McAfee Security Connected
Integrating ePO and MFECC

Table of Contents

Overview

The integration between ePolicy Orchestrator 4.6.6 (ePO) and McAfee Firewall Enterprise Control Center 5.3.1 (MFECC) creates a trusted communication channel allowing MFECC to send top-level data from multiple firewalls to ePO.

It is possible to view or drill down for detailed data on a firewall or the Control Center that monitors it. Added visibility includes:

1. Firewall alerts
2. Firewall health statistics
3. Historical performance trends
4. Tracking of version and patch levels
5. Hosts and endpoints used in policies
6. Host profile information directly from analytical tools

Alternatively MFECC admins can query ePO for host data on any network object or IP address.

This integration leverages McAfee Firewall Enterprise ePO extension 5.3.0.
Note: McAfee Firewall Enterprise ePO extension 5.3.0 is not compatible with ePolicy Orchestrator 5.x, only ePolicy Orchestrator 4.6.6.

User Accounts & Privileges

Integration will require:

Firewall Enterprise Control Center Administrator account.
ePO Global Admin account.
The steps below cover adding an optional Control Center admin user in ePO with the necessary permission sets.

Prerequisites

The McAfee Firewall Enterprise ePO extension 5.3.0 can be downloaded from the McAfee Product Download page. Log in with your Grant number to access this extension in the Firewall Related Software.

No changes are required prior to setting up integration between ePO and MFE.

Configuration Steps

Install the McAfee Firewall Enterprise ePO extension.

1. Log on to ePolicy Orchestrator.

2. In the ePolicy Orchestrator console, **select** Menu → Software → Extensions.
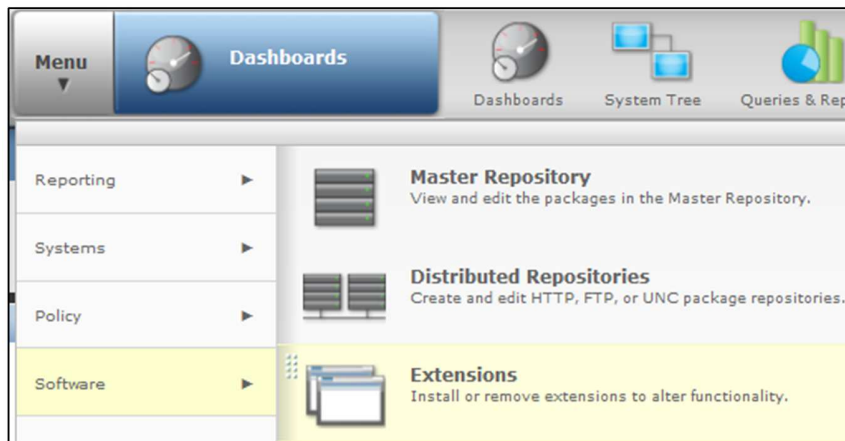

3. At the bottom of the Extensions pane on the left side of the Extensions page, **click** Install Extension.
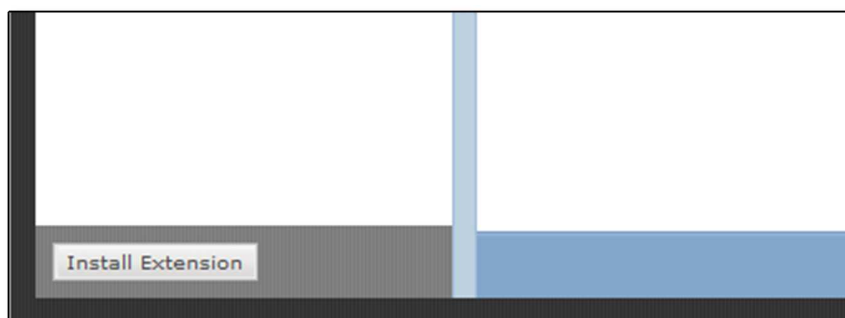
4. Browse to the Firewall Enterprise ePolicy Orchestrator Extension .zip file you downloaded from the McAfee downloads page. Click Open to select the file, then click OK to proceed with the selection. Click OK to install the extension.
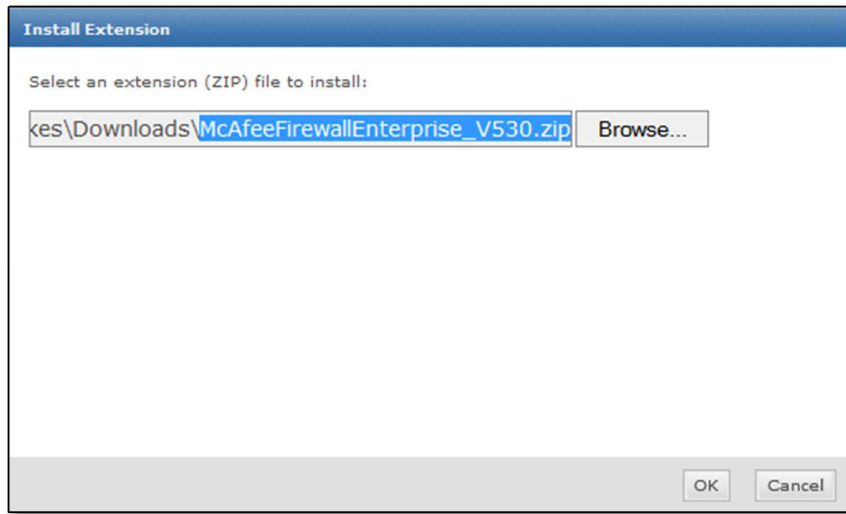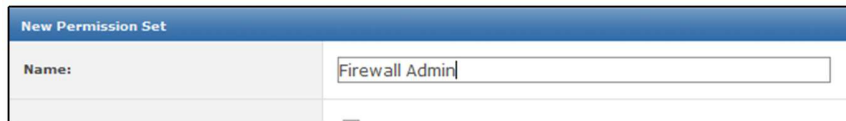

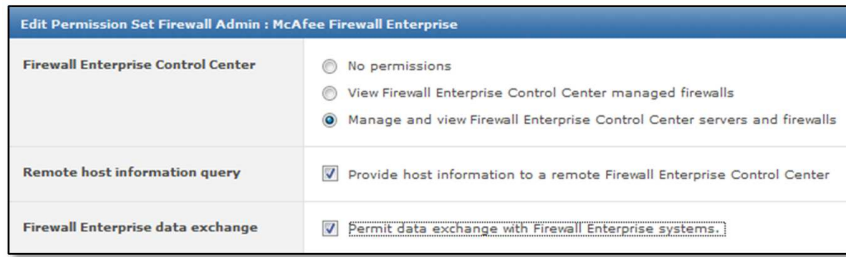5. In the ePO console select Menu → User Management → Permission Sets.
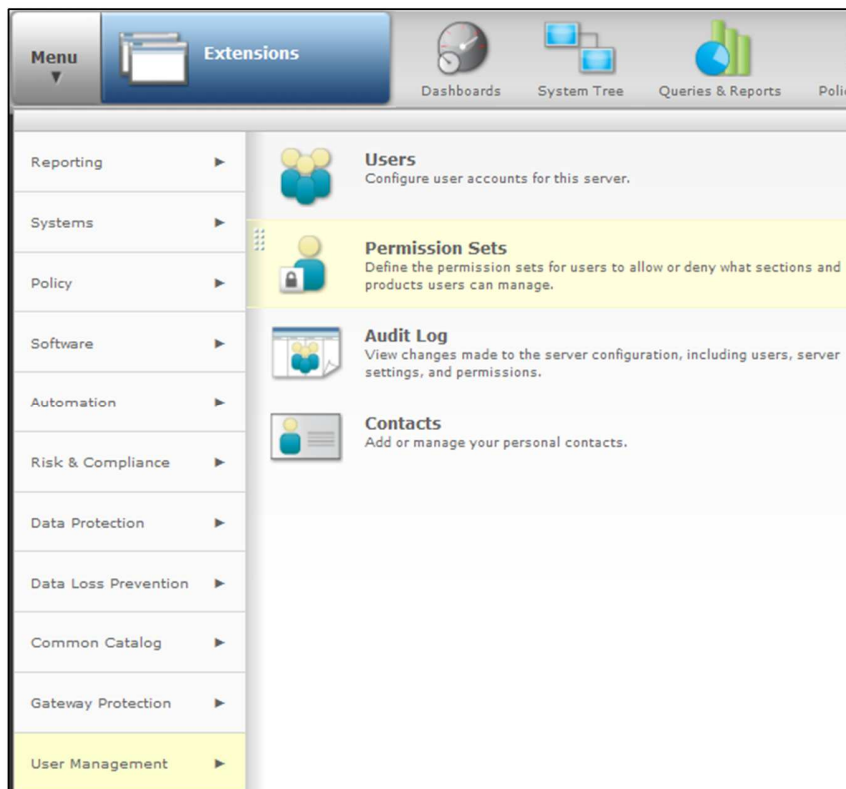
6. Create a permission set that allows data transmission. Select New from the bottom of the page.
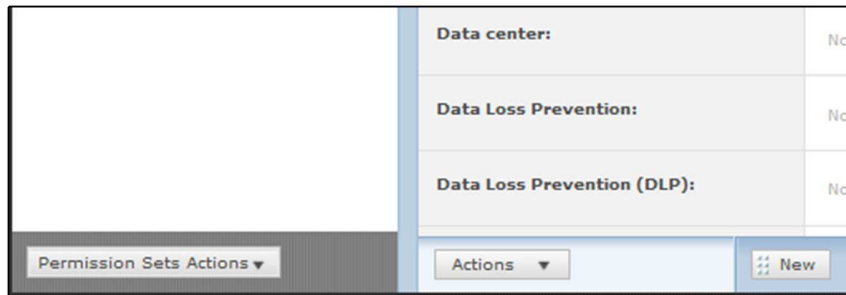
7. Name the Permission Set and **click** save.

8. Edit the permission set to have full rights for McAfee Firewall Enterprise.

9. [Optional] Consider adding the following permissions as well if the user created will need to log into ePO and view/create dashboards and queries.
   a. Audit log — View and purge audit log files.
   b. Dashboards — Use public dashboards, and edit and create personal dashboards.
   c. Extensions — Install and remove extensions.
   d. McAfee Firewall Enterprise — View and manage firewalls.
   e. Queries — Use and edit public queries, and edit and create personal queries.
   f. Registered servers — Use, create, and edit registered servers.

10. Create a new user with that permission set. In the ePO Console select Menu → User Management → Users.
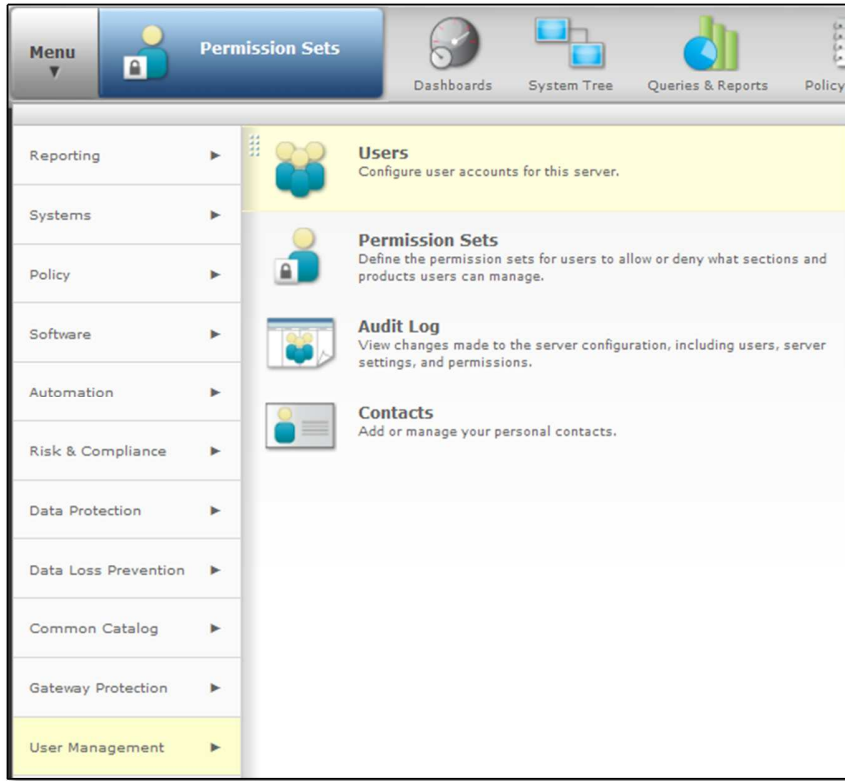
11. Click New User at the bottom left. Give the user a name and assign a password. Authentication type can be ePO authentication.

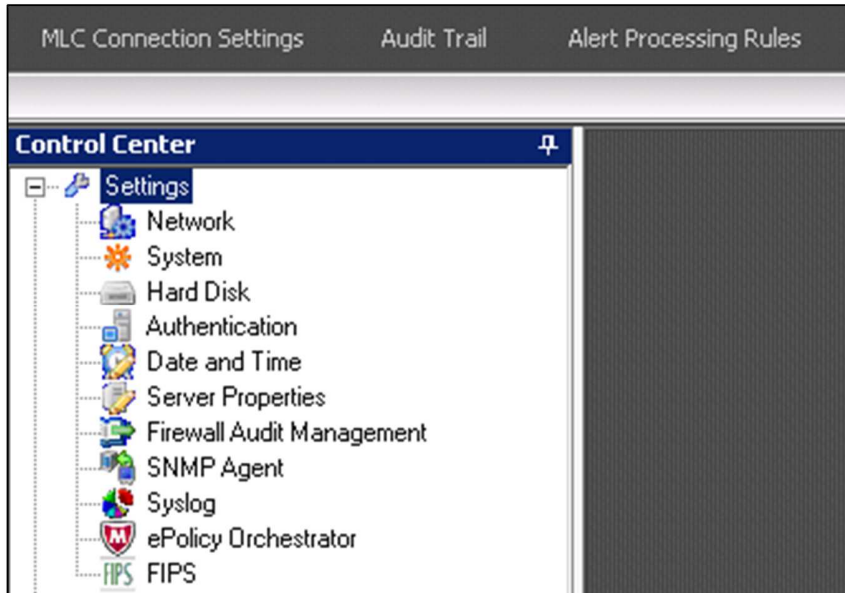**Set up Firewall Enterprise Control Center to transmit data to ePolicy Orchestrator.**
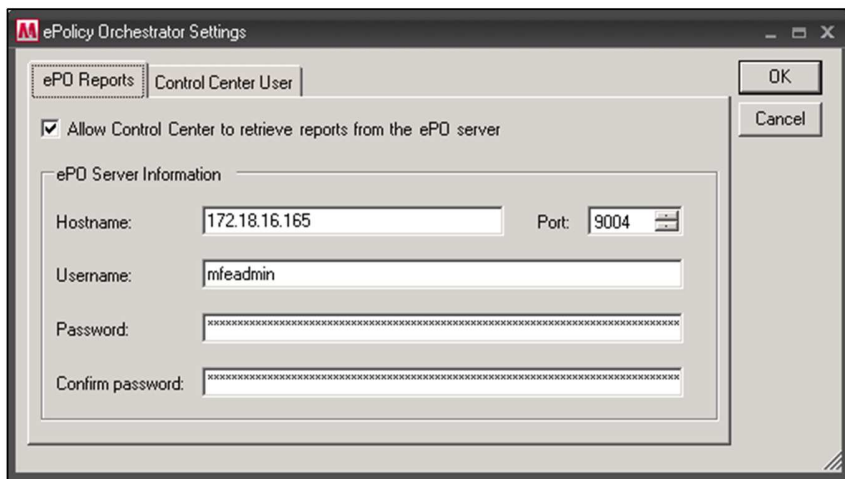1. Log on to the Control Center Client application.

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.
    a. 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.
    b. 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.
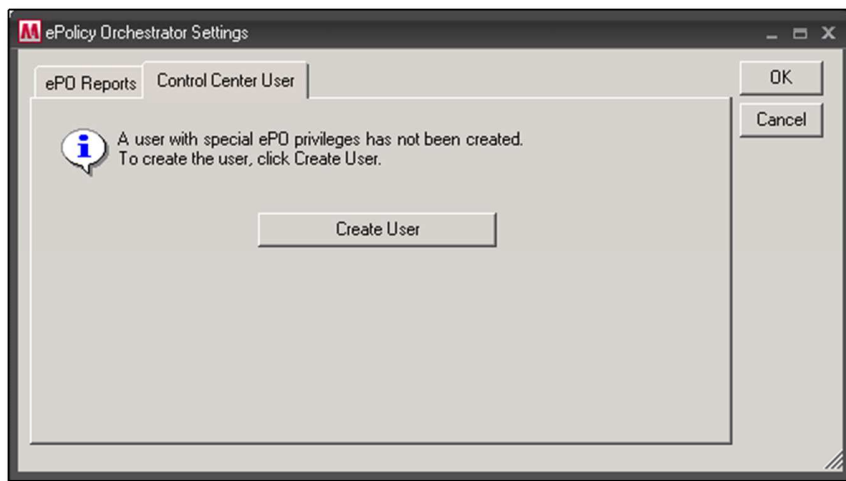
7. Click Create User. The Control Center User Manager window appears.
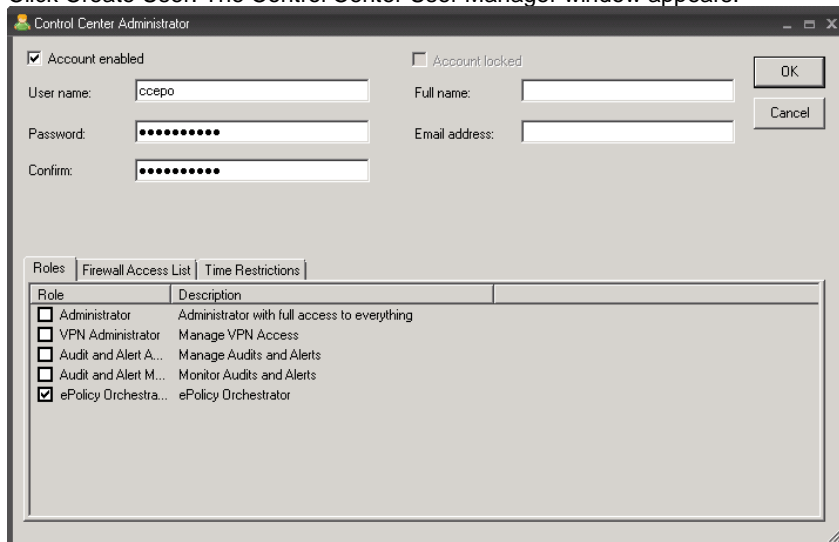
8. Create a new user with the ePolicy Orchestrator role.
   a. Select the Account Enabled checkbox to enable the ePolicy Orchestrator user.
   b. Type a user name and password for the ePolicy Orchestrator user.
      Make note of this user name and password, because you will need to specify both
      values when you register this Control Center Management Server with the ePolicy
      Orchestrator server.
   c. On the Roles tab, select the ePolicy Orchestrator checkbox.
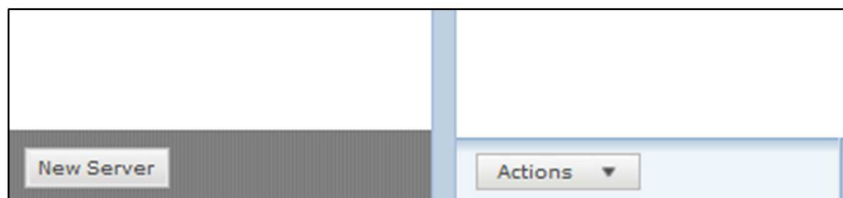   d. Click OK. The ePolicy Orchestrator user appears on the Control Center User tab.
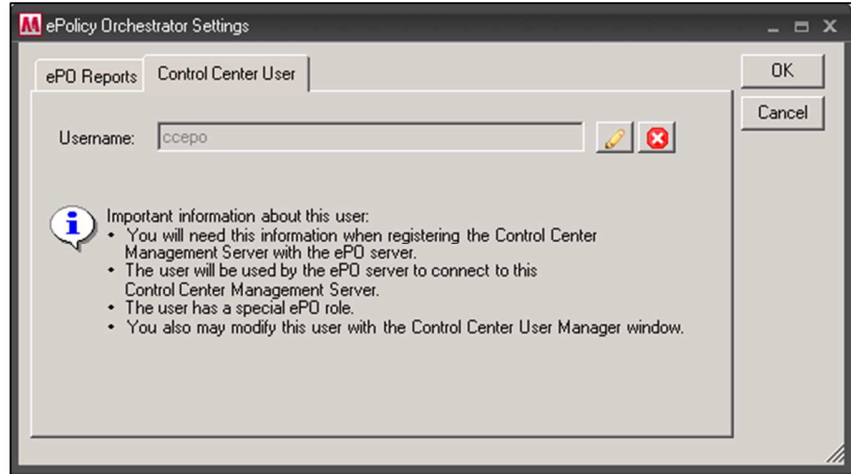
Register Control Center with ePO
1. In the ePolicy Orchestrator console, select Menu → Configuration → Registered Servers. The
   Registered Servers page appears.

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.

Registered Server Builder	1 Description
Server type:	Boot attestation server ▼
	Boot attestation server
Name:	Database Server
	Directory Services Connector
	DLP Manager
Notes:	Email and Web Security 5.x
	ePO
	LDAP Server
	MAM Console Server
	McAfee Email Gateway 6.7.x
	McAfee Email Gateway 7.0
	McAfee Firewall Enterprise Control Center

4. Specify a unique name and add any notes. Click Next. The Details page appears.

Registered Server Builder	1 Description
Server type:	McAfee Firewall Enterprise Control Center
Name:	mfecc
Notes:	

5. Specify the IP address or the name of the Control Center Management Server.

Registered Server Builder	1 Description
Server name or address:	172.18.16.34
Control Center user name:	ccepo
Control Center password:	Password: ●●●●●●●● Confirm password: ●●●●●●●●
Server web service port:	9005

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.
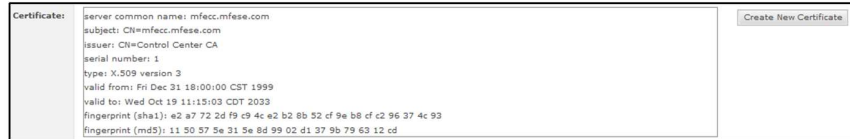
10. Click Save.

Value Add

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.

This integration is particularly beneficial regarding troubleshooting. It's common for help desk staff to have access to ePO, but no firewall administrative access.

When an outage occurs, the help desk staff can use the McAfee ePO server to troubleshoot the situation and determine if the firewall is the cause before contacting firewall administrators.