Contents

Preface 7
About this guide .................................. 7
Audience .................................. 7
Conventions ................................. 7
Find product documentation .................... 8

1 Introduction 9
Managing quarantine and spam .................... 9
What comes with the MQM software ............... 10

2 Deployment scenarios 11
Using MQM with supported McAfee products ....... 11
High Availability .................................. 11
Policy management ................................ 12
VMware support .................................. 13

Installation

3 Installation 17
Requirements ................................... 17
Overview of installation tasks .......................... 18
Preparing the installation environment ............... 19
Configure Microsoft SQL Server database ............. 19
Install MySQL for McAfee Quarantine Manager .......... 19
Configuring MySQL 5.1 for Linux or Microsoft Windows ................. 20
Install McAfee Quarantine Manager ..................... 21
Installing McAfee Quarantine Manager in a cluster environment ............. 21
Configure a cluster on Windows 2003 Server .......... 21
Configure a cluster on Windows 2008 or 2008 R2 Server .......... 22
Uninstall McAfee Quarantine Manager and components ................. 22
Uninstall the McAfee Quarantine Manager software ................. 23
Uninstall MySQL for McAfee Quarantine Manager ..................... 23
Upgrade to the latest version of MQM .................... 23

4 Integrating McAfee Quarantine Manager with ePolicy Orchestrator 25
Integration preparation tasks .......................... 25
Deploying the McAfee Quarantine Manager package and extensions ............. 25
Install MQM onto your McAfee ePO server ............. 25
Deploy the McAfee Agent onto your client computers .......... 26
Check in the McAfee Quarantine Manager package ............. 27
Check in the MySQL for McAfee Quarantine Manager package .......... 27
Deploy the MySQL for McAfee Quarantine Manager component .......... 27
Deploy MQM on client computers ..................... 28
Install the McAfee Quarantine Manager policy extension ............. 29
Install the McAfee Quarantine Manager reports extension ............. 29
5 Post-installation tasks
Configure the database .................................. 35
Test the installation ........................................ 36
Rebranding McAfee Quarantine Manager .................... 37

Configuration and use

6 Server administration .................................. 41
Administrator types ........................................ 41
Authentication modes ........................................ 42
Use LDAP groups as McAfee Quarantine Manager administrators ........................................ 42
Create administrators with restricted rights .................... 43

7 Domain management ...................................... 45
Add or import domains to McAfee Quarantine Manager ............... 45
Add domains ........................................ 46
Import domains in bulk .................................. 46
Export domains ........................................ 46
Assign domains to Domain Administrators ......................... 47
Change domain configurations ................................ 47
Change multiple domain configurations ......................... 48
Create mapping between domain and groups in connected McAfee products .................... 49

8 Managing user accounts .................................. 51
Create user accounts ...................................... 51
Import users from LDAP ................................... 51
Import users from a .csv or .txt file ......................... 52
Import users from an XML file ................................ 53
Register users automatically ................................ 53
Change user configuration .................................. 54
Register a distribution list .................................. 55

9 Managing quarantined items ............................... 57
Search quarantined items ................................... 57
Taking action on quarantined items ............................. 57

10 Managing tasks ........................................ 59
Configure a scheduled digest email ......................... 59
Configure scheduled database purges ......................... 60
Synchronize and register user lists automatically ............... 60
Send status reports automatically ............................ 61
Synchronizing distribution lists ................................ 61

11 User submissions ........................................ 63
Manage user submissions ................................... 63
## Maintenance and reporting

### 13 Server maintenance

Managing server configurations ................................................. 75
- View log entries .......................................................... 75
- Configure log settings ..................................................... 76
- Configure communication between MQM and other products .... 76
- Configure advanced server settings .................................. 78
- Configure certificates for secure SMTP communication ............ 81

Back up the database .............................................................. 82
- Back up the Microsoft SQL Server database ......................... 82
- Restore the Microsoft SQL Server database ......................... 83
- Back up the MySQL database ........................................... 83
- Restore the MySQL Database ........................................... 84
- Configure a scheduled backup task for MySQL Database .......... 84

### 14 Blacklist and whitelist management

Blacklist and whitelist levels .................................................... 85
- Configure the configuration push interval .......................... 86
- Manage blacklists and whitelists ...................................... 86
- Import blacklists and whitelists ....................................... 87
- Export blacklists and whitelists ....................................... 87

### 15 Dashboard and graphical reports

Viewing dashboard counters ..................................................... 89
- Test connected McAfee products ...................................... 89
- Performing a quick search ................................................. 90
- Calculate the size of the database .................................... 90
- Generate multi-dimensional reports .................................... 90
- Generate Top 10 reports .................................................. 91
- Generate advanced graphical reports .................................. 91
- Download a report ......................................................... 92

A Frequently asked questions ................................................ 93

B Rebranding McAfee Quarantine Manager .................................. 99
- Overview ................................................................. 99
- Adding your brand to the McAfee Quarantine Manager software ... 99
Preface

This guide provides the information you need to work with 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.

Conventions

This guide uses these typographical conventions and icons.

- **Book title, term, emphasis**: Title of a book, chapter, or topic; a new term; emphasis.
- **Bold**: Text that is strongly emphasized.
- **User input, code, message**: Commands and other text that the user types; a code sample; a displayed message.
- **Interface text**: Words from the product interface like options, menus, buttons, and dialog boxes.
- **Hypertext blue**: A link to a topic or to an external website.

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

**Tip**: Suggestions and recommendations.

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

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

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task


2. In the Knowledge Base pane, click a content source:
   - Product Documentation to find user documentation
   - Technical Articles to find KnowledgeBase articles

3. Select Do not clear my filters.

4. Enter a product, select a version, then click Search to display a list of documents.
McAfee® Quarantine Manager (MQM) consolidates the quarantine and anti-spam management functionality of multiple McAfee products.

The software provides a central point to analyze and act upon quarantined emails and files. These items were quarantined because they were identified as spam, phish, viruses, potentially unwanted programs, or other undesirable content.

Integration with McAfee® ePolicy Orchestrator® (McAfee ePO™) provides centralized policy management and graphical reporting.

Contents
- Managing quarantine and spam
- What comes with the MQM software

Managing quarantine and spam

McAfee Quarantine Manager allows administrators and users to continuously tune their anti-spam products, and increase the effectiveness of their spam filtering.

The McAfee Quarantine Manager allows you to:

- Create administrator accounts to manage data related to specific domains.
- Manage and configure settings remotely using ePolicy Orchestrator management software.
- Log on to McAfee Quarantine Manager using Active Directory or Lotus Domino, Novell eDirectory, Sun System Directory, or Open LDAP v3 credentials.
- Maintain your McAfee Quarantine Manager account: create administrators, assign administrators, queue items, generate reports, and reassign administrators.
- Manage user blacklists and whitelists, global blacklists and whitelists, and group blacklists and whitelists.
- Automatically synchronize users and distribution lists between multiple LDAP servers such as Active Directory, Lotus Domino, Novell eDirectory, Sun System Directory, and Open LDAP v3.
- Manage quarantined items such as spam, phish, or other potentially harmful items.
- Store quarantined items using MySQL5.1, MySQL on Linux, Microsoft SQL 2005, Microsoft SQL 2008, or Microsoft SQL 2012.
- Carry out quarantine tasks such as releasing messages or submitting samples to McAfee Labs.
- Manage logging, debug tracing, and report errors to McAfee.
- View digests of quarantined messages.
• Reassign quarantined items belonging to one user to another user.
• Release emails that were incorrectly quarantined as spam, phish, unwanted content, or a potentially unwanted program.
• Users can create or change their individual blacklists and whitelists, and release or delete all quarantined messages by clicking the relevant link in the email digest that users receive from McAfee Quarantine Manager.

What comes with the MQM software

McAfee distributes MQM as an archived file that you can download from the McAfee website.

Once you have obtained the MQM software from McAfee, the installation steps you follow are the same for each type of distribution.

MQM includes these components that you can install together or separately:
• MQM
• MySQL for MQM
• MQM package for McAfee ePO including policies, reports, and Help
Deployment scenarios

Each deployment scenario is presented here in detail, with diagrams and information to help you prepare for your deployment tasks.

Contents
- Using MQM with supported McAfee products
- High Availability
- Policy management
- VMware support

Using MQM with supported McAfee products

MQM provides quarantine management services for McAfee® Email Gateway, McAfee® Security for Microsoft Exchange (MSME) and McAfee® Security for Lotus Domino.

<table>
<thead>
<tr>
<th>Item</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Supported McAfee product</td>
</tr>
<tr>
<td>2</td>
<td>MQM server</td>
</tr>
<tr>
<td>3</td>
<td>Mail server</td>
</tr>
<tr>
<td>4</td>
<td>Administrator</td>
</tr>
<tr>
<td>5</td>
<td>User</td>
</tr>
</tbody>
</table>

Figure 2-1  MQM and supported products workflow
High Availability

You can install MQM in a two-node cluster environment to make sure that MQM is always available. MQM uses Microsoft Cluster Services. Common configuration data resides on the Quorum drive. As an administrator, you receive email notifications when a failover operation is in progress.

You must perform the full installation process on both nodes in an active/passive configuration.

See also
Configure a cluster on Windows 2003 Server on page 21
Configure a cluster on Windows 2008 or 2008 R2 Server on page 22

Policy management

McAfee ePO provides a scalable platform for centralized policy management and enforcement on your McAfee security products and systems where they reside.

You also get comprehensive reporting and product deployment capabilities, all through a single point of control.

This guide does not provide detailed information about installing or using McAfee ePO software. See the McAfee ePolicy Orchestrator Installation Guide and McAfee ePolicy Orchestrator Product Guide.

See also
Install MQM onto your McAfee ePO server on page 26
Set policies within ePolicy Orchestrator on page 30
Send an agent wake-up call to get new properties or policies on page 31
Configure reports on page 32
Uninstall McAfee Quarantine Manager using ePolicy Orchestrator on page 33
VMware support

You can configure MQM to work in a virtual environment, with VMware 5.0 and VMware 5.1.

This figure displays one scenario of the communication between a supported McAfee product and MQM in a virtual environment.

**Figure 2-2 Virtual environment scenario**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet</td>
</tr>
<tr>
<td>2</td>
<td>Virtual Machine 1</td>
</tr>
<tr>
<td>3</td>
<td>Physical Hardware Dell Power Edge 1850 Blade Server</td>
</tr>
<tr>
<td>4</td>
<td>Virtual Machine 2</td>
</tr>
<tr>
<td>5</td>
<td>Mail server</td>
</tr>
<tr>
<td>6</td>
<td>Supported McAfee product</td>
</tr>
<tr>
<td>7</td>
<td>VMware ESX Server</td>
</tr>
<tr>
<td>8</td>
<td>MQM</td>
</tr>
</tbody>
</table>
Installation

Now that you have decided on a deployment option, use the information in these chapters to install the software.

Chapter 3  Installation
Chapter 4  Integrating McAfee Quarantine Manager with ePolicy Orchestrator
Chapter 5  Post-installation tasks
3

Installation

Prepare your installation environment and install McAfee Quarantine Manager and its components on its own, or in a cluster environment. If you need to remove the software from your system, or upgrade to the latest version, you can find the information in this chapter too.

Contents
- Requirements
- Overview of installation tasks
- Preparing the installation environment
- Install McAfee Quarantine Manager
- Installing McAfee Quarantine Manager in a cluster environment
- Uninstall McAfee Quarantine Manager and components
- Upgrade to the latest version of MQM

Requirements
Before installing MQM, make sure that your environment is set up correctly.

Important considerations
- Do not install McAfee Security for Microsoft Exchange and MQM on the same computer.
- Do not install MQM and McAfee ePO on the same computer.
- McAfee recommends that you install MySQL for MQM, Microsoft SQL Server 2008, or Microsoft SQL Server 2012 on a computer where no other database product is installed.
- Verify that MQM can communicate over the network with the McAfee products that it works with.

Requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Supported versions</th>
</tr>
</thead>
</table>
| Supported server operating systems | • Windows Server 2008 R2 SP2 (64-bit)  
                                    | • Windows Server 2012 R2 SP2 (64-bit)                         |
| Supported databases           | • MySQL Server version 5.1 (available in the download package)  
                                    | • Microsoft SQL Server 2008 SP1 Standard/Enterprise (64-bit)  
                                    | • Microsoft SQL Server 2012 and Microsoft SQL Server 2012 R2 |

ℹ️ You can install the database on the same computer as MQM, or on different computers.
### Overview of installation tasks

These tasks are necessary to prepare your environment, install the software, and set up the database.

1. Install and configure the McAfee products for which you want McAfee Quarantine Manager to manage quarantined emails.

   McAfee Quarantine Manager allows management of the emails quarantined by McAfee Security for Microsoft Exchange and McAfee Email Gateway. See each product’s documentation for details about its installation and configuration.

2. Make sure that your system meets the requirements.

3. Install and configure a database for McAfee Quarantine Manager.

4. Install the McAfee Quarantine Manager server.
5 (Optional) Install the McAfee Quarantine Manager extensions, if you want to integrate the package with McAfee ePolicy Orchestrator.

6 Test your installation.

See also
- Install MySQL for McAfee Quarantine Manager on page 19
- Install McAfee Quarantine Manager on page 21
- Add or import domains to McAfee Quarantine Manager on page 45
- Managing server configurations on page 75
- Managing user accounts on page 4
- Managing tasks on page 4
- Blacklist and whitelist management on page 5
- Configure the database on page 35
- Assign domains to Domain Administrators on page 47
- Test connected McAfee products on page 89
- Change domain configurations on page 47

Preparing the installation environment
Set up the appropriate database environment for your McAfee Quarantine Manager installation.

Configure Microsoft SQL Server database
Configure the settings for the existing Microsoft SQL Server database for McAfee Quarantine Manager.

Task
For option definitions, click ? in the interface.

1 Enable Mixed mode authentication on the SQL Server.

2 Create a database user with Server Role as sysadmin.

3 Create a blank database that must be used with McAfee Quarantine Manager, and assign the user you created as the owner of this database.

4 Install Microsoft SQL Server Native Client on the McAfee Quarantine Manager server.

Install MySQL for McAfee Quarantine Manager
MySQL database and McAfee Quarantine Manager can be installed on two different servers or on the same server.

The supported MySQL databases are MySQL for McAfee Quarantine Manager (in the package), MySQL 5.1 for Windows and MySQL 5.1 for Linux.

McAfee recommends that you install the MySQL for McAfee Quarantine Manager software on a computer where no other database server is installed.

Task
1 From the MySQL for McAfee Quarantine Manager directory, extract the .zip file to a temporary directory, and double-click SETUP.EXE.

2 Click Next and follow the on-screen instructions.
In the **Database Server Settings** dialog box, specify the following configuration settings for **MySQL for McAfee Quarantine Manager**:

- **Username** — The default user name is `root`.
- **Password** — The default password is `root`.
- **Database name** — The default database name is `mqm`.
- **Port number** — The default port number is `3306`.
- **McAfee Quarantine Manager Super Administrator Username and Password** — The default user name is `super@mqm.com` and the default password is `super123`.

4. In the **Ready to Install** dialog box, click **Next**.

5. Click **Finish** to complete the installation.

### Configuring MySQL 5.1 for Linux or Microsoft Windows

Configure the parameters for the existing MySQL 5.1 database for McAfee Quarantine Manager.

Add the following parameters in the "MY.CNF" / "MY.INI" file:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default_storage_engine</td>
<td>InnoDB</td>
</tr>
<tr>
<td>lower_case_table_names</td>
<td>1</td>
</tr>
<tr>
<td>max_allowed_packet</td>
<td>At least 150 M (where M represents MB)</td>
</tr>
<tr>
<td>max_connections</td>
<td>At least 100</td>
</tr>
<tr>
<td>innodb_file_per_table</td>
<td>1</td>
</tr>
</tbody>
</table>

The following parameter settings are recommended:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_allowed_packet</td>
<td>1024 M (where M represents MB)</td>
</tr>
<tr>
<td>max_connections</td>
<td>500</td>
</tr>
<tr>
<td>innodb_flush_log_at_trx_commit</td>
<td>0</td>
</tr>
<tr>
<td>innodb_support_xa</td>
<td>0</td>
</tr>
<tr>
<td>innodb_locks_unsafe_for_binlog</td>
<td>1</td>
</tr>
<tr>
<td>innodb_doublewrite</td>
<td>0</td>
</tr>
</tbody>
</table>

- All "innodb_*" parameters must be uncommented.
- External MySQL database on Linux and Microsoft Windows is supported only with InnoDB engine.
Install McAfee Quarantine Manager

Perform the initial McAfee Quarantine Manager setup tasks, and set the port number that Internet Information Services uses to host the McAfee Quarantine Manager website

**Before you begin**
Make sure that Microsoft SQL Server Native Client is installed on the McAfee Quarantine Manager server, if you want to use Microsoft SQL Server 2005/2008 installed on a different computer.

**Task**
1. From the McAfee Quarantine Manager directory, extract the McAfee Quarantine Manager .zip file to a temporary directory and double-click `SETUP.EXE`.
2. Follow the on-screen instructions to install the software.
3. Provide the port number where the Internet Information Services will host the McAfee Quarantine Manager website. The default value is 80.
4. Click Finish to complete the installation.
5. Click Yes to restart the computer.

Installing McAfee Quarantine Manager in a cluster environment

You can install McAfee Quarantine Manager in a two-node cluster environment to make sure that McAfee Quarantine Manager is always available.

**Configure a cluster on Windows 2003 Server**
Set up a cluster environment with McAfee Quarantine Manager running on Windows 2003 Server computers.

**Task**
1. Open the Microsoft Cluster Administrator console.
3. Specify the following information:
   - **Name** — Specify the appropriate name for the cluster service.
   - **Desc** — Type an appropriate description for the cluster service.
   - **Resource Type** — Select McAfee MQM Cluster Framework.
   - **Group** — Select the appropriate group.
4. Select Possible Owner.
   - The possible owner is the cluster node where the resources can be brought online. Add both nodes as Possible Owner.
5. In Dependencies, add the quorum drive specifying the dependency of resources.
   - Make sure the Resource Type as "Physical Disk" exists for the selected group. The Resource Type is used by the McAfee Quarantine Manager Cluster Framework service to store the shared data.
Configure a cluster on Windows 2008 or 2008 R2 Server

Set up a cluster environment with McAfee Quarantine Manager running on Windows 2008 or 2008 R2 computers.

**Task**

1. Start the Failover Cluster Management console and select Services and Application | Configure a service or application.
2. In Select service or application, select Other Server.
3. On the Client Access Point dialog box, specify the name and IP address to access the MQM resources.
4. Select Storage used by MQM service to store shared data.
5. Select Resource Type as McAfee MQM cluster framework.
6. Select the newly configured service and select the properties of New McAfee MQM cluster framework.
7. Click the Properties tab.
8. For shared_data_drive, specify the value Drive Location to store MQM shared data.
9. Apply the configuration, select the newly configured service, and click Bring this service or application Online.
11. Enable If restart is unsuccessful, failover all resources in this service or application.
12. In the Policy tab under MQM Resource, specify a Maximum restart in the specified period value.
13. Make sure that the dependencies are added so that the disk drive comes up before the <MQM resource> comes online.

Uninstall McAfee Quarantine Manager and components

To remove the McAfee Quarantine Manager software from your computer, you must remove the McAfee Quarantine Manager software and the MySQL software.

**Tasks**

- **Uninstall the McAfee Quarantine Manager software on page 23**
  Remove the McAfee Quarantine Manager software from the server it is installed on.
- **Uninstall MySQL for McAfee Quarantine Manager on page 23**
  Remove the MySQL for McAfee Quarantine Manager utility from the computer where it is installed.
Uninstall the McAfee Quarantine Manager software
Remove the McAfee Quarantine Manager software from the server it is installed on.

Task
1. Click Start | Settings | Control Panel | Add or Remove Programs.
2. Select McAfee Quarantine Manager, then click Remove.
3. (Optional) Select Also Remove MQM data to remove the database created for storing quarantined items.
   
   Selecting this option deletes the McAfee Quarantine Manager database permanently.

Uninstall MySQL for McAfee Quarantine Manager
Remove the MySQL for McAfee Quarantine Manager utility from the computer where it is installed.

Task
1. Click Start | Settings | Control Panel | Add or Remove Programs.
2. Select MySQL for McAfee Quarantine Manager, then click Remove.

Upgrade to the latest version of MQM
Upgrade previous versions of the MQM software to the latest version.

You can upgrade to McAfee Quarantine Manager 7.1.0 from McAfee Quarantine Manager 7.0.1.

Task
1. Make a backup of the existing database.
   
   Start the McAfee Quarantine Manager service after performing the database backup.
2. Install the MySQL for McAfee Quarantine Manager component.
   
   Skip this step if you are using Microsoft SQL database.
3. Install the latest version of McAfee Quarantine Manager.
4. On completion, clear the browser cookies and temporary Internet files for proper user interface rendering, then restart the browser.
5. Configure and test your database.

   If you try to log on to MQM during database migration, this message is displayed:
   Migration of database is in progress. Please try after some time. Migration Status: <Y> out of <X> tables completed.

6. You can log on to MQM when the data migration is complete and the database is configured properly.

   McAfee recommends that you restart MQM services after data migration to successfully render the user interface.
7. Test the installation.
See also

- Back up the database on page 82
- Install MySQL for McAfee Quarantine Manager on page 19
- Install McAfee Quarantine Manager on page 21
- Configure the database on page 35
- Test the installation on page 36
Integrating McAfee Quarantine Manager with ePolicy Orchestrator

ePolicy Orchestrator provides a scalable platform for centralized policy management and enforcement on your McAfee security products and systems where they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control. McAfee recommends that you are familiar with the ePolicy Orchestrator software before you start the integration.

This guide does not provide detailed information about installing or using ePolicy Orchestrator software. See the ePolicy Orchestrator Product Guide and the ePolicy Orchestrator Installation Guide.

Contents

- Integration preparation tasks
- Deploying the McAfee Quarantine Manager package and extensions
- Set policies within ePolicy Orchestrator
- Send an agent wake-up call to get new properties or policies
- Configure reports
- Uninstall McAfee Quarantine Manager using ePolicy Orchestrator

Integration preparation tasks

Before you start to integrate McAfee Quarantine Manager and McAfee ePO, you must remove any previous versions of the McAfee Quarantine Manager package and extensions.

<table>
<thead>
<tr>
<th>Packages and extensions</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Quarantine Manager Package</td>
<td>To remove the software packages:</td>
</tr>
<tr>
<td>MySQL for McAfee Quarantine Manager</td>
<td>1 Click Menu</td>
</tr>
<tr>
<td></td>
<td>2 Select the respective package and click Delete.</td>
</tr>
<tr>
<td>McAfee Quarantine Manager Policy Extension</td>
<td>To remove the product extensions:</td>
</tr>
<tr>
<td>McAfee Quarantine Manager Reports Extension</td>
<td>1 Click Menu</td>
</tr>
<tr>
<td></td>
<td>2 Select the respective extension and click Remove.</td>
</tr>
</tbody>
</table>

Deploying the McAfee Quarantine Manager package and extensions

Deploy McAfee Quarantine Manager packages and extensions on client computers to manage them using McAfee ePO.
**Install MQM onto your McAfee ePO server**

Extract the MQM package onto your McAfee ePO server.

**Task**
For option definitions, click ? in the interface.

1. Log on to the McAfee ePO server as an administrator.
2. Create a temporary directory on your local drive.
3. Extract the MQM package to a temporary directory. You see the following folders:
   - McAfee Quarantine Manager
   - MySQL for McAfee Quarantine Manager
   - ePO

   > From the ePO folder, use the policies, reports, and Help .zip files to install the McAfee ePO extensions.

**Deploy the McAfee Agent onto your client computers**

The McAfee Agent is the distributed component of McAfee ePO that must be installed on each system in your network that you want to manage.

**Before you begin**
Before deploying the McAfee Agent, McAfee recommends that you verify communication between the server and systems, and the access to the default administrator share directory. You might also need to create firewall exceptions.

The agent collects and sends information to the McAfee ePO server. It also installs and updates the endpoint products, and applies your endpoint policies. McAfee ePO manages only systems that have the McAfee Agent installed.

**Task**
For option definitions, click ? in the interface.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Systems | System Tree, then click Systems on the menu bar.
3. Highlight a group. If this group has no systems, but has subgroups with systems, click the Level Filter drop-down list and select This Group and All Subgroups.
4. Select one or more systems from the list, and click Actions | Agent | Deploy Agents.
5. Type credentials that have rights to install software on client systems, such as a Domain Administrator, and click OK.

   It takes a few minutes for the McAfee Agent to install and for client systems to retrieve and execute the installation packages for the endpoint products. When first installed, the agent determines a random time within 10 minutes for connecting to the McAfee ePO server to retrieve policies and tasks.

   There are many other ways to deploy the McAfee Agent. For more information, see the ePolicy Orchestrator Product Guide or online Help.
Check in the McAfee Quarantine Manager package
Check in the McAfee Quarantine Manager package to the McAfee ePolicy Orchestrator Master Repository.

**Task**
For option definitions, click ? in the interface.

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu** | **Software** | **Master Repository** | **Actions** | **Check In Package**.
   The Package page appears.
3. Choose the **Package type** as **Product** or **Update (.ZIP)** and browse to MQM710Server.zip, which is saved in the McAfee Quarantine Manager folder.
4. Click **Next**.
   The Package Options page displays information about the package.
5. Choose a branch.
6. In **Options**, select the required options, then click **Save**.

Check in the MySQL for McAfee Quarantine Manager package
Check in the MySQL for McAfee Quarantine Manager package to the ePolicy Orchestrator Master Repository.

**Task**
For option definitions, click ? in the interface.

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu** | **Software** | **Master Repository** | **Action** | **Check In Package**.
   The Package page appears.
3. Choose the **Package type** as **Product** or **Update (.ZIP)**, then browse to the MQM710MySQL.zip file, which is saved in the MySQL for McAfee Quarantine Manager folder.
4. Click **Next**.
   The Package Options page displays information about the package.
5. Choose a branch.
6. In **Options**, select the required options, then click **Save**.

Deploy the MySQL for McAfee Quarantine Manager component
Add the MySQL for McAfee Quarantine Manager component to McAfee ePO-managed client computers.

**Task**
For option definitions, click ? in the interface.

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu** | **Systems** | **System Tree**.
3 Select a node, then click Actions | Agent | Modify Tasks on a Single System.

4 Create a task.
   a Click New Task.
   b On the Client Task Builder page, enter the task name and notes.
   c From the Type drop-down list, select Product Deployment.
   d Click Next.

5 Under Configuration, select the Target Platforms.

6 In Products and components, select MySQL for McAfee Quarantine Manager 7.1.x.x from the drop-down menu and select Install as the Action.

   You can also specify command-line arguments to install MySQL for McAfee Quarantine Manager using customized values. Separate multiple parameters with a space.

   For example: INSTALLDIR="C:\MySQL" SUPERID="superduper@mqm.com" SUPERIDPWD="superduper123"

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>INSTALLDIR=&quot;C:\MySQL&quot;</td>
<td>Installs MySQL in the specified folder location</td>
</tr>
<tr>
<td>MYSQLUSER</td>
<td>MYSQLUSER=&quot;root123&quot;</td>
<td>Sets the MySQL user name</td>
</tr>
<tr>
<td>MYSQLPASSWORD</td>
<td>MYSQLPASSWORD=&quot;root123&quot;</td>
<td>Sets the MySQL password</td>
</tr>
<tr>
<td>MYSQLDBNAME</td>
<td>MYSQLDBNAME=&quot;mymqm&quot;</td>
<td>Sets the MySQL database name</td>
</tr>
<tr>
<td>MYSQLPORT</td>
<td>MYSQLPORT=3361</td>
<td>Sets the MySQL port number</td>
</tr>
<tr>
<td>SUPERID</td>
<td>SUPERID=&quot;<a href="mailto:superduper@mqm.com">superduper@mqm.com</a>&quot;</td>
<td>Sets the Super Administrator email address</td>
</tr>
<tr>
<td>SUPERIDPWD</td>
<td>SUPERIDPWD=&quot;superduper123&quot;</td>
<td>Sets the Super Administrator password</td>
</tr>
</tbody>
</table>

7 In Options, select or deselect Run at every policy enforcement (Windows only).

8 Click Next to schedule this task as needed.

9 Click Next to view a summary of the task.

10 Click Save and send an agent wake-up call.

**Deploy MQM on client computers**

Perform a standard installation on your client computers using MQM default settings.

**Task**

For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Systems | System Tree.

3 Select a node and click Actions | Agent | Modify Tasks on a Single System.
4 Create a task.
   a Click New Task.
   b On the Client Task Builder page, enter the task name and notes.
   c From the Type drop-down list, select Product Deployment.
   d Click Next.

5 Under Configuration, select Target Platforms.

6 In Products to deploy, select McAfee Quarantine Manager 7.1.x.x from the drop-down list and select the Action as Install.
   You can also specify command-line arguments to custom install McAfee Quarantine Manager on the client computer without the default values. Separate multiple parameters with a space.
   For example: INSTALLDIR="C:\MQM" REBOOTREQUIRED=1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>INSTALLDIR=&quot;C:\MQM&quot;</td>
<td>Installs McAfee Quarantine Manager in the specified folder location.</td>
</tr>
<tr>
<td>REBOOTREQUIRED</td>
<td>REBOOTREQUIRED=1</td>
<td>Restarts the client computer after installation.</td>
</tr>
</tbody>
</table>

7 In Options, select or deselect Run at every policy enforcement (Windows only).

8 Click Next to schedule this task as needed.

9 Click Next to view a summary of the task.

10 Click Save and send an agent wake-up call.

**Install the McAfee Quarantine Manager policy extension**
Install the McAfee Quarantine Manager policy extension to manage the MQM clients remotely.

**Task**
For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Software | Extensions | Install Extension.
   The Install Extension dialog box appears.

3 Click Browse, select the extension file MQM710POLICIES.zip, then click OK.

   If you are managing more than one MQM server using McAfee ePO, McAfee recommends having a separate database configuration policy assigned for each of the servers. Assigning a separate configuration policy avoids conflicts between the servers trying to connect to the same database.

**Install the McAfee Quarantine Manager reports extension**
Install the MQM reports on the McAfee ePO server to query the MQM clients.
Task
For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Software | Extensions | Install Extension.

   The Install Extension dialog box appears.

3 Click Browse, select the extension file MQM710REPORTS.zip, and click OK.

Install the MQM Help extension
Install the MQM Help extension on the McAfee ePO server to add the McAfee Quarantine Manager Product Guide and online Help system to the McAfee ePO Help system.

Task
For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Software | Extension | Install Extension.

   The Install Extension dialog box appears.

3 Click Browse, select the extension file HELP_MQM_710.zip, and click OK.

Set policies within ePolicy Orchestrator
The ePolicy Orchestrator console allows you to enforce policies across groups of computers or on a single computer.

These policies override configurations set on individual computers. For information about policies and how they are enforced, see the McAfee ePolicy Orchestrator Product Guide.

Before configuring any policies, select the group of computers where you want to change McAfee Quarantine Manager policies. You can change McAfee Quarantine Manager policies from the pages and tabs that are available in the details pane of the ePolicy Orchestrator console. These pages resemble those you can access from the McAfee Quarantine Manager administrator interface.

After you change the appropriate policies and saved the changes for the intended computer or group of computers, you are ready to deploy new settings via the McAfee Agent.

Tasks
• Create or edit policies on page 30
  Create, edit, delete, or assign a policy to a specific group in the System Tree.

• Enforce policies on page 31
  Enforce a policy to multiple managed systems within a group.

Create or edit policies
Create, edit, delete, or assign a policy to a specific group in the System Tree.
Task
For option definitions, click ? in the interface.

1. Log on to the McAfee ePO server as an administrator.

2. Click Menu | Systems | System Tree.
   The System Tree page appears.

3. Click Assigned Policies.

4. Select Product as McAfee Quarantine Manager 7.1.
   A list of policies managed by MQM appears in the lower pane.

5. Locate the policy you want, and click Edit Assignment next to the policy. The policy assignment for the chosen group page appears.

6. Click Edit Policy or New Policy as needed.
   If you click New Policy, the Create a new policy dialog box appears. Select the policy that you want to duplicate from the Create a policy based on this existing policy drop-down list, type a name, then click OK. The new policy wizard appears.

7. Edit the policy setting as needed, then click Save.

Enforce policies
Enforce a policy to multiple managed systems within a group.

Task
For option definitions, click ? in the interface.

1. Log on to the McAfee ePO server as an administrator.

2. Select Menu | Systems | System Tree, then select the required group or systems.

3. Click Assigned Policies, then select McAfee Quarantine Manager 7.1 from the Product drop-down menu.

4. Select the Category, and click Edit Assignment.

5. From the Assigned policy drop-down menu, select the policy, then click Save.

6. Select the systems again.

7. Send an agent wake-up call.

   You can create and enforce MQM policies and view reports only after adding the MQM extension files.

Send an agent wake-up call to get new properties or policies
To get new policies or properties, use McAfee ePO to send an agent wake-up call.

All systems in the network are managed in the Systems tab. The System Tree contains all systems managed by the McAfee ePO server. It is the primary interface for managing policies and tasks on the systems, and you can use it to organize or sort the systems into logical groups.
My Organization is the root of the System Tree. It includes a Lost&Found group that stores systems whose locations the server can't determine. Depending on the methods you use to create and maintain the System Tree segments (systems), the server uses different characteristics to place the systems in the System Tree.

Task
For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.
2 Click Menu | Systems | System Tree.
3 In the System Tree, select a group.
4 Select the group Computer Name.
5 Select Actions | Agent | Wake Up Agents.
6 On the Wake Up McAfee Agent page, select Agent Wake-Up Call as the wake-up call type, then set a randomization period (0–60 minutes), which is the amount of time for systems to respond to the wake-up call.
7 For the agents to send complete properties instead of only properties that have changed since the last agent-server communication, select Get full product properties.
8 Click OK.

Configure reports
Reports are predefined queries that query the McAfee ePO database and generate a visual representations of the data.
McAfee ePO has its own querying and reporting capabilities. McAfee includes a set of default queries. However, you can create a query, edit, and manage all the queries related to MQM.

Task
For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

Configure reports
Reports are predefined queries that query the McAfee ePO database and generate a visual representations of the data.

Task
For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

Configure reports
Reports are predefined queries that query the McAfee ePO database and generate a visual representations of the data.

Task
For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

Configure reports
Reports are predefined queries that query the McAfee ePO database and generate a visual representations of the data.

Task
For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.
4. Select the query columns.
   a. From the Available Columns menu, select the columns to apply to your query.
   b. In the Selected Columns configuration area, select drag, and position each column data type.
   c. Click Next.

5. From the Available Properties menu, select the properties and configure the corresponding values.

6. Click Run.

7. Save the query.
   a. Click Save.
   b. On the Save Query page, enter the query name, add any notes, and select the group.
   c. Click Save.

---

Uninstall McAfee Quarantine Manager using ePolicy Orchestrator

Remove the McAfee Quarantine Manager package and extensions, and the MySQL for McAfee Quarantine Manager component from the client computers and from the ePolicy Orchestrator repository.

**Tasks**
- **Remove MQM from client computers on page 33**
  To remove MQM from client computers, use McAfee ePO.
- **Remove the packages on page 34**
  Uninstall the McAfee Quarantine Manager packages from McAfee ePO.
- **Remove the extensions on page 34**
  Uninstall the extensions from McAfee ePO.

**Remove MQM from client computers**
To remove MQM from client computers, use McAfee ePO.

**Task**
For option definitions, click ? in the interface.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Systems | System Tree.
3. Select the system, then select Actions | Agent | Modify Tasks on a Single System.
5. On the Client Task Builder page, add a name and notes, select Product Deployment from the Type drop-down list, then click Next.
6. In Configuration, configure the settings, then click Next.
   a. For Target Platforms, select Windows.
   b. For Products & Components, select McAfee Quarantine Manager 7.1.x.x.
For Action, select Remove.

Select the language.

If you remove only one client computer, deselect Run at every policy enforcement (Windows only).

7 To view a summary of the task, click Next, then click Save.

8 Send the agent wake-up call.

**Remove the packages**

Uninstall the McAfee Quarantine Manager packages from McAfee ePO.

**Task**

For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

2 Select Menu | Software | Master Repository.

3 Next to McAfee Quarantine Manager, click Delete.

4 To remove MySQL for McAfee Quarantine Manager package, repeat steps 1–2, then delete the MySQL for McAfee Quarantine Manager link.

**Remove the extensions**

Uninstall the extensions from McAfee ePO.

**Task**

For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Software | Extensions.

3 Remove the McAfee Quarantine Manager extension file.
   a From the left pane, click McAfee | McAfee Quarantine Manager.
   b Choose the McAfee Quarantine Manager extension file, then click Remove.
   c Select Force removal, bypassing any checks or errors, then click OK.

4 Remove the McAfee Quarantine Manager Reports extension file.
   a From the left pane, click McAfee | McAfee Quarantine Manager.
   b Select the McAfee Quarantine Manager Reports extension file, then click Remove.
   c Select Force removal, bypassing any checks or errors, then click OK.

5 Remove the McAfee Quarantine Manager Help extension file.
   a From the left pane, click McAfee | Help Content.
   b Select the McAfee Quarantine Manager help extension file, then click Remove.
   c Select Force removal, bypassing any checks or errors, then click OK.
5

Post-installation tasks

Complete the initial database configuration and test the installation.

Contents
- Configure the database
- Test the installation
- Rebranding McAfee Quarantine Manager

Configure the database

Configure a supported external database and check that McAfee Quarantine Manager can connect to it.

Task
1. Click Start | Programs | McAfee | Quarantine Manager | DB Management UI.

   You can also click Configure Database on the administrator logon page, and enter the System Administrator credentials.

2. On the Database Configuration page, configure the options.
   a. In the Database Type field, enter the database type.
   b. In the Database Server field, enter the database server IP address or host name.
      
      For SQL Server, specify named instances in the format: Server\Namedinstance.
   c. In the User Name field, enter the database user name that McAfee Quarantine Manager uses to connect to the database server. The user name must have write permissions for the database defined under Database Name.
   d. In the Password field, enter the password.
   e. In the Database name field, enter the database name.
   f. In the Database Port field, enter the port number that McAfee Quarantine Manager uses to connect to the database server.
   g. To connect to the database using the default port, select Use default port.
   h. To erase all data from the database and create a database schema, select Create Quarantine Manager schema, then enter the email address and password.

   Schema is the structure of the database that defines the objects in the database. It defines the tables, the fields, indexes, and procedures.
3 Click Test.
   A dialog box appears to confirm that the database is configured successfully.

4 To save the database configuration settings, click Apply.

5 To create a McAfee Quarantine Manager schema, select Create Quarantine Manager schema.

Test the installation

Verify the connection between McAfee Quarantine Manager and other McAfee products.

- If you configure McAfee Quarantine Manager with McAfee Email and Web Security Appliance or McAfee Email Gateway, enable the Use an off-box McAfee Quarantine Manager (MQM) service option.
- If you configure McAfee Quarantine Manager with McAfee Security for Microsoft Exchange, from the Settings & Diagnostics | Detected Items page, make sure that you have enabled the McAfee Quarantine Manager option.
- After you configure your McAfee product with McAfee Quarantine Manager, send malicious email samples to the connected McAfee product.

Task

1 After you install McAfee Quarantine Manager, select Start | Programs | McAfee | Quarantine Manager | Administrator UI.

2 Log on using the Super Administrator account that you specified during installation of the software. You must be able to log on successfully.

3 Click Dashboard.

4 From Connected McAfee Products, click Test to verify the connection between the software and the McAfee product.

   If the Use HTTP to communicate with the MQM server (MQM v6 and greater) option is enabled in McAfee Email and Web Security Appliance, the Test cannot verify connectivity.

5 Select Admin Management | Manage Domains. Enter the Domain Name, then click Add to create a domain to store the domain-based quarantined items.

   If you need items to quarantine for the xyz.com domain, create a @xyz.com Domain Name, then click Add.

6 Select Quarantine Management | Quarantined Items. Items quarantined by the supported McAfee product are listed in the View Results area.

7 From the Administrator user interface, click Quarantined Items, then select the domain name from the drop-down list to view the quarantined emails for the domain created.
Rebranding McAfee Quarantine Manager

McAfee Quarantine Manager rebranding kit allows you to add your company style and wording to components in both the administrator view and the user view of the McAfee Quarantine Manager software.

See also
Adding your brand to the McAfee Quarantine Manager software on page 99
Post-installation tasks
Rebranding McAfee Quarantine Manager
Configuration and use

Set up domains, and servers, configure how you want to handle your users' quarantine settings and submissions to work.

Chapter 6  Server administration
Chapter 7  Domain management
Chapter 8  Managing user accounts
Chapter 9  Managing quarantined items
Chapter 10 Managing tasks
Chapter 11 User submissions
Chapter 12 User interactions
Create administrator accounts and assign them to the domains that oversee the McAfee Quarantine Manager server.

Contents

- Administrator types
- Authentication modes
- Use LDAP groups as McAfee Quarantine Manager administrators
- Create administrators with restricted rights

Administrator types

McAfee Quarantine Manager supports several types of administrator accounts that you can configure and manage. Each type of administrator account has different rights and permissions.

Table 6-1 Types of Administrator accounts

<table>
<thead>
<tr>
<th>Administrator type</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Administrator</td>
<td>• Created during the installation of McAfee Quarantine Manager.</td>
</tr>
<tr>
<td></td>
<td>• Creates other administrators.</td>
</tr>
<tr>
<td></td>
<td>• Has all rights and permissions with full control over the product.</td>
</tr>
<tr>
<td>Super Administrator Alias</td>
<td>• Is a peer to the Super Administrator.</td>
</tr>
<tr>
<td></td>
<td>• Unable to create another Super Administrator alias.</td>
</tr>
<tr>
<td>Domain Administrator</td>
<td>• Manage domains independently.</td>
</tr>
<tr>
<td></td>
<td>• Has rights and permissions as defined by the Super Administrator.</td>
</tr>
<tr>
<td>Domain Administrator Alias</td>
<td>• Is a peer to the Domain Administrator.</td>
</tr>
<tr>
<td></td>
<td>• Unable to create another Domain Administrator alias.</td>
</tr>
<tr>
<td>Operator</td>
<td>Has the same rights and permissions as the Super Administrator except:</td>
</tr>
<tr>
<td></td>
<td>• View quarantined mail message body.</td>
</tr>
<tr>
<td></td>
<td>• Download or forward quarantined items.</td>
</tr>
<tr>
<td></td>
<td>• Modify administrator authentication.</td>
</tr>
</tbody>
</table>
Authentication modes

Different levels of authentication modes are available for administrators.

- **Directory Server Groups** — Authenticates LDAP groups as administrators. When you assign administrator rights to LDAP groups, all the LDAP group users are automatically assigned administrator rights.

- **Quarantine Manager Accounts** — Administrators authenticated on the McAfee Quarantine Manager server. The McAfee Quarantine Manager server stores the administrator logon information and executes the authentication.

- **Single Sign on via HTTP header** — Uses an HTTP header as the logon ID.

  The Single Sign on via HTTP header mode is used when an external server completes authentication. The external server forwards the request to McAfee Quarantine Manager.

Administrator authentications can switch from one mode to another. When you switch authentication, the previous authentication and domain associations with administrators become invalid. You must also configure the Super Administrator account for the new authentication.

For example, you have McAfee Quarantine Manager administering abc.com and xyz.com domains, and the authentication mode is *Quarantine Manager Accounts*. You are also the Super Administrator with the super@mqm.com ID, and you assigned both domains to the d1@mqm.com Domain Administrator.

When you switch to a different authentication mode, such as LDAP, all the administrator accounts and domain assignments become invalid.

When you create new administrators and assign domains under new authentication, the administrator configuration under *Quarantine Manager Accounts* remains deactivated. The administrators and domains remain on the server.

Use LDAP groups as McAfee Quarantine Manager administrators

Define users that belong to LDAP groups as administrators.

These groups are defined on the LDAP server. When groups on the LDAP server are defined to act as an administrator, any user belonging to the group can act as an administrator.

Enable users that belong to LDAP groups to act as administrators.

- You can configure the LDAP server under *Settings and Diagnostics | Communications*.

- McAfee Quarantine Manager does not support nested LDAP groups to act as administrators.

- For Active Directory, log on to the computer as the group member user that you want to act as an administrator.

**Task**

1. Log on to the McAfee Quarantine Manager administrator user interface using the Super Administrator account that you specified during installation.

2. Click *Administrator Management | Manage Administrator | Administrator Authentication*.

3. Select *Directory Server Groups* and click *Next*.

   A list of registered LDAP groups appears.

4. Select the group.
When prompted to confirm, click Yes.
The Administrator Authentication settings are changed, and you are logged out.

To log on with new credentials, select Click Here.
• For all LDAP groups except Active Directory, specify the logon credentials.
• For Active Directory, you automatically log on using the current Windows account.

Super Administrators can assign LDAP groups to act as Operator and Domain Administrators.
The Alias role is not applicable for Directory Server authentication.

Create administrators with restricted rights
Create Super and Domain Administrator accounts and assign administrator rights.

Task
1 Log on to the McAfee Quarantine Manager administrator user interface using the Super Administrator account.

2 Click Administrator Management | Manage Administrator | Add New Account.

3 On the Account Role and Details page, select Domain Administrator from the Account Role list, then enter the Account Details information.
   a In the Account Name field, enter the administrator name.
   b In the Account Email field, enter the administrator email address that you used to log on to the user interface.

   McAfee Quarantine Manager sends an email notification to the administrator if an SMTP server is configured for the domain.

   c Enter and confirm the account password.

   If you click Finish, the Domain Administrator account is created with access to all Quarantine queues and complete management rights.

4 To display the Visible Quarantine Queues section, click Next.

5 To allow access to all types of quarantined items, select All Queues.
   You can select a parent category to include all child queues. To grant access permissions to specific queues, select the queues and click Next.

   If you click Finish, the Domain Administrator account is created with complete management rights.

6 Under Management Privileges, assign administrator rights.
   To grant all rights to the Domain Administrator, select All Privileges.
   You can apply specific rights by deselecting the rights that you do not want to give the administrator. You can also deselect the rights within a category.

   By default, all rights are enabled.
7 To complete the process of assigning rights and permissions to the Domain Administrator, click Finish.

If any rights or permissions are not granted for a Domain Administrator, the irrelevant options are hidden in the user interface for that Domain Administrator. For example, if Generate reports is not granted to the Domain Administrator, they can't view the:

- Graphical Reports link
- Reports tab in the Dashboard
Domain management includes adding, importing, and exporting domains to McAfee Quarantine Manager, assigning domains, changing the configurations, and creating McAfee Connected product group mapping.

Contents

- Add or import domains to McAfee Quarantine Manager
- Assign domains to Domain Administrators
- Change domain configurations
- Change multiple domain configurations
- Create mapping between domain and groups in connected McAfee products

Add or import domains to McAfee Quarantine Manager

To search or view quarantined items from a specific domain, quarantine items specific to the created domains.

Adding all email domains managed by the organization is mandatory for various McAfee Quarantine Manager features. For example, email digests and user access. Use the Manage Domains section to:

- Add a domain or change a domain configuration.
- Import multiple domains from a CSV file.
- Select and assign Domain Administrators.
- Delete domains.

> If the domain is unregistered, and an item is quarantined, it is grouped under Others.

Tasks

- Add domains on page 46
  Add domains for McAfee Quarantine Manager to manage.
- Import domains in bulk on page 46
  Multiple domains can be imported from .csv or .txt files. In .csv files, domain names are listed in one column.
- Export domains on page 46
  Export all domains registered in McAfee Quarantine Manager to a specified location.
**Add domains**
Add domains for McAfee Quarantine Manager to manage.

**Task**
1. Log on to a Super Administrator or Operator account.
2. Select Administrator Management | Manage Domains | Add Domain.
3. In the Domain Name field, enter the domain name, then click Add.

- The domain name must not exceed 61 characters, and can contain letters, numbers, and dots.
- McAfee Quarantine Manager does not support wildcards and subdomains are explicitly registered.

The domain is listed in the Managed Domains List.

**Import domains in bulk**
Multiple domains can be imported from .csv or .txt files. In .csv files, domain names are listed in one column.

**Task**
1. Log on to a Super Administrator or Operator account.
2. Select Administrator Management | Manage Domains | Import / Export Domains.
3. To locate the file, enter the File Path or click Browse.
4. Click Import.

A report of successful and failed imported domains is generated. The domain is listed in the Managed Domains List. If multiple domains are imported, all domains listed in the .csv file are listed in the Managed Domains List.

**Export domains**
Export all domains registered in McAfee Quarantine Manager to a specified location.

**Task**
1. Log on to a Super Administrator or Operator account.
2. Select Administrator Management | Manage Domains | Import / Export Domains.
3. From the Managed Domains List, select one or more domains, then click Export.
   - Multiple domains are exported in a single text file.
4. On the File download window, click Open to view the domain list as a text file.
5. To save the text file in a specific location, click Save.
6. To return to the previous screen, click Cancel.
Assign domains to Domain Administrators

Assign administrators to one or more domains. To delegate the quarantine management for some domains, create a Domain Administrator and assign the domains.

**Task**
1. Log on to a Super Administrator or Operator account.
2. Select Administrator Management | Manage Domains.
3. From the Managed Domains List, select the domain, then click Assign Administrator.

   - To assign only one domain to Domain Administrators, click Assign on the Domain Admin column.
4. On the Assign Admin configuration area, select the administrators from the Administrators List, then click Add.
5. Click Assign.

   - If the Assigned Administrator(s) List remains empty, Super Administrator manages the domains.
   - When a single domain is assigned, the previously assigned administrators are automatically populated in the Assigned Administrator(s) List.
   - When multiple domains are assigned, the Assigned Administrator(s) List remains empty.
6. To remove the changes and return to the previous screen, click Cancel.

You can select multiple domains and assign a single administrator to all them, or you can select multiple domains and assign multiple administrators. You can also remove an assigned administrator for a domain.

Change domain configurations

Change the user and IP address settings for domains.

**Task**
For option definitions, click ? in the interface.
1. Log on to a Super Administrator or Operator account.
2. Select Administrator Management | Manage Domains.
3. From the Managed Domains List, select the domain, then click Modify Configuration.
4. Select the User and Queue Settings for each detection type, mail server parameters, and digest settings.
5 Under **Mail Settings**, set the parameters for the **Mail Server** to facilitate communication with the users of the selected domain.
   a In the **Server Name/IP Address** field, enter the host name or the IP address of the mail server for this domain.
   b In the **Port** field, specify the mail server.

   ![Info](image)
   By default, the port number (25) is the value specified during setup. You can change it as needed.

   c Select **Use TLS** (Transport Layer Security) to enhance the privacy of emails sent to the users of this domain.

   The TLS protocol allows client and server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography.

   ![Info](image)
   The SMTP server always supports the STARTTLS SMTP extension. Make sure that the corresponding certificate is placed in the required location.

6 In **Digest Settings**, define the parameters for McAfee Quarantine Manager to send digest messages to domain users.

7 Under the **Templates** tab, you can use predefined formats for the email messages sent to users.
   a Enter the sender email address. By default the sender address is McAfeeQuarantineManager@McAfee.com. You can change it as needed.
   b In the **Subject** field, enter the email subject.
   c In the **Mail Format** field, select the format to send the email.
   d If you select **HTML Attachment**, select **Post** or **Get** in the **Form Method** field.

---

**Change multiple domain configurations**

Change the configuration settings for multiple domains.

**Task**

1 Select **Administrator Management | Manage Domains**.

2 From the **Managed Domains List**, select the domains that you want to change, then click **Modify Configuration**.

3 Select the **User and Queue** settings for each detection type, mail server parameters, and digest settings.

   ![Info](image)
   When you change multiple domain templates, all values on the **Templates** tab are blank. Only the changed settings are applied to the selected domains.
Create mapping between domain and groups in connected McAfee products

Assign groups that are registered in connected McAfee products to a domain.

**Task**

1. From the McAfee Quarantine Manager main menu, click **Administrator Management | Manage Domains**.
2. From the **Managed Domains List**, select a domain and click **Modify/View**.
3. On the **Assign Groups** configuration area, select one or more groups from the **Groups List**, then click **Add**.
4. Click **Assign**.

- Administrators that manage the domain can add blacklists and whitelists for the groups assigned.
- When you click **Remove**, the group is assigned to the Super Administrator.
- When you click **Cancel**, you cancel all changes and return to **Manage Domains**.
Domain management
Create mapping between domain and groups in connected McAfee products
Managing user accounts

Managing the user accounts in McAfee Quarantine Manager includes creating, importing, registering, and changing the user accounts. You can also manage user accounts defined on the LDAP server.

Contents
- Create user accounts
- Import users from LDAP
- Import users from a .csv or .txt file
- Import users from an XML file
- Register users automatically
- Change user configuration
- Register a distribution list

Create user accounts

Create user accounts in McAfee Quarantine Manager.

Task
1. Click Start | Programs | McAfee | Quarantine Manager | User UI.
2. Click New user? Click here to register.
3. In the Email Address field, enter the email address that belongs to the domain managed by McAfee Quarantine Manager.
4. Click Register.

The user is created and an email is sent to the email address specified during registration with your logon credentials. The user name is listed on the User Management screen, under End User Management | Account Management.

Import users from LDAP

Import users that are registered with LDAP servers into McAfee Quarantine Manager.

Before you begin
Make sure that the authorization mode is set to LDAP Server Accounts.

To facilitate user authentication, user synchronization, and the expansion of distribution lists, configure, and establish connectivity with an LDAP server.
Task
1 From the McAfee Quarantine Manager main menu, click Settings and Diagnostics | Communications | LDAP Server.
   Each LDAP server type has parameters that you must define to facilitate communication with the McAfee Quarantine Manager server.
2 From the Server Type drop-down list, select the server type.
3 To check for connectivity, click Test.
   To assign administrator rights to users on an LDAP server, you can synchronize the user list on the McAfee Quarantine Manager LDAP server.
4 From the McAfee Quarantine Manager main menu, click End User Management | General.
5 From User Synchronization Settings, configure the options.
   • The registration notification for a user is sent only if that domain has a valid SMTP server specified for the domain in Settings and Diagnostics | Communications.
   • To customize the user registration email content, select Administrator Management | Domain Management | Your Domain | Modify Configuration | Templates.
6 Create a user synchronization task to import users from the LDAP server.

See also
Synchronize and register user lists automatically on page 60

Import users from a .csv or .txt file
 Register multiple users by importing a delimited text file containing the list of users. The supported file formats are .csv and .txt.

Only users from domains registered in McAfee Quarantine Manager are added. To add domains, select Administrator Management | Manage Domains.

Task
1 From the McAfee Quarantine Manager main menu, select End User Management | User Management | General.
2 In User Import, configure the settings.
   a To select the delimited file for the user list to import, click Browse.
   b If the file to import contains a header row, select Input file contains header.
   c From the Column delimiter drop-down list, select the character.
      Imported email addresses must not contain the delimiter characters.
   d In the Column number containing user list field, enter the column number that contains the user email addresses.
To notify successfully registered users, select **Send registration notifications**.
User notifications are sent only if the domain has a valid SMTP server configured for the domain using **Settings and Diagnostics | Communications**.

To customize the user registration email content, select **Administrator Management | Domain Management | Your Domain | Modify Configuration | Templates**.

3 To import the user list and generate accounts, click **Create Users**.

> Multi-byte characters, such as Arthur_brown@63-250-236-237-microsoft.com, are supported only if the imported file is in UTF-8 format.

### Import users from an XML file

To import users and corresponding configuration settings, use the Blacklists and Whitelists import function.

> Only users from domains registered in McAfee Quarantine Manager are added. To add domains, select **Administrator Management | Manage Domains**.

**Task**

1 From the McAfee Quarantine Manager main menu, select **Blacklists and Whitelists | Import and Export**.

2 In the **Import** configuration area, click **Browse** to locate the configuration file with the user configuration that you want to import.

3 To merge the new configuration imported with the earlier user configuration, select **Merge user configuration**.

> If you do not select this option, the user configuration is overwritten.

4 Click **Import Configuration**.

### Register users automatically

Configure the settings that allow users to automatically register using information available in the quarantine database.

**Task**

1 From the McAfee Quarantine Manager main menu, select **Administrator Management | Manage Domains**, then select the domain.

2 Click **Modify Configuration**.

3 On the **General** tab, select **Automatically register users from the quarantined database during Digest operation**.

> If this feature is enabled in McAfee Quarantine Manager, the corresponding **Recipient Check** feature is enabled in the products connected to McAfee Quarantine Manager.
There are four possible scenarios using these parameters.

- If you select only **Automatically register users from the quarantined database during Digest operation**:  
  - The user automatically registers during a scheduled digest activity.
  - A digest email is sent to the user email address.

- If you select **Send confirmation email before sending digest email** and **Automatically register users from the quarantined database during Digest operation**:  
  - A confirmation email is sent to the user with a link for registration.
  - After the user clicks the link and confirms the email address, a digest email is sent to the user.

- If you select **Send registration notifications** and **Automatically register users from the quarantined database during Digest operation**:  
  - The user automatically registers and receives an email with the user credentials.
  - The digest email is also sent to the user email address.

- If all options are selected:  
  - The user receives a confirmation email with a link to confirm the user email address.
  - When confirmed, the user receives an email with the user credentials.
  - The user then receives a digest email on completion of the next scheduled digest.

4. For all settings to take effect, click **Apply**.

5. To revert to the previous settings, click **Cancel**.

---

**Change user configuration**

Change the settings for MQM-registered users.

**Task**

1. From the MQM main menu, select **End User Management | User Management | Account Management**.

2. Configure the search options to locate the users you want to change.
   a. In **Include**, select the user categories to include in the search.
      
      You can select multiple options in **Account Type**. To search for users in all categories, select all options.
   b. To use the search function, select the first letter of the user account. For example, select **K** to search all accounts starting with K. To search for all user accounts, click **All**.
   c. To search by a user email address, enter it in the **Email address** field, then click **Search**.
      
      The available wildcard options include:
      
      - \* — Matches any number of characters
      - ? — Matches a single character

3. Select the user that you want to change, then click **Modify**.
   a. In **Blacklist**, enter the sender email address, then click **Add**.
   b. Click **Whitelist**, enter the sender email address, then click **Add**
c  Click Email Aliases, enter the email addresses in the Name field, then click Add.

These options are displayed only if the Quarantine Manager Account authentication mode is selected. For LDAP Server Accounts, email alias options are disabled.

The table displays the name under which the available alias members of the user are listed. The State column displays the current state of the alias email address.

d  Click Settings, then configure the password and digest settings.

To customize digest email content, select Administrator Management | Domain Management | Your Domain | Modify Configuration | Templates.

e  Click Email Reassignment, enter the email address, then click Reassign Emails.

To continue redirecting the emails to the new user, select Save Reassignment. If this option is not selected, any future quarantined emails are sent to the previous account.

Register a distribution list

When emails are sent to distribution lists, McAfee Quarantine Manager quarantines the email. McAfee Quarantine Manager creates a copy of the email and sends it to each user on the distribution list. When users receive the email, they can release, delete, or blacklist it.

Before you begin

Configure the LDAP server in Settings and Diagnostics | Communications.

McAfee Quarantine Manager does not support nested distribution lists.

Task

1  Under Server Type, select the required type of server from the drop-down list.

2  Select End User Management | Distribution List | Get Distribution List from LDAP server.

3  Select the distribution list, then click Register.

4  Select Settings and Diagnostics | Task Manager.

5  To pull the registered distribution list users to McAfee Quarantine Manager, schedule a User Synchronization Task.
Managing quarantined items

View all email messages that contain detected and quarantined potential threats. You can use filters to refine the search and find quarantined items, view the results, and take necessary action.

Contents
- Search quarantined items
- Taking action on quarantined items

Search quarantined items

View information about all email messages that contain potential threats that were detected and quarantined. You can use the filters to refine your search and find the quarantined items with the required information.

There are three fields to select the primary filters. You can select a search option in one field or a combination of options in two or three fields.

Task
1. On the Administrator screen, click Quarantine Management.
2. On the Quarantined Items page, click the drop-down icon next to a field, then select up to three filters.
3. Click Search.

The quarantined items matching your search criteria are displayed in the View Results grid.

Taking action on quarantined items

Select quarantined items to release, delete, or blacklist. More advanced actions are also available.

Task
1. On the View Results grid, select the quarantine items.
2. From the More Actions drop-down list, select an option, then click Go.
3. To release the quarantined email, click Release.
4. To remove the quarantined email, click Delete.
5. To add the quarantined email to the blacklist, click Blacklist.
Managing quarantined items
Taking action on quarantined items
Managing tasks

You can view, manage, or schedule tasks. Tasks are configurable actions that are performed at convenient times. You can configure and schedule a task to run later, or run an urgent task immediately.

There are certain tasks you must complete on a regular basis. For example, you can schedule a task to automatically purge the MQM database and remove old quarantined items.

When you use LDAP authentication, you must synchronize MQM with the users list defined in your LDAP server. Also, you must perform user-based tasks immediately, which include:

• Immediately send a quarantine summary to a user
• Delete user-quarantined items
• Send an urgent email to a user from MQM

Contents

» Configure a scheduled digest email
» Configure scheduled database purges
» Synchronize and register user lists automatically
» Send status reports automatically
» Synchronizing distribution lists

Configure a scheduled digest email

Schedule the delivery of digest emails to all users that include a synopsis of quarantined items for a particular time period, and detailed summaries of quarantined items, blacklists, and whitelists.

Task

1 In MQM, select Settings and Diagnostics | Task Manager | Scheduled Tasks.

2 In Task Type, select Email digest.

3 In Apply to Domains, select the domains. To send the email digest to all domain users, select Select All.

4 In When, select when to send the email digest

5 In the Task Name field, enter the task name.

6 To schedule the task based on the options selected, click Add.
   The Task successfully added message appears.

7 To confirm, click OK.

The email digest task is added to the Scheduled Tasks list.
Configure scheduled database purges

Periodically clear the database by removing old data, such as old log entries and quarantined items. Purging the database helps you to manage disk space.

Task
1. In MQM, select Settings and Diagnostics | Task Manager | Scheduled Tasks.
2. In Task Type, select Database Purge.
3. In Apply to Domains, select the domains. To purge the database of all domain users managed in MQM, select Select All. To purge the database of domain users not managed in MQM, select Others.
4. In the When field, when to purge the database.
5. In the Task Name field, type the task name.
6. To schedule the task based on the options selected, click Add.
   - The Task successfully added message appears.
7. To confirm, click OK.

The database purge task is listed on the Scheduled Tasks list.

Synchronize and register user lists automatically

Synchronize the list of LDAP server users and automatically register them for MQM. You can also synchronize added or changed user accounts in the LDAP distribution lists registered with MQM.

When you select the Delete users not found in the LDAP server option, the following task deletes all the users no longer available on the LDAP server.

Task
1. In MQM, select Settings and Diagnostics | Task Manager.
2. In Task Type, select User Synchronization.
3. In the When field, enter when to synchronize the user list.
4. In the Task Name field, enter the task name.
5. To confirm, click OK.

The User Synchronization task is added to the Scheduled Tasks list.
Send status reports automatically

Send a status report email to administrators providing detailed information about database sizing, counter status, task activities, and errors occurred.

**Task**

1. In MQM, select Settings and Diagnostics | Task Manager | Scheduled Tasks.

2. In Task Type, select Status Email.

3. In Apply to Domains, select the domains. The domains you select are sent the status email that contains the quarantined activities of the domain users. To send the status report to all Domain Administrators managed in MQM, select Select All. To send the status email to Domain Administrators not managed in MQM, select Others.

4. In the When field, select the task application time.

5. In the Task Name field, enter the task name.

6. To schedule the task based on the options selected, click Add.

   The Task successfully added message appears.

7. To confirm, click OK.

The Status Email task appears in the Scheduled Tasks list.

Synchronizing distribution lists

Create regular distribution list synchronization tasks.

**Task**

1. In MQM, select Settings and Diagnostics | Task Manager | Scheduled Tasks.

2. In Task Type, select DL Synchronization.

3. In the When field, select the task application time.

4. In the Task Name field, enter the task name.

5. To schedule the task based on the options selected, click Add.

   The Task successfully added message appears.

6. To confirm, click OK.

The task appears in the Scheduled Tasks list.
Managing tasks
Synchronizing distribution lists
11 User submissions

You can identify spam, phish, and other unwanted messages in your inbox, as well as incorrectly quarantined messages, and submit them to the McAfee Quarantine Manager administrator for release. You must submit any quarantined item type to the McAfee Quarantine Manager administrator when you believe that messages should be released from the quarantine or submitted to McAfee Labs for analysis.

The McAfee Quarantine Manager administrator uses user submissions to search for and act on messages that are submitted:
- By users for falsely identified spam
- As spam
- For release (the message is not spam or other type of undesirable object)

Contents
- Manage user submissions
- View search results

Manage user submissions

To search and view user submissions, you must assign various filter levels.

Task
1. From the McAfee Quarantine Manager menu, click Quarantine Management | User Submissions.
2. From the Queue drop-down list, select the type of submission.
3 Select up to three first-level filters.

4 To search by domain, select the domain from the Domain drop-down list.

5 Specify the time range.

6 Click Search. A list of items matching your search criteria is displayed in the View Results section.

View search results

Execute actions on selected quarantined items.

Task

• Under View Results, execute actions on selected quarantined items.
User interactions

Manage your quarantined email messages, submit spam samples to McAfee, and manage your McAfee Quarantine Manager account from the McAfee Quarantine Manager user interface.

As a user, you can access the McAfee Quarantine Manager user interface to:

- Maintain your McAfee Quarantine Manager account.
- View and manage your quarantine items.
- View and maintain a personal blacklist and whitelist.
- Release messages that were incorrectly quarantined.
- Submit missed spam messages to McAfee Labs for testing, so that similar messages can be recognized and quarantined.

Contents

- Log on to McAfee Quarantine Manager
- Manage quarantined emails from the interface
- Manage quarantined emails through digest emails
- Submit spam samples to McAfee Labs
- Manage your McAfee Quarantine Manager account

Log on to McAfee Quarantine Manager

Log on to McAfee Quarantine Manager to change and manage your account.

Task

1. In a web browser, go to http://<MQMServer>/MQMUserUI/<LocalID>/LogOn.html to open the user interface.

2. Log on as a user.
   - LDAP Authentication — If your organization uses an LDAP server, and your administrator has enabled LDAP authentication, you can log on to McAfee Quarantine Manager with the LDAP account user name and password.
   - Quarantine Manager authentication — If your administrator has enabled Quarantine Manager Account authentication, you can log on to McAfee Quarantine Manager with a user name and password of your McAfee Quarantine Manager account.
If you are using McAfee Quarantine Manager for the first time, and your organization uses McAfee Quarantine Manager authentication, generate your McAfee Quarantine Manager logon:

a. Click New user? Click here to register.

b. On the User Registration dialog box, enter your Email Address, then click Register.

A confirmation message appears, stating that an account is created and a default password has been sent to your email address. Click OK to confirm.

c. To complete the process, click Click here to return to the Login page and use the credentials received in the email to log on to McAfee Quarantine Manager.

The Quarantine Items page is displayed by default. This page lists the emails you received which are detected and quarantined. You can use search filters to find the quarantined items that are of interest to you. You can also use this page to analyze the quarantined emails and release the items, add them to the blacklist or whitelist, or submit to McAfee for analysis.

---

**Manage quarantined emails from the interface**

View a list of received emails that are detected and quarantined, so that you can analyze them and take action.

You can complete these management tasks:

- Release items to your mailbox that were quarantined by mistake.
- Delete spam messages and blacklist the senders.
- Delete selected or all items without any further action.
- Add trusted senders to your whitelist.
- Use search filters to find the quarantined items that are of interest to you.

**Task**

1. Log on to the McAfee Quarantine Manager user interface.
2. In View Results, view the list of your quarantined emails.

   By default, 20 items per page are displayed. To specify records per page, select 10, 20, 50 or 100 from the drop-down list. Use Next, Previous, First, and Last to navigate the pages.

3. To add or remove columns, click Columns to Display, then select the columns.
4. Select one or more emails, then choose the action.
   
   If the queues are not selected, or the results set does not contain an items from those queues, some of the actions might not appear. For example, if you do not select Spam under Queue in search filters, actions such as Submit as Non-Spam, Whitelist and Release, and Submit as Non-Spam and Whitelist do not appear. To select or deselect all items in the grid, use the checkbox on the header row.
5. To find quarantined items, create search filters.
   
   a. Select a comparison criteria for each filter.
   
   - **IS** — Matches a value equal to the specified value.
   - **IS NOT** — Match a value NOT equal to the specified value.
Specify a match value using these wildcards:

- * — Matches to any number of characters.
- ? — Matches a single character.
- \ — Matches any \ character in the search field.

Select the operator to use multiple search filters.

- AND — Considers both the former and the latter filters.
- OR — Considers either the former or the latter filters.

Repeat the steps to use additional filters.

Select All Dates, or a desired Date Range from the drop-down lists.

Select a queue to search quarantined items based on their classification.

To start the search based on the selected criteria, click Search. To return to the default filter settings, click Clear Filters.

You can use a maximum of three filters using the AND or OR operators. For example, to get a list of Quarantined Items with a subject that includes Quotation, which are sent by xyz@abc.com:

- Select Subject.
- Select Is, then enter Quotation.
- Select And | Sender.
- Select Is, then enter xyz@abc.com.
Manage quarantined emails through digest emails

Manage your quarantine emails using digest email actions.

The digest email is a customizable condensed report of all your quarantined items, black-white lists, and related quarantine activities. The information in the digest email depends on administrator configurations.

Task
1. Open the digest email.
2. Complete the digest email actions.

A response message appears for each action, as configured by your administrator.

Submit spam samples to McAfee Labs

Submit sample spam email messages to McAfee Labs. Before you submit the sample, save the email as an .eml file. Submit spam samples when spam emails are released to your mailbox by mistake and you want to submit it for analysis.

Before email messages are sent to McAfee Labs, administrators review them.
The McAfee Labs team analyzes the email message and identifies its traits. The more email messages submitted for correction, the better the message filtering.

To submit spam samples:
- Send a disk containing spam samples to your administrator
- Use the Submit Spam or Phish toolbar option in your email client
- Use the Submit Spam Sample page in your McAfee Quarantine Manager interface

**Tasks**
- Submit spam samples from a disk on page 69
  Submit spam samples using spam samples saved as .eml files on your computer.
- Submit spam samples with the McAfee Customer Submission Tool on page 69
  Submit spam samples from Microsoft Outlook using the McAfee Customer Submission Tool.
- Submit samples quarantined by mistake on page 70
  Submit samples of quarantine emails that are considered spam by mistake, and that you are sure were sent from trusted sources.

**Submit spam samples from a disk**
Submit spam samples using spam samples saved as .eml files on your computer.

**Task**
1. From your email client, save the emails as .eml files.
2. Log on to the McAfee Quarantine Manager user interface.
3. Click Submit Spam Sample | Browse, then locate the .eml files.
4. To send the spam samples to your administrator, click Submit.
   The administrator reviews the email messages, then submits them to McAfee Labs. The McAfee Labs team analyzes the email messages to identify the traits.

**Submit spam samples with the McAfee Customer Submission Tool**
Submit spam samples from Microsoft Outlook using the McAfee Customer Submission Tool.

**Before you begin**
The McAfee Customer Submission Tool must be installed by your administrator.

**Task**
1. From Microsoft Outlook, select the emails you want to submit.
2. On the toolbar, click one of these spam options.
   - Submit Spam
   - Submit Non- Spam
3. On the Submit Spam or Phish window, select the actions, then click OK.
   The administrator reviews the email messages you submit, then submits them to McAfee Labs. The McAfee Labs team analyzes the email message to identify traits.
Submit samples quarantined by mistake
Submit samples of quarantine emails that are considered spam by mistake, and that you are sure were sent from trusted sources.

Task
1 Log on to the McAfee Quarantine Manager user interface.
2 Select the quarantined email considered as spam by mistake.
3 Select More Actions | Submit as Non-Spam, then click Go. The administrator reviews the email message, then submits it to McAfee Labs. The McAfee Labs team analyzes the email messages and identifies the traits.

Manage your McAfee Quarantine Manager account
Manage the various settings in your McAfee Quarantine Manager account.
You can manage these McAfee Quarantine Manager account tasks:
• Maintain your blacklist and whitelist by adding or removing email addresses.
• So your quarantined items are in one place, add alternative email addresses.
• Change your password.
• Specify how many days you want to keep quarantined items. This limit can be overridden by the limit specified by your administrator.
• View the list of user quarantined items that you manage.

Tasks
• Manage your blacklist on page 70
  Manage your blacklist, which contains the email addresses that frequently send you spam messages or unwanted emails.
• Manage your whitelist on page 71
  Manage the whitelist, which contains the trusted sender email addresses. For example, business partners whose emails you want to receive.
• Change your password on page 71
  Change your account password.
• Configure quarantine report preferences on page 72
  Specify the preferences to receive quarantine activity reports.
• Manage aliases on page 72
  Manage your email aliases. Use email aliases when you have more than one email address.
• View email reassignments on page 72
  View the list of users and quarantine items that you manage.

Manage your blacklist
Manage your blacklist, which contains the email addresses that frequently send you spam messages or unwanted emails.

Task
1 Log on to the McAfee Quarantine Manager user interface.
2 Select Your Account | Blacklist.
3 To add email addresses to the list, enter the address in the Email Address field, then click Add.

The email address appears on the Members list.

4 To delete an individual email address from the blacklist, click ✗. To delete all email addresses on the blacklist, click Delete All.

A confirmation message appears.

5 On the dialog box, click OK to complete the deletion. To discard the changes, click Cancel.

6 To save the changes, click Apply.

**Manage your whitelist**

Manage the whitelist, which contains the trusted sender email addresses. For example, business partners whose emails you want to receive.

**Task**

1 Log on to the McAfee Quarantine Manager user interface.

2 Select Your Account | Whitelist.

3 To add email addresses to the list, enter the address in the Email Address field, then click Add.

The email address appears in the Members list.

4 To delete individual email addresses from the whitelist, click ✗. To delete all email addresses from the whitelist, click Delete All.

A confirmation message appears.

5 In the dialog box that appears, click OK to complete the deletion. To discard the changes, click Cancel.

6 To save the changes, click Apply.

**Change your password**

Change your account password.

**Task**

1 Log on to the McAfee Quarantine Manager user interface.

2 Select Your Account | Settings.

3 In the New password field, enter the password.

- Your password must be alphanumeric and contain at least 8 characters. You cannot change the password if the authentication mode is set to LDAP User Accounts.

4 In the Confirm new password field, retype the password.

5 To save the changes, click Apply.
Configure quarantine report preferences
Specify the preferences to receive quarantine activity reports.

Task
1. Log on to McAfee Quarantine Manager user interface.
2. Select Your Account | Settings.
3. In Configuration Settings, specify your digest email preferences.
   - To ensure that you receive email digests about your quarantined items and black-white lists, select I want to receive Digest Reports on quarantine activity.
   - To ensure that you receive email digests on every scheduled digest activity, even if you do not have quarantine items in your account, select Send a digest even when there are no quarantined items.
4. To save the changes, click Apply.

Manage aliases
Manage your email aliases. Use email aliases when you have more than one email address.
For example, the company you work for changes your email address, and you want your old email address to remain active. If you add the old address as an alias, quarantined emails for either address reside in the same place. When you add an alias, the activation code is sent to the alias address. Until you supply the activation code, the changes show as pending activation and are not operational.

If your administrator enables LDAP authentication, you can view any email aliases that exist for you in the LDAP server, but you cannot change them or add new aliases.

Task
1. Log on to the McAfee Quarantine Manager user interface.
2. Select Your Account | Email Aliases.
3. In the Name field, enter the email alias, then click Add.
   - The alias appears in the list, and you are prompted for an activation code.
4. To send the activation code to your email address, click Apply.
5. In the Enter the activation code here field, enter the activation code, then click Activate.
6. Click OK.
7. To delete the email alias, click X next to the alias in the Delete column.
8. To save the changes, click OK | Apply.

View email reassignments
View the list of users and quarantine items that you manage.

Task
1. Log on to the McAfee Quarantine Manager user interface.
2. Select Your Account | Email Reassignment.
Maintenance and reporting

Keep your blacklists and whitelists up-to-date, and manage McAfee Quarantine Manager critical functions using the dashboard and reports.

Chapter 13  Server maintenance
Chapter 14  Blacklist and whitelist management
Chapter 15  Dashboard and graphical reports
Maintenance and reporting
13 Server maintenance

Manage server configurations, create database backups, release emails in bulk, and create McAfee connected products reassignment maps.

Contents

- Managing server configurations
- Back up the database

Managing server configurations

Set the parameters for the Product Log, Diagnostics, Communications, and Advanced Settings.

Tasks

- View log entries on page 75
  View the health of the McAfee Quarantine Manager server using event, warning, and error log entries.
- Configure log settings on page 76
  Specify the type of logging required, the level of debug tracing, and configure the error report settings.
- Configure communication between MQM and other products on page 76
  Configure the settings for MQM to communicate with McAfee products, LDAP servers, and mail servers.
- Configure advanced server settings on page 78
  Configure the McAfee Quarantine Manager advanced preferences. You can configure the preferences for ePolicy Orchestrator events, McAfee Labs submissions, session timeout, and dashboard refresh intervals.
- Configure certificates for secure SMTP communication on page 81
  Configure certificates for the secure (TLS) SMTP communication.

View log entries

View the health of the McAfee Quarantine Manager server using event, warning, and error log entries. Use the search filters to find log entries. Find information about an initiated or ended task, connected or disconnected product, or an error regarding failure to push configuration settings to a product.

Task

1. From the McAfee Quarantine Manager main menu, click Settings and Diagnostics | Product Log.
2. Configure the search filters.
   a. Select a comparison criteria for each filter.
   b. Select an appropriate logical operator to use multiple search filters.
3 Select the dates for which you want to view the log.

4 Click Search.

5 The View Results section displays the product log entries for events, warnings, and errors.

**Configure log settings**

Specify the type of logging required, the level of debug tracing, and configure the error report settings.

**Task**

1 From the McAfee Quarantine Manager main menu, click Settings and Diagnostics | Diagnostics | Logging, then configure the available options.

2 Click the Debug Tracing tab, and configure the options.
   a From the Level drop-down list, select the debug trace level.
   b From the Location drop-down list, select where the debug trace files are written.
   c To export the debug trace files on to the disk, click Download.
   d In the Maximum File Size (MB) field, enter the maximum debug trace file size.
   e To specify a limitless size, select No Limit.

3 In Logging, select whether you want to log information, warning, and error events using the product log, or the Windows Event Log.
   By default, events are logged in the product log.

4 Click the Error Reporting tab, and configure the options.
   a To enable or disable the error reporting service, select Enable.
   b To enable or disable the information capture for exceptional events (fatal exceptions), such as system crashes, select Catch Exceptions.
   c To enable or disable unhandled exceptions to the administrator reports, select Report Exceptions on Screen.

**Configure communication between MQM and other products**

Configure the settings for MQM to communicate with McAfee products, LDAP servers, and mail servers.

**Task**

For option definitions, click ? in the interface.

1 Log on to McAfee ePO as an administrator.

2 From the MQM main menu, click Settings and Diagnostics | Communications | Default, then configure the options.

3 In McAfee Products, set the port number you want use to connect to.
4 Click **Mail Server**, specify the details of the SMTP server that communicates with users.
   - **Address** — The IP Address or DNS Host Name of the mail server.
   - **Port Number** — The number of the port used for outgoing email communication. Default port number is 25.
   - **TLS** — Use Transport Layer Security to secure email communication for all email communications.

   If you select TLS, ensure the mail server certificate is in the MQM installation folder.

5 Click **LDAP Server** and configure the options.
   Multiple LDAP servers can be configured.
   a From the **Server Type** drop-down list, select the LDAP server.
   b In the **Server** field, enter the LDAP server IP address or domain name.
   c In the **Port** field, enter the port number used to communicate with the LDAP server.
   d For a secure connection, select **Use SSL**.
   e In the **Username** field, enter the LDAP server user name.
   f In the **Password** field, enter the user password.
   g In the **Base DN** field, enter the organizational unit name in the LDAP server.
   h In the **Distribution List Object Class** field, enter the distribution list object class ID for the Open LDAP server.
   i In the **Members attribute name for Distribution List Object Class** field, enter the Distribution List Object Class members attribute.
   j To check the connectivity with the LDAP server, click **Test**.
   k To save the settings, click **Apply**.
   l To clear all changes and return to the default settings, click **Cancel**.

6 Click **Advanced**, then configure the options.
   a In the **Thread Pool Size** field, enter the number of simultaneous threads to run for processing incoming quarantined items, then restart MQM.
   b In the **Maximum Communication Retry** field, enter the number of times the MQM server establishes communication with a connected McAfee product while pushing configurations or releasing quarantined emails.
   c In the **Configuration Push Interval (seconds)** field, enter the interval between blacklist, whitelist, and user group updates on connected McAfee products.
   d In the **Item Push Interval (seconds)** field, enter the interval between the updates of quarantined items for release on connected McAfee products.

**See also**
*Configure certificates for secure SMTP communication on page 81*
Configure advanced server settings

Configure the McAfee Quarantine Manager advanced preferences. You can configure the preferences for ePolicy Orchestrator events, McAfee Labs submissions, session timeout, and dashboard refresh intervals.

**Tasks**

- *Configure the McAfee ePO settings on page 78*
  Configure the generation of McAfee ePO events and the frequency of MQM event generation that creates McAfee ePO reports.

- *Configure the database settings on page 79*
  For optimal database performance, configure the database settings.

- *Configure server communication with McAfee Labs on page 79*
  Provide SMTP server details to allow MQM to make submissions to McAfee Labs. This is the SMTP server that sends emails outside your network.

- *Configure email notification-related settings on page 79*
  Specify the sender and recipient email addresses for MQM notification emails.

- *Configure miscellaneous settings on page 80*
  Configure the parameters for miscellaneous settings.

- *Configure status email report settings on page 80*
  Preview, edit, and customize the status email that is sent to administrators.

- *Release emails in bulk on page 81*
  Define parameters to release emails in bulk. You can release more than 100 emails.

- *Reassign quarantined email releases to different products on page 81*
  Enable releases of quarantined emails of one McAfee product through another. MQM releases an email through the McAfee product that quarantined the email.

**Configure the McAfee ePO settings**

Configure the generation of McAfee ePO events and the frequency of MQM event generation that creates McAfee ePO reports.

**Task**

For option definitions, click ? in the interface.

1. In MQM, select **Settings and Diagnostics | Advanced Settings**.
2. To generate McAfee ePO events, select **Generate ePolicy Orchestrator Events**.
3. In the **ePolicy Orchestrator Event(s) Generating Interval (minutes)** field, enter the interval.
   The default is 10.
4. Restart the McAfee Quarantine Manager service.

You can view event reports in McAfee ePO.
Configure the database settings
For optimal database performance, configure the database settings.

**Task**
1. In MQM, select **Settings and Diagnostics | Database Management**.
2. In the **Maximum Item Size (MB)** field, enter the maximum size of a quarantined item that the database can accept.
   
   If the size of the quarantined item exceeds the size you specify, the item returns to the McAfee product. MQM supports a 100 MB maximum sample size.
3. In the **Maximum Query Size** field, enter the maximum number of rows that are returned from a query.
   
   To find more items than the number specified, you can navigate through the search results. When you click **Delete All** on the results table, only the number of items equal to the maximum query size are deleted.
   
   The default is 1000.
4. From the **For reporting store the meta-data for** list, select the maximum number of days the meta-data is stored and available for report generation.
   
   All graphical reports are based on the **For reporting store the meta-data for** parameter.
   
   The default is **90 Days**.

Configure server communication with McAfee Labs

Provide SMTP server details to allow MQM to make submissions to McAfee Labs. This is the SMTP server that sends emails outside your network.

For example, Administrators select user submitted items as non-spam. MQM uses the SMTP server to send submissions to McAfee Labs for further analysis.

**Task**
1. In MQM, select **Settings and Diagnostics | Advanced Settings**.
2. In the **Port** field, enter the port number that the SMTP server uses to enable McAfee Labs communication.
   
   The default is 25.
3. In the **IP Address** field, enter the SMTP server IP address that routes the submissions to McAfee Labs.
4. In the **Message From** field, enter the email address of the email sent to McAfee Labs.
   
   The default sender email address is McAfeeQuarantineManager@McAfee.dom.

Configure email notification-related settings

Specify the sender and recipient email addresses for MQM notification emails.

For example, notifications can include:
- The MQM server stops operating when the database is down.
- Due to a server failure in cluster environment, switch over to a standby server.

**Task**
1. In MQM, select **Settings and Diagnostics | Advanced Settings**.
2. Enter the sender email address.
   
   By default, the sender email address is McAfeeQuarantineManager@McAfee.dom. You can change this email address to help you identify the auto-generated email from MQM.
3. Enter the recipient email address.
   We recommend using the MQM administrator email address.

4. Customize the MQM URL used in email communications.
   - **Server Name** — IP address or domain name resolves to the server where MQM is installed.
     For example: domain.dom. If the MQM website runs on a custom port, specify the path as domain.dom:port number.
   - **Protocol** — Select HTTP or HTTPS to specify whether secured connection is required for domain access. The protocol depends on the configuration settings on the Microsoft Internet Information Services server.
   - **Sample End User Interface URL** — Preview a sample custom URL based on the options selected.
     For example, https://domain.dom/MQMUserUI. The domain name is domain.dom. and the protocol is http.

### Configure miscellaneous settings
Configure the parameters for miscellaneous settings.

The **Settings** tab is only available to Super Administrators and Operators. If you log on as a Domain Administrator, the tab does not appear.

**Task**
1. In MQM, select **Settings and Diagnostics** \| **Advanced Settings**.
2. In the **Administrators UI Session TimeOut (seconds)**, enter the number of seconds the administrator interface remains idle before the server closes it automatically.
   The default is 600.
3. In the **End-User UI Session TimeOut (seconds)** field, enter the number of seconds the user interface remains idle before the server closes it automatically.
   The default is 600.
4. In the **Dashboard Refresh Interval (seconds)** field, enter the dashboard counter refresh interval.
   The default is 60.

### Configure status email report settings
Preview, edit, and customize the status email that is sent to administrators.

**Task**
1. In MQM, select **Settings and Diagnostics** \| **Advanced Settings**.
2. Enter the status email report information.
   a. In the **Sender's Email Address** field, enter the sender email address.
   b. In the **Recipient's Email Address** field, enter the recipient email address.
   c. In the **Subject** field, enter the email subject.

   A window with the email content HTML code appears. You can edit the email content. If you do not want a particular token in the email, search for the tag containing the token and delete the tag. For example, to delete counter information, delete '%COUNTER_LIST%'.

---

80 McAfee Quarantine Manager 7.1.0 Product Guide
Release emails in bulk
Define parameters to release emails in bulk. You can release more than 100 emails.

**Task**
1. In the administrator UI, click Settings and Diagnostics | Communications | Advanced Settings | McAfee Products Operations.
2. To search for emails to be released in bulk, use a single search filter or a combination of filters.
3. Select All Dates, or select Date Range and specify a range of dates.
4. From the Domain drop-down list, select the domain.
5. To release multiple items, click Release.
6. To clear all selected filters, click Clear Filter.

**See also**
*Search quarantined items on page 57*

Reassign quarantined email releases to different products
Enable releases of quarantined emails of one McAfee product through another. MQM releases an email through the McAfee product that quarantined the email.

Reassign quarantined email releases to different products when a McAfee product is upgraded or unavailable.

Only Super Administrators and operators can reassign McAfee Product IDs. If you log on as a Domain Administrator, this option does not appear.

**Task**
1. In MQM, click Settings and Diagnostics | Advanced Settings | McAfee Products Operations.
2. On the Advanced Settings screen, select Enable McAfee Product Reassignment.
3. In the Old McAfee Product ID field, enter the McAfee product ID of the quarantined items.
4. In the New McAfee Product ID field, enter the McAfee product ID that executes the release.
5. To save, click Reassign.

The emails are sent to the reassigned McAfee product.

Configure certificates for secure SMTP communication
Configure certificates for the secure (TLS) SMTP communication.

To install on the SMTP server, the Transport Layer Security (TLS) communication needs a valid certificate signed by a valid CA (certificate authority). McAfee Quarantine Manager must have the CA certificate installed when the TLS option is enabled for sending emails.

Ensure that the certificate is PEM format.
**Task**

1. In the McAfee Quarantine Manager installation directory, navigate to `\bin\certs`.
2. Create a file. Use the name `ca.pem`.
3. Open the CA certificate file and copy the contents to `ca.pem`.

   If you have certificates from different CAs, copy the contents of all the CA certificates to the `ca.pem` file.

**Back up the database**

When a data loss occurs, you can restore McAfee Quarantine Manager using a backup the existing database. The database backup saves the following settings.

**Table 13-1  Database backup settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Quarantine Manager user account</td>
<td>Saves user information and email aliases.</td>
</tr>
<tr>
<td>Blacklists and whitelists</td>
<td>Saves the global blacklists and whitelists maintained by administrators.</td>
</tr>
<tr>
<td>Dashboards</td>
<td>Saves the report, McAfee Quarantine Manager server, and quarantined item dashboard data.</td>
</tr>
<tr>
<td>Quarantined data</td>
<td>Saves the quarantined data McAfee Quarantine Manager stores in the database.</td>
</tr>
</tbody>
</table>

**Tasks**

- *Back up the Microsoft SQL Server database on page 82*
  Back up the McAfee Quarantine Manager database stored in Microsoft SQL server.
- *Restore the Microsoft SQL Server database on page 83*
  In case of data loss, restore the McAfee Quarantine Manager database from an Microsoft SQL Server database backup.
- *Back up the MySQL database on page 83*
  Back up your existing MySQL database, which comes packaged with McAfee Quarantine Manager.
- *Restore the MySQL Database on page 84*
  In case of data loss, restore a MySQL database backup.
- *Configure a scheduled backup task for MySQL Database on page 84*
  Schedule a backup for your MySQL database, which comes packaged with McAfee Quarantine Manager.

**Back up the Microsoft SQL Server database**

Back up the McAfee Quarantine Manager database stored in Microsoft SQL server.

**Task**

1. Click **Start** | **Run**, type `services.msc`, then click **OK**.
2. From the **Services** window, stop the McAfee Quarantine Manager service.
3 Log on to Microsoft SQL Server Management Studio.

4 Navigate through the databases and select the McAfee Quarantine Manager database.

5 Right-click the database and select Tasks | Back Up.

6 On the Backup Database screen, configure the settings.
   a From the Backup type drop-down list, select Full.
   b From the Backup components drop-down list, select Database.
   c From the Backup set will expire drop-down list, select After | 0.
   d From the Destination drop-down list, select Disk.
   e If you want to change the default backup location, click Add, then browse to the location.
   f To save the backup file, click OK.

**Restore the Microsoft SQL Server database**

In case of data loss, restore the McAfee Quarantine Manager database from an Microsoft SQL Server database backup.

**Task**

1 Copy the backup file to the destination system.

2 On the destination system, log on to Microsoft SQL Server Management Studio.

3 Create, then select the database.

4 Right-click the database, then select Tasks | Restore.

5 On the Restore Database screen, configure the settings.
   a From the To database drop-down list, select the database.
   b From the Source for restore drop-down list, select From device and browse to the backup file (.bak) to restore.

**Back up the MySQL database**

Back up your existing MySQL database, which comes packaged with McAfee Quarantine Manager.

**Task**

1 Click Start | Run, type services.msc, then click OK.

2 From the Services window, stop the McAfee Quarantine Manager service.

3 From the command prompt, go to the bin directory of the MySQL installation folder.

4 Execute the following command:


For example, if the database name is mqm, user name is root, password is dbase, and backup location is C:\Backups\MQM\MQMBackup.sql, use the following command:

   mysqladmin --complete-insert -n --add-drop-table -R mqm -u root -p$dbase -r "C:\Backups\MQM\MQMBackup.sql" --max-allowed-packet=1024M
**Restore the MySQL Database**

In case of data loss, restore a MySQL database backup.

**Task**

1. Click Start | Run, type services.msc, then click OK.

2. From the Services window, stop the McAfee Quarantine Manager service.

3. From the command prompt, go to the bin directory of the MySQL installation folder.

4. Execute the following command:
   ```
   mysql -e "source <CompletePathofBackupFile>" -u <DatabaseUser> -p<DatabaseUserPassword> <Database>
   ```
   For example, if the database name is mqmv7, the user name is root, the password is dbase, and the backup location is C:\Backups\MQM\MQMBackup.sql, use the following command:
   ```
   mysql -e "source C:\Backups\MQM\MQMBackup.sql" -u root -pdbase mqmv7
   ```

**Configure a scheduled backup task for MySQL Database**

Schedule a backup for your MySQL database, which comes packaged with McAfee Quarantine Manager.

**Task**

1. Create a batch file with the following information:
   ```
   md c:\backups\%DATE%\
   cd c:\backups\%DATE%\
   <InstallPath>\bin\mysqldump.exe --complete-insert -n --add-drop-table -R <database-name> -u <username> -p<password> -r "MQMBackup.sql"
   ```

2. Select Start | Control Panel | Scheduled Tasks | Add Scheduled Task.

3. Click Next and browse for the batch file.

4. Click Next.

5. To schedule the task and complete the wizard, follow the on-screen instructions.
The blacklist is a list of email addresses from which you do not want to receive spam or unsolicited email messages.

The whitelist is a list of email addresses from trusted sources such as business partners, from whom you want to receive messages.

Email addresses added to a blacklist or whitelist are pushed to the connected McAfee products at regular intervals. Here you can manage the blacklists and whitelists using actions, such as adding or deleting email addresses.

Contents
- Blacklist and whitelist levels
- Configure the configuration push interval
- Manage blacklists and whitelists
- Import blacklists and whitelists
- Export blacklists and whitelists

Blacklist and whitelist levels

Blacklists are lists of email addresses that users do not want to receive emails from, and whitelists are lists of email addresses that users want to receive emails from.

In McAfee Quarantine Manager, users create personal blacklists, which are used in addition to the global or group blacklists that administrators maintain. Email messages from blacklisted addresses are blocked or quarantined. Emails sent to users are matched against blacklists. When matches are found, users do not receive the emails.

In McAfee Quarantine Manager, users create personal whitelists, which are used in addition to the global or group whitelists that administrators maintain. Email messages from whitelisted addresses are considered non-spam. Emails sent to users are matched against whitelists. When matches are found, users receive the emails. Messages from whitelisted email addresses are not subject to phish or spam scanning, but are subject to other types of scanning.

In McAfee Quarantine Manager, blacklists and whitelists are organized into three levels, which include:
- **Global** — Blacklists or whitelists are maintained globally for the entire organization.
- **Group** — Blacklists or whitelists are maintained for each user group defined on connected McAfee products.
- **User** — Blacklists or whitelists are maintained for individual users.

You can also add blacklists and whitelists to products connected to McAfee Quarantine Manager and sets of users.
Configure the configuration push interval

Push configuration changes to products connected to McAfee Quarantine Manager. The configuration push is completed at regular intervals. You can specify the minimum interval between the configuration updates on the connected McAfee products.

**Task**

For option definitions, click ? in the interface.

1. In the Administrator UI, click Settings and Diagnostics | Communications | Advanced.
2. In the Configuration Push Interval (seconds) field, enter the interval. The default is 14400.

Manage blacklists and whitelists

View and edit user blacklists and whitelists. You can also define user groups as lists of email addresses or references to existing user groups.

| Information: Email addresses added to blacklists or whitelists are pushed to connected McAfee products at regular intervals.

**Task**

1. From the McAfee Quarantine Manager main menu, click Blacklists and Whitelists | Organization.
2. Manage the blacklists.
   a. Click the Blacklists tab.
   b. In the Entry field, enter the blacklist email address.
   c. From the List Type drop-down list, select the email address list type, then click Search.

Only Super Administrators and Operators can change global blacklists. Domain Administrators have view access to global blacklists. When you add addresses group blacklists, the addresses are also added to the connected McAfee product group blacklists.

   d. To change the number of records on the page, select an option from the per page drop-down list.
   By default, 20 items appear on the page.
   e. To navigate the pages, click the arrows.
   f. To add the email address to the blacklist, click Add.
   g. To search for the email address, click Search.

To search or add multiple email addresses, you can use wildcard characters.
- ? — Searches for a single character.
- * — For multiple characters.

You can only use wild cards for user IDs, not domains. For example:
- To add all email addresses starting with ka from the abc.com domain, use ka*@abc.com
- Use *@abc.com for all abc.com domain senders
h. To clear all search parameters, click **Clear Filter**.

i. To remove selected email addresses, click **Delete**.

j. To remove all email addresses, click **Delete All**.

3. Manage the whitelists.
   a. Click **Whitelists**.
   b. The **Whitelist** tab options are the same as the **Blacklist** tab.

---

**Import blacklists and whitelists**

To use blacklists and whitelists in McAfee Quarantine Manager, you must import them. You can also import the global blacklist and whitelist.

**Task**

1. From the McAfee Quarantine Manager main menu, click **Blacklists and Whitelists | Import and Export**.
2. Under **Import**, click **Browse** and navigate to the blacklist or whitelist.
3. Click **Import Configuration**.
   - McAfee Quarantine Manager automatically detects the import file type and updates the database.
4. To merge the new user configuration with the earlier user configuration, select **Merge User configuration**.
   - If the **Merge User configuration** option is left blank, the earlier user configuration is overwritten. You can also use the **Merge User configuration** option to merge aliases and reassign users.

---

**Export blacklists and whitelists**

Export user configuration, group blacklists and whitelists, and global blacklists and whitelists.

**Task**

1. From the McAfee Quarantine Manager main menu, click **Blacklists and Whitelists | Import and Export**.
2. From the **Export Type** drop-down list, select an option.
   - When you select **User Configuration**, select the domains from the **Select Domains** drop-down list. When you select **Group B/W List**, select the groups from the **Groups** drop-down list.
3. Click **Export Configuration**.
   - The **File Download** screen appears. The user configuration exports as an .XML file.
4. Click **Save**.
   - The default file name is McAfeeBWList.xml.
   - To export group blacklists and whitelists, and global blacklists and whitelists, follow the same steps.
15 Dashboard and graphical reports

The user interface provides critical function for McAfee Quarantine Manager administrators. It is important for the administrators to know how well the server is protected from spam, phish, viruses, potentially unwanted programs, and unwanted content. The dashboard is your interface to the McAfee Quarantine Manager.

Contents
- Viewing dashboard counters
- Test connected McAfee products
- Performing a quick search
- Calculate the size of the database
- Generate multi-dimensional reports
- Generate Top 10 reports
- Generate advanced graphical reports
- Download a report

Viewing dashboard counters

The dashboard provides a high-level overview of the McAfee Quarantine Manager server, quarantined items, and reports.

Task
1. From the McAfee Quarantine Manager main menu, click Dashboard | Graphical Reports | Quarantined.
2. Configure the available options.

Test connected McAfee products

View and test all McAfee Quarantine Manager connected products.

Task
1. From the McAfee Quarantine Manager main menu, click Dashboard.
2. Click Connected McAfee Products, then select the product.
3. Click Test.

The Test function does not support HTTP-based McAfee products.
Performing a quick search

Quickly search for a quarantined item without having to navigate through the Quarantined Items page.

**Task**

1. From the McAfee Quarantine Manager main menu, click Dashboard.
2. Click the Quick Search tab.
3. In Time Span, configure the time period options.
4. From the Domain drop-down list, select the domain.
   To select domains that are not managed by the McAfee Quarantine Manager server, select Others.
5. In the Sender field, enter the sender email addresses.
6. In the Recipient field, enter the recipient email addresses.
7. In the Subject field, enter the email subject.
8. Click Search.
9. To view the results, click Quarantine Management | Quarantined Items.

**See also**

*Managing quarantined items* on page 4

Calculate the size of the database

Collect database size and disk space data.

**Task**

1. From the McAfee Quarantine Manager main menu, click Dashboard.
2. Click the Database Information tab.
3. To get the latest data related to database size and disk space usage, click Get Database Size. If the database size is large, it might take some time to retrieve the data.

Generate multi-dimensional reports

Generate graphical reports that display statistics data in bar graphs.

**Task**

1. From the McAfee Quarantine Manager main menu, click Dashboard.
2. On the Statistics page, click the Reports tab.
3. From the Domains drop-down list, select the domain.
4. In Time Span, configure the time period options.
5. From the Query On drop-down list, select the query.
6. Click Generate.
Generate Top 10 reports
Generate quarantine activity graphical reports.

**Task**
1. On the McAfee Quarantine Manager main menu, click Dashboard | Graphical Reports | Default.
2. From the **Time Span** drop-down list, select the time period.
3. From the **Type** drop-down list, select the quarantine item type.
4. From the **Filter** drop-down list, select the filter.
5. Click **Search**.

Generate advanced graphical reports
View quarantined items in a detailed graph, and find detections with filters.

**Task**
1. From the McAfee Quarantine Manager main menu, click Dashboard | Graphical Reports | Advanced.
2. Select up to three filters.
   a. From the drop-down list, select the condition, then enter the conditional search parameter in the corresponding field.
   b. To apply two or more search criteria, select **And**.
   c. To apply either rules, select **Or**.
3. Configure the time period.
   - To generate a report for the entire time period available, select **All Dates**.
   - To generate a report based on a specific time period, click **Date Range**, then click to select the date range.
4. Choose the graph type.
   - To generate a bar graph, click **Bar Graph**.
   - To generate a pie chart, click **Pie Chart**, select the data query from the **Query on** drop-down list, then enter the number of results to display in the **Maximum Results** field.
5. Click **Search**.
6. To clear all search settings, click **Clear Filter**.
Download a report

Download and save graphical reports as PDF or HTML files.

**Task**

1. To convert the graphical report into a PDF file, click the PDF icon.
   
   a. To display the report as a PDF, click **Open**.
   
   b. To save the report as a PDF, click **Save**.

2. To convert the graphical report into an HTML file, click the Internet Explorer icon.
   
   a. To open the .zip file, click **Open**.
   
   b. To save the report, click **Save**.
Frequently asked questions

Where can I find out more about the effect of a virus?

How do I contact Technical Support?
See https://support.mcafee.com for details.
Before calling technical support, have the following information ready:
• Make and model of the computer where MQM is installed
• Operating system and its version
• Any additional hardware that is installed
• Web browser being used and its version
• A diagnostic report regarding the issue

What is the recommended screen resolution for MQM?
MQM is best viewed with a minimum screen resolution of 1024 x 768 pixels.

Is there any tool to integrate MQM and Outlook?
Yes, it’s known as McAfee Customer Submission Tool (MCST). You can download it from the McAfee website.

How do I set the User Authentication mode to LDAP Server?
Click End-User Management | General | Authentication, then select LDAP Server Accounts.

Which versions of MQM can be upgraded or migrated to this version?
You can migrate to this version from MQM 7.0.1.

How long does it take to convert data from MySQL database to Microsoft SQL server database?
It takes approximately one hour to convert 45 GB data.

When do I reassign users?
Reassign users if a user is leaving the organization or the user account is being deleted from the LDAP server.
**How do I optimize or shrink the MySQL database?**

1. From the command prompt, go to the bin directory of MySQL installation folder.

2. Execute the following command to log on to the MySQL database:
   
   ```
   mysql --user=<database user name> --password=<database password> <database name>
   ```
   
   For example:
   
   ```
   mysql --user=scott --password=tiger mqm
   ```

3. Execute the following command to optimize the database:
   
   ```
   call pOptimize();
   ```
   
   The MySQL prompt appears when the optimization is complete.

4. Execute the following command to exit the MySQL database:
   
   ```
   quit
   ```

**How do I fine-tune my MySQL database to improve MQM performance?**

1. Go to the MySQL installation folder and edit the my.ini file.

2. Change the following parameters with the specified values:
   
   ```
   Innodb_buffer_pool_size = 1G
   Innodb_Log_File_Size = 512M
   Innodb_Thread_Concurrency = 512
   ```

3. From the services console, restart the MySQL for McAfee Quarantine Manager service.

**How do I fine-tune my Microsoft SQL Server 2005 database to improve MQM performance?**

1. Open SQL Server Management Studio.

2. Right-click the database mqm and select Properties.

3. Click Files on the left pane and change the following parameters on the right pane.
   
   **Initial size for Data file** = (~30 GB)
   
   **Autogrowth for Data file** = 1 GB
   
   **Initial size for log file** = 1 GB
   
   **Autogrowth for Log file** = 512 MB

4. Click Options in the left pane, then change the Recovery model to Simple in the right pane.

5. Right-click Database Instance and select Properties.

6. Click Advanced in the left pane, then change the Network Packet Size to 32767 in the right pane.


**I have blacklisted a sender, but I am still receiving emails from the sender. Why?**

MQM allows management of blacklists and whitelists, which connected McAfee products manipulate and maintain. Blocking an email address is not in the scope of MQM. Requests to add blacklists and whitelists are sent to the connected McAfee products, which take appropriate actions to block or allow the emails.
Is MQM integrated with products, for example, VirusScan Enterprise and the desktop anti-spyware software?
No, MQM supports McAfee Email Gateway, McAfee Security for Microsoft Exchange and McAfee Security for Lotus Domino (Windows and Linux) gateway products.

To how many users can MQM scale?
MQM can support up to 200,000 users.

What is the maximum database size that MQM supports?
McAfee Quarantine Manager supports a maximum database size of 500 GB.

Can we collapse multiple email IDs into a single quarantine view for a user?
Yes, by creating email aliases.

How frequently do you recommend running an MQM Email Digest task?
Run an email digest task at least once a week.

Can we see an email body for banned content in MQM?
Yes, you can view the content of the quarantined email under Banned Content.

Can the Super Administrator schedule a task for the domains that are managed by a Domain Administrator?
Yes. The Super Administrator has all rights to schedule tasks for any domain, even domains managed by the Domain Administrator.

Is it possible to send digests for unregistered users in MQM?
Yes. MQM supports sending digests for unregistered users.

Can the user interface be rebranded?
Yes.

If an appliance ID in McAfee Email and Web Security or McAfee Email Gateway has changed, can we release the old quarantined emails using the old appliance ID?
Yes, you can use the Product Reassignment feature to assign a new McAfee product ID and release the quarantined emails.

How do we convert packaged MySQL to external MySQL?
Make a backup of existing data using the DB Tools and reimport it to external MySQL.

What are the common issues in connecting McAfee Security for Microsoft Exchange to MQM?
You might see one or more of the following issues while working with McAfee Security for Microsoft Exchange:
• McAfee Security for Microsoft Exchange does not connect to MQM.
• McAfee Security for Microsoft Exchange is visible on the MQM dashboard, but the test connection fails.
• Product log shows too many binds and unbind entries.

**Workaround:** Set the following registry key on the McAfee Security for Microsoft Exchange box:

```
HKLM\SOFTWARE\McAfee\<Product>\RPC\ThreatQuarantineManager_Connect_Timeout = 10000
```

<i>\<Product> refers to McAfee Security for Microsoft Exchange.</i>

**What do I do if I can't connect to MQM?**

Try the following steps:

1. Check if a firewall blocks the MQM listen port (which is 49500 by default). Changing the port is not recommended. However, in unavoidable circumstances, change the port from the administrator interface. Click **Settings and Diagnostics | Communications**.

   ![Check that the same port number is mentioned in the connected McAfee product.]

2. Check the connected McAfee product listening port.

   • For the McAfee Email and Web Security and McAfee Email Gateway family of appliances, the listen port is specified in `/etc/McAfee/TQMClient/SAFE.ini` under `[TQMCallback].

     ![Port=#49500]

   • For the McAfee Security for Microsoft Exchange appliances, the listen port is specified in the following registry key.

     ![HKLM\SOFTWARE\McAfee\<Product>\TQMCallback\Port = 49500]

3. Restart MQM services and observe the threat count of the RPCServ.exe process. If the thread count is not around 70, there might be an issue in the MQM server application.

4. If the issue persists, restart McAfee product services.

**How do I customize the application URL?**

By default, the MQM URL that is referred to in email communications such as digest email and password reminders, contains http protocol and a fully qualified domain name in the format http://<yourdomain>/MQMUserUI. You can customize this URL using **Advanced Settings | Settings | Email Notifications Related**. Available options are:

• **Customize Server URL** — Select this to customize the application URL.

• **Server Name** — Specify the IP address or domain name that can resolve to the server where MQM is installed. For example: domain.dom. If MQM website is running on a custom port, specify the path as domain.dom:port number.

• **Protocol** — Select **HTTP** or **HTTPS** to specify whether secured connection is required for domain access, depending on the configuration settings done in Microsoft Internet Information Services server.

• **Sample End User Interface URL** — Preview a sample custom URL based on the options selected. For example: https://domain.dom/MQMUserUI, where the domain name is domain.com and the protocol used is http.
See also
Upgrade to the latest version of MQM on page 23
Change user configuration on page 54
Rebranding McAfee Quarantine Manager on page 5
Reassign quarantined email releases to different products on page 81
Rebranding McAfee Quarantine Manager

The McAfee Quarantine Manager rebranding kit allows some user interface components to be rebranded in the administrator view and user view of the McAfee Quarantine Manager software.

Contents

- Overview
- Adding your brand to the McAfee Quarantine Manager software

Overview

The McAfee Quarantine Manager rebranding kit allows you to apply your own colors and text to several interface components.

You can change these components:

- Company logo
- Title bar color
- Top link bar color
- Company name and product name
- Data table color

Adding your brand to the McAfee Quarantine Manager software

Learn how to add your company logo, use your corporate colors and wording, and make other changes to the McAfee Quarantine Manager interface.

Add your own logo

Change how the MQM interface looks by adding your company logo.

- Do not delete the existing logo.gif file.
- Do not place the logo file outside the MQMAdministrator UI directory. Always provide the relative path from the MQMAdministrator UI folder.
- You can use any image format which can be rendered in a web browser.
- Do not use a logo image more than 1 MB in size.
Task
1. Resize your company logo to a 3:1 aspect ratio.

2. Open the Rebrand folder \&lt;installation folder\adminui\Rebrand\.

3. Open the Rebrand.js file and change the following line from LogoImagePath ../Rebrand.logo.gif to ../Rebrand/&lt;your_logo&gt;.gif.

**Use your corporate colors**
Add your company’s corporate colors to the MQM top link bar and title bar.

> Make sure you use only a valid color code that your browser can interpret. Invalid color codes can cause scripting errors that mean the interface does not render properly.

**Task**
1. From the MQM installation folder, open the Rebrand.js file.

2. Change the TitlebarColor = #B00C33 line to TitlebarColor = #99CC33 where #99CC33 is the color code of the color you want.

3. Change the TopLinkBarColor = #000000 line to TopLinkBarColor = #B00C33 where #B00C33 is the color code of the color you want.

**Change the company name and product name**
Use your company name on the MQM interface.

To avoid distorting the title bar, the length of the company name and product name together must not exceed 100 characters.

**Task**
1. From the Rebrand folder in the installation directory, open the Rebrand.js file.

2. Locate the line

   CompanyName = McAfee
   ProductName = Quarantine Manager.

3. Change the company name to your company name and the product name to Quarantined Mail Store.

**Make changes to the user view of the interface**
Change the way that the interface looks to your users.

**Task**
1. Open the &lt;MQMInstallFolder&gt;\userUI\Rebrand folder.

2. Change the Rebrand.js file:
   a. Open the Rebrand.js file.
   b. Make the necessary changes, then save the file.
Index

**A**

about this guide 7
access
  user UI 65
add
  aliases 72
administrator
  types 41
  using LDAP groups 42
administrator interface
  rebranding 99
administrator type
  domain administrator 41
  domain administrator alias 41
  operator 41
  super administrator 41
  super administrator alias 41
advanced
  graphical reports 91
  server settings 78
advanced graphical reports
  generating 91
advanced settings
  database related 79
  email notifications related 79
  ePolicy Orchestrator related 78
  miscellaneous 80
  status report email 80
  submission to McAfee Labs 79
agent wake-up call
  sending an 31
aliases
  adding 72
application URL
  customizing 93
assign domains
  domain administrators 47
authentication
  modes 42

**B**

backing up database (continued)
  MySQL 83
blacklist
  management 85
  managing 70
  types 85
blacklists
  exporting 87
  importing 87
  managing 86
bulk emails
  releasing 81

**C**

calculate
  database size 90
catch exceptions 76
centralized policy management
ePolicy Orchestrator 25
certificate authority 81
certificates
  configuring 81
change
  configuration settings 72
  domain configurations 47
  end-user configuration 54
  password 71
check in package
  McAfee Quarantine Manager 27
  MySQL for McAfee Quarantine Manager 27
cluster
  configuration on Windows 2003 21
  configuration on Windows 2008 22
  configuration on Windows 2008 R2 22
cluster installation 21
collapse
  multiple email ids 93
command-line arguments
  McAfee Quarantine Manager 28
  MySQL for McAfee Quarantine Manager 27
communications
  configuring 76
Configuration Push Interval 76
configuration settings
  changing 72
configure
  advanced settings 78
certificates 81
cluster 21, 22
communications 76
database 35
database related settings 79
diagnostics 76
e-mail notifications 79
High Availability 12
LDAP Server 76
McAfee Email and Web Security Appliance 36
McAfee Security for Microsoft Exchange 36
miscellaneous settings 80
MySQL 5.1 Linux 20
MySQL 5.1 Windows 20
reports 32
status report email 80
submission to McAfee Labs 79
VMware support 13
configure database
  Microsoft SQL Server 19
configuring reports
ePolicy Orchestrator 32
connected McAfee products
testing 89
contents, what comes with the product 10
conventions and icons used in this guide 7
create
  administrators 43
database backup 82
  domain-McAfee Connected Product group mapping 49
email digest task 59
end-user 51
purge task 60
status email task 61
user synchronization task 60
creating policies
ePolicy Orchestrator 30
custom queues 89
customize
  application URL 93

D
dashboard 89
dashboard counters
  viewing 89
data leakage prevention 89
database
  configuring 35
  fine-tuning 93
data (continued)
  optimizing 93
database backup
  creating 82
database related settings
  configuring 79
database size
  calculating 90
databases, supported 17
deployment
  McAfee Agent 26
  McAfee Quarantine Manager 28
  MySQL for McAfee Quarantine Manager 27
  package and extension 25
diagnostics 76
diagnostics settings
  configuring 76
digest email 68
digest emails
  managing quarantine from 68
disk
  submitting samples from 69
distribution list
  registering 55
documentation
  audience for this guide 7
  product-specific, finding 8
typographical conventions and icons 7
domain
  adding new 46
  exporting 46
  importing 46
  managing 45
domain administrators
  assigning domains 47
domain configurations
  changing 47
domains
  adding 45
  importing 45
download
  report 92
E
editing policies
ePolicy Orchestrator 30
e-mail
  view reassignments 72
e-mail digest task
  creating 59
e-mail notifications
  configuring 79
encryption compliance 89
end users
  creating 51
  import 53
end-user configuration
  changing 54
end-users
  importing from a file 52
  importing from LDAP 51
  registering automatically 53
enforcing policies
  ePolicy Orchestrator 31
ePolicy Orchestrator
  configure reports 32
  create policies 30
  edit policies 30
  enforce policies 31
  installing the software using 26
  integration 25
  prerequisites 25
  setting policies within 30
  uninstalling the software using 33
ePolicy Orchestrator related
  advanced settings 78
error reporting 76
export
  blacklists 87
  domain 46
  whitelists 87
extension
  deployment 25

F
false negative 89
false positive 89
faqs 93
features
  product 9
frequently asked questions 93

G
generate
  advanced graphical reports 91
group mapping 49

H
help extension
  installing 30
High Availability, configuring 12
high-availability 21
import
  blacklists 87
  domain 46
  end users 53
  end-users 51, 52
  whitelists 87
import users
  from a file 52
  from LDAP 51
install
  McAfee Quarantine Manager 21
  MySQL for McAfee Quarantine Manager 19
installation
  cluster installation 21
  help extension 30
  overview of tasks 18
  policy extension 29
  reports extension 29
  supported McAfee products 11
interface
  change the color 100
  rebranding 99, 100
introduction
  McAfee Quarantine Manager 9
Item Push Interval 76
LDAP groups
  act as an administrator 42
  as administrators 42
LDAP Server
  configuring 76
logging 76
logo
  add your company logo 99
magnify graph 89
manage
  blacklist 70, 85
  blacklists 86
  domains 45
  quarantine 66, 68
  quarantined items 57
  server configuration 75
  user submissions 63
  whitelist 71, 85
  whitelists 86
management software
  ePolicy Orchestrator 25
  Maximum Communication Retry 76
  McAfee Agent
  deploying 26
McAfee Customer Submission Tool 93
McAfee Email and Web Security Appliance
    configuring 36
McAfee ePO
    deploy package and extension 25
    managing Quarantine Manager 12
McAfee Product reassignment map
    create 81
McAfee Quarantine Manager
    checking in the package 27
    command-line arguments 28
    deploying on client computers 28
    installing 21
    integrating with ePolicy Orchestrator 25
    rebranding 37
    removing from client computers 33
    removing the package 34
    testing 36
    uninstalling 23
    upgrading 23
McAfee Quarantine Manager, introducing 9
McAfee Security for Microsoft Exchange
    configuring 36
McAfee ServicePortal, accessing 8
    memory 17
Microsoft Outlook
    submitting samples from 69
Microsoft SQL database
    backup 82
    restore 83
Microsoft SQL Server
    configuring database 19
    miscellaneous
        advanced settings 80
    miscellaneous settings
        configuring 80
    modes
        authentication 42
    multi-dimensional reports
        generating 90
    multiple email ids
        collapsing 93
MySQL 5.1
    Linux, configuring 20
    Windows, configuring 20
MySQL database
    backup 83
    restore 84
    schedule backup 84
MySQL for McAfee Quarantine Manager
    checking in the package 27
    command-line arguments 27
    deploying on client computers 27
    installing 19
    (continued)
    removing from client computers 33
    removing the package 34
    uninstalling 23

O
    operating systems 17
    operator
        administrator type 41
        optimize
            database 93
    own account
        managing 70

P
    package
        deployment 25
        packers 89
        password
            changing 71
        perform
            quick search 90
        phish 89
        policy extension
            installing 29
        potentially unwanted programs 89
        pre-installation 19
        prerequisites
            ePolicy Orchestrator 25
    product
        features 9
        product contents 10
        product log 76
            viewing 75
        purge task
            creating 60
        push interval
            configure 86

Q
    Quarantine Manager
        with McAfee ePO 12
    quarantine messages
        delete 68
        delete blacklist 68
        delete whitelist 68
        release 68
        retain 68
    quarantined items
        managing 57
        searching 57
        taking action 57
quarantines
  submitting samples from 70
quick search
  performing 90

R
reassign 81
reassignment map 81
rebrand
  McAfee Quarantine Manager 37
rebranding 99
  add your company logo 99
  change the color 100
change the user interface 100
  changing the administrator interface 99
  use your company name 100
register
  distribution list 55
  end-users automatically 53
release
  bulk emails 81
remove
  extensions 25
  McAfee Quarantine Manager from client computers 33
  McAfee Quarantine Manager package 34
  McAfee Quarantine Manager product extension 34
MySQL for McAfee Quarantine Manager from client computers 33
MySQL for McAfee Quarantine Manager package 34
software packages 25
report
  downloading 92
reports
  configuring 32
  generating 91
  multi-dimensional 90
reports extension
  installing 29
requirements
  disk space 17
  memory 17
  network 17
  system 17
restoring database
  Microsoft SQL 83
  MySQL 84
restricted rights
  create administrators with 43

S
scenarios
  VMware 13
schedule backup
  for MySQL database 84
screen resolution
  recommended 93
search
  quarantined items 57
send an agent wake-up call 31
server administration 41
server configuration
  managing 75
server settings
  advanced 78
ServicePortal, finding product documentation 8
setting policies within
  ePolicy Orchestrator 30
SMTP Communication 81
spam 89
spam samples
  submitting 68
statistics 89
status email 61
status email task
  creating 61
status report email
  configuring 80
submission to McAfee Labs
  configuring 79
submit samples 68
  disk 69
  Microsoft Outlook 69
  quarantines 70
supported
  browsers 17
  databases 17
  McAfee products 11, 17
  operating systems 17
  upgrades 17, 23
system requirements 17

T
take action
  quarantined items 57
Technical Support 93
technical support, finding product information 8
test
  connected McAfee products 89
  McAfee Quarantine Manager 36
Thread Pool Size 76
top 10 reports 91
Transport Layer Security 81
types
  administrator 41

U
uninstall 22
  McAfee Quarantine Manager 23
uninstall 22 (continued)
  MySQL for McAfee Quarantine Manager 23
uninstallation 22
unwanted content 89
upgrade
  supported 23
upgrade to
  McAfee Quarantine Manager 7.0 23
upgrades, supported 17
user interactions 65
user interface
  change the color 100
  managing quarantine from 66
  rebranding 93, 99, 100
user submissions 63
  managing 63
  viewing search results 64
user synchronization 60
user synchronization task
  creating 60
user UI
  accessing 65
users
  import 53

V
view
  product log 75
  view search results
    user submissions 64
viruses 89
VMware
  scenarios 13
VMware support
  configuring 13

W
whitelist
  management 85
  managing 71
  types 85
whitelists
  exporting 87
  importing 87
  managing 86
Windows components, required 17