



Installation Guide

McAfee Enterprise Mobility Management 11.0 Software

For use with ePolicy Orchestrator 4.6.5-5.0 Software

COPYRIGHT

Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS

McAfee, the McAfee logo, McAfee Active Protection, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure 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.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

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	5
About this guide	5
Audience	5
Conventions	5
Find product documentation	6
1 Planning your installation	7
McAfee EMM components	7
Server components	7
Client components	8
Configuration modes	8
Enhanced security configuration (dual servers)	8
Basic security configuration (single server)	8
Installation requirements	9
System requirements	9
Certificate requirements	11
Network requirements	11
2 Installing McAfee EMM	13
Install the McAfee EMM extension in ePolicy Orchestrator	13
Run the Deployment Helper	13
Run the Deployment Helper for enhanced security configurations	14
Run the Deployment Helper for basic security configurations	15
Install McAfee EMM server components	15
Install server components in enhanced security configuration	16
Install server components in basic security configuration	16
Add McAfee EMM as a registered server in ePolicy Orchestrator	17
3 Upgrading McAfee EMM	19
Install the McAfee EMM extension in ePolicy Orchestrator	19
Upgrade McAfee EMM server components	20
Upgrade for enhanced security configurations and High Availability environments	20
Upgrade for basic security configurations	20
Add McAfee EMM as a registered server in ePolicy Orchestrator	21
A Settings for components	23
Database settings	23
LDAP server settings	24
Hub server settings	24
Portal certificate settings	24
MDM certificate settings	25
Communication settings	26
ActiveSync server settings	27
DMZ settings	27

B	Specialized installation tasks	29
	Back up an existing installation	29
	Install McAfee EMM in High Availability environments	29
	Uninstall McAfee EMM	30
C	Troubleshooting	31
	Index	33

Preface

Contents

- ▶ *About this guide*
- ▶ *Find product documentation*

About this guide

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

Audience





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

The information in this guide is intended primarily for:

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

Conventions

This guide uses these typographical conventions and icons.

<i>Book title, term, emphasis</i>	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
User input, code, message	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

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

Task

- 1 Go to the McAfee Technical Support ServicePortal at <http://mysupport.mcafee.com>.
- 2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	<ol style="list-style-type: none">1 Click Product Documentation.2 Select a product, then select a version.3 Select a product document.
KnowledgeBase	<ul style="list-style-type: none">• Click Search the KnowledgeBase for answers to your product questions.• Click Browse the KnowledgeBase for articles listed by product and version.

1

Planning your installation

Before installing McAfee® Enterprise Mobility Management (McAfee EMM™) for McAfee® ePolicy Orchestrator®, learn about the software components, decide on a configuration model, and verify that your system meets minimum requirements.

Contents

- ▶ *McAfee EMM components*
- ▶ *Configuration modes*
- ▶ *Installation requirements*

McAfee EMM components

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

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

Server components

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

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

Client components

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

McAfee EMM client component	Description
McAfee EMM app	Free app for iOS or Android that enables easy configuration by the user, and allows push notifications to deliver profile and security policy changes.
McAfee® Secure Container app (Android devices)	Free app that encrypts, passcode-secures, and segregates enterprise email, contacts, and calendars.

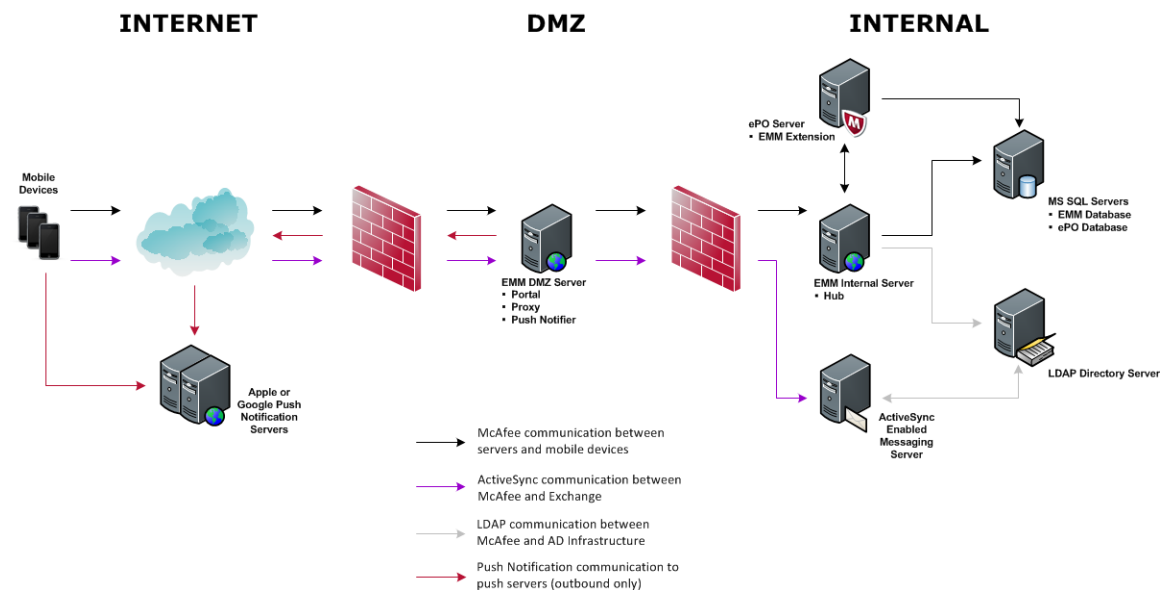
Configuration modes

Your McAfee EMM configuration depends on the unique needs of your environment.

Enhanced security configuration (dual servers)

McAfee recommends enhanced security configuration for most McAfee EMM installations. This configuration provides maximum security and verifies web traffic before it enters your private network. The enhanced security configuration installs McAfee EMM on two servers. The McAfee EMM Portal, Proxy, and Push Notifier are installed on an Internet-facing IIS server in the DMZ. The McAfee EMM Hub is installed in the internal subnet.

The ePolicy Orchestrator user interface provides access to all administrative functions for McAfee EMM.

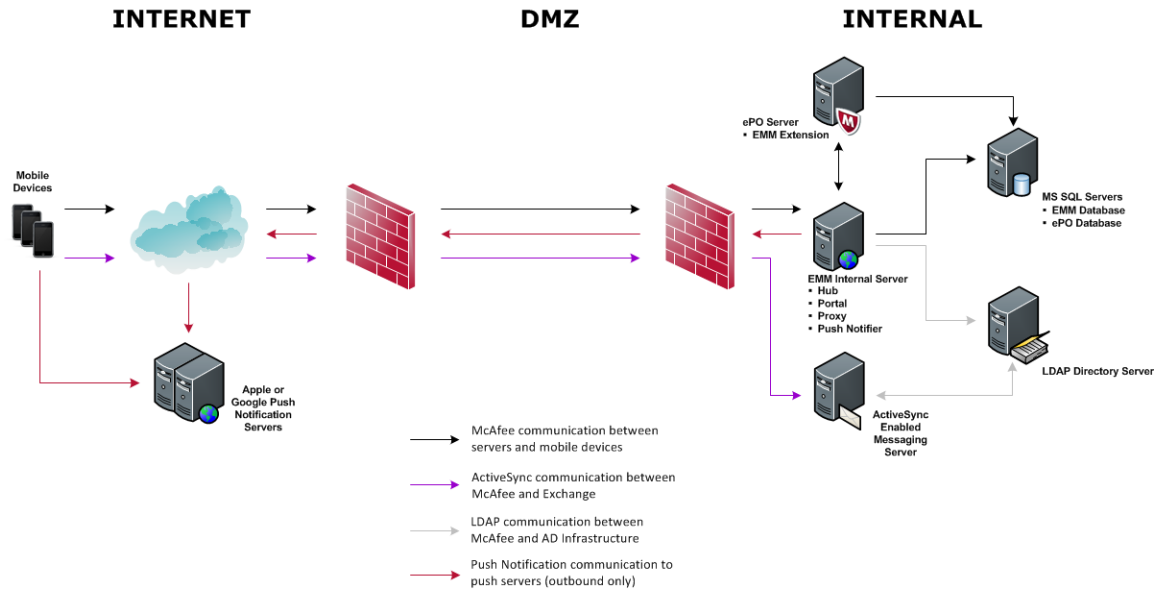


Basic security configuration (single server)

The basic security configuration is appropriate for smaller organizations without complex security requirements, or for trial installations.

The basic security configuration installs all McAfee EMM server components on a single server located in the internal subnet.

The ePolicy Orchestrator user interface provides access to all administrative functions for McAfee EMM.



Installation requirements

McAfee EMM has specific system, certificate, and network requirements for installation and operation.

McAfee EMM 11.0 supports these mobile operating systems:

- iOS version 4.3 and later
- Android version 2.2 and later
- Windows Phone 7 and Windows Phone 8

System requirements



Before installing McAfee EMM, verify that your system meets these minimum operating requirements.

These are the requirements for the McAfee EMM server components. For details on ePolicy Orchestrator requirements, see the ePolicy Orchestrator documentation.



The account used to install McAfee EMM must be a local administrator account that has permission to create a database on the SQL Server.

Component	Requirement
Software	ePolicy Orchestrator 4.6.5 or later
Hardware (physical or virtual)	<ul style="list-style-type: none"> • 4 GB RAM • Dual Core CPU
Operating system	<ul style="list-style-type: none"> • Windows Server 2008 64-bit with Service Pack 2 (Standard or Enterprise Edition) • Windows Server 2008 R2 64-bit with Service Pack 1 (Standard or Enterprise Edition)

Component	Requirement
SQL Server	<ul style="list-style-type: none"> • 2005 with Service Pack 3 or later (Enterprise, Standard, or Workgroup Edition) • 2008 R2 32- and 64-bit with Service Pack 1 or later (Enterprise, Standard, or Workgroup Edition) <p>Configuration and limitations:</p> <ul style="list-style-type: none"> • Database collation must be configured to the U.S. English default: SQL_Latin1_General_Cp1_CI_AS. • SQL Express is appropriate only for <i>trial installations</i>, with a single, on-premise server used in non-production environments.
ActiveSync server	Microsoft Exchange ActiveSync 2.5 or later
Mail server	<ul style="list-style-type: none"> • Exchange 2003, 2007, or 2010 • Domino 8.5.1 or 8.5.2 <p> Other mail servers may work, but aren't tested for use with Exchange ActiveSync.</p>
Internet browsers	<ul style="list-style-type: none"> • Internet Explorer 8.0 or later • Firefox 10.0 or later • Chrome 17 or later <p> To access certain McAfee EMM features, Microsoft Silverlight 3.0 or later must be installed on the browser and pop-ups must be allowed for your ePolicy Orchestrator site.</p>

Supported languages

McAfee EMM software runs on any supported operating system regardless of the OS language.

The McAfee EMM user interface has been translated into the languages shown here. Language support varies by ePolicy Orchestrator version. When the software is installed on an operating system using a language that is not on this list, the interface attempts to display text in English.

ePolicy Orchestrator 4.6.5

Chinese (Simplified)
 Chinese (Traditional)
 English
 French
 German
 Japanese
 Korean
 Russian
 Spanish

ePolicy Orchestrator 5.0 and later


Chinese (Simplified) Japanese
 Chinese (Traditional) Korean
 Danish Norwegian
 Dutch Portuguese (Brazilian)
 English Portuguese (Iberian)
 Finnish Russian
 French Spanish
 German Swedish
 Italian Turkish

Certificate requirements

Before installing McAfee EMM, understand and verify these credentials. The McAfee EMM Deployment Helper walks you through obtaining portal, Mobile Device Management (MDM), and iOS Agent Push Notification certificates.



Retain a copy of your portal and MDM certificates and passwords in a secure location in case you need to restore them later.

Credential	Used for	Used by	Expiration	Notes
Portal certificate	Mobile device verification and secure communication between the McAfee EMM server and client components.	McAfee EMM Portal Windows IIS	Varies. Obtain updates from your certificate authority.	Must be a public certificate (not self-signed) obtained from a recognized certificate authority like Verisign or Go Daddy. Must match the address (A) record defined in the Domain Name System (DNS) unless a wildcard (*) certificate is used.
MDM certificate	Communication with Apple push notification services.	McAfee EMM Push Notifier	Annually. Obtain updates from Apple. See KB73382 for details.	<div style="border: 1px solid gray; padding: 5px; background-color: #f0f0f0;">  Update MDM certificates before they expire to avoid reconfiguring all iOS devices on your network. </div>
iOS Agent Push Notification certificate	Communication with Apple push notification services.	McAfee EMM Push Notifier	Annually. Obtain updates by visiting the McAfee Downloads site and entering a valid McAfee EMM grant number.	Installed automatically with McAfee EMM.
Google Cloud Messaging (GCM) account credentials	Communication with Google push notification services.	McAfee EMM Push Notifier	Does not expire unless you generate a new token using the same Sender ID.	


Network requirements

Before installing McAfee EMM, verify that your network meets these requirements.

Publicly registered domain

You have a valid URL to access the McAfee EMM Portal and Proxy.

Router and firewall access rules

Configuration	Allow traffic on this port	From	To
Enhanced security configuration (dual servers)	443	Internet	McAfee EMM DMZ server
	443	McAfee EMM DMZ server	Email servers providing ActiveSync or Notes Traveler
	443	McAfee EMM DMZ server	McAfee EMM internal server
	389	McAfee EMM internal server	LDAP server
	88	McAfee EMM internal server	LDAP server
	1433 (or dynamic SQL port)	McAfee EMM internal server	SQL Server where the McAfee EMM database is installed
	25	McAfee EMM internal server	SMTP server
Basic security configuration (single server)	443	Internet	McAfee EMM server
	443	McAfee EMM server	Email servers providing ActiveSync or Notes Traveler
	389	McAfee EMM server	LDAP server
	88	McAfee EMM internal server	LDAP server
	1433 (or dynamic SQL port)	McAfee EMM server	SQL Server where the McAfee EMM database is installed
	25	McAfee EMM internal server	SMTP server
iOS devices	2195	McAfee EMM server (DMZ in enhanced security mode)	Apple Push Notification service at gateway.push.apple.com
	2196	McAfee EMM server (DMZ in enhanced security mode)	Apple Push Notification service at feedback.push.apple.com
	5223	Devices connected to Wi-Fi	Internet
		For specific port and configuration details for iOS devices in a business environment, see the Apple guide to iPhone and iPad in Business .	
Android devices	443	McAfee EMM server (DMZ in enhanced security mode)	Google Cloud Messaging service at android.googleapis.com
	5228	Devices connected to Wi-Fi	Internet



For outbound connections to Apple and Google push services, don't set IP-specific firewall restrictions because the IP addresses are subject to change.

2

Installing McAfee EMM

To install McAfee EMM, complete these tasks in order.

Contents

- ▶ *Install the McAfee EMM extension in ePolicy Orchestrator*
- ▶ *Run the Deployment Helper*
- ▶ *Install McAfee EMM server components*
- ▶ *Add McAfee EMM as a registered server in ePolicy Orchestrator*

Install the McAfee EMM extension in ePolicy Orchestrator

Install the McAfee EMM extension before installing or upgrading the server components so that you can prepare policies for quick deployment.

Check in the McAfee EMM extension to ePolicy Orchestrator automatically using the Software Manager. For other methods of checking in product packages, see the ePolicy Orchestrator documentation.

Task

For option definitions, click ? in the interface.

- 1 On the ePolicy Orchestrator console, select **Menu | Software | Software Manager**.
- 2 Select the McAfee EMM extension from the **Product Categories** list, then click **Check in**.
- 3 Review and accept the product details and license agreement, then click **OK**.
- 4 (Optional) Configure McAfee EMM policies. See the *McAfee EMM Product Guide* for details.



To preserve policies or iOS web clips from an existing McAfee EMM installation, manually transfer them to ePolicy Orchestrator.

Run the Deployment Helper

The Deployment Helper verifies the McAfee EMM installation requirements and prepares your environment for installation.

The Deployment Helper is available on the [McAfee Downloads](#) site.

Tasks

- [Run the Deployment Helper for enhanced security configurations on page 14](#)
In an enhanced security installation, the Deployment Helper guides you through configuring settings for the Hub on the internal server, and for the Portal, Push Notifier, and Proxy on the DMZ server.
- [Run the Deployment Helper for basic security configurations on page 15](#)
In a basic security installation, the Deployment Helper guides you through configuring settings for the Hub, Portal, Push Notifier, and Proxy on the server.

Run the Deployment Helper for enhanced security configurations

In an enhanced security installation, the Deployment Helper guides you through configuring settings for the Hub on the internal server, and for the Portal, Push Notifier, and Proxy on the DMZ server.



Complete this task on your internal server first, then repeat it on your DMZ server.

Task

- 1 Install the Deployment Helper.
 - a Log on to a Windows server.
 - b Locate and double-click the installer file DeploymentHelperInstall.msi.
 - c Review and accept the terms of the license agreement, then click **Install**.
- 2 Select **Start | All Programs | McAfee EMM | EMM Deployment Helper**.
- 3 Review the instructions, then click **Next**.
- 4 Select the installation appropriate to your server type:
 - **Enhanced Security Model - Internal Server**
 - **Enhanced Security Model - External Server**
- 5 Review your installation configuration, then click **Next**.
- 6 Complete the component settings screens.
Appendix A: Settings for components provides option definitions for all component settings screens.
- 7 Review the information on the **Confirm Installation Settings** screen, then click **Run Scan**.

When the scan is complete, results are shown. If any tasks are marked failed, review the information, then click **Launch KB Assistance** for help resolving any issues.

See also

[Database settings on page 23](#)
[LDAP server settings on page 24](#)
[Hub server settings on page 24](#)
[Portal certificate settings on page 24](#)
[MDM certificate settings on page 25](#)
[ActiveSync server settings on page 27](#)

Run the Deployment Helper for basic security configurations

In a basic security installation, the Deployment Helper guides you through configuring settings for the Hub, Portal, Push Notifier, and Proxy on the server.

Task

- 1 Install the Deployment Helper.
 - a Log on to a Windows server.
 - b Locate and double-click the installer file DeploymentHelperInstall.msi.
 - c Review and accept the terms of the license agreement, then click **Install**.
- 2 Select **Start | All Programs | McAfee EMM | EMM Deployment Helper**.
- 3 Review the instructions, then click **Next**.
- 4 Select **Basic Security Model - Single Server**, then click **Next**.
- 5 Complete the component settings screens.

Appendix A: Settings for components provides option definitions for all component settings screens.
- 6 Review the information on the **Confirm Installation Settings** screen, then click **Run Scan**.

When the scan is complete, results are shown. If any tasks are marked failed, review the information, then click **Launch KB Assistance** for help resolving any issues.

See also

[Database settings on page 23](#)
[LDAP server settings on page 24](#)
[Portal certificate settings on page 24](#)
[MDM certificate settings on page 25](#)
[ActiveSync server settings on page 27](#)

Install McAfee EMM server components

The server installation process depends on your planned configuration.



Don't install or upgrade individual components from version 11.0 with an earlier version of McAfee EMM.

Tasks

- [Install server components in enhanced security configuration on page 16](#)
Use enhanced security installation for maximum security. This configuration installs the server components on dual servers.
- [Install server components in basic security configuration on page 16](#)
Use a basic security installation if your organization doesn't have complex security requirements. This configuration installs the server components on a single server.

Install server components in enhanced security configuration

Use enhanced security installation for maximum security. This configuration installs the server components on dual servers.

Before you begin

Run the Deployment Helper for enhanced security mode. See *Run the Deployment Helper for enhanced security configurations*.



Complete this task on your internal server first, then repeat it on your DMZ server.

Task

- 1 Locate and right-click the installer file Setup.exe, then select **Run as Administrator**.
 - Click **Continue** if prompted to install Windows installer or .NET version.
 - Click **Yes** if prompted to restart the server. The installer continues automatically after restarting.
- 2 Review and accept the terms of the license agreement, then click **Next**.
- 3 Click the installation appropriate to your server type:
 - **Dual Server (Internal)**
 - **Dual Server (External)**
- 4 Complete the component settings screens.
Appendix A: Settings for components provides option definitions for all component settings screens.
- 5 Review the information on the **Summary** screen, then click **Install**. When installation is complete, click **Finish**.

See also

Run the Deployment Helper for enhanced security configurations on page 14

Database settings on page 23

LDAP server settings on page 24

Communication settings on page 26

DMZ settings on page 27

Install server components in basic security configuration

Use a basic security installation if your organization doesn't have complex security requirements. This configuration installs the server components on a single server.

Before you begin

Run the McAfee Deployment Helper for basic security mode. See *Run the Deployment Helper for basic security configurations*.

Task

- 1 Locate and right-click the installer file Setup.exe, then select **Run as Administrator**.
 - Click **Continue** if prompted to install Windows installer or .NET version.
 - Click **Yes** if prompted to restart the server. The installer continues automatically after restarting.
- 2 Review and accept the terms of the license agreement, then click **Next**.
- 3 Click **Single Server**.

- 4 Complete the component settings screens.

Appendix A: Settings for components provides option definitions for all component settings screens.

- 5 Review the information on the **Summary** screen, then click **Install**. When installation is complete, click **Finish**.

See also

Run the Deployment Helper for basic security configurations on page 15

Database settings on page 23

LDAP server settings on page 24

Communication settings on page 26

DMZ settings on page 27

Add McAfee EMM as a registered server in ePolicy Orchestrator

Set up access to the McAfee EMM server by adding it as a registered server.

Before you begin

Install the McAfee EMM extension.

Task

For option definitions, click ? in the interface.

- 1 On the ePolicy Orchestrator console, select **Menu | Configuration | Registered Servers**, then click **New Server**.
- 2 From the **Server type** drop-down list, select **EMM Hub**, enter a unique name for the server, then click **Next**.
- 3 Provide details about the connection to your McAfee EMM server, click **Establish Connection** to test your configuration, then click **Save**.

The default logon credentials are:

- User name — admin
- Password — TDadmin*



To secure the connection between the McAfee EMM Hub and the ePolicy Orchestrator server, change the default system administrator logon credentials after adding the registered server. See the *McAfee EMM Product Guide* for details.

Installing McAfee EMM

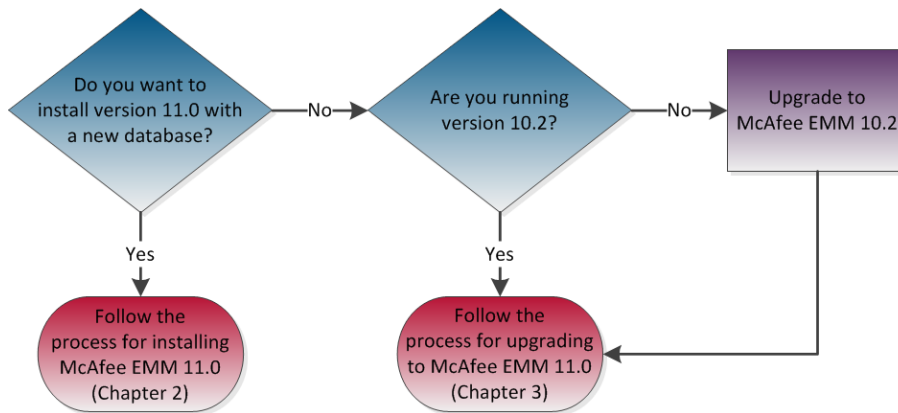
Add McAfee EMM as a registered server in ePolicy Orchestrator

3

Upgrading McAfee EMM

The upgrade process varies depending on your existing version of McAfee EMM and whether you want to install version 11.0 with a new database or upgrade an existing 10.2 database. Upgrading an existing 10.2 database preserves packages and all settings specified in System Settings, like certificates and authorization directories.

Use this chart to determine the recommended upgrade process for your situation.



iOS and Android devices configured for McAfee EMM 10.2 must be updated for version 11.0 whether you install with a new database or upgrade an existing database. See the *McAfee EMM Product Guide* for details on updating devices.

To upgrade from version 10.2, complete these tasks in order:

Contents

- ▶ *Install the McAfee EMM extension in ePolicy Orchestrator*
- ▶ *Upgrade McAfee EMM server components*
- ▶ *Add McAfee EMM as a registered server in ePolicy Orchestrator*

Install the McAfee EMM extension in ePolicy Orchestrator

Install the McAfee EMM extension before installing or upgrading the server components so that you can prepare policies for quick deployment.

Check in the McAfee EMM extension to ePolicy Orchestrator automatically using the Software Manager. For other methods of checking in product packages, see the ePolicy Orchestrator documentation.

Task

For option definitions, click ? in the interface.

- 1 On the ePolicy Orchestrator console, select **Menu | Software | Software Manager**.
- 2 Select the McAfee EMM extension from the **Product Categories** list, then click **Check in**.
- 3 Review and accept the product details and license agreement, then click **OK**.
- 4 (Optional) Configure McAfee EMM policies. See the *McAfee EMM Product Guide* for details.



To preserve policies or iOS web clips from an existing McAfee EMM installation, manually transfer them to ePolicy Orchestrator.

Upgrade McAfee EMM server components

Upgrading from an existing version 10.2 installation preserves your McAfee EMM database, packages, and all settings specified in System Settings, like certificates and authorization directories. The upgrade process differs based on your configuration.

Before you begin

Back up your existing McAfee EMM installation. See *Back up an existing installation*.



Don't install or upgrade individual components from version 11.0 with an earlier version of McAfee EMM.

Tasks

- [Upgrade for enhanced security configurations and High Availability environments on page 20](#)
For enhanced security configurations and High Availability environments, the McAfee EMM servers must be upgraded in a specific order.
- [Upgrade for basic security configurations on page 20](#)
For basic security configurations, upgrade all McAfee EMM server components simultaneously.

See also

[Back up an existing installation on page 29](#)

Upgrade for enhanced security configurations and High Availability environments

For enhanced security configurations and High Availability environments, the McAfee EMM servers must be upgraded in a specific order.

Task

- Follow the instructions in [KB78440](#).

Upgrade for basic security configurations

For basic security configurations, upgrade all McAfee EMM server components simultaneously.

Task

- 1 Locate and right-click the installer file Setup.exe, then select **Run as Administrator**.
Click **Yes** if prompted to restart the server. The installer continues automatically after restarting.

- 2 Review and accept the terms of the license agreement, then click **Next**.
Select **Use Configuration from Previous Installations** if you want to keep settings from a previous upgrade. If you're reusing an existing McAfee EMM database for upgrade, settings from the previous installation are preserved by default, regardless of any changes you make in the installer.
- 3 Click **Upgrade**.
- 4 Review the information on the **Summary** screen, then click **Upgrade**. When installation is complete, click **Finish**.
Since they're no longer used in version 11.0, the McAfee EMM Console, Device Management Gateway (DMG), Blackberry Enterprise Server (BES) Agent, and Public Key Infrastructure (PKI) Agent are automatically uninstalled during upgrade.

Add McAfee EMM as a registered server in ePolicy Orchestrator

Set up access to the McAfee EMM server by adding it as a registered server.

Before you begin

Install the McAfee EMM extension.

Task

For option definitions, click ? in the interface.

- 1 On the ePolicy Orchestrator console, select **Menu | Configuration | Registered Servers**, then click **New Server**.
- 2 From the **Server type** drop-down list, select **EMM Hub**, enter a unique name for the server, then click **Next**.
- 3 Provide details about the connection to your McAfee EMM server, click **Establish Connection** to test your configuration, then click **Save**.

The default logon credentials are:

- User name — admin
- Password — TDadmin*



To secure the connection between the McAfee EMM Hub and the ePolicy Orchestrator server, change the default system administrator logon credentials after adding the registered server. See the *McAfee EMM Product Guide* for details.

Upgrading McAfee EMM

Add McAfee EMM as a registered server in ePolicy Orchestrator

A

Settings for components

Use these tables to configure settings for the Deployment Helper and McAfee EMM server components.



If you use the installer to upgrade components while reusing an existing database, the new component is installed with existing settings, regardless of any changes you make in the installer. This functionality prevents accidentally overriding McAfee EMM database settings that affect your network. If you upgrade an individual component and create a new database, you can reuse old settings, or change them as needed.

Contents

- ▶ [Database settings](#)
- ▶ [LDAP server settings](#)
- ▶ [Hub server settings](#)
- ▶ [Portal certificate settings](#)
- ▶ [MDM certificate settings](#)
- ▶ [Communication settings](#)
- ▶ [ActiveSync server settings](#)
- ▶ [DMZ settings](#)

Database settings

These settings in the Deployment Helper and installer identify the SQL Server that hosts the McAfee EMM database.

Option	Definition
Use SQL Express (Deployment Helper only)	Select to install SQL Express on the local system and create the McAfee EMM database.
Server name	Host name or IP address of the SQL Server where you want to install the McAfee EMM database.
Authentication	<ul style="list-style-type: none">• Windows Authentication (recommended)• SQL Authentication
Login	User name for the connection to the McAfee EMM database server.
Password	Password for the connection to the McAfee EMM database server.
Database	Name for the McAfee EMM database.

See also

- [Run the Deployment Helper for enhanced security configurations on page 14](#)
- [Run the Deployment Helper for basic security configurations on page 15](#)
- [Install server components in enhanced security configuration on page 16](#)
- [Install server components in basic security configuration on page 16](#)

LDAP server settings

These settings in the Deployment Helper and installer identify the server for authenticating users. Fields vary depending on which authentication type you select.

Option	Definition
Authentication	<ul style="list-style-type: none"> • Active Directory • Domino • ActiveSync Protocol
Domain FQDN	Fully qualified domain name of the LDAP server.
Domain DN	Domain distinguished name of the LDAP server. <ul style="list-style-type: none"> • Active Directory — This field is populated when Domain FQDN is completed. • Domino — Leave this field blank.
ActiveSync Server	IP address or fully qualified domain name of the ActiveSync server.
Domain Name	Domain name of the server.
Username or Verification Username	User name for the connection to the server.
Password or Verification Password	Password for the connection to the server.
External EMM Proxy Server Address	Fully qualified domain name of the McAfee EMM Proxy. Devices connect to this McAfee EMM Proxy address for ActiveSync.

See also

Run the Deployment Helper for enhanced security configurations on page 14

Run the Deployment Helper for basic security configurations on page 15

Install server components in enhanced security configuration on page 16

Install server components in basic security configuration on page 16

Hub server settings

These settings in the Deployment Helper connect the DMZ server in an enhanced security installation to the internal McAfee EMM Hub server.

Option	Definition
Server address	Fully qualified domain name or IP address of the McAfee EMM Hub server

See also

Run the Deployment Helper for enhanced security configurations on page 14



Portal certificate settings

These settings in the Deployment Helper specify the portal certificate. The Deployment Helper can also assist with generating a certificate signing request (CSR), then creating a portal certificate from the verified CSR.

On the **Provide a Portal Certificate** screen of the Deployment Helper, select one of these options:

- **Create new SSL certificate** to generate an SSL certificate, followed by specifying the certificate you created.
- **Use existing SSL certificate** to specify an existing, valid SSL certificate.

Generate a portal certificate

Step	Option	Definition
1. Generate the CSR	Common Name	URL that you want customers to connect to. For a wildcard certificate, add an asterisk before the common name, for example, *.domainname.com.
	Organization	Legal name of your organization.
	Organization Unit	Unit within your organization requesting the certificate, for example, Engineering or Human Resources.
		 You can enter a DBA (doing business as) name in this field.
	City/Locality	Unabbreviated city where your organization is legally registered.
	State/Province	Unabbreviated state or province where your organization is legally registered.
	Country/Region	Two-letter ISO country code where your organization is legally registered, like US or FR.
	Certificate Request File Path	Browse to select the location to store the certificate request.
2. Verify the CSR		This step is completed outside the Deployment Helper. Contact a valid certificate authority (CA) for verification.
3. Generate the portal certificate	Certificate File Path	Browse to select the .cer or .pem file created in step 2.
	Certificate Password	Password for the certificate.

Specify a portal certificate

Option	Definition
File Path	Browse to select the .pfx file.
Password	Password for the certificate.

See also

[Run the Deployment Helper for enhanced security configurations on page 14](#)

[Run the Deployment Helper for basic security configurations on page 15](#)


MDM certificate settings

These settings in the Deployment Helper specify the MDM certificate. The Deployment Helper can also assist with generating a CSR, then creating an MDM certificate from the verified CSR.

On the **Provide an MDM Certificate** screen of the Deployment Helper, select one of these options:

- **Create new/renew existing MDM certificate** to generate an MDM certificate, followed by specifying the certificate you created.
- **Use existing MDM certificate** to specify an existing, valid MDM certificate.

Generate an MDM certificate

Step	Option	Definition
1. Generate the CSR	Common Name	URL that you want customers to connect to.
	Email	Email address of the administrator making the request.
	Country/Region	Two-letter ISO country code where your organization is legally registered, like US or FR .
	Certificate Request File Path	Browse to select the location to store the certificate request.
2. Verify the CSR	 This step is completed outside the Deployment Helper. Follow the instructions in KB73382 to verify the CSR through Apple.	
3. Generate the MDM certificate	Certificate File Path	Browse to select the .pem file created in step 2.
	Certificate Password	Password for the certificate.

Specify an MDM certificate

Option	Definition
File Path	Browse to select the .pfx file.
Password	Password for the certificate.

See also

[Run the Deployment Helper for enhanced security configurations on page 14](#)

[Run the Deployment Helper for basic security configurations on page 15](#)

Communication settings

These settings in the installer specify portal and MDM certificates, and GCM account credentials.

Option	Definition	
Portal Certificate	Available Certificates	Select an existing certificate from an earlier McAfee EMM installation, or select Use New Certificate to specify a new certificate.
	File Path	Browse to select the portal certificate.
	Password	Password for the portal certificate.
MDM Push Certificate	File Path	Browse to select the MDM certificate.
	Password	Password for the MDM certificate.
GCM Settings	Sender ID	Project number of your Google API project.
	Token	API key value of your Google API project.

See also

[Install server components in enhanced security configuration on page 16](#)

[Install server components in basic security configuration on page 16](#)

ActiveSync server settings

These settings in the Deployment Helper identify the ActiveSync server that communicates with the McAfee EMM Proxy.

Option	Definition
Server Address	IP address or fully qualified domain name of the ActiveSync server. For a Domino server, enter <servername>/servlet/traveler.
Domain Name	Domain name of the ActiveSync server.
Username	User name for the connection to the ActiveSync server.
Password	Password for the connection to the ActiveSync server.


See also

Run the Deployment Helper for enhanced security configurations on page 14

Run the Deployment Helper for basic security configurations on page 15

DMZ settings

These settings in the installer identify the ActiveSync server that communicates with the McAfee EMM Proxy.

Option	Definition
ActiveSync Server Address	IP address or fully qualified domain name of the ActiveSync server.  To verify connection to the server, click the green checkmark next to the server address, then click Verify .

See also

Install server components in enhanced security configuration on page 16

Install server components in basic security configuration on page 16

B

Specialized installation tasks

These installation tasks are performed infrequently or in atypical installation environments.

Contents

- ▶ *Back up an existing installation*
- ▶ *Install McAfee EMM in High Availability environments*
- ▶ *Uninstall McAfee EMM*

Back up an existing installation

Save a copy of your McAfee EMM database and export an encryption key to back up McAfee EMM versions 10.2 and earlier.

Task

- 1 On the McAfee EMM 10.2 Console, click the name of the server in the upper-left corner.
- 2 Enter a **Key Password**, then select **Export Encryption Key**.
- 3 Save a copy of the McAfee EMM database by copying the database file from the SQL Server.

Install McAfee EMM in High Availability environments

High Availability (HA) environments require modified installation to ensure continuous access.


Plan your installation using hardware redundancy options like Network load balancing (NLB), SQL Server replication, or clustering options built into the operating system and applications.

For details on installing McAfee EMM in HA environments, see [KB70278](#).

Task

- 1 Install the McAfee EMM extension in ePolicy Orchestrator.
See [Install the McAfee EMM extension in ePolicy Orchestrator](#).
- 2 Use the custom installation option to install the McAfee EMM Hub and database on a single server.
- 3 Add McAfee EMM as a registered server in ePolicy Orchestrator.
See [Add McAfee EMM as a registered server in ePolicy Orchestrator](#).

- 4 Export an encryption key from ePolicy Orchestrator.
 - a Select **Menu | Configuration | Server Settings | EMM Server Settings | System Settings**.
 - b Click **Export Encryption Key**.
 - c Enter a **Key Password**, then click **OK**.
- 5 Use the encryption key to install the McAfee EMM Hub and database on more servers.

 You must install both the McAfee EMM Hub and database on each server.
- 6 Pair systems using load balancing appropriate for your setup.
- 7 Update the McAfee EMM registered server in ePolicy Orchestrator with the virtual IP address of the load balancer.

See *Add McAfee EMM as a registered server in ePolicy Orchestrator*.

See also

[Install the McAfee EMM extension in ePolicy Orchestrator on page 13](#)

[Add McAfee EMM as a registered server in ePolicy Orchestrator on page 17](#)

Uninstall McAfee EMM

To remove McAfee EMM, follow these steps for each server where you installed components.

Task

- 1 Locate and right-click the installer file Setup.exe, then select **Run as Administrator**.
- 2 Click **Uninstall**.
- 3 Review the information on the **Uninstall Summary** screen, then click **Uninstall**. When uninstall is complete, click **Finish**.

C

Troubleshooting

Use these troubleshooting tips to work through issues encountered during installation.

Task	Issue	Resolution
Configuring servers	Unhandled exception when configuring the SQL Server.	See KB75444 .
	Failed connection to ActiveSync server.	Do one of the following based on the error code: <ul style="list-style-type: none">• Error code 403 — Verify that the user credentials are valid, the user has a mailbox configured on the Exchange server, and the Exchange server is accessible from the McAfee EMM server.• Error code 500 — Verify that the Exchange server is operational.
Specifying certificates	Error specifying a portal certificate.	Check for these issues with the portal certificate: <ul style="list-style-type: none">• Incorrect password.• Invalid, missing, or empty certificate file.• Expired dates for the certificate file.• No certificate chain in the certificate file.• Invalid or missing certificate authority in the certificate chain of the certificate file.• None of the certificates in the certificate chain are marked as certificate authority certificates.• The portal certificate installed on the McAfee EMM Proxy server doesn't match the portal certificate specified in the software (Menu Configuration Server Settings EMM Server Settings System Settings Certificates).

Task	Issue	Resolution
Installing in customized environments	Connectivity issues with McAfee EMM Proxy to Hub communication over Port 80.	See KB75667 .
Upgrading	Failed upgrade of the McAfee EMM Hub.	<ol style="list-style-type: none">1 Navigate to C:\Program Files\McAfee\EMMPlatform\, then open the latest installation log in a text editor.2 Search the log for 1603, then scroll up until you see a readable error message. Typical reasons for failure include:<ul style="list-style-type: none">• The McAfee EMM Hub isn't configured correctly. Check the Event Viewer for details. See the <i>McAfee EMM Product Guide</i> for information on viewing log files.• The connection to the McAfee EMM Database is invalid. Verify the installation specifications in the InstallerData.xml file. If you're using Windows Authentication to connect to the SQL Server, verify that the account used for installation is a local administrator account that has permission to create a database on the SQL Server.

Index

A

- about this guide [5](#)
- Active Directory
 - ActiveSync server settings [27](#)
 - LDAP server settings [24](#)
- ActiveSync Protocol, LDAP server settings [24](#)
- ActiveSync server
 - Deployment Helper settings [27](#)
 - installation settings [27](#)
 - port requirements [11](#)
 - server requirements [9](#)
 - troubleshooting [31](#)
- Agent, EMM, *See* app, EMM
- Android devices
 - EMM app description [8](#)
 - port requirements [11](#)
 - Secure Container description [8](#)
 - supported versions [9](#)
- app, EMM, description [8](#)
- Apple Push Notification
 - certificates, requirements [11](#)
 - MDM certificates, Deployment Helper, generating and specifying [25](#)
 - MDM certificates, installation settings [26](#)
 - port requirements [11](#)
- authentication, server settings [24](#)

B

- backups, EMM database
 - upgrade prerequisite [20](#)
 - versions 10.2 and earlier [29](#)
- basic security configuration
 - Deployment Helper [15](#)
 - description [8](#)
 - installation [16](#)
 - port requirements [11](#)
 - upgrade [20](#)
- Blackberry Enterprise Server (BES) Agent, EMM, uninstalled automatically in 11.0 upgrade [20](#)
- browsers, requirements [9](#)

C

- .cer file, certificate signing request (CSR), portal certificate [24](#)

- certificate authority (CA)
 - certificate requirements [11](#)
 - certificate verification, portal certificate [24](#)
 - troubleshooting certificate errors [31](#)
- certificate signing request (CSR)
 - .cer and .pem files [24](#)
 - MDM certificate [25](#)
 - portal certificate [24](#)
- certificates
 - installation settings [26](#)
 - obtaining and renewing [11](#)
 - requirements [11](#)
- clusters, fail-safe installation [29](#)
- communication
 - between server components [7](#)
 - with certificate authorities and push services [11](#)
- components
 - client-side [8](#)
 - server-side [7](#)
- configurations, basic security
 - Deployment Helper [15](#)
 - description [8](#)
 - installation [16](#)
 - upgrade [20](#)
- configurations, enhanced security
 - Deployment Helper [14](#)
 - description [8](#)
 - installation [16](#)
 - upgrade [20](#)
- Console, EMM
 - encryption key, backing up versions 10.2 and earlier [29](#)
 - uninstalled automatically in 11.0 upgrade [20](#)
- conventions and icons used in this guide [5](#)
- custom installation
 - HA environments [29](#)
 - troubleshooting [31](#)
 - unsupported for components from different product versions [15](#)

D

- database collation, SQL Server [9](#)
- database, EMM
 - backups [29](#)
 - existing vs. new, effects on upgrading components [23](#)

- database, EMM (*continued*)
 - HA environments, installation considerations [29](#)
 - settings [23](#)
 - Deployment Helper
 - basic security configuration [15](#)
 - description and availability [13](#)
 - enhanced security configuration [14](#)
 - Device Management Gateway (DMG), EMM, uninstalled automatically in 11.0 upgrade [20](#)
 - devices, *See* mobile devices
 - DMZ
 - configuration [7](#)
 - port requirements [11](#)
 - settings [27](#)
 - documentation
 - audience for this guide [5](#)
 - product-specific, finding [6](#)
 - typographical conventions and icons [5](#)
 - documentation, EMM Product Guide
 - changing default system administrator logon credentials [17](#), [21](#)
 - policies [13](#), [19](#)
 - updating devices [19](#)
 - viewing log files [31](#)
 - documentation, ePO Product Guide
 - checking in product packages [13](#), [19](#)
 - system requirements [9](#)
 - documentation, McAfee KnowledgeBase
 - enhanced security configuration and HA environments, upgrading, KB78440 [20](#)
 - HA environments, installing, KB70278 [29](#)
 - MDM certificate creation, KB73382 [11](#), [25](#)
 - port 80 connectivity issues, KB75667 [31](#)
 - SQL Server unhandled exception, KB75444 [31](#)
 - domain name system (DNS) server, certificate requirements [11](#)
 - Domino
 - ActiveSync server settings [27](#)
 - LDAP server settings [24](#)
 - supported mail servers [9](#)
 - dual servers, *See* configurations, enhanced security
- E**
- encryption key
 - version 11.0, installing in HA environments [29](#)
 - versions 10.2 and earlier, creating a backup [29](#)
 - enhanced security configuration
 - Deployment Helper [14](#)
 - description [8](#)
 - installation [16](#)
 - port requirements [11](#)
 - upgrade [20](#)
 - ePO
 - EMM extension, checking in [13](#), [19](#)
 - encryption key, exporting for HA installation [29](#)
 - registered server, connecting EMM to ePO [17](#), [21](#)
 - ePO (*continued*)
 - supported versions, 4.6.5 and later [9](#)
 - Exchange, supported mail servers [9](#)
 - extension, EMM, checking in to ePO [13](#), [19](#)
- F**
- figures
 - basic security configuration [8](#)
 - enhanced security configuration [8](#)
 - upgrade flowchart [19](#)
 - firewalls, access rules [11](#)
- G**
- Go Daddy, certificate authority (CA) [11](#)
 - Google Cloud Messaging (GCM)
 - certificates, installation settings [26](#)
 - certificates, requirements [11](#)
 - port requirements [11](#)
- H**
- hardware requirements [9](#)
 - High Availability (HA) environments
 - installation [29](#)
 - upgrade [20](#)
 - Hub, EMM
 - description [7](#)
 - registered server in ePO [17](#), [21](#)
 - settings [24](#)
- I**
- installation
 - basic security configuration [16](#)
 - EMM extension, checking in to ePO [13](#), [19](#)
 - enhanced security configuration [16](#)
 - permissions [9](#)
 - preparation with the Deployment Helper [13](#)
 - process overview [13](#)
 - registered server, connecting EMM to ePO [17](#), [21](#)
 - server components [15](#)
 - uninstalling [30](#)
 - unsupported for components from different product versions [15](#)
 - internet browsers, requirements [9](#)
 - Internet Information Services (IIS), Windows
 - certificate requirements [11](#)
 - stopping before upgrade [20](#)
 - iOS Agent Push Notification certificate, requirements [11](#)
 - iOS devices
 - EMM app description [8](#)
 - port requirements [11](#)
 - supported versions [9](#)
 - iPad, *See* iOS devices
 - iPhone, *See* iOS devices
 - iPod, *See* iOS devices

K

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

L

languages, supported 9

LDAP server

port requirements 11

settings 24

load balancing, HA environments 29

M

mail server, requirements 9

McAfee Downloads

iOS Agent Push Notification certificate updates 11

obtaining the Deployment Helper 13

McAfee ServicePortal, accessing 6

Microsoft Silverlight, supported versions 9

mobile device management (MDM) certificates

Deployment Helper, generating and specifying 25

installation settings 26

requirements 11

mobile devices

port requirements 11

supported versions 9

updating for version 11.0 19

Mobile ePO (MePO) extension, automatic installation with EMM 7

N

network load balancing (NLB), fail-safe installation 29

network requirements 11

O

operating system requirements 9

P

.pem file, certificate signing request (CSR)

MDM certificate 25

portal certificate 24

permissions, installation 9

.pfx file, personal information exchange

MDM certificate 25

portal certificate 24

policies, transferring from previous EMM installations 13, 19

pop-ups, required for some EMM features 9

portal certificates

Deployment Helper, generating and specifying 24

installation settings 26

requirements 11

troubleshooting 31

Portal, EMM

certificate requirements 11

description 7

Portal, EMM (*continued*)

domain requirements 11

ports

access rules 11

troubleshooting 31

process overviews

installation 13

upgrade 19

Product Guide, EMM

changing default system administrator logon credentials 17, 21

policies 13, 19

updating devices 19

viewing log files 31

Product Guide, ePO

checking in product packages 13, 19

system requirements 9

product packages, checking in to ePO 13, 19

Proxy, EMM

description 7

domain requirements 11

Public Key Infrastructure (PKI) Agent, EMM, uninstalled automatically in 11.0 upgrade 20

Push Notifier, EMM

certificate requirements 11

description 7

push technology

certificate requirements 11

port requirements 11

R

redundancy, installation planning 29

registered servers, connecting EMM to ePO 17, 21

requirements

certificate 11

network 11

system 9

routers, access rules 11

S

Secure Container, description 8

ServicePortal, finding product documentation 6

settings

Deployment Helper and installer 23

preserving during upgrade 20

Silverlight, Microsoft, supported versions 9

single server, *See* configurations, basic security

.skx file, encryption key

version 11.0, installing in HA environments 29

versions 10.2 and earlier, creating a backup 29

SMTP server, port requirements 11

Software Manager, checking in EMM extension 13, 19

SQL Server

port requirements 11

replication, fail-safe installation 29

SQL Server (*continued*)
server requirements [9](#)
settings [23](#)
troubleshooting [31](#)

SSL certificates, *See* portal certificates
system requirements [9](#)

T

Technical Support, finding product information [6](#)
troubleshooting [31](#)

U

uninstallation [30](#)
upgrade
EMM database, effects of existing vs. new [23](#)
EMM extension, checking in to ePO [13](#), [19](#)
mobile devices [19](#)

upgrade (*continued*)
process overview [19](#)
registered server, connecting EMM to ePO [17](#), [21](#)
server components [20](#)
supported from version 10.2 [20](#)
troubleshooting [31](#)
unsupported for components from different product
versions [20](#)

URL, EMM Portal and Proxy [11](#)
user interface languages [9](#)

V

Verisign, certificate authority (CA) [11](#)

W

web clips, transferring from previous EMM installations [13](#), [19](#)
Windows Phones, supported versions [9](#)

