Integration Guide

Revision A

McAfee Firewall Enterprise ePolicy Orchestrator Extension

version 5.3.2

COPYRIGHT

TRADEMARK ATTRIBUTIONS

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

LICENSE INFORMATION

License Agreement

Contents

Preface 5

About this guide 5

Audience 5

Conventions 5

Find product documentation 6

1 Introduction 7

About McAfee Firewall Enterprise ePolicy Orchestrator Extension 7

Managed products 7

Compatible products 8

Firewall Enterprise overview 8

Control Center overview 8

How the Firewall Enterprise ePolicy Orchestrator Extension works 8

2 Firewall Enterprise ePolicy Orchestrator Extension setup 11

Setup overview 11

Download and install the Firewall Enterprise ePolicy Orchestrator Extension 11

Download the Firewall Enterprise ePolicy Orchestrator Extension 11

Install the McAfee Firewall Enterprise ePolicy Orchestrator Extension 12

[Upgrade only] Export policies from McAfee Firewall Enterprise 5.3.0 ePolicy Orchestrator extension 12

Needed permission sets and users 14

Create a permission set for Firewall Enterprise or Control Center access to ePolicy Orchestrator . . 15

Create a user account for access to ePolicy Orchestrator 15

Create a permission set that allows users to view firewall data 16

Create a user that can view firewall data 18

3 Firewall Enterprise setup 21

Configure Firewall Enterprise appliances for ePolicy Orchestrator reporting 21

Configure managed firewalls for ePolicy Orchestrator reporting 22

Troubleshooting Firewall Enterprise to ePolicy Orchestrator communication 23

4 Control Center setup 25

Setup overview 25

Configure Control Center for ePolicy Orchestrator 25

Register Control Center 27

Control Center Management Servers, High Availability (HA), and the ePolicy Orchestrator platform 27

Add a Control Center Management Server 27

Delete a Control Center Management Server from the ePolicy Orchestrator server 28

5 Firewall data 29

View Firewall Enterprise and Control Center data in the ePolicy Orchestrator console 29

View internal host activity 29

View firewall resources 30

View firewall statuses 31
View all firewalls managed by a Control Center Management Server 32
Change how ePolicy Orchestrator displays firewall data 33
Change data refresh settings and host retention 33
View ePolicy Orchestrator Host Data reports from the Control Center Client application 34

6 Queries 37
Firewall Enterprise ePolicy Orchestrator Extension queries 37
Firewall Enterprise Report queries 37
Generate a Firewall Enterprise Report query 38
Control Center queries 38
Generate a Control Center query 39

Index 41

Preface

Contents

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

About this guide

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

Audience

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

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

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.
ℹ	**Note:** Additional information, like an alternate method of accessing an option.
💡	**Tip:** Suggestions and recommendations.
❗	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
⚠	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

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

Task

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

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introduction

Contents

- *About McAfee Firewall Enterprise ePolicy Orchestrator Extension*
- *Managed products*
- *How the Firewall Enterprise ePolicy Orchestrator Extension works*

About McAfee Firewall Enterprise ePolicy Orchestrator Extension

McAfee® Firewall Enterprise ePolicy Orchestrator® Extension (hereinafter Firewall Enterprise ePolicy Orchestrator Extension) version 5.3.2 provides communication between McAfee® ePolicy Orchestrator® (hereinafter ePolicy Orchestrator) and McAfee® Firewall Enterprise (hereinafter Firewall Enterprise) and McAfee® Firewall Enterprise Control Center (hereinafter Control Center).

In ePolicy Orchestrator, you can view top-level data about multiple firewalls, or you can drill down to view data about an individual firewall and the Control Center that manages it. You can also view resource and statistical dashboards across multiple firewalls. These dashboards are presented in a graphical format, which allows you to click within the graph to display more specific information.

Control Center can display information retrieved from the ePolicy Orchestrator server about hosts that are referenced in a policy, or hosts that are passing traffic through Firewall Enterprise appliances.

The McAfee Firewall Enterprise 5.3.2 ePolicy Orchestrator extension supports Dashboard reporting support for Firewall Enterprise resources (from Control Center), firewall statistics, and firewall internal host mapping (Firewall Enterprise).

> For Endpoint Intelligence Agent 2.0.0 and Network Integrity Agent 1.0.1 policy and configuration management, refer to the *Endpoint Intelligence Management 2.0.0 help extension documentation*.

> McAfee Firewall Enterprise 5.3.2 ePolicy Orchestrator extension does not support Firewall Profiler.

Managed products

The Firewall Enterprise ePolicy Orchestrator extension supports Firewall Enterprise and Control Center. To find the latest information on the McAfee firewall products and versions that Firewall Enterprise ePolicy Orchestrator extension supports, refer to KnowledgeBase article KB67462.

Compatible products

McAfee Firewall Enterprise 5.3.2 ePolicy Orchestrator extension supports these products.

Table 1-1 Version support matrix

	Supports
McAfee Firewall Enterprise 5.3.2 ePolicy Orchestrator extension	ePolicy Orchestrator 4.6.0 to 5.0.1
	McAfee Agent
	Control Center 5.3.0, 5.3.1, and 5.3.2
Endpoint Intelligence Management 2.0.0 extension	Network Integrity Agent 1.0.1
	Endpoint Intelligence Agent 2.0.0 For more details, refer to *Endpoint Intelligence Agent 2.0.0 Product Guide*.
Upgrade from McAfee Firewall Enterprise 5.3.0 ePolicy Orchestrator extension to McAfee Firewall Enterprise 5.3.2 ePolicy Orchestrator extension	ePolicy Orchestrator 4.6.0 to 5.0.1
Export policy configuration from McAfee Firewall Enterprise 5.3.0 ePolicy Orchestrator extension with Network Integrity Agent 1.0.0	Install Endpoint Intelligence Management 2.0.0 extension and perform policy configuration for Network Integrity Agent 1.0.0.

Firewall Enterprise overview

Firewall Enterprise appliances are designed to protect organization information technology infrastructure by keeping out unauthorized users, code, and applications, both internally and externally.

ePolicy Orchestrator and Firewall Enterprise appliances share information about protected hosts and firewall versions.

Control Center overview

Control Center is an enterprise-class management tool for creating and applying security policies across multiple firewalls. Use Control Center to remotely manage, maintain, and monitor firewalls for one or more domains.

ePolicy Orchestrator and Control Center share data about hosts, firewalls, and the Control Center Management Server. Control Center displays information about hosts, whereas ePolicy Orchestrator displays health and status information about firewalls and the Control Center Management Server.

See the *McAfee Firewall Enterprise Control Center Product Guide* for more information.

How the Firewall Enterprise ePolicy Orchestrator Extension works

Use ePolicy Orchestrator to poll and monitor firewall data from one or more Firewall Enterprise appliances or Control Center Management Servers. View host data from ePolicy Orchestrator from the Control Center Client application.

Firewall Enterprise appliances at version 8.3.0 or later can be configured to send information directly to the ePolicy Orchestrator server. Information on registered firewalls can be viewed on ePolicy Orchestrator dashboards.

On the Control Center, an ePolicy Orchestrator user is created and communication parameters are specified so that the Control Center Management Server can communicate information to the ePolicy Orchestrator server. After each Control Center Management Server is registered in ePolicy Orchestrator, administrators can view data about managed firewalls.

2 Firewall Enterprise ePolicy Orchestrator Extension setup

Contents

- *Setup overview*
- *Download and install the Firewall Enterprise ePolicy Orchestrator Extension*
- *[Upgrade only] Export policies from McAfee Firewall Enterprise 5.3.0 ePolicy Orchestrator extension*
- *Needed permission sets and users*
- *Create a permission set for Firewall Enterprise or Control Center access to ePolicy Orchestrator*
- *Create a user account for access to ePolicy Orchestrator*
- *Create a permission set that allows users to view firewall data*
- *Create a user that can view firewall data*

Setup overview

To complete the configuration of ePolicy Orchestrator so that you can view firewall data from within ePolicy Orchestrator, you must perform the following tasks:

1. Download and install the Firewall Enterprise ePolicy Orchestrator Extension.
2. Configure permission sets and users to allow Firewall Enterprise appliances or Control Center Management Servers to communicate with ePolicy Orchestrator.
3. Configure a permission set that allows access to Firewall Enterprise Extension functionality, and assign this permission set to one or more ePolicy Orchestrator users.

Download and install the Firewall Enterprise ePolicy Orchestrator Extension

Use the tasks in this section to download and install the Firewall Enterprise ePolicy Orchestrator Extension onto your ePolicy Orchestrator server.

Download the Firewall Enterprise ePolicy Orchestrator Extension

Before you begin

Know your grant number.

Use this task to download the Firewall Enterprise ePolicy Orchestrator Extension to the ePolicy Orchestrator server.

Task

1. In a web browser, navigate to www.mcafee.com/us/downloads
2. Provide your grant number, then navigate to the appropriate product and version.
3. Download the McAfee Firewall Enterprise ePolicy Orchestrator Extension (.zip) file.

Install the McAfee Firewall Enterprise ePolicy Orchestrator Extension

Before you begin

- Make sure the ePolicy Orchestrator server that you intend to use to monitor your firewalls is at version 4.6.0 or later.
- Make sure you have downloaded the McAfee Firewall Enterprise ePolicy Orchestrator Extension from the McAfee downloads website and have saved it to a location that is accessible by the ePolicy Orchestrator server.

Use this task to install the McAfee Firewall Enterprise ePolicy Orchestrator Extension from your download location onto your ePolicy Orchestrator server.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1. Log on to ePolicy Orchestrator.
2. In the ePolicy Orchestrator console, select **Menu | Software | Extensions**.
3. At the bottom of the Extensions pane on the left side of the Extensions page, click **Install Extension**.

   The Install Extension window appears.
4. Browse to the McAfee Firewall Enterprise ePolicy Orchestrator Extension .zip file you downloaded from the McAfee downloads page.
5. Click **Open** to select the file, then click **OK** to proceed with the selection.
6. Click **OK** to install the extension.

[Upgrade only] Export policies from McAfee Firewall Enterprise 5.3.0 ePolicy Orchestrator extension

If you want to retain Control Center features, upgrade to McAfee Firewall Enterprise 5.3.2 ePolicy Orchestrator extension or uninstall the 5.3.0 extension and install the Endpoint Intelligence Management 2.0.0 extension.

Before you begin

Download the McAfee Firewall Enterprise 5.3.2 ePolicy Orchestrator and Endpoint Intelligence Management 2.0.0 extensions.

Follow this workflow to export and import policy configuration from McAfee Firewall Enterprise 5.3.0 ePolicy Orchestrator extension on supported ePolicy Orchestrator versions.

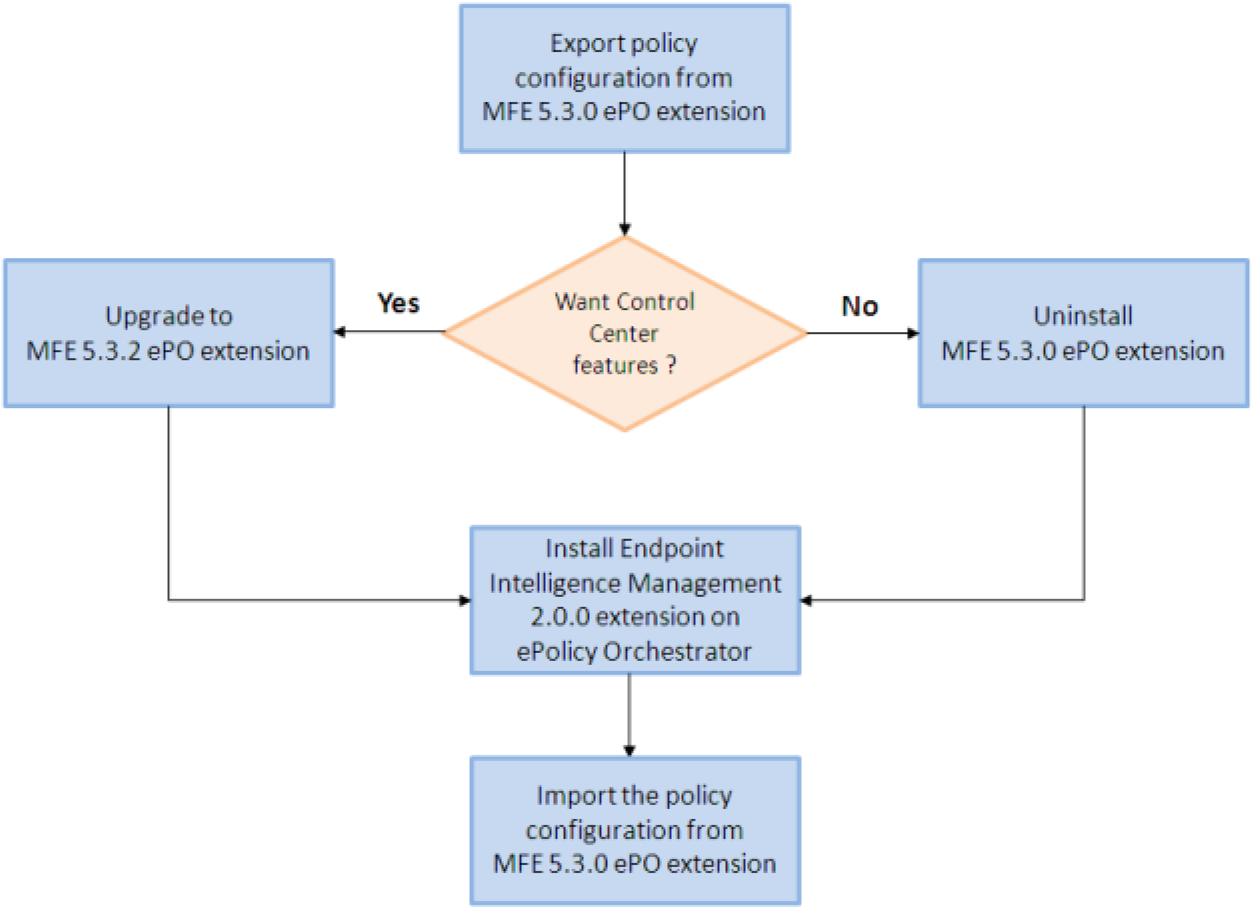
Export policy configuration from MFE 5.3.0 ePO extension
Want Control Center features ?
Yes
No
Upgrade to MFE 5.3.2 ePO extension
Uninstall MFE 5.3.0 ePO extension
Install Endpoint Intelligence Management 2.0.0 extension on ePolicy Orchestrator
Import the policy configuration from MFE 5.3.0 ePO extension

Figure 2-1 Paths from Firewall Enterprise 5.3.0 ePolicy Orchestrator extension

Task

1 Export the policy configuration from McAfee Firewall Enterprise 5.3.0 ePolicy Orchestrator extension.

   a In the ePolicy Orchestrator console, go to **Menu | Policy | Policy Catalog**.

   b Select **Network Integrity Agent1.0.0**.

   c Click **Export**.

   d On the Export window, right-click the link and select **Save Target As**… and save the configuration as an xml file.

2 If you wish ePolicy Orchestrator to manage Firewall Enterprise and Control Center, upgrade from MFE 5.3.0 ePolicy Orchestrator extension to MFE 5.3.2 ePolicy Orchestrator extension.

   a In the ePolicy Orchestrator console, go to **Menu | Software Extensions**.

   b Click **<Install Extension>**.

   c Click **Browse** to navigate to the downloaded MFE 5.3.2 ePolicy Orchestrator extension. Click **Open**.

   d Click **OK**.

This overrides the existing MFE 5.3.0 ePolicy Orchestrator extension and installs the MFE 5.3.2 ePolicy Orchestrator extension.

3. If you do not wish to use the Control Center features, uninstall MFE 5.3.0 ePolicy Orchestrator extension.
4. Install Endpoint Intelligence Management 2.0.0 extension on ePolicy Orchestrator.
   - a. In the ePolicy Orchestrator console, go to **Menu | Software Extensions**.
   - b. Click **<Install Extension>**.
   - c. Click **Browse** to navigate to the downloaded Endpoint Intelligence Management 2.0.0 extension. Click **Open**.
   - d. Click **OK**.

   Refer to *Endpoint Intelligence Agent 2.0.0 Product Guide* for more details.
5. Import the policy configuration that you saved as an xml file in Step 1.
   - a. In the ePolicy Orchestrator console, go to **Menu | Policy | Policy Catalog**.
   - b. Select **Network Integrity Agent1.0.0**.
   - c. Click **Import**.
   - d. On the Import Policies window, click **Browse** to navigate to the saved xml file. Click **Open**.
   - e. Click **OK**.

This allows Endpoint Intelligence Management 2.0.0 extension to manage Network Integrity Agent 1.0.1. For Endpoint Intelligence Agent 2.0.0, define fresh policies and configuration.

Needed permission sets and users

Firewall Enterprise appliances and Control Center Management Servers require user credentials to authenticate with ePolicy Orchestrator.

For Firewall Enterprise and Control Center, creating user credentials is a two-part process:

Task

1. Create a permission set that allows data transmission.
2. Create a new user with that permission set.

   In addition to the appliance or server user credentials, you must create a permission set that allows ePolicy Orchestrator users to view firewall data and assign this permission set to one or more users.

See also

Create a permission set for Firewall Enterprise or Control Center access to ePolicy Orchestrator on page 15
Create a user account for access to ePolicy Orchestrator on page 15
Create a permission set that allows users to view firewall data on page 16
Create a user that can view firewall data on page 18

Create a permission set for Firewall Enterprise or Control Center access to ePolicy Orchestrator

Before you begin

- Make sure that you have downloaded and installed the Firewall Enterprise ePolicy Orchestrator Extension on your ePolicy Orchestrator server.
- You must be an ePolicy Orchestrator global administrator to perform this task.

Use this procedure to create a permission set for these user accounts.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1. In the ePolicy Orchestrator console, select **Menu** | **User Management** | **Permission Sets**
2. At the bottom of the Permission Sets page, click **New**.

   The New Permission Set page appears.
3. Enter a name for the permission set, then click **Save**.
4. Make sure that this permission set name is selected in the left pane of the Permission Sets page.
5. Scroll down to the **McAfee Firewall Enterprise** setting and click **Edit**.

   The Edit Permission Set page appears.
6. Enable communication.
   - For ePolicy Orchestrator Management Server user accounts, select **Provide host information to a remote Firewall Enterprise Control Center**.
   - For Firewall Enterprise appliance user accounts, select **Permit data exchange with Firewall Enterprise systems**.
7. Click **Save**.

Create a user account for access to ePolicy Orchestrator

Before you begin

- Make sure that you have downloaded and installed the Firewall Enterprise ePolicy Orchestrator Extension on your ePolicy Orchestrator server.
- You must be an ePolicy Orchestrator global administrator to perform this task.

Create a user account to enable communication with ePolicy Orchestrator.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1. In the ePolicy Orchestrator console, select **Menu** | **User management** | **Users**.
2. Do one of the following:
   - To edit an existing user, select the user name on the left and click **Edit** at the bottom of the Users page. The Edit User *user_name* page appears. Skip to Step 4.
   - To add a new user, in the lower left corner of the Users page, click **New User**. The New User page appears. Go to the next step.
3. Type a unique name for this user in the **User name** field.
4. Select the checkbox for the permission set you created in the **Permission sets** field.
5. Specify values in the other fields as needed.
6. Click **Save**. If you added a new user, this user is added to the list of users on the Users page. If you edited an existing user, your changes are saved and you are returned to the Users page.

Create a permission set that allows users to view firewall data

> **Before you begin**
>
> - Make sure that you have downloaded and installed the Firewall Enterprise ePolicy Orchestrator Extension on your ePolicy Orchestrator server.
> - You must be an ePolicy Orchestrator global administrator to perform this task.

You can edit existing permission sets or add new sets to provide access to the information provided by the Firewall Enterprise ePolicy Orchestrator Extension. McAfee recommends creating at least one general permission set for use by any user that needs to view Firewall Enterprise ePolicy Orchestrator Extension data.

The following permissions can be added to existing permission sets to provide Firewall Enterprise ePolicy Orchestrator Extension functionality to ePolicy Orchestrator users:

- **Audit log** — View and purge audit log files.
- **Dashboards** — Use public dashboards, and edit and create personal dashboards.
- **Extensions** — Install and remove extensions.
- **McAfee Firewall Enterprise** — View and manage firewalls.
- **Queries** — Use and edit public queries, and edit and create personal queries.
- **Registered servers** — Use, create, and edit registered servers.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1. In the ePolicy Orchestrator console, select **Menu** | **User Management** | **Permission Sets**.
2. Do one of the following:
   - To edit an existing permission set, select the permission set in the list on the left. Skip to Step 6.
   - To create a new permission set, in the lower left corner of the Permission Sets page, click **New Permission Set**. The New Permission Set page appears. Go to the next step.
3. Specify a name for the permission set and select the users the set is assigned to.
4. Click **Save**.
5. In the Permission Sets page, select the new permission set from the Permission Sets list. The details for the selected permission set are displayed on the right.
6. To view all of the information that the Firewall Enterprise ePolicy Orchestrator Extension provides about the Firewall Enterprise appliances and Control Center Management Servers, configure the following settings. For most settings, higher levels of access are optional.

   a. For each setting that is listed, scroll to the setting and click **Edit**. The Edit Permission Set page for that setting appears.

   b. When you have finished editing the setting, click **Save**.

   > You can also add these settings to an existing permission set to provide access to the Firewall Enterprise ePolicy Orchestrator Extension information.

   - **Audit log** — **No permissions** is the default setting. To change the setting, select one of the following options:
     - **View audit log**
     - **View and purge audit log**
   - **Dashboards** — **No permissions** is the default setting. To change the setting, select one of the following options:

     > To work with the Firewall Enterprise ePolicy Orchestrator Extension, you must select at least the **Use public dashboards** setting, although higher settings are also allowed.

     - **Use public dashboards**
     - **Use public dashboards; create and edit personal dashboards**
     - **Use public dashboards; create and edit personal dashboards; make personal dashboards public**
   - **Extensions** — Select the **Install and remove extensions** checkbox to install and remove extensions. This checkbox is deselected by default.

     > You must have this setting selected in order to install and remove extensions. However, this setting is optional for viewing Firewall Enterprise ePolicy Orchestrator Extension data in the ePolicy Orchestrator console.

- **McAfee Firewall Enterprise** — **No permissions** is the default setting. To change the setting, select one of the following options:

  > To work with the Firewall Enterprise ePolicy Orchestrator Extension, you must select at least the **View McAfee Firewall Enterprise Control Center managed firewalls** or the **Permit data exchange with Firewall Enterprise systems** setting, although higher settings are also allowed.

  - **View McAfee Firewall Enterprise Control Center managed firewalls**
  - **Manage and view McAfee Firewall Enterprise Control Center servers and firewalls**
  - **Provide host information to a remote Firewall Enterprise Control Center** — McAfee recommends selecting this checkbox only for the unique permission set that is assigned to Control Center Management Server user accounts. You should not select this checkbox for other permission sets.
  - **Permit data exchange with Firewall Enterprise systems** — Select this checkbox for the unique permission set that is assigned to Firewall Enterprise appliance user accounts.

    > Do not select this checkbox for other permission sets.

- **Queries** — **No permissions** is the default setting. To change the setting, select one of the following options:

  > To work with the Firewall Enterprise ePolicy Orchestrator Extension, you must select at least the **Use public queries** setting, although higher settings are also allowed.

  - **Use public queries**
  - **Use public queries; create and edit personal queries**
  - **Use public queries; create and edit personal queries; make personal queries public**

- **Registered servers** — **No permissions** is the default setting. To change the setting, select one of the following options:
  - **Use registered servers**
  - **Create and edit registered servers**

7 Add or edit any additional permission settings as needed.

Create a user that can view firewall data

Before you begin

Make sure that you have downloaded and installed the Firewall Enterprise ePolicy Orchestrator Extension on your ePolicy Orchestrator server. Also, you must be an ePolicy Orchestrator global administrator to perform this task.

You can edit existing users or create new users so that you can provide them with access to the Firewall Enterprise ePolicy Orchestrator Extension data. This is accomplished by associating the user with one or more permission sets that provide this access. You can specify the permission set or sets in the User page or you can specify the User field of the Permission Settings page. This section describes the way to assign the permission set to the user.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1. In the ePolicy Orchestrator console, select **Menu** | **User management** | **Users**.
2. Do one of the following:
   - To edit an existing user, select the user name on the left and click **Edit** at the bottom of the Users page. The Edit User *user_name* page appears. Skip to Step 4.
   - To add a new user, in the lower left corner of the Users page, click **New User**. The New User page appears. Go to the next step.
3. Type a unique name for this user in the User name field.
4. Select the checkbox for the permission set that allows users to view firewall data, and for any other permission set you want to assign to the user in the Permission sets field.
5. Specify values in the other fields as needed.
6. Click **Save**. If you added a new user, this user is added to the list of users on the Users page. If you edited an existing user, your changes are saved and you are returned to the Users page.

3 Firewall Enterprise setup

Contents

- *Configure Firewall Enterprise appliances for ePolicy Orchestrator reporting*
- *Configure managed firewalls for ePolicy Orchestrator reporting*
- *Troubleshooting Firewall Enterprise to ePolicy Orchestrator communication*

Configure Firewall Enterprise appliances for ePolicy Orchestrator reporting

Configure data transmission from Firewall Enterprise to ePolicy Orchestrator.

> The firewall must be at version 8.3.0 or later.

Task

1. Set up ePolicy Orchestrator using the getting started instructions in the *McAfee ePolicy Orchestrator Product Guide*.

2. Install Firewall Enterprise ePO Extension 5.3.2 on the ePolicy Orchestrator.

3. Set up Firewall Enterprise to transmit data to ePolicy Orchestrator.

   a. From the Firewall Enterprise Admin Console, select **Monitor | ePolicy Orchestrator**.

      The ePolicy Orchestrator window appears.

   b. Complete the following fields to configure the contact information for connections to the ePolicy Orchestrator server:

      - **IP Address** — Type the IP address of the ePolicy Orchestrator server. To find the IP address associated with a host name, use the DNS Lookup window.

        > Do not use an IPv6 address.

      - **Port** — Type the ePolicy Orchestrator Client-to-server authenticated communication port that ePolicy Orchestrator is listening on for connections. Standard deployments of ePolicy Orchestrator use port 8444.

      - **User name** — Type the user name of an ePolicy Orchestrator user configured on the ePolicy Orchestrator server.

      - **Password** — Type the password of the ePolicy Orchestrator user specified in the User name field.

      - **Confirm password** — Type the password again.

c Click **Save**.

d Configure the Certificate Authority (CA) to use for validating the certificate that the ePolicy Orchestrator server presents during a connection.

- **Self-signed certificate** — If ePolicy Orchestrator uses a self-signed certificate, click Retrieve ePO root cert to retrieve the root certificate from the ePolicy Orchestrator server. Then, select ePO Server Certificate Authority from the Cert authority drop-down list.
- **CA certificate** — If ePolicy Orchestrator uses a certificate that has been signed by a CA, select the CA from the Cert authority drop-down list.

e Click **Save**.

f Select the **Enable communication with ePO** checkbox.

g Click **Save**.

Configure managed firewalls for ePolicy Orchestrator reporting

Use the Control Center Client application to set up a managed firewall to pass information to ePolicy Orchestrator.

Task

1 Create an ePolicy Orchestrator settings object.

a From the Control Center Client application, click **Policy**. The Policy icon page appears.

b On the Firewall Settings tab, right-click **ePolicy Orchestrator**, then select **Add Object**. The ePolicy Orchestrator window appears.

c Enter a name and description for the ePolicy Orchestrator settings object.

d Select **Enabled**.

e Enter the IP address of the ePolicy Orchestrator server.

f Enter the user name and password used to communicate with the ePolicy Orchestrator server.

g Click **Retrieve ePO root certificate**. The ePO root certificate is added to and selected in the CA certificate list.

h Click **OK**.

The new ePolicy Orchestrator settings object appears on the Firewall Settings tab under the ePolicy Orchestrator node.

2 Apply the ePolicy Orchestrator settings object to a managed firewall.

a In the Policy area, double-click the firewall. The Firewall window appears.

b Click **Offbox**. The Offbox area appears.

c In the ePolicy Orchestrator section, from the Configuration drop-down list, select the ePolicy Orchestrator settings object you created in step 1.

d Click **OK**. The Firewall window closes.

e Click **Apply**. The Apply Configuration window appears.

f Select the firewall, then click **OK**. The ePolicy Orchestrator settings are applied to the firewall.

The firewall sends information to the ePolicy Orchestrator server. Firewall details can be viewed on the ePolicy Orchestrator dashboards.

Troubleshooting Firewall Enterprise to ePolicy Orchestrator communication

Perform the following troubleshooting steps if communication is failing from Firewall Enterprise to ePolicy Orchestrator:

Task

1. Ensure you have installed **Firewall Enterprise ePO Extension 5.3.2** on the ePolicy Orchestrator server.

2. Ensure the user configured on the ePolicy Orchestrator server has been assigned a permission set with the **Permit data exchange with Firewall Enterprise systems** option selected.

3. Verify connectivity from the firewall to the ePolicy Orchestrator server using ping. You can perform a ping in the Firewall Enterprise Admin Console in the **Tools | Ping host** area.

4. Make sure the user name the Firewall Enterprise appliance uses to communicate with the ePolicy Orchestrator server is accurate.

   From the Firewall Enterprise command line, enter the following command.

   ```
   cf epo q
   ```

   The command returns the user name the firewall uses for ePO communication, and the IP address and port of the ePolicy Orchestrator server. For example:

   ```
       epo set cert_authority=EpoRootCert_192_168_254_200_8444 enabled=on \
              user=AuthorizedUser address=192.168.254.200 password='*****' port=8444
   ```

4 Control Center setup

Contents

- *Setup overview*
- *Configure Control Center for ePolicy Orchestrator*
- *Register Control Center*

Setup overview

Configuring Control Center for ePolicy Orchestrator communication is a three step process.

For each Control Center that will communicate with ePolicy Orchestrator, you must perform the following tasks:

1. In the Control Center Client application, configure the Control Center for ePolicy Orchestrator.
2. In ePolicy Orchestrator, create a user account for the Control Center.
3. In ePolicy Orchestrator, register the Control Center.

Configure Control Center for ePolicy Orchestrator

Before you begin

- Make sure that the Control Center Management Servers that ePolicy Orchestrator will communicate with are at version 5.3.0 or later.
- You must be a Control Center administrator to perform this task. If you do not have these privileges, contact your Control Center administrator and have him or her perform this task.

Use the ePolicy Orchestrator Settings window to configure the Control Center Management Server to communicate with the ePolicy Orchestrator server.

> You can create only one user with the ePolicy Orchestrator role.

You cannot register a Control Center Management Server with ePolicy Orchestrator until you have configured communication on the Control Center.

ePolicy Orchestrator requires a Control Center user with privileges to obtain and display health and status information from the Control Center about firewalls and the Control Center Management Server. When you create the ePolicy Orchestrator user, the user is automatically assigned the ePolicy Orchestrator role, which is available only to one ePolicy Orchestrator user. Additionally, the ePolicy Orchestrator user is allowed to access only the ePolicy Orchestrator configuration domain, in which read-only access to all firewall objects is allowed, but in which all other object access is denied. By default, this user has access to all of the firewalls. However, you can restrict this access on the Firewall Access List tab of the Control Center Administrator window.

> This information is also documented in the *McAfee Firewall Enterprise Control Center Product Guide* and in the Control Center Help.

For option definitions, press **F1** in the Control Center Client application.

Task

1. Log on to the Control Center Client application.
2. In the Client application navigation bar, select **Control Center**.
3. In the Control Center tree, expand the **Settings** node.
4. Double-click **ePolicy Orchestrator**. The ePolicy Orchestrator Settings window appears. Make sure that the ePO Reports tab is selected.
5. Complete the fields on the ePO Reports tab.
   - **Allow Control Center to retrieve reports from the ePO server** — Select this checkbox. This checkbox determines whether the Control Center will be able to retrieve reports from the ePolicy Orchestrator server. This checkbox is deselected by default.
   - **ePO Server Information** — Use the fields in this area to configure the settings that are required to access the ePolicy Orchestrator server. All of the fields in this area are required if the **Allow Control Center to retrieve reports from the ePO server** checkbox is selected.
     - **Hostname** — Type the IP address or host name of the ePolicy Orchestrator server you want the Control Center to communicate with.
     - **Port** — Specify the port that will be used to communicate with the ePolicy Orchestrator server. The default value is port 8443.
     - **Username** — Type the user name that is required to access the ePolicy Orchestrator server.
     - **Password** — Type the password for the ePolicy Orchestrator user name.
     - **Confirm password** — Type the password again to confirm it.
6. Click the **Control Center User** tab.
7. Click **Create User**. The Control Center User Manager window appears.
8. Create a new user with the ePolicy Orchestrator role.
   a. Select the **Account Enabled** checkbox to enable the ePolicy Orchestrator user.
   b. Type a user name and password for the ePolicy Orchestrator user.

   > Make note of this user name and password, because you will need to specify both values when you register this Control Center Management Server with the ePolicy Orchestrator server.

   c. On the Roles tab, select the **ePolicy Orchestrator** checkbox.
   d. Click **OK**. The ePolicy Orchestrator user appears on the Control Center User tab.

Register Control Center

The Control Center Management Server provides information on managed appliances to ePolicy Orchestrator. Add, edit, and delete Control Center Management Servers on the Registered Servers page.

Control Center Management Servers, High Availability (HA), and the ePolicy Orchestrator platform

If you have the High Availability (HA) feature configured on one or more pairs of Control Center Management Servers, you should register only the primary Management Server of each pair of HA servers with the ePolicy Orchestrator server on the Registered Servers page.

If the primary Control Center Management Server fails, the ePolicy Orchestrator server will not automatically switch over to the backup (secondary) Management Server. You can monitor the connection failures by viewing the audit log (**User Management** | **Audit Log**). When you verify the failure in the audit log, you must manually edit the registered server information in the Registered Servers page by changing the IP address of the registered Control Center Management Server from the primary IP address to the IP address of the backup Management Server. You must also request a new client certificate from the backup Management Server.

Add a Control Center Management Server

You must configure the Control Center Management Servers on the Registered Servers page before you can view information about the Firewall Enterprise appliances or the Control Center Management Server.

> Although there is information about the Registered Servers pages in the ePolicy Orchestrator console Help, there are specific fields that are unique to the Control Center Management Server. The following task describes these fields when you are adding a new Control Center Management Server to the ePolicy Orchestrator server.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1. In the ePolicy Orchestrator console, select **Menu** | **Configuration** | **Registered Servers**. The Registered Servers page appears.
2. In the lower left corner, click **New Server**. The Registered Server Builder page appears.
3. In the Server type field, select **McAfee Firewall Enterprise Control Center**.
4. Specify a unique name and add any notes. Click **Next**. The Details page appears.
5. Specify the IP address or the name of the Control Center Management Server.
6. In the Control Center user name field, type the user name you set on the Control Center User tab of the ePolicy Orchestrator Settings window on the Control Center.
7. In the Control Center password fields, type the password you set on the Control Center.
8. In the Server web service port field, enter the port the Control Center Management Server uses for web traffic. The default is port 9005.

9 For the Certificate field, you can create a new, server-signed, client certificate.

 a Make sure that the Control Center Management Server is running and that the Control Center user has been configured on it (in the ePolicy Orchestrator Settings window).

 b Click **Create New Certificate**. The certificate from the Control Center Management Server appears.

 c Confirm that the certificate identifies the registered Control Center Management Server.

10 Click **Save**.

Delete a Control Center Management Server from the ePolicy Orchestrator server

Use this task to remove a Control Center Management Server from ePolicy Orchestrator management.

> If you ever need to re-register this Control Center Management Server, you must re-acquire the client certificate. To do this, edit the server and click Create New Certificate on the Details page.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1. In the ePolicy Orchestrator console, select **Menu** | **Configuration** | **Registered Servers**.
2. In the Firewall Management group bar, select the Control Center Management Server to be deleted.
3. Click **Actions**, then click **Delete**.
4. Accept the change in the confirmation message that appears.

5 Firewall data

Contents

- *View Firewall Enterprise and Control Center data in the ePolicy Orchestrator console*
- *Change how ePolicy Orchestrator displays firewall data*
- *View ePolicy Orchestrator Host Data reports from the Control Center Client application*

View Firewall Enterprise and Control Center data in the ePolicy Orchestrator console

After communication has been established between firewalls, Control Center, and the ePolicy Orchestrator server, and you have configured your users and permission sets, you can view firewall data in the ePolicy Orchestrator console.

The Firewall Enterprise ePolicy Orchestrator Extension provides several dashboards for quickly viewing firewall data:

- Firewall internal host mappings
- Firewall Resources
- Firewall Stats

See the *McAfee ePolicy Orchestrator Product Guide* for more information on working with dashboards.

Detailed information on managed and monitored firewalls can be accessed on the Enterprise Firewalls pages.

View internal host activity

Before you begin
You must have a registered Firewall Enterprise appliance communicating with ePolicy Orchestrator.

Use the Firewall internal host mappings dashboard to view information on protected hosts and firewall versions.

The Firewall internal host mappings dashboard displays the following chart-based queries.

FWADDR: Firewall Internal Host Grouping query

FWADDR: New Host Information query

FWADDR: Firewall Hit Count Grouping query

FWADDR: Firewall Top 10 Internal Hosts query

Do not edit or remove firewall queries.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1 In the ePolicy Orchestrator console, click **Dashboards**.

2 From the **Dashboards** drop-down list, select **Firewall internal host mapping**. The Firewall internal host mapping dashboard appears.

From the Firewall internal host mapping dashboard, you can do the following.

Task	Steps
Expand a report	Click the drop-down menu arrow in the upper left corner of the report, then select **Full Screen**.
View information about a specific firewall	Click a firewall on the report. Information on the specified firewall is displayed.

View firewall resources

Before you begin

You must have a registered Control Center Management Server communicating with the ePolicy Orchestrator.

Use the Firewall Resources dashboard to quickly view information on the performance of managed firewalls, including memory use, proxy and VPN sessions, and data flow.

The Firewall Resources dashboard displays the following chart-based queries.

FWCC: Firewall Physical Memory Usage

FWCC: Firewall Filter Sessions

FWCC: Firewall Inbound Data (Bytes)

FWCC: Firewall Virtual Memory Usage

FWCC: Firewall Proxy Sessions

FWCC: Firewall Inbound Data Rate (Bytes/Sec)

FWCC: Firewall CPU Usage

FWCC: Firewall Active VPN Sessions

FWCC: Firewall Outbound Data (Bytes)

FWCC: Firewall Disk Usage

FWCC: Firewall Idle VPN Sessions

FWCC: Firewall Outbound Data Rate (Bytes/Sec)

You can edit the settings for the queries that produce these charts from the Queries page.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1 In the ePolicy Orchestrator console, click **Dashboards**.

2 From the **Dashboards** drop-down list, select **Firewall Resources**. The Firewall Resources dashboard appears.

From the Firewall Resources dashboard, you can do the following.

Task	Steps
Expand a report	Click the drop-down menu arrow in the upper left corner of the report, then select **Full Screen**.
View information about a specific firewall	Select the firewall from the Firewall drop-down list on any report. All the queries on the dashboard display information about the selected firewall.
View details about a specific time period	1 Click the desired data point on a report. Information for the selected time period is displayed in a table. 2 Click a row in the table to view the McAfee Firewall Activity Details page for the firewall.

View firewall statuses

Before you begin

You must have a registered Control Center Management Server communicating with the ePolicy Orchestrator.

Use the Firewall Stats dashboard to quickly view status information about registered Control Center Management Servers and managed firewalls.

The Firewall Stats dashboard displays the following chart-based queries.

FWCC: Firewall Enterprise Control Center Run Statuses

FWCC: Firewall Versions

FWCC: Firewall Run Statuses

FWCC: Alert Summary

You can edit the settings for the queries that produce these charts from the Queries page.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1. In the ePolicy Orchestrator console, click **Dashboards**.
2. Click the **Firewall Stats** tab. The Firewall Stats dashboard appears.

   From the Firewall Stats dashboard, you can do the following.

Task	Steps
Expand a report	Click the drop-down menu arrow in the upper left corner of the report, then select **Full Screen**.
View details about Control Center Management Servers with a specific run status	Click a run status in the FWCC: Firewall Enterprise Control Center Run Statuses report. The McAfee Firewall Enterprise Control Centers Details page appears. Use the Previous and Next arrows to view details about other Control Centers with the same status.
View details about managed firewalls with a specific run status	1 Click a run status in the FWCC: Firewall Run Statuses report. The FWCC: Firewall Run Statuses page appears. 2 Click a firewall entry. The McAfee Firewalls Details page appears. Use the **Previous** and **Next** arrows to view details about other firewalls with the same status.

Task	Steps
View details about managed firewalls running a specific software version	Click a software version in the FWCC: Firewall Versions report. The McAfee Firewalls Details page appears. 💡 Use the Previous and Next arrows to view details about other firewalls with the same software version.
View alert information about a specific firewall	Select the firewall from the **Firewall** drop-down list. All the queries on the dashboard display information about the selected firewall.
View details about alerts of a specific priority	Click an alert priority in the FWCC: Alert Summary report. The McAfee Firewall Alert Summary Details page appears. 💡 Use the Previous and Next arrows to view details about other alerts with the same priority.

View all firewalls managed by a Control Center Management Server

Use the Enterprise Firewalls page to view details about all the firewalls under Control Center Management.

For option definitions, click **?** in the ePolicy Orchestrator console.

In the ePolicy Orchestrator console, select **Menu** | **Network** | **Firewalls**. The Enterprise Firewalls page appears.

From the Enterprise Firewalls page, you can do the following.

Task	Steps
Refresh firewall data	Select **Actions** | **Update**.
View additional details about a specific firewall	Click a row in the table. The McAfee Firewalls Details page appears for the selected firewall. Use the left and right arrows at the bottom of the page to view details about other managed firewalls.
View blackholed IP addresses for selected firewalls	1 Select the checkboxes of the firewalls you want to see blackholed IP addresses for. 2 Select **Actions** | **Blackholed IPs**. The firewall - Blackholed IPs page appears, displaying the IP address, zone, and expire time for each IP address blackholed by one of the selected firewalls. Click **Close** to return to the Enterprise Firewalls page.
View the cluster status of selected firewalls	1 Select the checkboxes of the firewalls you want to see the interfaces of. 2 Select **Actions** | **Interfaces**. The firewall - Interfaces page appears, displaying the name, IP address, zone, active network interface card (NIC), active speed, and status of the interfaces of the selected firewalls. Click **Close** to return to the Enterprise Firewalls page.

Task	Steps
View the interfaces for selected firewalls	1 Select the checkboxes of the firewalls you want to see routing tables for. 2 Select **Actions** | **Routing Table**. The firewall - Routing Table page appears, displaying the destination, gateway, flags, zone, network interfaces, and expire information for routes on the selected firewalls. Click **Close** to return to the Enterprise Firewalls page.
View the routing tables for selected firewalls	1 Select the checkboxes of the firewalls you want to see signature versions for. 2 Select **Actions** | **Blackholed IPs**. The firewall - Blackholed IPs page appears, displaying the IP address, zone, and expire time for each IP address blackholed by one of the selected firewalls. Click **Close** to return to the Enterprise Firewalls page.
View signature versions for selected firewalls	1 Select the checkboxes of the firewalls you want to see blackholed IP addresses for. 2 Select **Actions** | **Signature Versions**. The firewall - Signature Versions page appears, displaying the name and version of the signatures of the selected firewalls. Click **Close** to return to the Enterprise Firewalls page.
View the system load of selected firewalls	1 Select the checkboxes of the firewalls you want to see the system load of. 2 Select **Actions** | **System Load**. The firewall - System Load page appears, displaying the name and value for different load averages for the selected firewalls. Click **Close** to return to the Enterprise Firewalls page.
Export the Enterprise Firewalls table	1 Select **Actions** | **Export Table**. The Export window appears, providing configuration options for exporting the file. 2 Complete the fields. 3 Click Export.
View the VPN tunnels of selected firewalls	1 Select the checkboxes of the firewalls you want to see the VPN tunnels of. 2 Select **Actions** | **VPN Tunnels**. The firewall - VPN Tunnels page appears, displaying the names and statuses for the VPN tunnels used by the firewalls. 3 Click **Close** to return to the Enterprise Firewalls page.

Change how ePolicy Orchestrator displays firewall data

You can configure how often firewall data is retrieved and how long the activity records are kept.

Change data refresh settings and host retention

Use the Edit Mcafee Firewall Enterprise page of the Server Settings window to configure how often Firewall Enterprise data displayed in ePolicy Orchestrator is refreshed and how long host records are retained.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1. In the ePolicy Orchestrator console, select **Menu** | **Configuration** | **Server Settings**.
2. From the Setting Categories list, select **McAfee Firewall Enterprise**. The Refresh interval and Activity record retention settings are displayed.
3. Click **Edit**. The Edit McAfee Firewall Enterprise page appears.
4. In the **Refresh interval** field, type the number of minutes to wait before refreshing health and status data.
5. In the **Activity record retention** field, type the number of hours to retain information in the firewall activity table.
6. In the **Internal host records retention** field, type the number of days to keep host records.
7. Click **Save**.

View ePolicy Orchestrator Host Data reports from the Control Center Client application

Before you begin

- The Firewall Enterprise ePolicy Orchestrator Extension must be installed on the ePolicy Orchestrator server.
- You must configure settings for the ePolicy Orchestrator server in the ePolicy Orchestrator Settings window. This is to allow the Control Center to communicate with the ePolicy Orchestrator server.
- You must have selected the Allow Control Center to retrieve reports from the ePO server checkbox on the ePolicy Orchestrator Settings window.

After you have configured the report communication on both the Control Center and the ePolicy Orchestrator server, you can view information about hosts in an ePolicy Orchestrator Host Data report that is available for a host in Control Center. This host data is maintained on the ePolicy Orchestrator server. To display data about a particular host, the host object must be managed by the ePolicy Orchestrator server.

For option definitions, press **F1** in the Control Center Client application.

Task

1. Log on to the Control Center Client application.
2. From the navigation bar, select **Policy**.
3. In the lower left corner of the window, click the **Rule Objects** tab.
4. Expand the **Network Objects** node.
5. Click the Policy group bar and then expand the **Network Objects** branch in the tree. The subnodes are displayed.

6. Expand the **Hosts** subnode. All of the defined host objects are displayed.
7. Right-click the object for which you want to view ePolicy Orchestrator server data and select **Show ePO Data**. The ePO Host Data page appears.

   > In the System tree, the host object must be managed by the ePolicy Orchestrator server to retrieve the ePO Host Data, else no data is displayed.

6 Queries

Contents

- *Firewall Enterprise ePolicy Orchestrator Extension queries*
- *Firewall Enterprise Report queries*
- *Generate a Firewall Enterprise Report query*
- *Control Center queries*
- *Generate a Control Center query*

Firewall Enterprise ePolicy Orchestrator Extension queries

Several queries are provided as part of the Firewall Enterprise ePolicy Orchestrator Extension. The results of Firewall Enterprise-specific queries can be viewed on the appropriate dashboards, or by running the queries on the Queries page. Each query that polls information from Firewall Enterprise appliances begins with the prefix FWADDR. Each query that polls information from a Control Center begins with the prefix FWCC.

See the *McAfee ePolicy Orchestrator Product Guide* for more information about working with queries.

Firewall Enterprise Report queries

The following Firewall Enterprise queries are provided with the Firewall Enterprise ePolicy Orchestrator Extension.

Table 6-1 Firewall Enterprise Report queries

Query	Description
FWADDR: Firewall Details query	Displays firewall information.
FWADDR: Firewall Hit Count Grouping query	Displays firewalls by hit count.
FWADDR: Firewall Top 10 Internal Hosts query	Displays the internal hosts with the most traffic through the firewall.
FWADDR: Firewall Version Grouping query	Displays firewalls by software version.
FWADDR: New Host Information query	Displays new host information.

Use the drop-down lists at the top of the report to run Firewall Enterprise Report queries for specific firewalls or for different time periods.

Generate a Firewall Enterprise Report query

Use the Queries page to run a Firewall Enterprise Report query.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1 In the ePolicy Orchestrator console, select **Queries & Reports**. The Queries page appears.

2 Scroll down to the desired query, and click **Run**. The results of the query are displayed.

For Firewall Enterprise Report queries, you can perform the following action.

Task	Steps
Export report data	1 Select **Options** | **Export Data**. The Export window appears, providing configuration options for exporting the file. 2 Complete the fields. 3 Click **Export**.

Control Center queries

The following Control Center queries are provided with the Firewall Enterprise ePolicy Orchestrator Extension.

Table 6-2 Control Center queries

Query	Description
FWCC: Active Firewall VPN Sessions	Displays the average number of active VPN sessions taking place on managed firewalls by hour.
FWCC: Alert Summary	Displays the total number of alerts on managed firewalls by type.
FWCC: Firewall CPU Usage	Displays the average CPU use of managed firewalls by hour.
FWCC: Firewall Disk Usage	Displays the average disk use percentage of managed firewalls by hour.
FWCC: Firewall Enterprise Control Center Run Statuses	Displays the number of Control Center Management Servers organized according to run status.
FWCC: Firewall Filter Sessions	Displays the average number of filter sessions for managed firewalls by hour.
FWCC: Firewall Physical Memory Usage	Displays the average percentage of physical memory used by managed firewalls by hour.
FWCC: Firewall Proxy Sessions	Displays the average number of proxy sessions for managed firewalls by hour.
FWCC: Firewall Run Statuses	Displays the number of managed firewalls according to run status of each firewall.
FWCC: Firewall Versions	Displays the number of managed firewalls according to the version of each firewall.
FWCC: Firewall Virtual Memory Usage	Displays the average percentage of virtual memory used by managed firewall by hour.
FWCC: Idle Firewall VPN Sessions	Displays the average number of idle VPN session for managed firewalls by hour.

Table 6-2 Control Center queries *(continued)*

Query	Description
FWCC: Inbound Data Rate Through Firewall (Bytes/Sec)	Displays the average inbound data rate for managed firewalls in bytes per second by hour.
FWCC: Inbound Data Through Firewall (Bytes)	Displays the average amount inbound data for managed firewalls in bytes by hour.
FWCC: Outbound Data Rate Through Firewall (Bytes/Sec)	Displays the average outbound data rate for managed firewalls in bytes per second by hour.
FWCC: Outbound Data Through Firewall (Bytes)	Displays the average outbound data rate for managed firewalls in bytes per second by hour.

Generate a Control Center query

Use the Queries page to run a Control Center query.

For option definitions, click **?** in the ePolicy Orchestrator console.

Task

1 In the ePolicy Orchestrator console, select **Queries & Reports**. The Queries page appears.

2 Scroll down to the desired query, and click **Run**.

The results of the query are displayed. For Control Center queries, you can perform the following actions.

Task	Steps
View details about a specific time period	Click the desired data point on a report. Information for the selected time period is displayed in a table. Click a row in the table to view the McAfee Firewall Activity Details page for the firewall.
[FWCC Alert Summary only] View details about alerts	Click an alert priority in the FWCC: Alert Summary report. The McAfee Firewall Alert Summary Details page appears. Use the left and right arrows at the bottom of the page to view details about other alerts with the same priority.
[FWCC: Firewall Enterprise Control Center Run Statuses only] View details about Control Center Management Servers	Click a run status in the FWCC: Firewall Enterprise Control Center Run Statuses report. The McAfee Firewall Enterprise Control Centers Details page appears. Use the left and right arrows at the bottom of the page to view details about other Control Centers with the same status.
[FWCC: Firewall Run Statuses and FWCC: Versions only] View details about managed firewalls	Click a run status in the FWCC: Firewall Run Statuses report. The McAfee Firewalls Details page appears. Use the left and right arrows at the bottom of the page to view details about other firewalls with the same status.
Export report data	1 Select **Options** | **Export Data**. The Export window appears, providing configuration options for exporting the file. 2 Complete the fields. 3 Click **Export**.

Index

A

about this guide 5
alerts
    displaying for firewalls and Control Center Management Servers 31, 39
    displaying totals for each firewall or Control Center Management Server 31, 39

C

Control Center
    setting up for ePolicy Orchestrator 25
    viewing managed firewalls 32
Control Center Management Servers
    deleting from ePolicy Orchestrator 28
    display run status 31, 39
    displaying alerts in ePolicy Orchestrator 31, 39
    displaying information about 31, 39
    registering High Availability (HA) servers with ePolicy Orchestrator 27
    registering with ePolicy Orchestrator 27
conventions and icons used in this guide 5

D

dashboards 29
    Firewall internal host mapping 29
    Firewall Resources 30
    Firewall Stats 31
data
    changing host retention period 33
    changing refresh rate 33
documentation
    audience for this guide 5
    product-specific, finding 6
    typographical conventions and icons 5

E

ePO Extension 7
    using with Control Center 8
    using with Firewall Enterprise 8
ePolicy Orchestrator
    adding Control Center Management Servers 27
    configuring Control Center for 25
    deleting Control Center Management Servers 28

ePolicy Orchestrator *(continued)*
    downloading the Firewall Enterprise ePO Extension 11
    registering the primary HA Management Serve 27
    setup overview 11
    user 25
extensions 12

F

Firewall Enterprise 8
    configuring for ePolicy Orchestrator communication 21
    troubleshooting ePolicy Orchestrator communication 23
Firewall Enterprise ePO Extension
    downloading 11
Firewall internal host mapping dashboard 29
Firewall Resources dashboard 30
Firewall Stats dashboard 31
firewalls 8
    configuring for ePolicy Orchestrator communication 21
    displaying alerts in ePolicy Orchestrator 31, 39
    troubleshooting ePolicy Orchestrator communication 23
    viewing Control Center managed 32
    viewing data 29
    viewing details about 31, 39
    viewing host data 29
    viewing resource data 30
    viewing statuses 31
    viewing versions 31

H

HA Management Servers
    registering the primary server with ePolicy Orchestrator 27
    viewing failover information 27
High Availability Management Servers
    see HA Management Servers 27
host objects
    viewing ePO Data reports in Control Center 34

M

McAfee ServicePortal, accessing 6

P

permission sets
- configuring for general access 16

Q

queries 37
- Control Center 38
- Firewall Enterprise Report 37
- generating Control Center 39
- generating Firewall Enterprise Report 38

R

run status
- displaying for Control Center Management Servers 31, 39
- displaying for firewalls 31, 39

S

ServicePortal, finding product documentation 6

T

Technical Support, finding product information 6

U

users
- configuring for data access 18

V

viewing firewall data 29