users

User Notifications allow you to bulk-authorize many users at once and automatically send them emails or text messages with provisioning details. You can bulk-authorize users based on LDAP groups or by importing a list in comma-separated value (CSV) format.

**Before you begin**

If you want users to provision with a provisioning token, you must set the provisioning token requirement in **System Settings**. Select **System Settings | Authorized Users**. Under **User Authorization**, select **Allow Only Authorized Users**, select **Require Provisioning Token**, and enter a **Token Length** (number of characters) and **Hours Valid**. Selecting these options automatically generates provisioning tokens for each bulk-authorized user.
**Task**

1. Click **User Notifications**.

2. Near the top left of the screen, click **Provision Users**.

3. On the **Provision Users** screen, complete the fields, then click **Next**.

<table>
<thead>
<tr>
<th>User Option</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users based on LDAP group</td>
<td>Source</td>
<td>Search LDAP</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Domain.</td>
</tr>
<tr>
<td></td>
<td>User/Group</td>
<td>Select the users or groups to add as authorized users. Entering a user or group name populates the <strong>Search Results</strong>.</td>
</tr>
<tr>
<td></td>
<td>Search Results</td>
<td>Select users from this list and use the arrows to move them to the list of <strong>Users to Provision</strong>.</td>
</tr>
<tr>
<td>Allow users based on a CSV list</td>
<td>Source</td>
<td>Import CSV</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Domain.</td>
</tr>
<tr>
<td></td>
<td>CSV File Path</td>
<td>Select the CSV file.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delivery Method</strong></td>
<td>Email — This option is available only with CSV import.</td>
</tr>
<tr>
<td><strong>Notification Message</strong></td>
<td>Enter the message you want to send to users.</td>
</tr>
<tr>
<td>• If you select <strong>Email</strong> as your delivery method, a default notification message is provided. You can edit the message before sending.</td>
<td></td>
</tr>
<tr>
<td>• If you select <strong>SMS</strong> as your delivery method, your notification message can’t exceed 140 characters.</td>
<td></td>
</tr>
</tbody>
</table>

⚠️ 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 you are authorizing. |

**CSV format for list-based user authorization**

Use these guidelines to format your comma-separated value (CSV) file to import a list of authorized users.

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

The CSV format for McAfee EMM version 9.7 is no longer supported. To successfully import users, you must use the CSV format shown below.

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

A provisioning token is a temporary password for users to provision their device. Provisioning tokens can only be used for iOS and Android devices provisioning with the McAfee EMM app.

**Task**

1. Click **System Settings** | **Authorized Users**.

2. On the **Authorized Users** screen under **User Registration**, complete the fields, then click **Add**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Only Authorized Users</td>
<td>Select to allow only authorized users.</td>
</tr>
<tr>
<td>Require Provisioning Token</td>
<td>Select to require a provisioning token. The following fields appear:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Token Length</strong> — Enter the number of characters required for the temporary password.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hours Valid</strong> — Enter the number of hours the temporary password is valid.</td>
</tr>
</tbody>
</table>

3. On the **Add Authorized User(s)** screen, complete the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td><strong>Search LDAP</strong></td>
</tr>
<tr>
<td>Location</td>
<td><strong>Domain</strong></td>
</tr>
<tr>
<td>User/Group</td>
<td><strong>Users or groups to add as authorized users.</strong></td>
</tr>
</tbody>
</table>

4. Select the user from the list and edit the additional fields as needed, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Token</td>
<td><strong>Temporary password.</strong></td>
</tr>
<tr>
<td>Hours Valid</td>
<td>Number of hours the temporary password is valid.</td>
</tr>
<tr>
<td>Delivery Action</td>
<td>• <strong>No Action</strong> — Does not notify the user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Send SMS</strong> — Opens the Provisioning SMS screen. Enter the phone number, carrier, subject, and message, then click <strong>Send SMS</strong> to send a text message to the user containing their temporary password.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Send Email</strong> — Opens an email to the user containing the temporary password. Send the message.</td>
</tr>
</tbody>
</table>

Delete users

Deleting a user from the authorized users list will prevent them from syncing or provisioning their device. The user's device still appears in the Helpdesk.

**Task**

1. Click **System Settings** | **Authorized Users**.

2. On the **Authorized Users** screen, select the user you want to remove, then click **Delete**.
Managing your McAfee EMM software

Day-to-day management of your McAfee EMM software is accomplished through the Helpdesk. On a less frequent basis, you can administer security policies and work with packages, which distribute files to mobile devices on your system.
Helpdesk functions

The Helpdesk allows you to troubleshoot issues on mobile devices. Users are added to the McAfee EMM Helpdesk when their device is provisioned.

Contents
- Device details
- Remove data from user devices
- Manage access to user devices
- Query MDM devices
- Override compliance for a device
- Send a text message to users
- Delete devices from the Console

Device details

In the McAfee EMM Helpdesk, device details appear on tabs below the list of users. Device details vary depending on device type, operating system, and pending actions. You can search for a specific user or device using the search box at the top right of the Helpdesk.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Details</td>
<td>Device name, policy information, compliance information, identification information, encryption status, and more.</td>
</tr>
<tr>
<td>Applications</td>
<td>Applications and versions installed on the device.</td>
</tr>
<tr>
<td>Certificates</td>
<td>Security certificate, certificate issuer, generation date, and expiration dates for iOS devices.</td>
</tr>
<tr>
<td>Config Profiles</td>
<td>Configuration profiles stored on iOS devices.</td>
</tr>
<tr>
<td>Pending Actions</td>
<td>Action type and date/time the action was created. This tab appears only if the device has pending actions.</td>
</tr>
<tr>
<td>Provisioning Profiles</td>
<td>Provisioning profile for iOS devices.</td>
</tr>
<tr>
<td>Security Details</td>
<td>Hardware encryption, password protection, and password compliance.</td>
</tr>
</tbody>
</table>

Remove data from user devices

There are many options for removing data from provisioned user devices. These include wiping the device completely, deleting proprietary data from iOS devices, or uninstalling the McAfee EMM profile and configurations.

These actions do not remove devices from the Helpdesk. You must delete a device from the Helpdesk before it can re-provision.
Tasks

- **Wipe a device on page 36**
  This is the fastest method and most thorough method for wiping a device.

- **Delete email and PIM data from iOS devices on page 36**
  Deleting email and PIM data (contacts and calendars) from a user's device leaves software, profiles, and applications intact.

- **Uninstall the McAfee EMM profile from a device on page 36**
  You can uninstall the McAfee EMM profile from iOS and Android devices. For Windows Mobile devices, you should perform a complete wipe.

### Wipe a device

This is the fastest method and most thorough method for wiping a device.

**Task**

1. Click Helpdesk, then select the device you want to wipe.
2. Click Wipe.
3. Click OK to confirm.

### Delete email and PIM data from iOS devices

Deleting email and PIM data (contacts and calendars) from a user's device leaves software, profiles, and applications intact.

For iOS devices versions 4 and later with MDM enabled, deleting email and PIM data removes the Enterprise Activation profile, which contains the Exchange configuration and all email data. The MDM profile remains so the device can be fully wiped in the future.

For iOS versions prior to iOS 4, the Inbox folder name remains on the device, but all emails, email folders, contacts, and calendar data are deleted.

**Task**

1. Click Helpdesk, then select the device you want to delete email and PIM data from.
2. Click Delete Email & PIM Data.
3. Click OK to confirm deletion.

   The next time the device connects to the server, deletion begins. Once the data is deleted from the device, the device status changes to Delete PIM Completed.

### Uninstall the McAfee EMM profile from a device

You can uninstall the McAfee EMM profile from iOS and Android devices. For Windows Mobile devices, you should perform a complete wipe.

The effects of uninstalling the McAfee EMM profile vary by device:
• For iOS devices, the McAfee EMM app and Wi-Fi configurations remain after uninstalling. For iOS versions prior to iOS 4, the user is prompted to install an Uninstall profile, which replaces their existing McAfee EMM profile. The Uninstall configuration profile can be removed manually after uninstall.

• For Android devices, the McAfee EMM app and Wi-Fi nodes not configured by the app remain after uninstalling.

• For Windows Mobile Devices, uninstalling the app removes PDASecure. Any encrypted data stored on the device and SD card is decrypted. The Download Manager, Exchange data, and Exchange configuration remain after uninstalling.

**Task**

1. Click **Helpdesk**, select a device, then click **Uninstall**.

2. Click **OK** to confirm uninstall.

   A prompt appears indicating the uninstall notification was sent.

---

**Manage access to user devices**

You can remotely lock and unlock user devices from the Helpdesk, reset device passwords, and create provisioning tokens so new users can provision their device.

**Tasks**

- **Lock a device on page 37**
  You can remotely lock MDM-provisioned iOS devices and MDM/C2DM-provisioned Android devices versions 2.2 or later. Remote lock does not prevent the user from unlocking the device if they know the device password.

- **Unlock a device on page 38**
  Remotely unlock a device from the EMM Console after the user exceeds the allowed password attempts when accessing the McAfee EMM app or EMM Portal. Remote unlock does not work for Windows Mobile devices.

- **Reset a device password on page 38**
  Remotely reset a device password for MDM-enabled iOS or Android devices. Remote password reset is not available for Windows Mobile devices.

- **Unlock a Windows Mobile device and reset the password on page 38**
  You must unlock a Windows Mobile device and reset the password at the same time. This procedure requires that the device user and Helpdesk operator exchange authentication and unlock codes.

- **Update a provisioning token on page 39**
  A provisioning token is a one-time password for a device. If you authorized users with LDAP groups in **System Settings**, you must create a provisioning token before users can provision their devices.

**Lock a device**

You can remotely lock MDM-provisioned iOS devices and MDM/C2DM-provisioned Android devices versions 2.2 or later. Remote lock does not prevent the user from unlocking the device if they know the device password.

**Task**

1. Click **Helpdesk**, then select a device.

2. Click **Lock** at the bottom of the screen.
Unlock a device
Remotely unlock a device from the EMM Console after the user exceeds the allowed password attempts when accessing the McAfee EMM app or EMM Portal. Remote unlock does not work for Windows Mobile devices.

Task
1. Click Helpdesk | Unlock User.
2. On the Unlock User screen, select the user you want to unlock, then click Remove User.
   The user is removed from the locked users list.

Reset a device password
Remotely reset a device password for MDM-enabled iOS or Android devices. Remote password reset is not available for Windows Mobile devices.

Task
1. Click Helpdesk, then select a device.
2. Click Reset Password.
   - For an iOS device, the device is unlocked and prompts the user to set a new password.
   - For an Android device, a dialog box appears in the McAfee EMM Console displaying a temporary password. Read the temporary password to the user to unlock the Android. The user is prompted to set a new password.

Unlock a Windows Mobile device and reset the password
You must unlock a Windows Mobile device and reset the password at the same time. This procedure requires that the device user and Helpdesk operator exchange authentication and unlock codes.

Task
1. Click Helpdesk, then select the device to be unlocked.
2. Click Reset Password.
3. On the Reset Password confirmation screen, click OK.
   The Reset Password screen appears asking for an authentication code.
4. Guide the user through obtaining the authentication code from their device. Ask the user to:
   a. Manually lock the device.
   b. Click Remote Unlock from the Password screen.
   c. Read you the sixteen-character authentication code displayed on their device.
5. On the Password Reset screen, type the authentication code the device user reads to you, then click Save.
   The authentication code must be entered in uppercase characters.
   An unlock code appears in the EMM Console.
6 Read the unlock code to the user to enter on their device. Tell the user to click **Next** and follow the prompts to change their power-on password.

7 Click **OK** to close the dialog box in the EMM Console.

**Update a provisioning token**

A provisioning token is a one-time password for a device. If you authorized users with LDAP groups in **System Settings**, you must create a provisioning token before users can provision their devices.

**Task**

1 Click **Helpdesk | Update Token**.

2 On the **Update Token** screen, type a user name in the search box, then select a user from the name list.

3 Complete the fields, then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</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.</td>
</tr>
<tr>
<td>Delivery Action</td>
<td>• No Action — Does not notify the user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Send SMS</strong> — Opens the <strong>Provisioning SMS</strong> screen. Enter the phone number, carrier, subject, and message, then click <strong>Send SMS</strong> to send a text message to the user containing their temporary password.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Send Email</strong> — Opens an email to the user containing the temporary password. Send the message.</td>
</tr>
</tbody>
</table>

**Query MDM devices**

For MDM-enabled iOS devices and MDM/C2DM-enabled Android devices, you can view general and security info and get a list of installed apps. For iOS devices, you can also view installed profiles.

**Task**

1 Click **Helpdesk**, then select a device.

2 Click **Query**.

![Query button is not shown if the selected device is not MDM or MDM/C2DM-enabled.]

Pending actions are queued. At the next MDM check-in interval, the device details tabs are updated in the Helpdesk.
Override compliance for a device

You can set a device to always be compliant or never be compliant. This may be useful when a user goes on extended leave.

**Task**

1. Click Helpdesk, then select a device.
2. Click Compliance Override.
3. On the Compliance Override screen, complete the fields, then click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Compliance Override</td>
<td>Select to allow the device to override compliance.</td>
</tr>
<tr>
<td>Compliance Status</td>
<td>• Always Compliant — Permits the user to check in and sync when they are out of compliance.</td>
</tr>
<tr>
<td></td>
<td>• Never Compliant — Restricts the user from checking in and syncing when they are out of compliance.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Expiration date for the compliance override.</td>
</tr>
</tbody>
</table>

**See also**

*Enable or disable compliance enforcement on page 22*

Send a text message to users

You can send a text message to all registered users or to individual users.

**Before you begin**

Configure the SMTP relay server in System Settings.

**Task**

1. Click Helpdesk | Send SMS.
2. On the Send SMS screen, complete the fields, then click Send SMS.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send to All Registered Devices</td>
<td>Select to send the text message to all registered users.</td>
</tr>
<tr>
<td>Recipient's Phone Number</td>
<td>If you want to text one user, enter their phone number. This field is disabled if you select to send to all registered devices.</td>
</tr>
<tr>
<td>Carrier</td>
<td>If you want to text one user, select their carrier. This field is disabled if you select to send to all registered devices.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject line of your message.</td>
</tr>
<tr>
<td>Message</td>
<td>Body of your message.</td>
</tr>
</tbody>
</table>

**See also**

*Specify an SMTP server on page 22*
Delete devices from the Console

A device can be deleted from the Console after it has been wiped, uninstalled, or had email and PIM data removed. Deleting a device from the Console does not remove the McAfee EMM software, user account, or any data or applications on the device.

**Task**

1. Click Helpdesk, then select a device.
2. Click Delete.
3. Click OK to confirm deletion.
Helpdesk functions
Delete devices from the Console
Policies

Security policies determine how devices interact with the network to keep the organization’s resources secure.

Contents

- Policy overview and recommendations
- Create new policies
- Prioritize policies
- Assign membership to policies
- Change device ownership
- Change policy settings
- Publish policies
- Delete policies

Policy overview and recommendations

Understand how security policies are set and assigned, and learn best practices for working with policies.

Default policy

The default policy is assigned to all users who aren’t assigned another policy. The default policy appears at the bottom of the list on the Policies screen.

The McAfee EMM system provides a starter policy, and you can use or change the starter policy’s settings. Use the starter policy as the default policy, or create another policy to use as the default.

Policy membership and prioritization

Policies are assigned to users based on LDAP group membership and corporate device ownership.

When users provision their devices, they receive the first security policy listed in the Console that applies to them based on LDAP group membership or corporate device ownership. For this reason, it’s important to prioritize your security policies appropriately. Priority is assigned based on list order on the Policy screen, with the highest priority policy on top.

Use these guidelines to prioritize your policies:
- Set up policy-specific LDAP groups and create corresponding policies for each group. For example, you might create a Sales group in the directory and assign that group to the Sales Policy.

- If you create a policy based on corporate device ownership, place it at the bottom of your list of policies to avoid overriding any LDAP-based policies.

- If you are using ActiveSync Protocol for user authentication, you can't assign groups to policies. In addition to the default policy, you can create a second policy that applies to corporate devices. Users are assigned one of the two policies based on their device ownership as shown in the Helpdesk.

![Figure 6-1 Example of policy prioritization with LDAP groups and corporate devices](image)

**How devices respond to policy publishing**

Publishing affects devices differently depending on the device operating system.

- MDM devices contact the server to get the new policy after receiving a push notification. When this happens, the policy exchange account configuration is removed and re-added to the device, which causes all mailbox data to re-sync. The user's email may seem to disappear briefly until the re-sync is complete.

- Non-MDM iOS 4 and later devices that provision using the EMM Portal must re-provision to receive a new policy or policy update.

- Non-MDM iOS versions earlier than iOS 4 receive an alert when a policy is published. Devices display a pop-up window to indicate a new policy is available. Users can click OK or Cancel, but if they cancel, the device will be marked as noncompliant until the user accepts the policy change.

- ActiveSync devices are updated with the new policy at their next sync attempt.

- Windows Mobile devices automatically restart every time a new policy is published.
Best practices for implementing policies
For best results, follow these steps to create, test, and verify a new security policy.

Task
1. Create the policy.
2. Change the policy settings as needed.
3. Assign the policy to a test group of users.
4. Save the policy.
5. Publish the policy.
6. Evaluate the policy on the test devices and adjust the policy as needed.
7. Change policy membership to the appropriate production groups.
8. Publish the policy.

Create new policies
Console users assigned the System Administrator or Policy Administrator role can create new policies.

Task
1. Click Policy Settings | Create New.
2. On the Create Policy screen, complete the fields, then click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>• New Policy</td>
</tr>
<tr>
<td></td>
<td>• Copy Policy — If you are copying a policy, the Policy to Copy field appears. Select a policy to copy.</td>
</tr>
<tr>
<td>New Policy Name</td>
<td>Unique name for the policy.</td>
</tr>
</tbody>
</table>

The new policy is created and appears at the right of the Policy screen. An exclamation mark appears next to the policy's icon, indicating it has not yet been published.

3. Change the policy settings as needed.
4. Publish the policy.

See also
Change policy settings on page 47
Publish policies on page 56
**Prioritize policies**

Reordering policies on the Policy screen determines which policy is the default, and sets the priority of policies. The default policy appears at the bottom of the list.

**Task**
1. Click Policies | Reorder Policies.
2. On the Reorder Policies screen, select a policy and click the up or down arrows to reposition it in the list, then click Save.

**Assign membership to policies**

Assign users to policies based on LDAP group membership or corporate device ownership.

**Before you begin**
If you want to assign membership based on LDAP groups, create groups and assign users in your Active Directory or Domino server.

**Task**
1. Click Policies, select the policy to be changed, then select the Membership tab.
2. Do one or both of the following:
   - To assign the policy based on LDAP groups, click Add. On the Add Group screen, complete the fields, then click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Domain.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Enter at least three characters of the group name, or press Enter, then select a group.</td>
</tr>
</tbody>
</table>

- To assign the policy to corporate-owned devices, select This policy applies to corporate owned devices.

**Change device ownership**

When a device is provisioned, it’s marked as personal by default. You can change ownership to indicate that the device is corporate-owned. Doing so allows you to tailor security policies to corporate-owned devices.

If you’ve created security policies that apply to corporate-owned devices, changing device ownership may result in a policy update. To limit disruption caused by policy updates, we recommend that you change device ownership during off-peak hours.

**Task**
1. Click Helpdesk, then select a device.
2. At the bottom right of the screen, click Change Ownership.
3. Click OK to confirm that you want to change ownership.

Device ownership is updated in the Helpdesk. Any policies that now apply based on the change in ownership are pushed to the device.
Change policy settings

Policy settings allow you to fine-tune your security policies.

Tasks

- **Change compliance settings on page 47**
  Compliance settings allow you to block devices based on encryption support, jailbroken/rooted status, or iOS operating system version.

- **Change email settings on page 48**
  Email settings allow you to activate ActiveSync and configure how email traffic is directed.

- **Change password settings on page 49**
  Password settings allow you to control password type, requirements, and length.

- **Change device restrictions on page 49**
  Restrictions allow you to control which device resources users can access.

- **Change Secure Container settings on page 51**
  Control access to the Secure Container for Android by specifying password requirements. You can also control some Secure Container settings, including syncing while roaming and whether email attachments can be opened by other programs.

- **Change VPN profile settings on page 51**
  You can set up VPN profiles for iOS devices and Motorola devices running Android versions 2.2 and later.

- **Change Wi-Fi profile settings on page 53**
  You can create Wi-Fi profiles for iOS devices and Android devices versions 2.2 and later. All Wi-Fi types are supported for iOS devices. For Android devices, only WEP, WPA, and open Wi-Fi networks are supported.

- **Change certificate settings on page 54**
  Add a certificate from a certificate authority if you are operating in a PKI environment and want to set up Wi-Fi or VPN profiles with certificate authentication.

- **Change APN settings on page 55**
  iOS devices may use an APN to connect to a specific mobile network.

- **Change blacklist settings on page 56**
  Blacklisted apps prevent users from syncing mail to their device by marking the device non-compliant.

Change compliance settings

Compliance settings allow you to block devices based on encryption support, jailbroken/rooted status, or iOS operating system version.

Task

1. Click **Policies**, select the policy to be changed, then select the **Compliance** tab.

2. Select the options you want, then click **Save**.

   To manually change the OS versions to be blocked, click **Add OS Version**. On the **Add OS Versions** screen, select a **Device Model**, enter a **Version**, then click **Save**.
Change email settings

Email settings allow you to activate ActiveSync and configure how email traffic is directed.

- Setting a policy-based proxy server overrides your authorization directory settings.

**Task**

1. Click Policies, select the policy to be changed, then select the Email tab.

2. Select Configure an ActiveSync account while provisioning, complete the fields, then click Save.

<table>
<thead>
<tr>
<th>User Option</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want to direct email traffic through an EMM Proxy server…</td>
<td>Direct traffic through an EMM Proxy server</td>
<td>Leave this option selected.</td>
</tr>
</tbody>
</table>
| | ActiveSync Endpoint | • Use Auth Directory Configuration  
• Alternate EMM Proxy — Enter the Proxy address. |
If you want to configure an alternate server for directing email traffic...

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct traffic through an EMM Proxy server</td>
<td>Deselect this option.</td>
</tr>
<tr>
<td>ActiveSync Endpoint</td>
<td>• Exchange</td>
</tr>
<tr>
<td></td>
<td>• Domino</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td>External EMM Proxy server address</td>
<td>Proxy server address.</td>
</tr>
<tr>
<td>Send User's Domain</td>
<td>Select this option if you chose Other as the ActiveSync Endpoint.</td>
</tr>
</tbody>
</table>

## Change password settings

Password settings allow you to control password type, requirements, and length.

**Task**

1. Click Policies, select the policy to be changed, then select the Passwords tab.

2. Select the options you want, then click Save.

<table>
<thead>
<tr>
<th>Option</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power-On Password</td>
<td>Select or deselect to require a password when accessing a device. If a password is required, select the remaining password settings.</td>
</tr>
<tr>
<td>Profile Removal Password</td>
<td>Click Show to show or hide the administrator's password. This is an embedded device password that allows removal of config profiles from iOS devices earlier than iOS 4 and administrative access on Windows Mobile devices. You can change the default administrator password by entering a new password.</td>
</tr>
</tbody>
</table>

## Change device restrictions

Restrictions allow you to control which device resources users can access.

**Task**

1. Click Policies, select the policy to be changed, then select the Restrictions tab.

2. Select the general, Windows Mobile, and iOS 5 restrictions you want to apply, then click Save.

<table>
<thead>
<tr>
<th>Option</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Restrictions</td>
<td></td>
</tr>
<tr>
<td>Block iTunes Explicit Content</td>
<td>Prevents downloading content categorized as &quot;explicit.&quot;</td>
</tr>
<tr>
<td>Block YouTube</td>
<td>Disables the YouTube application and removes the icon from the home screen. This does not prevent YouTube access from other applications.</td>
</tr>
<tr>
<td>Block iTunes</td>
<td>Prevents access to iTunes.</td>
</tr>
<tr>
<td>Block Camera</td>
<td>Disables camera on the device.</td>
</tr>
<tr>
<td>Option</td>
<td>Details</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow FaceTime</td>
<td>Allows FaceTime to be used on the device. This can only be selected if the camera capabilities of the device are not restricted.</td>
</tr>
<tr>
<td>Block Screen Capture</td>
<td>Prevents screen captures on the device.</td>
</tr>
<tr>
<td>Block Automatic Sync While Roaming</td>
<td>Prevents device from syncing when roaming.</td>
</tr>
<tr>
<td>Block In-App Purchases</td>
<td>Prevents In App purchases.</td>
</tr>
<tr>
<td>Block Multiplayer Gaming</td>
<td>Prevents user from multiplayer gaming.</td>
</tr>
<tr>
<td>Block Voice Dialing</td>
<td>Prevents voice dialing capabilities.</td>
</tr>
<tr>
<td>Block Installing Non-Enterprise Applications</td>
<td>Prevents user from installing non-enterprise applications.</td>
</tr>
<tr>
<td>Block Safari</td>
<td>Disables the Safari browser on iOS devices and removes the icon from the home screen. This also prevents users from opening web clips. If you do not restrict the browser, you can select to allow or disallow Autofill, fraud warnings, Javascript, pop-ups, or cookies.</td>
</tr>
</tbody>
</table>

**WM5/WM6 Client Restrictions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Beam/IR</td>
<td>Disables Beam/IR capabilities.</td>
</tr>
<tr>
<td>Block Desktop Sync</td>
<td>Prevents device from syncing to a desktop using ActiveSync.</td>
</tr>
<tr>
<td>Block Wi-Fi</td>
<td>Disables Wi-Fi on the device.</td>
</tr>
<tr>
<td>Block Storage Card</td>
<td>Prevents user from saving information to the storage card.</td>
</tr>
<tr>
<td>Block SMS/MMS/Text Messaging</td>
<td>Disables text messaging on the device. This applies only to Windows Mobile devices.</td>
</tr>
<tr>
<td>Block All Bluetooth</td>
<td>Disables all Bluetooth operations.</td>
</tr>
<tr>
<td>Allow Hands Free</td>
<td>Allows hands-free Bluetooth operation.</td>
</tr>
</tbody>
</table>

**iOS 5 Restrictions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force iTunes Store Password Entry</td>
<td>Requires user to enter their iTunes password for all purchases.</td>
</tr>
<tr>
<td>Block Cloud Backup</td>
<td>Prevents iOS devices from backing up to the Apple cloud service.</td>
</tr>
<tr>
<td>Block Cloud Document Sync</td>
<td>Prevents user from uploading documents to the Apple cloud service.</td>
</tr>
<tr>
<td>Block Cloud Key-Value Sync</td>
<td>Prevents user from syncing their app configurations to the Apple cloud service.</td>
</tr>
<tr>
<td>Block Photo Stream</td>
<td>Prevents photos from syncing to other devices associated with the user's Apple ID.</td>
</tr>
<tr>
<td>Block Untrusted TLS Certificate Prompt</td>
<td>Prevents user from accessing email or websites if the SSL certificate is untrusted.</td>
</tr>
<tr>
<td>Block Siri (Voice Assistant)</td>
<td>Disables Siri.</td>
</tr>
<tr>
<td>Block Diagnostic Data From Being Sent</td>
<td>Prevents diagnostic data from being sent to Apple.</td>
</tr>
<tr>
<td>Block Sending Corporate Email Via Other Email Accounts</td>
<td>Prevents user from sending enterprise emails from other accounts provisioned on their device.</td>
</tr>
</tbody>
</table>
### Change Secure Container settings

Control access to the Secure Container for Android by specifying password requirements. You can also control some Secure Container settings, including syncing while roaming and whether email attachments can be opened by other programs.

**Task**

1. Click **Policies**, select the policy to be changed, then select the **Secure Container** tab.

2. Select the options you want, then click **Save**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Third Party Applications From Using Corporate Email</td>
<td>Prevents applications from accessing enterprise email.</td>
</tr>
<tr>
<td>Control Roaming</td>
<td>Prevents device from roaming outside the mobile network. Select to restrict data roaming or voice roaming.</td>
</tr>
</tbody>
</table>

If you are unable to select data and voice roaming and you recently upgraded from McAfee EMM version 9.x to 10.x verify that you have upgraded your iOS MDM access rights. Click **System Settings** | **General Settings**, check **Upgrade iOS MDM access rights**, then click **Save**. Once this option is selected, you are unable to deselect it.

### Change VPN profile settings

You can set up VPN profiles for iOS devices and Motorola devices running Android versions 2.2 and later.

**Before you begin**

- Make sure an Enrollment Agent is configured in **System Settings** | **Enrollment Agents**.
- Add identity (device) certificates in **Policies** | **Certificates**.

**Task**

1. Click **Policies**, select the policy to be changed, then select the **VPN Profiles** tab.

2. Click **Add**.

3. On the **Add VPN Payload** screen, complete the fields, then click **Save**.
### Tab | Option | Details
--- | --- | ---
General | Connection Name | Name for the VPN settings.
Connection Type | • L2TP | Cisco AnyConnect
| • PPTP | Juniper SSL
| • IPSec (Cisco) | 
Server Address | IP address or host name of the VPN.
Authentication | Username Template | Specify if users will be required to enter only their user name or domain\user name.
Authentication Type | Select the authentication type for the connection. The fields change according to the connection type and authentication type. See Authentication data for VPN profiles.
Proxy | Configuration | • None
| • Manual — Enter the Proxy Address, Port, Username, and Password.
| • Automatic — Enter the URL of the VPN server.

### See also
* Enrollment Agents for PKI environments on page 23
* Change certificate settings on page 54

### Authentication data for VPN profiles
When you set up a VPN profile, you must provide additional information based on your connection type and authentication type. These settings are explained here.

You can modify the list of available identity (device) certificates in Policies | Certificates.

| On the General tab, if you choose connection type... | On the Authentication tab, you can choose authentication type... | Complete these fields for your authentication type |
--- | --- | ---
L2TP | Password RSA SecurID | • Shared Secret — Password for the connection.
| RSA SecurID | • Send All Traffic — Select to disable split tunneling. |
PPTP | Password RSA SecurID | • Encryption Level — Select the level of data encryption applied for the connection: None, Automatic, or Maximum (128 bit).
| RSA SecurID | • Send All Traffic — Select to disable split tunneling. |
IPSec (Cisco) | Shared Secret (Group Name) | • Group Name — Group identifier for the connection.
| | • Shared Secret — Password for the connection.
| | • Use Hybrid Authentication — Authenticate using shared secret, name, and server-side certificate.
| | • Prompt for Password — Prompt user for password on the device.
On the General tab, if you choose connection type...

<table>
<thead>
<tr>
<th>On the Authentication tab, you can choose authentication type...</th>
<th>Complete these fields for your authentication type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>• Identity Certificate — Select a certificate.</td>
</tr>
<tr>
<td></td>
<td>• Include User PIN — Request a PIN during connection and send with authentication.</td>
</tr>
<tr>
<td></td>
<td>• Enable VPN on Demand — Select to have domain and host names establish a VPN. If selected, enter Domain/Host and Action.</td>
</tr>
</tbody>
</table>

Cisco AnyConnect

<table>
<thead>
<tr>
<th>Password</th>
<th>Group — Group identifier for the connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>Identity Certificate — Select a certificate.</td>
</tr>
<tr>
<td></td>
<td>Enable VPN on Demand — Select to have domain and host names establish a VPN. If selected, enter Domain/Host and Action.</td>
</tr>
</tbody>
</table>

Juniper SSL

<table>
<thead>
<tr>
<th>Password</th>
<th>Realm — Realm for authenticating the connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>Role — Role for authenticating the connection.</td>
</tr>
<tr>
<td></td>
<td>Password — Password for the connection.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Realm — Realm for authenticating the connection.</td>
</tr>
<tr>
<td></td>
<td>Role — Role for authenticating the connection.</td>
</tr>
<tr>
<td></td>
<td>Identity Certificate — Select a certificate.</td>
</tr>
<tr>
<td></td>
<td>Enable VPN on Demand — Select to have domain and host names establish a VPN. If selected, enter Domain/Host and Action.</td>
</tr>
</tbody>
</table>

**Change Wi-Fi profile settings**

You can create Wi-Fi profiles for iOS devices and Android devices versions 2.2 and later. All Wi-Fi types are supported for iOS devices. For Android devices, only WEP, WPA, and open Wi-Fi networks are supported.

**Before you begin**

- Make sure an Enrollment Agent is configured in System Settings | Enrollment Agents.
- Add identity (device) certificates and trusted certificates in Policies | Certificates.

**Task**

1. Click Policies, select the policy to be changed, then select the Wi-Fi Profiles tab.
2. Click Add.
3. On the Add Wi-Fi Payload screen, complete the fields, then click Save.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network SSID</td>
<td>Network SSID.</td>
</tr>
<tr>
<td>Hidden Network</td>
<td>Select if your access point is not broadcasting the SSID.</td>
</tr>
<tr>
<td>Security Type</td>
<td>Select the encryption for your wireless network and complete the additional fields.</td>
</tr>
<tr>
<td></td>
<td>WEP Password — Password for the Wi-Fi connection.</td>
</tr>
<tr>
<td></td>
<td>WPA/WPA2</td>
</tr>
<tr>
<td></td>
<td>Any (Personal)</td>
</tr>
<tr>
<td></td>
<td>WEP Enterprise</td>
</tr>
<tr>
<td></td>
<td>WPA/WPA2 Enterprise</td>
</tr>
<tr>
<td></td>
<td>Any (Enterprise)</td>
</tr>
<tr>
<td></td>
<td>On the Protocols tab, select the appropriate protocols:</td>
</tr>
<tr>
<td></td>
<td>• If you're using TLS or TTLS, select PAP, CHAP, MSCHAP, or MSCHAPv2.</td>
</tr>
<tr>
<td></td>
<td>• If you're using EAP-FAST, select to use PAC, Provision PAC, or Provision PAC Anonymously.</td>
</tr>
<tr>
<td></td>
<td>On the Authentication Tab:</td>
</tr>
<tr>
<td></td>
<td>• Username Template — Specify if users are required to enter only their user name or domain\user name.</td>
</tr>
<tr>
<td></td>
<td>• Use Per Connection Password — Select if you want to use a per-connection password.</td>
</tr>
<tr>
<td></td>
<td>• Identity Certificate — Select a certificate.</td>
</tr>
<tr>
<td></td>
<td>You can modify the list of available identity (device) certificates in Policies</td>
</tr>
<tr>
<td></td>
<td>On the Trust Tab:</td>
</tr>
<tr>
<td></td>
<td>• Use the Add or Delete buttons to indicate which certificates devices should trust and automatically connect to.</td>
</tr>
<tr>
<td></td>
<td>You can modify the list of available trusted certificates in Policies</td>
</tr>
<tr>
<td></td>
<td>• Allow Trust Exceptions — Select to allow trust decisions to be made by the user.</td>
</tr>
</tbody>
</table>

See also

*Enrollment Agents for PKI environments* on page 23

*Change certificate settings* on page 54

**Change certificate settings**

Add a certificate from a certificate authority if you are operating in a PKI environment and want to set up Wi-Fi or VPN profiles with certificate authentication.

**Before you begin**

Make sure an Enrollment Agent is configured in System Settings | Enrollment Agents.

**Task**

1. Click Policies, select the policy to be changed, then select the Certificates tab.
2. Click Add.
3 On the Add Certificate Configuration screen, complete the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Name</td>
<td>Name of the certificate configuration.</td>
</tr>
<tr>
<td>Enrollment Agent</td>
<td>Select the Enrollment Agent.</td>
</tr>
<tr>
<td>Certificate Template</td>
<td>Certificate template to request a certificate from the certificate authority.</td>
</tr>
<tr>
<td>Subject Template</td>
<td>Template for the subject name, for example E=${EmailAddress}, CN=${Username}, CN=${Domain}, O=QA. Acceptable values are: • User-related — Username, Domain, EmailAddress. • Device-related — SerialNumber, DeviceID, PhoneNumber, IMEI, UDID, DeviceModel, DevicePlatform, DeviceOSVersion, DeviceCarrier, DeviceWiFiMac.</td>
</tr>
<tr>
<td>Key Size</td>
<td>Select a key size.</td>
</tr>
<tr>
<td>Use as Digital Signature</td>
<td>Select to use as a digital signature.</td>
</tr>
<tr>
<td>Use for Key Encipherment</td>
<td>Select to use for key encipherment.</td>
</tr>
<tr>
<td>Additional OIDs</td>
<td>If necessary, click Add to enter a new OID or Delete to remove an OID from the list.</td>
</tr>
</tbody>
</table>

4 Verify the connection to the certificate authority by doing the following:
   a Click Verify Connection.
   b On the Verify Connection screen, complete the fields, then click Verify Connection.
   c Click OK to return to the Verify Connection screen, then click Cancel to return to the Add Certificate Configuration screen.

5 Click Save.

See also
Enrollment Agents for PKI environments on page 23

Change APN settings
iOS devices may use an APN to connect to a specific mobile network.

Task
1 Click Policies, select the policy to be changed, then select the APN tab.
2 Select Use custom carrier Access Point Network Name (APN).
3 Complete the fields, then click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the APN.</td>
</tr>
<tr>
<td>Username</td>
<td>User name to log on to the APN.</td>
</tr>
<tr>
<td>Password</td>
<td>Password to access the APN.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Proxy server of the APN.</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>Port of the proxy server.</td>
</tr>
</tbody>
</table>
**Change blacklist settings**

Blacklisted apps prevent users from syncing mail to their device by marking the device non-compliant. Users receive a notification identifying any blacklisted apps installed on their device with instructions on how to remove the apps. After removal, users can refresh their device by opening the McAfee EMM app, clicking Blacklisted Apps, and refreshing the list. The device returns to compliance and starts syncing within ten minutes.

It can take up to 24 hours for a device with a blacklisted app to stop syncing. This timeframe depends on when the blacklisted app was installed and when the last device query occurred.

**Task**

1. Click Policies, select the policy to be changed, then select the Blacklisting Applications tab.
2. Select Enable Blacklisting Applications, then click Add.
3. On the Add Application screen, do one of the following:
   - To manually enter an application, under Source, leave Manually Define Application selected. Enter the application name or bundle identifier/package name. Click Save.
   
   You can use a wildcard (*) at the beginning or end of your search term; however, doing so will reduce the number of compliance incidents and increase the load on the McAfee EMM Hub and Database.
   
   • To search for an application currently installed on user devices as shown in the Helpdesk, under Source, select Search Applications. Enter the name of an application in the Search field, select the application, then click Save. On the Add Application screen, verify the information, then click Save.
4. Click Save.

**See also**

*Find package names for Android on page 67*
*Find bundle identifiers for iOS on page 67*

---

**Publish policies**

After you’ve created a new policy or modified policy settings, you must publish the policy. Publishing a policy pushes it to the devices on your network at their next device check-in.

**Task**

1. Click Policies, then select the policy you want to publish.
   
   If you’ve changed a policy but not yet published it, a red exclamation mark appears next to the policy name in the policy list.
   
   2. Click the publish icon for the policy:
      
      ![Publish icon]
   
   3. Click OK to confirm that you want to publish the policy.
      
      You can also publish policies from any of the policy settings tabs by clicking the Publish icon at the bottom of the policy window.
Delete policies

You can delete a policy when it is no longer needed. When a policy is deleted, all users associated with that policy will be assigned to the Starter Policy, which is the default. You can't delete the default policy.

**Task**

1. Click Policies, then select the policy to be deleted.
2. At the top right of the Policy window, click the red X to delete the policy.
3. Click **OK** to confirm deletion.
Packages

Packages allow you to distribute and install corporate applications without having physical access to user devices. Packages can be created for iOS, Android, and Windows Mobile devices, and can be pushed to devices based on users or groups.

Each package can only be sent to one operating system. For Windows Mobile devices, applications must be in the installable .CAB format.

Contents
- Create a new package
- Change a package
- Assign and push a package to users
- Delete a package
- Download recommended apps to a device

Create a new package

You can create packages for Android, iOS, Windows Mobile PPC (for Windows Mobile Pocket), or Windows Mobile SP (for Windows Mobile Smartphone). The McAfee EMM system provides three packages that you can use and rename, or you can create a new package.

Task
1. Click Packages | Create New.
2. On the Create Package screen, select the platform, provide a name for your package, then click Save.
   - If you select a Windows Mobile platform, you can require a reboot after the package files are installed. Select Requires Reset.

Change a package

After creating a package, you can add and remove files from it and change the installation order of the files.

For iOS packages, click Push Web Clips on the Applications & Files tab to update assigned iOS devices with web clips immediately. This can also be helpful if a user doesn't see a particular web clip on their device, or if they accidentally deleted it.
**Tasks**

- **Add files to a package** on page 60
  The types of files you can add to packages depends on the mobile device platform.

- **Remove files from a package** on page 61
  Remove files from a package if you no longer want to distribute them to mobile devices.

- **Reorder files in a Windows Mobile package** on page 61
  If you want to change the order that files are installed on Windows Mobile devices, you can do so by reordering the files in the package.

**Add files to a package**
The types of files you can add to packages depends on the mobile device platform.

**Task**
1. Click **Packages**, then select a package from the list at right.
2. Click **Add**.
3. On the **Add File** screen, complete the fields, then click **Add**.

<table>
<thead>
<tr>
<th>For mobile device platform...</th>
<th>Select a file type...</th>
<th>Complete these fields...</th>
</tr>
</thead>
</table>
| iOS                          | Mobile Config         | - File Name — Select the mobilconfig file.  
- Version — File version.  
- Notes — Optional description. |
| Enterprise Application       |                       | - IPA Path — Select the application file.  
- Icon Path — Select an optional icon. |
| App Store Application        |                       | - Application Name — Name of the App Store app.  
- Application Link — Link to the App Store app.  
- Icon Path — Select an optional icon. |
| Web Clip                     |                       | - Display Name — Name that will appear for the web clip.  
- URL — URL of the website.  
- Icon Path — Select an icon.  
- Allow Removal — Enable or disable the user option to remove the web clip.  
- Use Full Screen — Enable or disable the web clip from using the full display screen. |
| Android                      | Marketplace Application | - Application Name — Name of the Marketplace app.  
- Application Link — Link to the Marketplace app.  
- Icon Path — Select an optional icon. |
<table>
<thead>
<tr>
<th>For mobile device platform...</th>
<th>Select a file type...</th>
<th>Complete these fields...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Application</td>
<td><strong>Application Name</strong> — Name of the Marketplace app.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Version</strong> — File version.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>APK Path</strong> — Select the application file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Icon Path</strong> — Select an optional icon.</td>
<td></td>
</tr>
<tr>
<td>Windows Mobile</td>
<td><strong>File Name</strong> — Select the file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Notes</strong> — Optional description.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Silent Install</strong> — Select to install files in the background without notifying the user. If the file requires a user prompt to install, don’t select this option.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Supported Platforms</strong> — Platforms for the file.</td>
<td></td>
</tr>
</tbody>
</table>

When you add a MobileConfig, Enterprise App, or App Store Application, the McAfee EMM app on the device shows the files in the **Recommended Apps** section. When you add a Web Clip, it is installed when the device provisions or receives a policy update.

**Remove files from a package**

Remove files from a package if you no longer want to distribute them to mobile devices.

**Task**

1. Click Packages, then select a package from the list at right.
2. Click the Applications & Files tab, then select the file to be removed.
3. Click Remove.
4. Click Save.

**Reorder files in a Windows Mobile package**

If you want to change the order that files are installed on Windows Mobile devices, you can do so by reordering the files in the package.

**Task**

1. Click Packages, then select a package from the list at right.
2. Click the Applications & Files tab, then click Reorder.
3. On the Reorder Files screen, click the green arrows to set the installation order of the files.
4. Click Save.
Assign and push a package to users

Specify which users or groups receive a package.

**Task**
1. Click **Packages**, then select a package from the list at right.
2. Select 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 Web Clips**.
   - For Windows Mobile PPC and SP packages, click **Push to Devices**.

Delete a package

You can delete a package if there are no pending actions on any device assigned to the package.

**Task**
1. Click **Packages**, then select a package from the list at right.
2. At the lower left of the main screen, click **Remove**.

Download recommended apps to a device

Files assigned to iOS and Android devices appear in the **Recommended Apps** section of the McAfee app. Users must click to download the applications or files.

**Task**
1. From the McAfee EMM app, click **Recommended Apps**.
2. Select the application or file to install.
Monitoring network activity

Monitor the activity of mobile devices on your network using built-in reports.
Monitoring network activity
Reports

Reports help you track activity on your network and user devices. Reports are generated in real-time and are not cached.

Contents

- View reports
- Export reports
- Types of reports

View reports

Viewing reports in the Console provides real-time information about your network.

Task

1. Click Reports.
2. Select the report you want to view from the list at right.

Export reports

You can export any McAfee EMM report into Microsoft Excel format.

Task

1. Click Reports, then select the report to be exported.
2. Click Export.
3. When prompted, save or open the report.

Types of reports

These are the default reports available in McAfee EMM. You can't create additional reports.

<table>
<thead>
<tr>
<th>Report</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Log</td>
<td>The Audit Log report provides an audit trail of actions initiated by all Console users. It lists events such as logons, policy changes, and device updates. Only the system administrator can view the Audit Log.</td>
</tr>
<tr>
<td>Compliance Status</td>
<td>The Compliance Status report shows all registered mobile devices and information on whether those devices are compliant or noncompliant. You can view all users, compliant users, or noncompliant users by selecting an option from the filter drop-down menu.</td>
</tr>
</tbody>
</table>
### Reports

#### Types of reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Deployment</td>
<td>The Package Deployment report shows the status of packages being pushed to devices. You can view which packages are downloading, pending, acknowledged, or downloaded.</td>
</tr>
<tr>
<td>Pending Actions</td>
<td>The Pending Actions report lists outstanding actions for devices. Pending actions include package updates, delete commands, uninstall commands, and wipe commands. This report shows which devices did or didn't receive commands.</td>
</tr>
<tr>
<td>Registered Users</td>
<td>The Registered Users report lists all users that have provisioned mobile devices.</td>
</tr>
<tr>
<td>Software Status</td>
<td>The Software Status report lists each mobile device and its version of PDA Secure, Download Manager, and the security policy. The McAfee EMM app for iOS devices isn't shown on this report.</td>
</tr>
<tr>
<td>Unregistered Devices</td>
<td>The Unregistered Devices report lists noncompliant devices that attempt to sync to the ActiveSync server. If compliance enforcement is enabled, noncompliant devices are blocked from getting email.</td>
</tr>
</tbody>
</table>
Finding bundle identifiers (iOS) and package names (Android)

Using bundle identifiers or package names to blacklist mobile applications improves the accuracy of your blacklist. Bundle identifier for iOS and package name for Android are unique strings identifying an application, for example com.mcafee.apss.emmagent.

Contents
- Find package names for Android
- Find bundle identifiers for iOS

Find package names for Android
Package names are shown in the URL of the application page on the Android Marketplace.

Task
2. Locate the application you want to blacklist.
3. Click the application.
   The package name is shown in the URL between "id=" and "&feature".

Find bundle identifiers for iOS
Bundle identifiers for iOS are embedded in the application metadata. You must download the application in order to find the ID.

Task
1. Open iTunes and locate the application you want to block.
2. Download the application and use a file explorer in your operating system to locate the application's .ipa file.
3. Change the extension of the .ipa file to .zip.
4. Inside the archive, locate the file Payload\{appname}.app\Info.plist.
5. Open the .plist file using a text editor.
   The bundle identifier appears in the file preceded by a "com." prefix.
Finding bundle identifiers (iOS) and package names (Android)
Find bundle identifiers for iOS
Policy settings for mobile devices

These are the current and legacy policy settings for all device types.

**Current policy settings**

These are the current policy settings available in the Console for all supported device types.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Feature or setting</th>
<th>Description</th>
<th>Valid Options/Formats</th>
<th>iOS</th>
<th>Android</th>
<th>Windows Phone 7</th>
<th>Windows Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security: Authentication Management</td>
<td>User password for logon</td>
<td>User password required when logging on to the device.</td>
<td>Must satisfy the password strength requirements</td>
<td>X</td>
<td>X</td>
<td>X (except Exchange 2003)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Admin password</td>
<td>Admin password applied to Windows Mobile and iOS devices provisioned using SCEP only (non-MDM profile). WM: Used to uninstall software. iOS: Used to remove SCEP profile from device.</td>
<td>10 characters</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Password length</td>
<td>Minimum length in characters of the power-on passwords.</td>
<td>1 to 15</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Password expiration</td>
<td>Password age on the device</td>
<td>ON, OFF, VALUE</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X (versions 3.0 and later)</td>
</tr>
<tr>
<td></td>
<td>Require alphanumeric password</td>
<td>Composition of password</td>
<td>ON, OFF, VALUE</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Password history</td>
<td>Previous user password restriction.</td>
<td>ON, OFF, VALUE</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Functionality</td>
<td>Feature or setting</td>
<td>Description</td>
<td>Valid Options/Formats</td>
<td>iOS</td>
<td>Android</td>
<td>Windows Phone 7</td>
<td>Windows Mobile</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------</td>
<td>-------------</td>
<td>-----------------------</td>
<td>-----</td>
<td>----------</td>
<td>------------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>Password delay/ inactivity timer</td>
<td>Timeout for password inactivity on the device.</td>
<td>ON, OFF, VALUE</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Password failure action</td>
<td>Incorrect password attempts. Wipes the device when it reaches the limit. Wiping the device will return it to factory defaults.</td>
<td>ON, OFF, VALUE</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Allow simple password</td>
<td>User password may be a four-digit number.</td>
<td>ON, OFF</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Block iTunes Explicit Content</td>
<td>Restricts explicit content on iTunes.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Block YouTube</td>
<td>Restricts YouTube.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Block iTunes</td>
<td>Restricts iTunes.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Block Camera</td>
<td>Restricts camera on the device.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Allow FaceTime</td>
<td>Allows FaceTime if the camera is not restricted.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Block Screen Capture</td>
<td>Restricts screen captures on the device.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Block Automatic Sync While Roaming</td>
<td>Restricts the device from syncing when roaming.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Block In-App Purchases</td>
<td>Restricts In-App purchases.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Block Multiplayer Gaming</td>
<td>Restricts the user from multiplayer gaming.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Block Voice Dialing</td>
<td>Restricts voice dialing capabilities.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functionality</td>
<td>Feature or setting</td>
<td>Description</td>
<td>Valid Options/Formats</td>
<td>iOS</td>
<td>Android</td>
<td>Windows Phone 7</td>
<td>Windows Mobile</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>-----</td>
<td>----------</td>
<td>------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Block Installing Non-Enterprise Applications</td>
<td></td>
<td>Restricts non-enterprise applications from being installed.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Safari</td>
<td></td>
<td>Restricts Safari browser.</td>
<td>ON, OFF</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Block Beam/IR</td>
<td></td>
<td>Restricts IR resources on the device.</td>
<td>ON, OFF</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Block Desktop Sync</td>
<td></td>
<td>Disables Desktop ActiveSync. OTA Exchange ActiveSync remains enabled.</td>
<td>ON, OFF</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Block Wi-Fi</td>
<td></td>
<td>Restricts Wi-Fi on the device.</td>
<td>ON, OFF</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Block Storage Card</td>
<td></td>
<td>Restricts SD card on the device.</td>
<td>ON, OFF</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Block SMS/MMS/Text Messaging</td>
<td></td>
<td>Restricts SMS/ MMS/text messaging on the device.</td>
<td>ON, OFF</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Block Bluetooth</td>
<td></td>
<td>Restricts Bluetooth completely on the device.</td>
<td>ON, OFF, AUDIO, FILE TRANSFER</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Allow Hands Free</td>
<td></td>
<td>Allows Bluetooth hands-free.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Force iTunes Store Password Entry</td>
<td></td>
<td>Requires user to enter their iTunes password for all purchases.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Cloud Backup</td>
<td></td>
<td>Restricts backup to the Apple cloud service.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Cloud Document Sync</td>
<td></td>
<td>Restricts uploading documents to the Apple cloud service.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functionality</td>
<td>Feature or setting</td>
<td>Description</td>
<td>Valid Options/Formats</td>
<td>iOS</td>
<td>Android</td>
<td>Windows Phone 7</td>
<td>Windows Mobile</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>-----</td>
<td>----------</td>
<td>------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Block Cloud Key-Value Sync</td>
<td>Restricts syncing app configuration to the Apple cloud service.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Photo Stream</td>
<td>Restricts syncing photos to other devices associated with the user's Apple ID.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Untrusted TLS Certificate Prompt</td>
<td>Restricts user from accessing email or websites with untrusted SSL certificates.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Siri (Voice Assistant)</td>
<td>Restricts Siri.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Diagnostic Data From Being Sent</td>
<td>Restricts diagnostic data from being sent to Apple.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Sending Corporate Email Via Other Email Accounts</td>
<td>Restricts sending enterprise emails from other accounts provisioned on the device.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Third Party Applications From Using Corporate Email</td>
<td>Restricts applications from accessing enterprise email.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control Roaming</td>
<td>Restricts roaming outside the mobile network with options to restrict data or voice roaming specifically.</td>
<td>ON, OFF</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management: Centralized Administration</td>
<td>Enterprise visibility</td>
<td>All mobile devices in the enterprise viewable in a single console.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>EMM Portal</td>
<td>End-user portal for provisioning and wipe.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Functionality</td>
<td>Feature or setting</td>
<td>Description</td>
<td>Valid Options/Formats</td>
<td>iOS</td>
<td>Android</td>
<td>Windows Phone 7</td>
<td>Windows Mobile</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>-----</td>
<td>----------</td>
<td>------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Secure Container</td>
<td>Optional app for Android that sandboxes enterprise email, contacts,</td>
<td>X</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy management</td>
<td>One place to create and manage policies for all devices; platform agnostic policies; LDAP group-based associations.</td>
<td>X</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>User authorization</td>
<td>Choice of user authorization methods, including bulk and manual authorization, and authorization based on LDAP groups or a CSV list.</td>
<td>X</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Software distribution</td>
<td>OTA distribution of apps; group-based.</td>
<td>X</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Helpdesk</td>
<td>Unified Helpdesk for common tasks like wipe, delete Email and PIM data, uninstall (remove configuration profile).</td>
<td>X</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Reports</td>
<td>Status of policies, packages, devices, and users.</td>
<td>X</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-based console</td>
<td>Server access from anywhere.</td>
<td>X</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role-based access control</td>
<td>Levels of access; can be tied to AD and Domino groups.</td>
<td>X</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functionality</td>
<td>Feature or setting</td>
<td>Description</td>
<td>Valid Options/ Formats</td>
<td>iOS</td>
<td>Android</td>
<td>Windows Phone 7</td>
<td>Windows Mobile</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>-----</td>
<td>----------</td>
<td>------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Compliance enforcement</td>
<td>Monitoring of device health and network access based on status.</td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blacklisting of mobile apps</td>
<td>Prevents users from syncing their device if blacklisted apps are installed.</td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wipe (full)</td>
<td>Hard reset of the device. Removes McAfee EMM software, all data, and all applications and returns device to factory settings.</td>
<td>X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wipe (selective)</td>
<td>Email and PIM data removal. (with Secure Container)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legacy policy settings for Windows Mobile devices**

These are the legacy policy settings for Windows Mobile devices that are no longer available in the Console. These settings can't be changed in the Console in McAfee EMM 9.6 or later. Changes made to these settings before upgrading will be carried over, but they can't be edited once you upgrade to version 9.6 or later.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Feature or setting</th>
<th>Description</th>
<th>Valid Options/ Formats</th>
<th>Pre-Defined Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security: Authentication Management</td>
<td>Logon monitor</td>
<td>Log on monitor where the device is wiped if not logged on x number of days.</td>
<td>ON, OFF, VALUE</td>
<td>30</td>
</tr>
<tr>
<td>Security: Encryption Management</td>
<td>Encryption method</td>
<td>Encryption algorithm used to encrypt data on the device.</td>
<td>AES 256</td>
<td>AES 192</td>
</tr>
<tr>
<td>SD card encryption</td>
<td>Encryption of data on SD cards.</td>
<td>ON, OFF</td>
<td>OFF</td>
<td></td>
</tr>
<tr>
<td>Internal memory encryption</td>
<td>Rules on what files and folders are encrypted.</td>
<td>ON, OFF</td>
<td>ON</td>
<td></td>
</tr>
<tr>
<td>Security: Resource Management</td>
<td>Restrict GPRS</td>
<td>Restrict GPRS on the device.</td>
<td>ON, OFF</td>
<td>OFF</td>
</tr>
<tr>
<td>Restrict serial USB</td>
<td>Restrict Serial USB on the device.</td>
<td>ON, OFF</td>
<td>OFF</td>
<td></td>
</tr>
</tbody>
</table>
Index

A
about this guide 7
access roles, See administrative accounts
ActiveSync
    Protocol, authorizing users based on 30
    Proxy, description 11
administrative accounts
    about 18
    creating 18, 19
    defaults 17
    deleting 19
    permissions 17
administrators
    Helpdesk 17
    policy 17
Android devices, See devices
APN, policy settings 55
apps
    Android package names 67
    blacklist 56
    downloading to a user device 62
    iOS bundle identifiers 67
audit log, report 65
authentication
    servers 27
    users 28
authorization directories
    about 27
    adding or editing 27
    deleting 28
authorized users
    adding 28–30
    deleting 32

B
Beam/IR, restricting 49
BES Agent
    description 11
    viewing 24
blacklist
    locating bundle identifiers for iOS 67
    locating package names for Android 67
    policy settings 56

C
Bluetooth, restricting 49
browser, restricting 49
bundle identifier, locating for iOS 67
camera, restricting 49
catalog, device 23
cloud backup, restricting 49
corporate devices, See ownership, devices
compliance
    about 21
    enabling or disabling 22
    Filter, description 11
    overriding 40
    policy settings 47
    status report 65
components
    client-side 12
    server-side 11
Console
    about 13
    deleting devices from 41
    description 11
    initial log on 17
    launching 17
    navigating 13
conventions and icons used in this guide 7
corporate devices, See ownership, devices
CSV
    authorizing users based on 30
    formatting 31

D
device compliance
    about 21
    enabling or disabling 22
    overriding 40
devices
    catalog 23
deleting email and PIM data (iOS only) 36
details 35
downloading applications 62
locking and unlocking 37, 38
Index

devices (continued)
  ownership, See ownership, devices
  registration 21
  response to policy updates 44
  unregistered, report of 65
  viewing pending actions 39
  wiping 36
DMG, description 11
documentation
  audience for this guide 7
  product-specific, finding 8
  typographical conventions and icons 7
Download Manager
description 12
status report 65

E
e-mail
  corporate, restricting access 49
  deleting from a device (iOS only) 36
  policy settings 48
EMM app
description 12
  downloading recommended apps 62
EMM Portal
  accessing 17
  description 11
EMM profile, uninstalling from a device 36
encryption, device
  blocking users based on 47
  determining compliance 21
  status 35
Enrollment Agent
  about 23
  deleting 24
  editing 24

F
FaceTime, restricting 49
features, overview 9

H
Helpdesk
  about 35
  administrator 17
  default view 35
  functions 13
  tabs 35
  wiping devices using 36
Hub, description 11

I
iCloud, restricting 49
In App, restricting 49
iOS devices, See devices
iPad, See devices
iPhone, See devices
iPod, See devices
iTunes, restricting 49

L
LDAP groups
  authorizing administrators based on 18
  authorizing users based on 29, 30
  basing policies on 43
licenses 21

M
McAfee ServicePortal, accessing 8
MDM
  updating certificate 23
  viewing pending actions 39
multiplayer games, restricting 49

O
ownership, device
  basing policies on 43
  changing 46

P
package name, locating for Android 67
packages
  about 59
  adding files to 60
  assigning users or groups to 62
  creating 59
  deleting 62
  deployment report 65
  modifying 59
  removing files from 61
  reordering files in 61
  screen, functions 13
passwords
  policy settings 49
  resetting on user devices 38
PDA Secure, description 12
pending actions
  report 65
  viewing 39
permissions 17
personal devices, See ownership, devices
Photo Stream, restricting 49
PIM data 36
PKI
  Agent, description 11
  environment, Enrollment Agents for 23
Index

policies about 43
administrator 17
assigning membership 46
best practices 45
creating 45
default 43
deleting 57
membership 43
prioritization 43
publishing 44, 56
reordering 46
screen, functions 13

policy settings about 47
APN 55
blacklist 56
certificates 54
compliance 47
current 69
default 43
deleting 57
email 48
legacy 69
passwords 49
restrictions 49
Secure Container 51
VPN 51
Wi-Fi 53
portal certificate, updating 23
prioritization, policies 43
provisioning tokens
creating 32
updating 39
Proxy, configuring for email 48
push certificate, updating 23
Push Notifier
description 11
viewing 25

R
registered users, report 65
reports
about 65
defaults 65
exporting 65
screen, functions 13
viewing 17, 65
restrictions, policy settings 49
roaming, restricting 49

S
screen capture, restricting 49
Secure Container
Android policy settings 51
Secure Container (continued)
description 12
iOS policy settings 49
security certificates
policy settings 54
updating 23
serial number 21
ServicePortal, finding product documentation 8
Siri, restricting 49
SMS, See text messages
SMTP server, specifying 22
software status, report 65
starter policy 43
storage card, restricting 49
sync, restricting 49
system settings screen, functions 13

T
Technical Support, finding product information 8
temporary passwords, See provisioning tokens
text messages
configuring server for 22
restricting 49
sending to users 40
tokens, See provisioning tokens

U
uninstall, EMM profile 36
untrusted websites, restricting access to 49
use agreement 21
user authorization
about 27, 28
based on ActiveSync Protocol 30
based on LDAP groups 29, 30
bulk 30
manual 30
user devices, See devices
user notifications screen, functions 13

V
voice dial, restricting 49
VPN
authentication data 52
policy settings 51

W
Wi-Fi
policy settings 53
restricting 49

Y
YouTube, restricting 49