



User Guide

# McAfee Security-as-a-Service Extension

For use with ePolicy Orchestrator® 4.6.0 Software

## **COPYRIGHT**

Copyright © 2011 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

## **TRADEMARK ATTRIBUTIONS**

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

## **LICENSE INFORMATION**

### **License Agreement**

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents

	<b>Preface</b>	<b>5</b>
	About this guide . . . . .	5
	Audience . . . . .	5
	Conventions . . . . .	5
	Finding product documentation . . . . .	6
<b>1</b>	<b>Introduction to the Security-as-a-Service extension</b>	<b>7</b>
	Management of McAfee SaaS protection services . . . . .	7
	Required components . . . . .	8
	Component setup and integration . . . . .	8
<b>2</b>	<b>Installing and configuring the extension</b>	<b>11</b>
	Overview of installation and setup . . . . .	11
	Features added to the ePolicy Orchestrator environment . . . . .	12
	Overview of feature configuration . . . . .	13
	Install the product extension . . . . .	14
	Configuration of registered servers . . . . .	16
	Register a SecurityCenter account . . . . .	16
	View or edit a list of registered SecurityCenter accounts . . . . .	17
	Delete a registered SecurityCenter account . . . . .	18
	Data synchronization with the SecurityCenter . . . . .	18
	About the synchronized data . . . . .	19
	Create a synchronization point in the System Tree . . . . .	20
	Synchronize data from the SecurityCenter . . . . .	22
	View the status of synchronization points . . . . .	24
	Configuration of permission sets . . . . .	25
	Configure permission sets for user roles . . . . .	26
	Configuration of a synchronization administrator account . . . . .	26
	Create or update a synchronization administrator account . . . . .	27
<b>3</b>	<b>Monitoring and managing McAfee SaaS security</b>	<b>29</b>
	Overview of the monitoring process . . . . .	29
	Features for monitoring protection services . . . . .	30
	Dashboards and monitors for Security-as-a-Service . . . . .	31
	Queries and reports for Security-as-a-Service . . . . .	32
	Predefined queries . . . . .	33
	Custom queries and reports . . . . .	33
	System Information page . . . . .	33
	Threat Event Log . . . . .	34
	Purge Threat Events . . . . .	34
	Open the SecurityCenter . . . . .	35
	Compatibility with other McAfee products . . . . .	35
	Considerations when using McAfee Risk Advisor . . . . .	36

<b>4</b>	<b>Troubleshooting</b>	<b>39</b>
	Troubleshooting solutions . . . . .	39
	Manual deletion of files and events . . . . .	42
	Delete data manually . . . . .	43
	Find more information . . . . .	43
	<b>Index</b>	<b>45</b>

# Preface

This guide provides the information you need for all phases of product use, from installation to configuration to troubleshooting.

## Contents

- [About this guide](#)
- [Finding 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 the following typographical conventions and icons.

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

---

## Finding product documentation

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

### Task

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

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

# 1

## Introduction to the Security-as-a-Service extension

The McAfee® Security-as-a-Service reporting extension lets you monitor the status of computers that are protected by McAfee Security-as-a-Service (McAfee SaaS) services and managed with the McAfee® SecurityCenter administrative website.

The extension is for use with McAfee® ePolicy Orchestrator (McAfee ePO™) software version 4.6 or later.

### Contents

- ▶ *Management of McAfee SaaS protection services*
- ▶ *Required components*
- ▶ *Component setup and integration*

---

## Management of McAfee SaaS protection services

The Security-as-a-Service reporting extension lets you use the ePolicy Orchestrator console to monitor status and event information for managed systems that are protected by McAfee SaaS services.

Your subscription to McAfee SaaS protection services includes an account for a web-based management tool known as the SecurityCenter, which includes:

- **Database server** — Maintains information about the McAfee SaaS protection services and the computers protected by them.
- **SecurityCenter console** — Displays information from the database for the purpose of managing the systems where McAfee SaaS services are installed (for example, by creating policies and detailed detection reports).

The extension establishes a communication link between the ePolicy Orchestrator server and one or more SecurityCenter accounts. It then pulls (or copies) data from the SecurityCenter database and synchronizes it with the ePolicy Orchestrator database. You can use the monitoring and reporting features provided by the extension to view basic SaaS information in the ePolicy Orchestrator console.

## Required components

Management of McAfee SaaS protection services with the Security-as-a-Service extension requires the following components be set up and running.

- **ePolicy Orchestrator 4.6 (or later) server and database** — The enterprise security management tool that monitors activity and creates reports on managed systems running McAfee security products.
- **McAfee SecurityCenter** — A web-based management tool for McAfee SaaS services. Used by a site administrator to install client software, deploy policies, monitor activity and detections, create reports, and manage account information.
- **Security-as-a-Service extension** — Software that provides the interface between the SecurityCenter and the ePolicy Orchestrator server and database.
- **McAfee SaaS protection services** — Protection services that monitor and report activity, and detect and respond to threats, on client computer systems. Some protection services include account configuration or installation of a client software component.

## Component setup and integration

Once your ePolicy Orchestrator environment is running, four tasks are required to set up proper interaction between the management components and the McAfee SaaS protection services.



If you have already set up an administrative SecurityCenter account and performed any necessary installation, activation, or configuration for McAfee SaaS protection services, begin with task 3.

### Process overview

#### 1 — Set up an administrative account in the SecurityCenter.

When you purchase a subscription to McAfee SaaS services, McAfee or your service provider:

- Creates an account for you.
- Sets up a web-based administrative tool, the SecurityCenter. The SecurityCenter is used to manage the status of the computers protected by your McAfee SaaS services.
- Sends you credentials for logging on to the SecurityCenter console. You need to log on to your account and configure settings as needed.

#### 2 — Install client software and activate protection services as needed.

Some protection services require installation of software on client computers, activation, or configuration before protection can begin. For more information, see the welcome email you received when you subscribed to McAfee SaaS services and documentation that is available on the **Help & Support** page of the SecurityCenter console.



Verify that data for McAfee SaaS managed systems appears in the SecurityCenter console before proceeding. For example, check the **Computers** page to make sure the managed systems in the account show up. Check the widgets on the **Dashboard** page to see status and detection information at-a-glance. Information cannot be viewed in the ePolicy Orchestrator console until it becomes available in the SecurityCenter.

#### 3 — Install and set up the extension.

Instructions are provided in this guide and in a quick start guide that is available from the SecurityCenter console, on the **ePO Servers** tab of the **Utilities** page.



#### 4 – Manage computers protected by McAfee SaaS services from two locations.

When installation is complete, you can access information for managed systems from two consoles:

- **ePolicy Orchestrator console** — Monitor status and event information. When you need to install client software, configure policies, or perform other management tasks, select links in the **McAfee SecurityCenter** monitor on the **Security-as-a-Service** dashboard to open the SecurityCenter console.
- **SecurityCenter console** — Create customized policies, install client software, and run detailed reports. For more information, see the McAfee® SaaS Endpoint Protection documentation, which is available on the **Help & Support** page of the SecurityCenter console.



# 2

## Installing and configuring the extension

These topics explain how to install, set up, and configure features for the extension.

### Contents

- ▶ *Overview of installation and setup*
- ▶ *Features added to the ePolicy Orchestrator environment*
- ▶ *Install the product extension*
- ▶ *Configuration of registered servers*
- ▶ *Data synchronization with the SecurityCenter*
- ▶ *Configuration of permission sets*
- ▶ *Configuration of a synchronization administrator account*

---

## Overview of installation and setup

Four general tasks are required to install and set up the extension.

### Process overview

#### 1 **Download and install the extension.**

Download the product extension .zip file from either the SecurityCenter or ePolicy Orchestrator console, then install it from the ePolicy Orchestrator console.

#### 2 **Register your SecurityCenter account with the ePolicy Orchestrator software.**

This requires login credentials for an administrative SecurityCenter account. If you do not have them, create a synchronization administrator account before performing this task.

#### 3 **Create a container (*synchronization point*) for McAfee SaaS data in the System Tree.**

Synchronized data from McAfee SaaS managed systems will be placed in this container.

#### 4 **Synchronize SaaS data from the SecurityCenter with the ePolicy Orchestrator database.**

This makes current McAfee SaaS data accessible to the monitoring and reporting features of the extension and the ePolicy Orchestrator software.

### See also

*Install the product extension on page 14*

*Create or update a synchronization administrator account on page 27*

*Register a SecurityCenter account on page 16*

*Create a synchronization point in the System Tree on page 20*

*Synchronize data from the SecurityCenter on page 22*

## Features added to the ePolicy Orchestrator environment

The extension adds or uses these features in the ePolicy Orchestrator environment to obtain data from a SecurityCenter account and synchronize it with the ePolicy Orchestrator server.

**Table 2-1 Features added for synchronizing SaaS data**

Feature	Details
Registered servers	Requires one type of registered database server: <ul style="list-style-type: none"> <li>• <b>SecurityCenter account</b> — Registration requires administrative login credentials for each SecurityCenter account you want to register.</li> </ul>
Server tasks	Adds one preconfigured, scheduled pull task: <ul style="list-style-type: none"> <li>• <b>SaaS Data Synchronization</b> — Pulls data from the registered SecurityCenter account and synchronizes it with the ePolicy Orchestrator database. This server task is disabled by default.</li> </ul> Adds one new option on the <b>Actions</b> menu: <ul style="list-style-type: none"> <li>• <b>Synchronize SaaS Systems</b></li> </ul>
System Tree	Adds two <b>Actions</b> menu options to the <b>Group Details</b> tab: <ul style="list-style-type: none"> <li>• <b>Manage Group Synchronization Settings</b> — Lets you associate a group with a registered SecurityCenter account. (The group becomes the <i>synchronization point</i> for the account.)</li> <li>• <b>List All SaaS Synchronization Points</b> — Shows when SaaS data was last synchronized for each registered SecurityCenter account.</li> </ul>
Permission sets	Adds two preconfigured user roles: <ul style="list-style-type: none"> <li>• <b>SaaS Admin</b> — By default, the SaaS Admin can create, edit, or delete SaaS registered servers, server tasks, and queries.</li> <li>• <b>SaaS Reviewer</b> — By default, the SaaS Reviewer can view registered servers, view synchronized data, and run queries.</li> </ul>

The extension also adds features that are used for monitoring the synchronized data. These features are described elsewhere in this document.

### See also

[Features for monitoring protection services](#) on page 30

[Configuration of registered servers](#) on page 16


[Data synchronization with the SecurityCenter](#) on page 18

[Configuration of permission sets](#) on page 25


## Overview of feature configuration

Use the ePolicy Orchestrator console to set up or change the way the basic features operate for the extension.

**Table 2-2 Configuration tasks that are always required**

For this...	Perform these tasks...
Registered servers	<p>For each SecurityCenter account:</p> <ul style="list-style-type: none"> <li>Register the SecurityCenter account with the ePolicy Orchestrator server as an external database server. This requires administrative login credentials for the SecurityCenter account.</li> </ul> <p> If you do not have administrative login credentials, create a synchronization administrator account before using this feature.</p>
SaaS Data Synchronization server task	<p>For each registered SecurityCenter account:</p> <ul style="list-style-type: none"> <li>Configure a synchronization point in the System Tree. This is the location for storing McAfee SaaS data pulled from the SecurityCenter.</li> <li>Configure the server task, then run it now or enable it to run automatically at regular intervals.</li> </ul> <p>One server task is created when the extension is installed. Create others as needed for additional registered SecurityCenter accounts.</p>

**Table 2-3 Configuration tasks that are sometimes required**

For this...	Perform these tasks...
Permission sets for user roles	<p>For the administrators who work with the extension in your ePolicy Orchestrator environment:</p> <ul style="list-style-type: none"> <li>Grant Security-as-a-Service user roles to existing permission sets, or create new permission sets and add them there. (For more information, see the ePolicy Orchestrator documentation.)</li> <li>Specify access (read/write) permission sets for each role.</li> </ul>
Synchronization administrator account	<p>For users who do not have credentials for an administrative SecurityCenter account:</p> <ul style="list-style-type: none"> <li>Create a synchronization administrator account.</li> </ul> <p>This is required to configure registered servers and server tasks.</p> <p> If a synchronization administrator account is required, links for creating and editing the account appear in the SecurityCenter, on the <b>ePO Servers</b> tab of the <b>Utilities</b> page.</p>

### See also

[Install the product extension on page 14](#)

[Register a SecurityCenter account on page 16](#)

[Create a synchronization point in the System Tree on page 20](#)

[Synchronize data from the SecurityCenter on page 22](#)

## Install the product extension

For McAfee SaaS protection services to be managed by ePolicy Orchestrator software, you must first download and install the Security-as-a-Service extension.

### Before you begin

If you have previously installed and uninstalled the extension, you need to remove some leftover files manually.

### Task

For option definitions, click ? in the interface.

- 1 Download the extension using one of these methods:

#### From the ePolicy Orchestrator console

- a Click **Menu | Software | Software Manager | Extensions**.
- b In the **Product Categories** pane, click **Management Solutions**.
- c In the right pane under **Software**, click **McAfee SaaS <version number>**.

The screenshot shows the ePolicy Orchestrator console interface. The top navigation bar includes 'Menu', 'Software Manager', 'Dashboards', 'System Tree', 'Queries & Reports', and 'Policy Catalog'. The left pane shows 'Product Categories' with a search box and a list of categories including 'Management Solutions' (6 items). The main pane displays 'Software (by Label) > Management Solutions' with a table of products. The 'McAfee SaaS 1.0' product is highlighted, showing its status as 'Up to Date' and installed on 'May 17, 2011'. Below this, the 'McAfee SaaS 1.0' details are shown, including a description and a 'Language Filter' dropdown. A table of components is displayed at the bottom, with columns for Component, Type, Language, Available, Checked In, and Actions.

Product	Status	Installed
McAfee Agent 4.0	Not Checked In	
McAfee Agent 4.5	Not Checked In	
McAfee Agent 4.6	Not Checked In	
McAfee ePolicy Orchestrator 4.6	Not Checked In	
McAfee Risk Advisor 2.6	Not Checked In	
McAfee SaaS 1.0	Up to Date	May 17, 2011

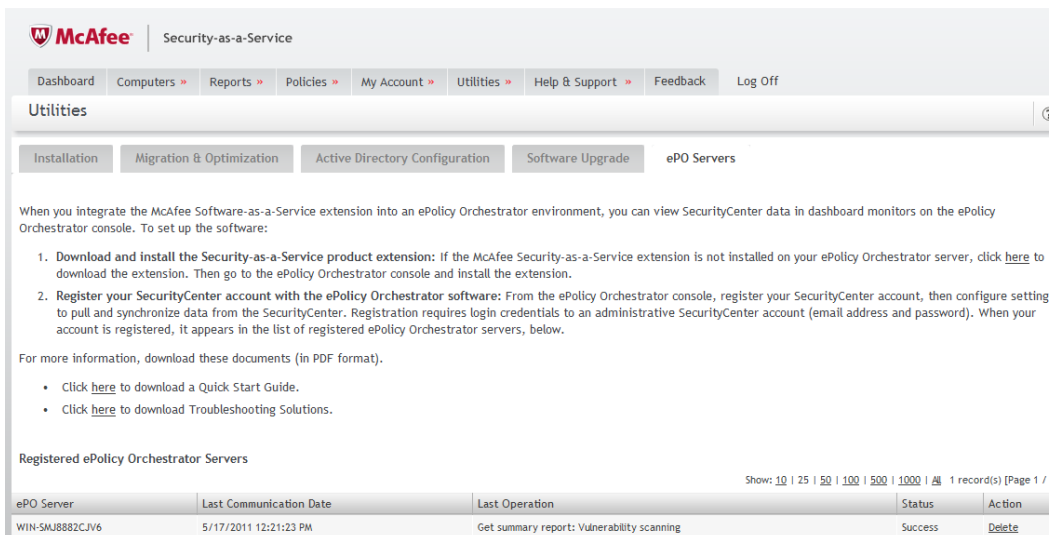
  

Component	Type	Language	Available	Checked In	Additional Che	Actions
McAfee Security-as-	Extension	Neutral	1.0.0.167	1.0.0.173		<a href="#">Remove</a>   <a href="#">Download</a>
McAfee Security-as-	Other	English	1.0.0			<a href="#">Download</a>
McAfee Security-as-	Other	English	1.0.0			<a href="#">Download</a>

- d In the right pane under **Components**, find the extension, then click **Download**.
- e In the **File Download** dialog box, save the McAfee Security-as-a-Service.zip file to a local folder, then click **OK**.

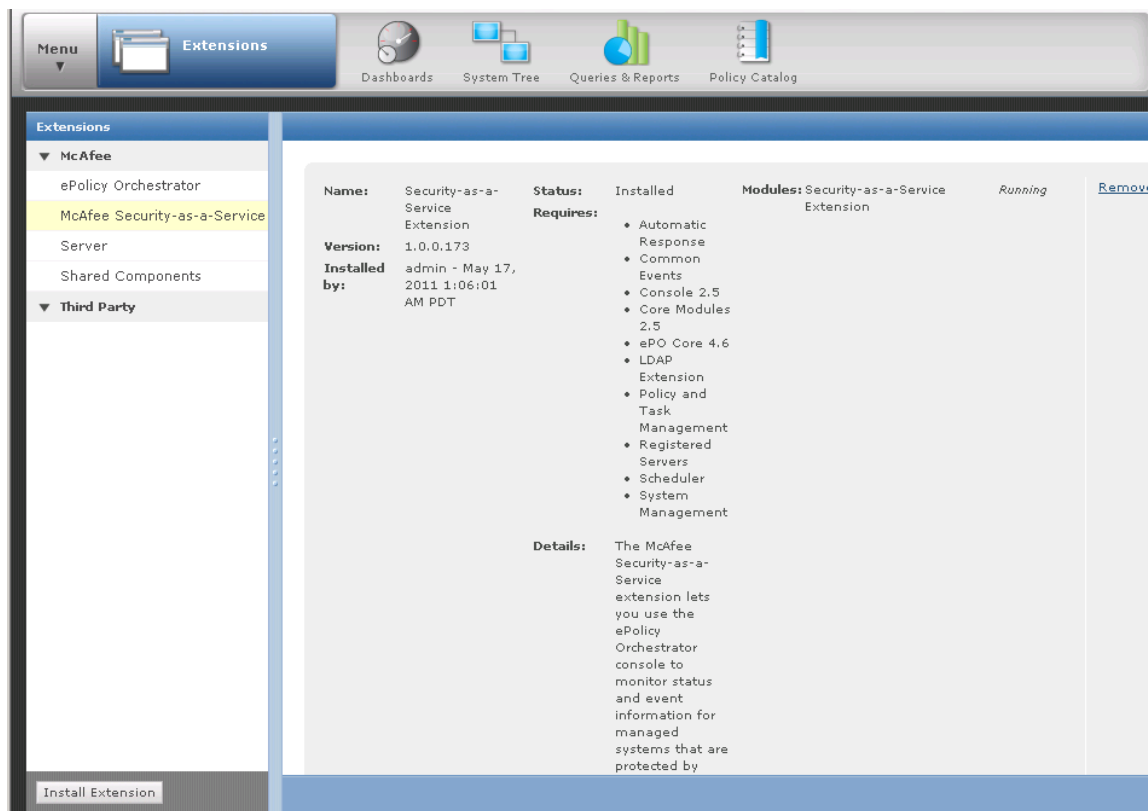
**From the SecurityCenter console**

- a On the **Utilities** page, click the **ePO Servers** tab.



- b Click the link to download the extension.
- c In the **File Download** dialog box, save the McAfee Security-as-a-Service.zip file to a local folder, then click **OK**.

- 2 From the ePolicy Orchestrator console, click **Menu | Software | Extensions**, in the **Extensions** pane select **McAfee Security-as-a-Service**, then in the right pane click **Install Extension**.



**See also***Manual deletion of files and events* on page 42*Delete data manually* on page 43

## Configuration of registered servers

To enable communication between the extension and the SecurityCenter database, you need to register each SecurityCenter account with the ePolicy Orchestrator server. You can do this from the ePolicy Orchestrator console.



Registration requires login credentials for each administrative SecurityCenter account you want to register.

When you register a SecurityCenter account, your ePolicy Orchestrator server is then recognized by the SecurityCenter as a registered ePolicy Orchestrator server. You can view a list of registered ePolicy Orchestrator servers from the SecurityCenter console, on the **ePO Servers** tab of the **Utilities** page.

**Table 2-4 Tasks for registered servers**

From this console...	You can...
ePolicy Orchestrator	<ul style="list-style-type: none"> <li>• Register an account.</li> <li>• Edit registration information.</li> <li>• View a list of registered accounts.</li> <li>• Delete registered accounts.</li> </ul> <p> After registering or deleting an account in the ePolicy Orchestrator console, an alert appears on the <b>Dashboard</b> page of the SecurityCenter console.</p>
SecurityCenter	<ul style="list-style-type: none"> <li>• View information about the ePolicy Orchestrator server where you registered your SecurityCenter account.</li> <li>• Delete registration for your ePolicy Orchestrator server.</li> </ul> <p> For instructions, see the McAfee SaaS Endpoint Protection documentation, which is available on the <b>Help &amp; Support</b> tab of the SecurityCenter console.</p>

## Register a SecurityCenter account

Register your SecurityCenter account with the ePolicy Orchestrator software, which enables the extension to pull McAfee SaaS data and synchronize it with the ePolicy Orchestrator database.

**Before you begin**

If you do not have login credentials for an administrative SecurityCenter account, create a synchronization administrator account.

An alert appears on the **Dashboard** page of the SecurityCenter console whenever an account is registered.

If you have multiple SecurityCenter accounts, register each separately.

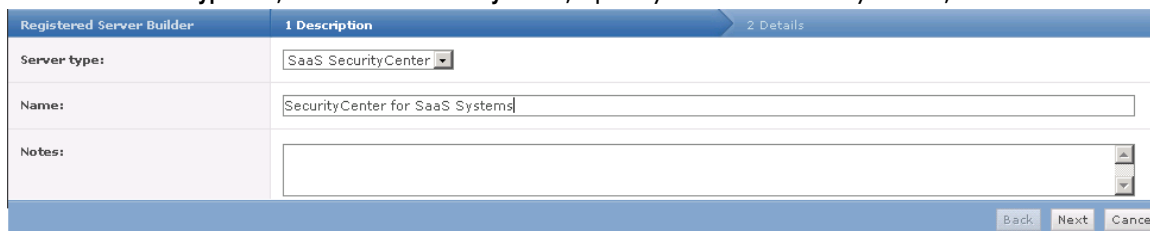
**Task**

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, click **Menu** | **Configuration** | **Registered Servers**, then click **New Server**. The Registered Server Builder wizard opens to the **Description** page.



- 2 From the **Server type** list, select **SaaS SecurityCenter**, specify a name and any notes, then click **Next**.

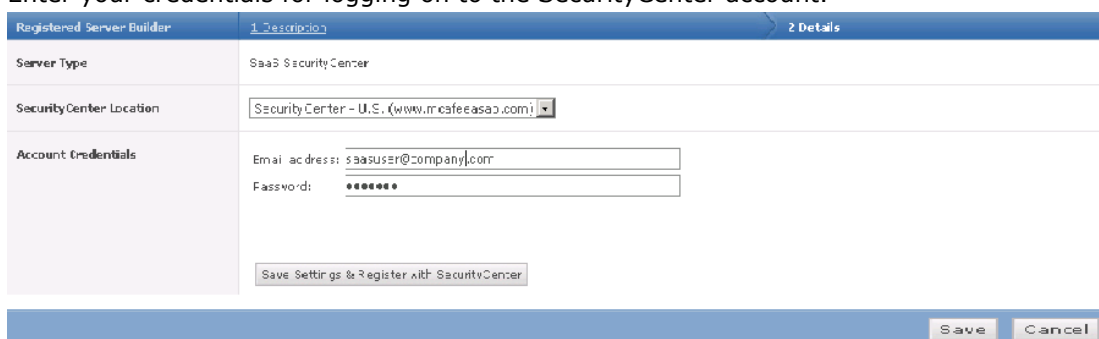


Registered Server Builder	1 Description	2 Details
Server type:	SaaS SecurityCenter	
Name:	SecurityCenter for SaaS Systems	
Notes:		
Back Next Cancel		

- 3 From the **SecurityCenter Location** list, select the data center that hosts your account.

The data center is identified by the domain portion of the URL used to access the SecurityCenter console (for example, [www.mcafee.com](http://www.mcafee.com) or [www.yourserviceprovider.com](http://www.yourserviceprovider.com)). If you are unsure which data center to select, check the URL provided in the welcome email you received when you purchased a subscription to McAfee SaaS protection services.

- 4 Enter your credentials for logging on to the SecurityCenter account.



Registered Server Builder	1 Description	2 Details
Server Type	SaaS SecurityCenter	
SecurityCenter Location	SecurityCenter - U.S. (www.mcafeeasap.com)	
Account Credentials	Email address: saasuser@company.com Password: *****	
Save Settings & Register with SecurityCenter		
Save Cancel		

You received these in a welcome email from your service provider when you purchased a subscription to McAfee SaaS protection services. If McAfee or your service provider did not send credentials, use credentials for a synchronization administrator account.

- 5 Save your settings by clicking one of these buttons:
- **Save Settings & Register SecurityCenter** — Saves the information and registers the server.
  - **Save** (lower-right corner) — Saves the information without registering. You can complete the registration later without re-entering the information.

When registration is complete, the email address for the account appears in the **McAfee SecurityCenter** monitor in the default **Security-as-a-Service** dashboard, along with links to pages on the SecurityCenter console.

#### See also

[Purge Threat Events](#) on page 34

[Create or update a synchronization administrator account](#) on page 27

## View or edit a list of registered SecurityCenter accounts

View a list of the registered SecurityCenter accounts in the ePolicy Orchestrator console and edit the settings as needed.

**Task**

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Registered Servers** to display a list of all registered servers.
- 2 To view the settings for a server, select the registered server from the list, then click **Actions | Edit**.
- 3 Change the settings as needed, then click **Save**.

**Delete a registered SecurityCenter account**

Delete the registration for a SecurityCenter account that is no longer used. This is equivalent to "unregistering" a registered server.

An alert appears on the **Dashboard** page of the SecurityCenter console when a registered server is deleted.

**Task**

For option definitions, click ? in the interface.

- 1 Click **Menu | Configuration | Registered Servers**.
- 2 Select the registered server from the list, then click **Actions | Delete**.
- 3 Delete the group container in the System Tree that served as the synchronization point for the deleted account.
  - a Click **Menu | Systems | System Tree**.
  - b In the **System Tree** pane, select the group container.
  - c Click **System Tree Actions | Delete Group**.
- 4 Decide whether to purge the Threat Events for the deleted account.
  - If you are cancelling the SecurityCenter account, you can retain the Threat Events for reference.
  - If you plan to re-register the same SecurityCenter account in the future, purge all Threat Events. Otherwise, historical data will be pulled when you synchronize data for the re-registered account, which might result in duplicate event entries.

**See also**

[Purge Threat Events](#) on page 34

---

**Data synchronization with the SecurityCenter**

Before you can view McAfee SaaS data in the ePolicy Orchestrator console, the data must be pulled from a registered SecurityCenter account and synchronized with the ePolicy Orchestrator server and database.

When the extension is installed, a SaaS Data Synchronization server task is created and preconfigured to pull data from a registered SecurityCenter account.

Synchronized data appears in the System Tree and in monitors on the **Security-as-a-Service** dashboard, and you can run queries on the data.

During subsequent updates, the SaaS data is updated and synchronized to reflect the newer data from the SecurityCenter account.

## Where the data is placed: synchronization points

Data for McAfee SaaS managed systems is placed in a container in the System Tree called a *synchronization point*. You need to create this container before running the server task for the first time. From this location, you can view the groups and computers protected by McAfee SaaS services.



If you have multiple SecurityCenter accounts, create a synchronization point and a server task for each account. Create each synchronization point at the root level in the System Tree; do not nest one group within another.

## Full and incremental data synchronization

The first time a data synchronization task pulls SaaS data from a SecurityCenter account, it pulls all relevant data for the last 30 days. The volume of data, among other things, determines how much time and how many system resources are required. The expectation is that an initial data synchronization task uses system resources more intensively than subsequent data synchronization tasks for the same SecurityCenter account.

Subsequent data synchronization tasks pull only the data that has been added or changed since the last synchronization. This typically affects a smaller volume of data, so these updates usually require fewer resources from the network, the ePolicy Orchestrator server, and the ePolicy Orchestrator database (which might run on a different system).

## On-demand and scheduled data synchronization

You can synchronize SaaS data at any time on demand, and you can schedule SaaS data synchronization to occur automatically at regular intervals.

You can schedule synchronization to run during times of reduced network and ePolicy Orchestrator console activity. This might be an especially important consideration when pulling data from a SecurityCenter account for the first time.

## About the synchronized data

You can specify the types of data to retrieve for McAfee SaaS protection services by selecting options for the SaaS Data Synchronization server task.

The SaaS Data Synchronization server task can retrieve these types of data:

- Endpoints (managed systems)
- Groups into which managed systems are organized
- Events, such as detections, blocked communications, or blocked websites
- Protection status
- Summary information related to specific protection services, such as the number of emails or websites scanned

When SaaS data synchronization is complete, you can access the data in the ePolicy Orchestrator console by using the monitoring features provided by the ePolicy Orchestrator software and the Security-as-a-Service extension.

### See also

[Features for monitoring protection services](#) on page 30

## Create a synchronization point in the System Tree

Create a container in the System Tree where data for McAfee SaaS protection services is placed when it is pulled from the SecurityCenter account and synchronized with the ePolicy Orchestrator database. This container is called a *synchronization point*.

### **Before you begin**

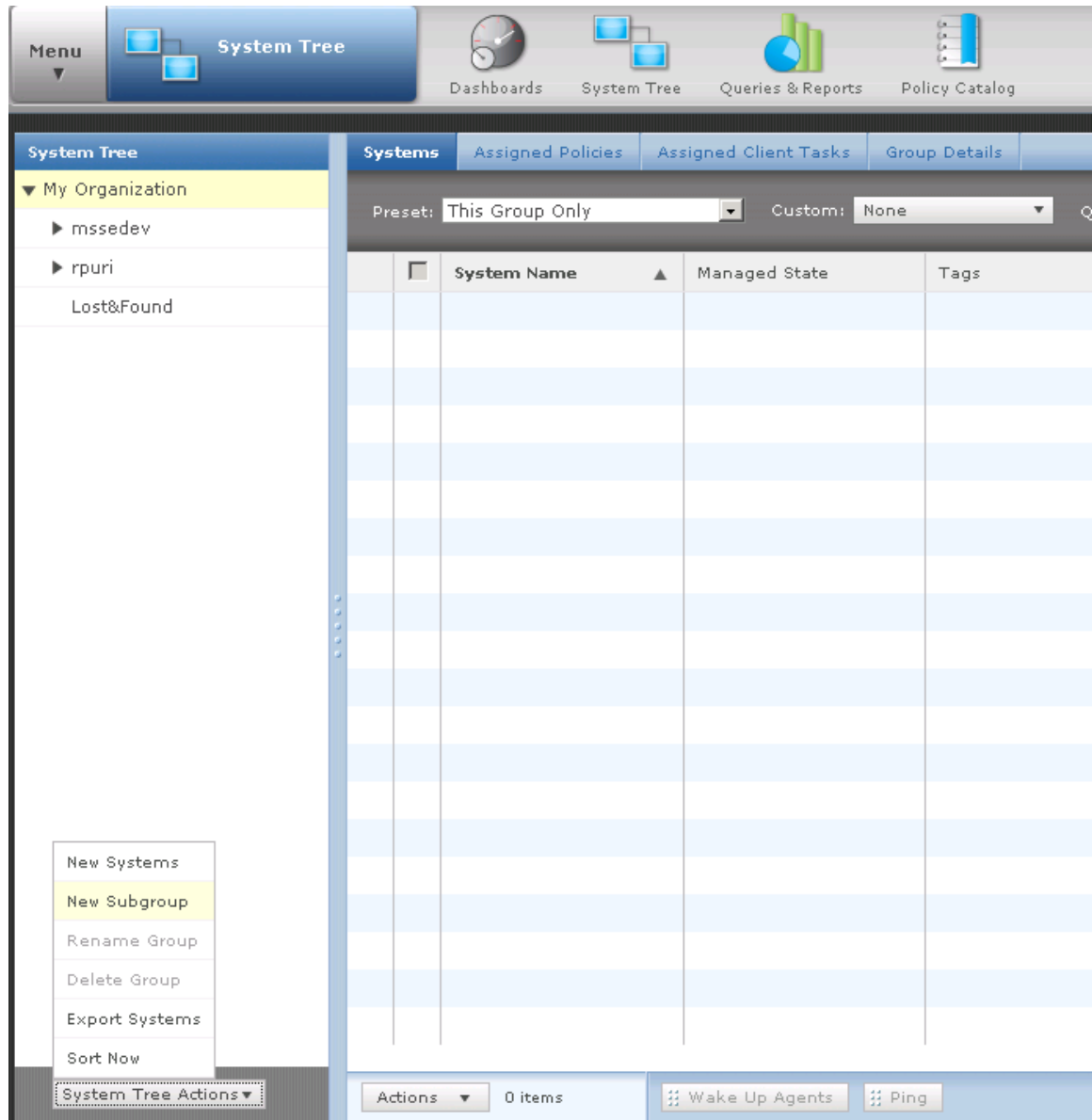
Register your SecurityCenter account with the ePolicy Orchestrator software. You must have correct permissions configured for the System Tree and Server Tasks permission sets. For information on configuring permission sets, see the ePolicy Orchestrator documentation.

If you have multiple SecurityCenter accounts, create a separate synchronization point at the root level of the System Tree for each one. Do not nest one synchronization container within another.

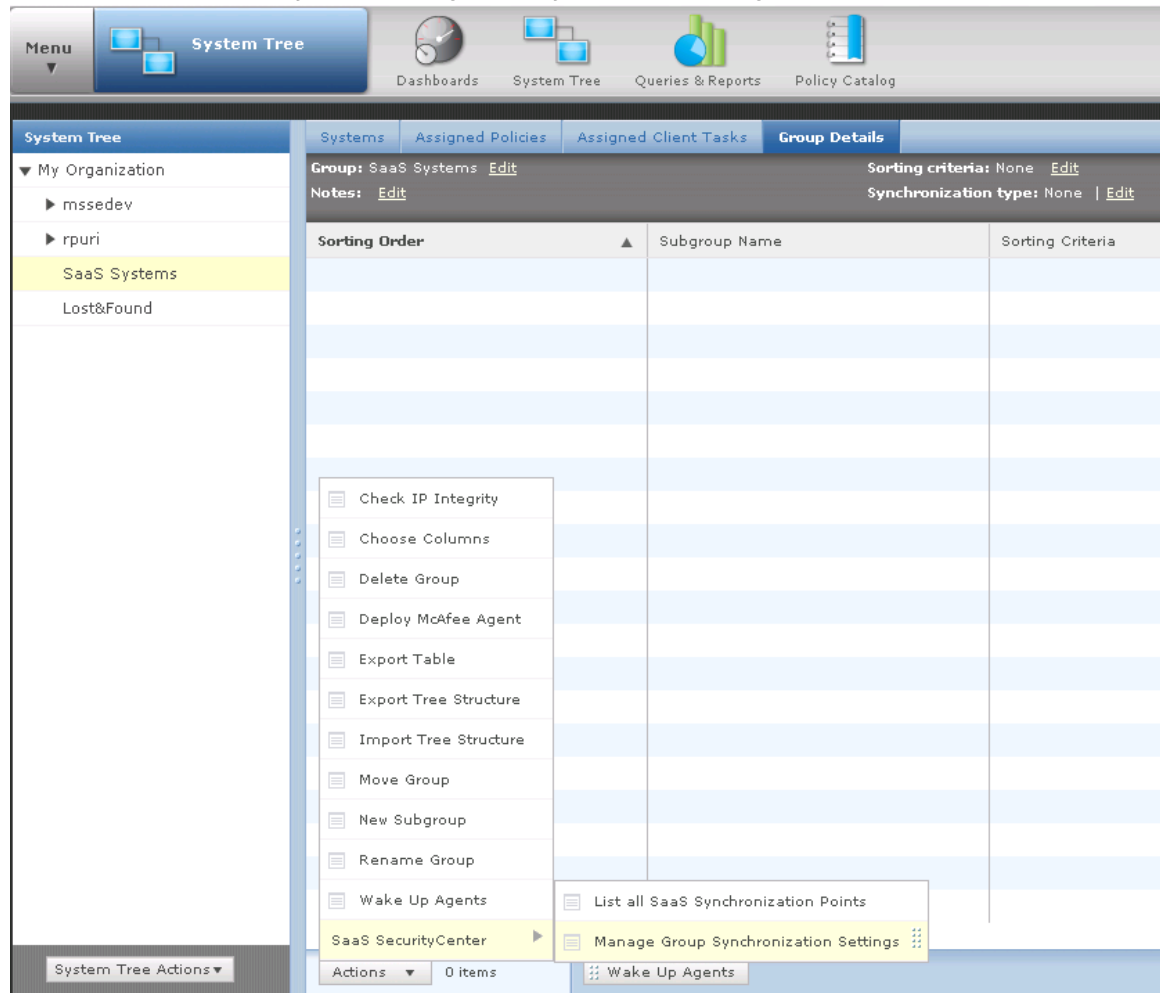
**Task**

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, click **Menu | Systems | System Tree**.
- 2 Click **System Tree Actions | New Subgroup**.



- 3 Type a name for the new subgroup.
- 4 In the System Tree pane, select the new group, then click the **Group Details** tab.

**5 Click Actions | SaaS SecurityCenter | Manage Group Synchronization Settings.**

**6 Select a registered SecurityCenter account.**
**7 Save your settings by clicking one of these buttons:**

- **Save Settings & Synchronize Now** — Saves the synchronization settings and pulls data immediately.
- **Save** (lower-right corner) — Saves settings without pulling data. You can perform the synchronization later without re-entering the information.

## Synchronize data from the SecurityCenter

You can pull McAfee SaaS data from a registered SecurityCenter account and synchronize it with the ePolicy Orchestrator database by running a server task. The task can be run on demand or automatically at regular intervals. For example, you can schedule the task to pull data at the same time every night during off-peak hours for your network.

### Before you begin

Register each SecurityCenter account with the ePolicy Orchestrator software and create its synchronization point in the System Tree. You must have the correct permissions configured for the Server Tasks permission set. For information on configuring permission sets, see the ePolicy Orchestrator documentation.

After the SaaS data is synchronized, the McAfee SaaS managed systems appear in the System Tree and SaaS data appears in monitors on the **Security-as-a-Service** dashboard.



If you delete an existing synchronization point, its associated server task no longer runs. If you re-create the synchronization point, you need to reconfigure its server task or create a new server task to synchronize data for it. Re-creating the synchronization point does not cause the server task associated with the previous instance of the synchronization point to begin synchronizing data for the new instance of the synchronization point automatically.

**Task**

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, click **Menu | Automation | Server Tasks**.
- 2 If this is the first time you are using this server task to synchronize data, you need to configure it:
  - a Locate the **SaaS Data Synchronization** task in the list, then click **Edit**.

Name	Status	Type	Schedule	Next Run	Last Run	Actions
Download Software Product List	Enabled	User	Daily	5/18/11 1:00 AM	5/17/11 12:59 AM	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>
Duplicate Agent GUID - clear error	Disabled	User	Weekly	No next run time	Task has never run	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>
Duplicate Agent GUID - remove sys	Disabled	User	Weekly	No next run time	Task has never run	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>
Issue synchronization	Disabled	System	Daily	No next run time	Task has never run	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>
Purge Threat and Client Events Olc	Disabled	User	Daily	No next run time	5/16/11 11:44 PM	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>
RSD: Default Delete Detected Syst	Disabled	User	Daily	No next run time	Task has never run	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>
RSD: Update Sensor Deployment C	Disabled	User	Monthly	No next run time	Task has never run	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>
<input checked="" type="checkbox"/> SaaS Data Synchronization	Disabled	User	Disabled	No next run time	Task has never run	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>
Synchronize Shared Policies	Disabled	User	Daily	No next run time	Task has never run	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>
Synchronize Shared Tasks	Disabled	User	Daily	No next run time	Task has never run	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Run</a>

- b In the wizard, type any notes you want on the **Description** page, select whether to enable scheduling, then click **Next**.

If you want the server task to run automatically at regular intervals, select **Enabled**, then configure scheduling options later in this task. You can configure them regardless of whether they are enabled or disabled.

Server Task Builder: 1 Description > 2 Actions > 3 Schedule

Name: SaaS Data Synchronization

Notes: This task synchronizes your SecurityCenter account with the ePolicy Orchestrator server. Please set up the schedule and enable this task. It runs automatically to retrieve data from the SecurityCenter about SaaS managed systems, activities monitored by McAfee SaaS services, and events detected by McAfee SaaS services.

Schedule status:  Enabled  Disabled

Buttons: Back, Next, Cancel

- c From the **Actions** list, make sure **Synchronize SaaS Systems** is selected.

- d Select the synchronization point(s) for this task, then click **Next**.

Server Task Builder | 1 Description | 2 Actions

What actions do you want the task to take?

1. Actions: Synchronize SaaS Systems

Synchronize:  All Synchronization Points  
 Selected Synchronization Points: 0 [Select Synchronization Point](#)

Data to Synchronize:  Groups, Computers, and Properties  
 Endpoint Threat Events  
 SaaS Service Summary Data

Back Next Cancel

The types of data to be synchronized are preselected.

- e Select scheduling options, then click **Next**.

These selections are ignored unless you enabled scheduling earlier in this task. You can configure and save the options, then enable and disable them as needed.

Server Task Builder | 1 Description

Schedule type: Daily

Start date: 05 / 17 / 2011

End date:  05 / 18 / 2011  
 No end date

Schedule: at 1 : 00 AM

- f Review the summary, then click **Save**.
- 3 To run the task at any time, click **Menu | Automation | Server Tasks**, locate the task in the listing, then click **Run**.

If you have enabled scheduling, the server task runs automatically at scheduled intervals.

#### See also

[Create a synchronization point in the System Tree](#) on page 20

[Create or update a synchronization administrator account](#) on page 27

## View the status of synchronization points

Verify that McAfee SaaS data is up-to-date for all your synchronization points in the System Tree.



**Task**

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, click **Menu | Systems | System Tree**, then select a group.
- 2 In the **Group Details** tab, click **Actions | SaaS SecurityCenter | List All SaaS Synchronization Points**, then view the **Last Synchronization Time** and other information listed for each synchronization point.

## Configuration of permission sets

A permission set is a group of access rights granted to a user account for specific features of a product. Permission sets only *grant* permissions — they never remove permissions.

All permissions to all products and features are automatically assigned to global administrators. Other users must have permissions assigned manually. Global administrators can assign existing permission sets when they create or edit user accounts and permission sets.

For more information on permission sets, see the ePolicy Orchestrator documentation.

### Security-as-a-Service permission sets

The extension adds a **Security-as-a-Service** section to the permission sets with two user roles that are preconfigured. These define the access rights to the extension's features. The global administrators must grant Security-as-a-Service user roles to existing permission sets or create new permission sets and add them there.

**Table 2-5 Permissions for Security-as-a-Service user roles**

User roles	Default permissions
SaaS Reviewer	View registered servers, view synchronized data, and run queries.
SaaS Admin	Create, edit, or delete registered servers, server tasks, and queries.

If needed, global administrators can change the permissions defined for these roles or create permission sets for new roles.

### Other required permission sets

ePolicy Orchestrator needs permissions to grant access to other features that work with the extension, including queries and dashboards. For example, to manage SaaS data synchronization and synchronized data, a user needs view permissions for the Threat Event Log, view permissions for Systems, view permissions for System Tree access, and view and change permissions for the SaaS Data Synchronization server task.

**Table 2-6 Permissions required per feature**

Features	Required permission sets
Dashboards	Dashboards, Queries
Queries	Queries
Server tasks	Server Tasks
Events on SaaS managed systems	Systems, System Tree access, Threat Event Log

## Configure permission sets for user roles

Update the read/write access permissions assigned to the Security-as-a-Service user roles that have been defined for your ePolicy Orchestrator environment.

### Before you begin

Determine the extension features to which you want to give access and the additional permission sets that must be assigned to access all aspects of that feature.

### Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, click **Menu | User Management | Permission Sets**.
- 2 Select a user role.
  - **SaaS Admin** — Can create, edit, or delete registered servers, server tasks, and queries.
  - **SaaS Reviewer** — Can view registered servers, view synchronized data, and run queries.
- 3 From the **Actions** list, select **Edit**.
- 4 Select the permission for each feature:
  - **None**
  - **View settings only**
  - **View and change settings**
- 5 Click **Save**.

To create additional roles, see the ePolicy Orchestrator documentation.

---

## Configuration of a synchronization administrator account

Tasks that include communication between the SecurityCenter server and other servers require login credentials for an administrative SecurityCenter account.

If you don't already have an administrative SecurityCenter account, you need to create a synchronization administrator account before performing these tasks. This account provides the credentials necessary to access the SecurityCenter for only these tasks. (Credentials for an administrative account are typically provided by McAfee or the provider from whom you purchased McAfee SaaS protection services.)

Use a synchronization administrator account to:

- Register a SecurityCenter account with the ePolicy Orchestrator software.
- Run or schedule data synchronization between the SecurityCenter server and an Active Directory or ePolicy Orchestrator server.
- Use the Push Install utility to deploy client software to systems in the Active Directory domain from the SecurityCenter console.

Only one synchronization administrator account can be created for a SecurityCenter account.



If a synchronization administrator account is required, links for creating and editing the account appear in the SecurityCenter, on the **Active Directory Configuration** or **ePO Servers** tab of the **Utilities** page.

## Create or update a synchronization administrator account

If you do not have an administrative SecurityCenter account, you need to create a synchronization administrator account before you can perform tasks that require the SecurityCenter server to communicate with other servers.

Only one synchronization administrator account can be created for a SecurityCenter account.



If you have an administrative SecurityCenter account, the links described in this task do not appear. They are displayed only when a synchronization administrator account is required.

### Task

For option definitions, click ? in the interface.

1 From the SecurityCenter console, click the **Utilities** tab, then do one of the following:

- Click the **ePO Servers** tab.
- Click the **Active Directory Configuration** tab.

A message is displayed if you need to create an administrator account before performing a task, along with a **Create** link. If an administrator account already exists, an email address for the account and an **Edit** link appear.

2 Click the appropriate link.

- **Create** — Enter the email address and password for a new account.
- **Edit** — Update the email address or password for an existing account.

3 Click **Save**.



# 3

## Monitoring and managing McAfee SaaS security

With the extension features, you can monitor the status of managed systems and protection services, and use the ePolicy Orchestrator console to identify problems.

### Contents

- ▶ *Overview of the monitoring process*
- ▶ *Features for monitoring protection services*
- ▶ *Dashboards and monitors for Security-as-a-Service*
- ▶ *Queries and reports for Security-as-a-Service*
- ▶ *System Information page*
- ▶ *Threat Event Log*
- ▶ *Open the SecurityCenter*
- ▶ *Compatibility with other McAfee products*

---

## Overview of the monitoring process

We recommend using a two-prong approach to monitor and manage McAfee SaaS protection services in an ePolicy Orchestrator environment.

### 1 View synchronized SaaS data from the ePolicy Orchestrator console.

Use monitoring features in the ePolicy Orchestrator console to check SaaS data and identify issues with McAfee SaaS managed systems.

**Table 3-1 Where to access the monitoring features**

Type of data	Where to view
Status and activity summary information in charts and graphs	<b>Security-as-a-Service</b> dashboard and monitors
Selectable types of information on the status of McAfee SaaS managed systems	<b>Security-as-a-Service</b> queries and reports
McAfee SaaS protection services and their properties	On the <b>System Information</b> page, the <b>SaaS Products</b> tab and details monitor data
Details for detection events on McAfee SaaS managed systems	Threat Event Log; <b>Security-as-a-Service</b> monitors, queries, and reports
Groups and systems protected by McAfee SaaS services	In the System Tree, on the <b>Systems</b> tab
Synchronization status for each synchronization point	In the System Tree, on the <b>Group Details</b> tab, click <b>Actions</b>   <b>SaaS SecurityCenter</b>   <b>List All SaaS Synchronization Points</b>

## 2 Address issues from the SecurityCenter console.

Visit the SecurityCenter console to install client software on managed systems, configure policies, and take other steps to fix problems. The default **Security-as-a-Service** dashboard provides easy access through the **McAfee SecurityCenter** monitor, which provides direct links to the SecurityCenter console for each registered account.

For more information on using SecurityCenter features, see the McAfee SaaS Endpoint Protection documentation, which is available on the **Help & Support** page of the SecurityCenter console.

### Considerations for monitoring security with other McAfee products

It is important to check for and address any compatibility issues between the extension and other McAfee software running in your ePolicy Orchestrator environment.

#### See also

*Dashboards and monitors for Security-as-a-Service* on page 31

*Queries and reports for Security-as-a-Service* on page 32

*System Information page* on page 33

*Threat Event Log* on page 34

*Open the SecurityCenter* on page 35

*Compatibility with other McAfee products* on page 35

## Features for monitoring protection services

The extension adds features that are used for viewing and monitoring synchronized data for McAfee SaaS protection services.

**Table 3-2 Features for monitoring SaaS data**

For this feature in the McAfee ePO software...	The extension adds...
Dashboards	One preconfigured dashboard: <ul style="list-style-type: none"> <li>• <b>Security-as-a-Service</b> — Displays monitors corresponding to the widgets displayed in the <b>Dashboard</b> page of the SecurityCenter console.</li> </ul>
Queries	Preconfigured queries and options for building custom queries: <ul style="list-style-type: none"> <li>• New Shared Query group, <b>Security-as-a-Service</b>, with a set of queries related to SaaS data.</li> <li>• New group of Query Result Types, <b>Security-as-a-Service</b>, in Query Builder. The group contains a set of query targets related to SaaS data.</li> </ul>
System Tree	On the <b>Group Details</b> tab, two new <b>Actions</b> menu options: <ul style="list-style-type: none"> <li>• <b>SaaS SecurityCenter   Manage Group Synchronization Settings</b> — Lets you associate a group container in the System Tree with a registered SecurityCenter account. (This becomes the synchronization point for the account.)</li> <li>• <b>SaaS SecurityCenter   List All SaaS Synchronization Points</b> — Shows when data was last synchronized for each registered account.</li> </ul>
System Information page	<ul style="list-style-type: none"> <li>• New <b>SaaS Products</b> tab.</li> <li>• New group of customizable details monitors.</li> </ul>

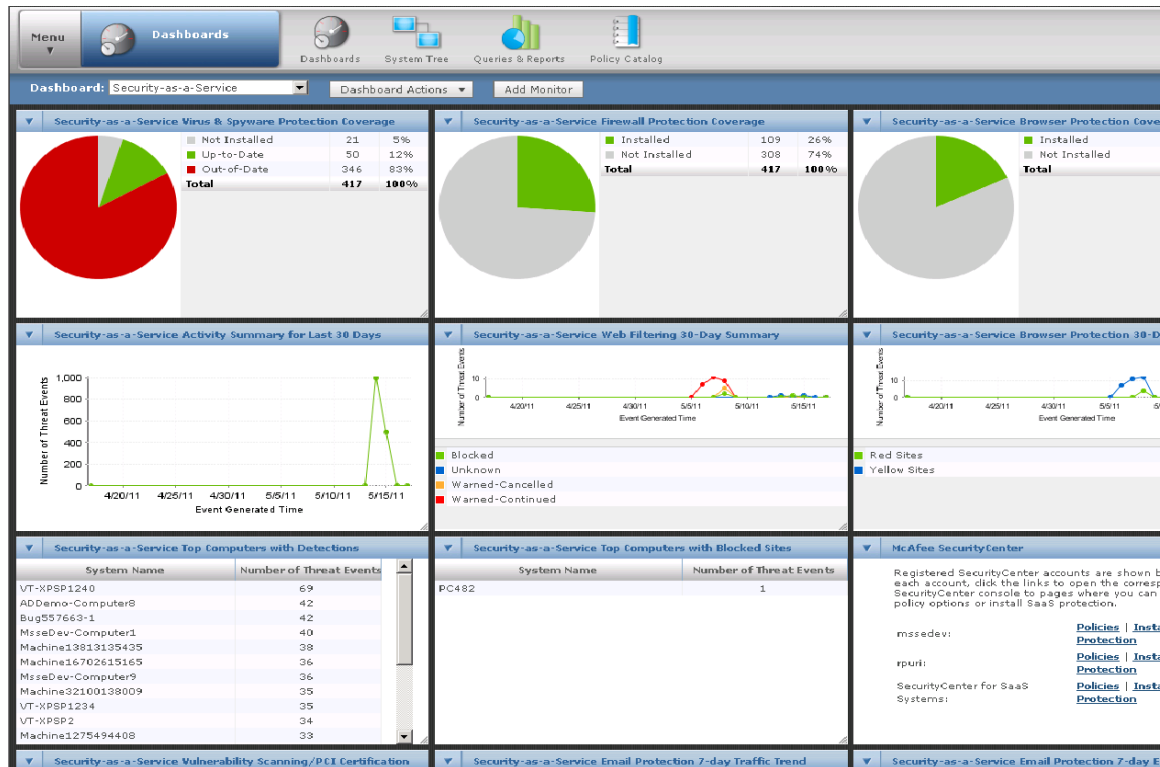
## Dashboards and monitors for Security-as-a-Service

When the extension is installed, a preconfigured **Security-as-a-Service** dashboard is created. It displays **Security-as-a-Service** monitors.

Dashboards are a collection of monitors that are an essential tool for managing your environment. You can create and edit multiple dashboards if you have the appropriate permissions.

### Default Security-as-a-Service dashboard

The extension provides one default dashboard with monitors that correspond to widgets from the **Dashboard** page of the SecurityCenter. *Widgets* are small, interactive reports that provide summary and overview information for your account.



If you register and synchronize data for multiple SecurityCenter accounts, the monitors display summary data for all the accounts.

These SaaS data monitors are available for the **Security-as-a-Service** dashboard:

**Table 3-3 Security-as-a-Service monitors**

This monitor...	Shows...
<b>McAfee SecurityCenter</b>	Links to each registered SecurityCenter account. Select a link to open a browser window and display a page in the SecurityCenter console.
<b>SaaS Virus and Spyware Protection Coverage</b>	The number of computers in your account where protection is up-to-date, out-of-date, and not installed. Up-to-date computers have downloaded the latest threat detection definition (DAT) files. Out-of-date computers need to update their DAT files. Click a color on the widget's pie chart to display a list of computers in a specific category.
<b>SaaS Firewall Protection Coverage</b>	The number of computers in your account where protection is and is not installed. Click a color on the widget's pie chart to display a list of computers in a specific category.

**Table 3-3 Security-as-a-Service monitors** *(continued)*

<b>This monitor...</b>	<b>Shows...</b>
<b>SaaS Browser Protection Coverage</b>	The number of computers in your account where protection is and is not installed. Click a color on the widget's pie chart to display a list of computers in a specific category.
<b>SaaS Top Computers with Detections</b>	The computers with the greatest number of threats detected over the last 7 days. Click a computer name or detection quantity to display details.
<b>SaaS Top Computers with Blocked Sites</b>	The computers with the greatest number of sites blocked over the last 7 days by the browser protection service. Click a computer name or detection quantity to display details.
<b>SaaS Activity Summary for Last 30 Days</b>	The number of threats detected daily over the last month.
<b>SaaS Browser Protection 30-Day Summary</b>	A history of attempts to access blocked websites categorized by site safety ratings over the last 30 days. Click a category to display details.
<b>SaaS Web Filtering 30-Day Summary</b>	A history of attempts over the last 30 days to access websites that the web filtering service blocks or warns users about based on policy settings for content filtering. Click a category to display details.
<b>SaaS Email Protection 7-Day Trend</b>	The number and type of email threats detected daily over the last week by the SaaS email protection service. Click a category to display details.
<b>SaaS Email Protection 7-day Summary</b>	The total number of email messages sent to your account over the last week, the number and type of threats detected by the SaaS email protection service, and the number of messages containing no threats. Click a category to display details.
<b>SaaS Vulnerability Scanning/ PCI Certification</b>	The total number of vulnerabilities detected as of your last scan. It ranks the severity level as low, medium, high, critical, or urgent. Click a category to display details.

### Custom dashboards

You can create custom dashboards and select which monitors and queries to display.

For more information about creating and using dashboards, see the ePolicy Orchestrator documentation.

## Queries and reports for Security-as-a-Service

The extension includes query and report generation through the ePolicy Orchestrator software.

You can create queries from properties stored in the ePolicy Orchestrator database or use predefined queries. For more information, see the ePolicy Orchestrator documentation.

The extension adds these reporting features to the ePolicy Orchestrator environment:

- Several predefined queries that can be run with or without editing.
- A group of Query Result Types, **Security-as-a-Service**, in Query Builder. The group contains a set of query targets related to SaaS data that allow you to create custom queries.

Organize and maintain custom queries to suit your needs, then use them to run reports. You can export reports into a variety of file formats.



## Predefined queries

The extension provides several predefined queries. You can use their default settings, or edit them to obtain just the information you need.

The names of the predefined queries exactly match the names of the predefined SaaS monitors for the **Security-as-a-Service** dashboard.

## Custom queries and reports

You can create customized queries and reports with Query Builder. The result types selected in Query Builder identify what type of data the query retrieves.

The extension adds a new group of Query Result Types, **Security-as-a-Service**, in Query Builder. The group contains a set of query targets related to SaaS data.

**Table 3-4 Security-as-a-Service query result types**

Query result type	Shows this information...
SaaS Event Properties	Detection events
SaaS Managed Systems	Systems managed by the SecurityCenter
SaaS Product Properties	Properties for the McAfee SaaS products installed on managed systems
SaaS Products	McAfee SaaS products in use
SaaS Summary Reports	Summary data for the SaaS email protection and SaaS vulnerability scanning services

For each result type, the extension adds a variety of Available Properties in Query Builder for use in custom queries.

For more information about creating and using queries and reports, see the ePolicy Orchestrator documentation.

## System Information page

The extension adds query data and product information to the **System Information** page in the ePolicy Orchestrator console.

Access the **System Information** page by clicking any managed system in the System Tree.

### Monitor and query data

The extension adds data for the customizable details monitor that appears in the top-right corner of the **System Information** page. Click **Customize** to display and select a monitor.

**Table 3-5 Queries available for the details monitor**

Query category	Queries
Shared Groups - Security-as-a-Service	<ul style="list-style-type: none"> <li>Security-as-a-Service Activity Summary for the Last 30 Days</li> <li>Security-as-a-Service Browser Protection 30-Day Summary</li> <li>Security-as-a-Service Web Filtering 30-Day Summary</li> </ul>

Summary information is available only for the McAfee SaaS protection services in use for the managed system.

## SaaS Products tab

The extension creates a **SaaS Products** tab, which lists each McAfee SaaS protection service in use for the managed system.

Use this tab to quickly view the properties for each protection service. The properties listed depend on the service.

**Table 3-6 Information displayed in the SaaS Products tab**

Property	Shows this information...
Product Name	The name of the McAfee SaaS protection service.
Product Version	The product version number.
Product Engine Version	The product engine number. Displayed only if it is applicable to the product and information is available in the SecurityCenter account.
Product DAT Version	The version number for the threat definition (DAT) file currently in use. Displayed only if it is applicable to the product and information is available in the SecurityCenter account.
Product DAT Timestamp	The date and time that the DAT file was created. Displayed only if it is applicable to the product and information is available in the SecurityCenter account.

## Threat Event Log

Events detected on managed systems that are protected by McAfee SaaS services appear in the McAfee Threat Event Log.

Access the Threat Event Log by clicking **Menu | Reports | Threat Event Log** in the ePolicy Orchestrator console, to view details about these events and their resolutions.

- Virus and spyware detections
- Inbound events blocked by the firewall service
- Web filtering events



The date and time shown for events indicate the local time for the ePolicy Orchestrator server when the events occurred. By contrast, the time shown for events in the SecurityCenter reports indicate the local time for the managed system where the events occurred.

For more information on the Threat Event Log, see the ePolicy Orchestrator documentation.

### When to purge Threat Events

To prevent duplicate or outdated data from appearing in the Threat Event Log, we recommend purging Threat Events manually in these situations:

- **After deleting a registered SecurityCenter account** — If you delete a registered account from the list of ePolicy Orchestrator registered servers, purge the Threat Events for that account. (If you do not plan to re-register the account, you can keep Threat Events for reference purposes.)
- **Before re-installing the Security-as-a-Service extension** — If you installed the software and synchronized SaaS data previously, purge the associated Threat Events.

### Purge Threat Events

When re-installing the extension or re-registering a SecurityCenter account that has been registered previously, you need to purge the contents of the Threat Event Log. This prevents old or duplicate data from appearing.

**Task**

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Threat Event Log**.
- 2 Click **Actions | Purge**.
- 3 In the **Purge** dialog box next to **Purge records older than**, type a number and select a time unit.
- 4 Click **OK**.

Records older than the specified age are deleted permanently.

---

## Open the SecurityCenter

Use the SecurityCenter console to address issues related to McAfee SaaS protection services. Access the SecurityCenter console directly from the ePolicy Orchestrator console by using a dashboard monitor that appears on the **Security-as-a-Service** dashboard.

**Before you begin**

You must register your SecurityCenter account with the ePolicy Orchestrator software.

For more information on using SecurityCenter features, see the McAfee SaaS Endpoint Protection documentation, which is available on the **Help & Support** page of the SecurityCenter console.

**Task**

For option definitions, click ? in the interface.

- 1 Click **Menu | Reporting | Dashboards**.
- 2 From the **Dashboards** list, select **Security-as-a-Service**.
- 3 In the **McAfee SecurityCenter** monitor, select one of these links to open a web browser window and display the SecurityCenter console:
  - **Policies** — Opens the **Policy** page, where you can edit existing policies or create new policies for McAfee SaaS managed systems.
  - **Install Protection** — Opens the **Install Protection** page, where you can install McAfee SaaS protection services on client computers.

If you have multiple SecurityCenter accounts, links to each appear. Identify the account by the name specified during registration.

**See also**

[Register a SecurityCenter account on page 16](#)

---

## Compatibility with other McAfee products

The extension is compatible with other McAfee products in the ePolicy Orchestrator environment. However, additional configuration steps are required when used with McAfee® Risk Advisor.

## Considerations when using McAfee Risk Advisor

Scans performed by McAfee Risk Advisor, which analyzes managed systems and identifies vulnerabilities, need to be set up in a particular way when run in an ePolicy Orchestrator environment that includes McAfee SaaS managed systems.

McAfee Risk Advisor pulls current threat data from McAfee® Labs, then analyzes data stored in the ePolicy Orchestrator database and identifies vulnerabilities for managed systems.

For McAfee SaaS managed systems, only a subset of data relevant to calculating risk is pulled from the SecurityCenter account and synchronized with the ePolicy Orchestrator database. Therefore, McAfee Risk Advisor cannot accurately assess the vulnerabilities for these systems.

To more accurately identify vulnerabilities on systems not using McAfee SaaS services, we recommend that you exclude the Security-as-a-Service synchronization points from analysis by using one of these methods:

- Manually select all McAfee SaaS managed systems in the System Tree and disable the analysis for them.
- Create an ePolicy Orchestrator query to identify McAfee SaaS managed systems, and a server task to disable the analysis for these systems.

### Exclude SaaS managed systems manually

Manually exclude McAfee SaaS managed systems from analysis by McAfee Risk Advisor by selecting the systems in the System Tree, then disabling the analysis for them.

#### Task

For option definitions, click ? in the interface.

- 1 Click **Menu | Systems | System Tree**.
- 2 In the System Tree, select the synchronization point that contains McAfee SaaS managed systems.
- 3 In the right pane, click the **Systems** tab, then select the systems to exclude.
- 4 Click **Actions | Risk Advisor | Change Analysis Status**.
- 5 Select **Disable**, then click **OK**.
- 6 Verify the change.
  - a Click **Menu | Systems | System Tree**.
  - b In the right pane, click the **Systems** tab, then click a computer name.
  - c On the **System Information** page, click the **Risk Advisor** tab, then make sure that the **Analysis Status** is **Disabled**.

### Exclude SaaS managed systems with a server task

To automate the process for excluding McAfee SaaS managed systems from analysis by McAfee Risk Advisor, create an ePolicy Orchestrator query that identifies SaaS managed systems and a server task that disables the analysis for these systems.

The extension adds a management type, **Security-as-a-Service**, to the ePolicy Orchestrator reporting feature. This management type makes it possible for queries to locate SaaS managed systems automatically.

## Task

For option definitions, click ? in the interface.

- 1 Create a query to identify and select all McAfee SaaS managed systems.
  - a Click **Menu | Reporting | Queries & Reports**.
  - b Click the **Query** tab, then click **New**.
  - c Select options for the query.

In this tab...	Do this...
<b>Result Type</b>	<ol style="list-style-type: none"> <li>1 In the <b>Feature Group</b> pane, select <b>System Management</b>.</li> <li>2 In the <b>Result Types</b> pane, click <b>Managed Systems</b>, then click <b>Next</b>.</li> </ol>
<b>Chart</b>	<ol style="list-style-type: none"> <li>1 In the <b>Display Results As</b> pane, select <b>Table</b>.</li> <li>2 In the right pane select <b>Computer Properties   Management Type</b> from the <b>Sort by</b> list, then click <b>Next</b>.</li> </ol>
<b>Columns</b>	<ul style="list-style-type: none"> <li>• In the <b>Available Columns</b> pane under <b>Computer Properties</b>, add the <b>Management Type</b> field, then click <b>Next</b>.</li> </ul>
<b>Filters</b>	<ol style="list-style-type: none"> <li>1 In the <b>Available Properties</b> pane under <b>Computer Properties</b>, add the <b>Management Type</b> field.</li> <li>2 In the right pane select <b>Management Type   Equals   Security as a Service</b>, then click <b>Save</b>.</li> </ol>

- d Type a name for the query, specify a new or existing query group, then click **Save**.
- 2 Create a server task to disable analysis for these systems.
  - a Click **Menu | Automation | Server Tasks**.
  - b Click **New Task**.
  - c Type a name for the task, select a schedule status of **Enabled**, then click **Next**.
  - d From the **Actions** menu, select **Run Query**.
  - e In the query field, click the browser icon, select the query created in step 1 from the list, then click **OK**.
  - f In the **Sub-Actions** field, click the browse icon, select **Disable or Enable Threat(s) or Asset(s)** from the list, then click **OK**.
  - g For **Analysis Status**, select **Disable**, then click **Next**.
  - h Select scheduling options, then click **Next**.
  - i Click **Save**.
- 3 Run the server task manually or wait for it to run as scheduled.

The server task identifies each SaaS managed system and sets its **Analysis Status** to **Disabled**. These systems will not be included in analyses performed by McAfee Risk Advisor.

- 4 Verify the results of the server task.
  - a Click **Menu | Systems | System Tree**.
  - b In the right pane, click the **Systems** tab, then click a computer name.
  - c On the **System Information** page, click the **Risk Advisor** tab, then check that the **Analysis Status** is **Disabled**.

# 4

## Troubleshooting

These topics provide additional information related to installing and using the extension.

### Contents

- ▶ *Troubleshooting solutions*
- ▶ *Manual deletion of files and events*
- ▶ *Find more information*

---

## Troubleshooting solutions

Here are solutions to common problems.

### Installing the extension

#### The extension does not appear in the Software Download Manager on the ePolicy Orchestrator server

Download a copy of the extension from the SecurityCenter console. The link is available on the **ePO Servers** tab of the **Utilities** page.

#### To re-install the extension after it has already been installed and uninstalled

Not all items associated with the extension are removed during the uninstallation process. Before re-installing the extension, you need to manually delete the **Security-as-a-Service** dashboard, **Security-as-a-Service** queries, the default SaaS Data Synchronization server task, and Threat Events.

### Connecting to the SecurityCenter

#### You can't create a registered server from the ePolicy Orchestrator console

Do one or more of the following:

- **Verify that you can access the SecurityCenter console from the ePolicy Orchestrator server.** On the computer where the server is running, open a browser window, enter the URL for accessing the SecurityCenter, then try to connect.
- **Verify that your SecurityCenter account credentials are correct.** Open a new tab in the same browser or open a new browser window, then enter your credentials and try to log on.
- **Check whether your ePolicy Orchestrator server is listed as a registered server in the SecurityCenter console.** On the **Utilities** page, click the **ePO Servers** tab, then check the **Registered ePolicy Orchestrator Servers** list. If your account is listed, you can't register it again. If it isn't listed, contact technical support.

## Registering a server

### You register a SecurityCenter account and receive an error message that it is already registered

Unregister the account, then register it again. If the problem persists, contact technical support.

## Synchronizing SaaS data

### You don't see your data after you register a SecurityCenter account

Data does not appear until a SaaS data synchronization server pull task runs successfully.

- **Check the Server Task Log to see whether the task has run or is complete.** If the task is scheduled to run at a specific time, it might not have run yet. If this is the first time it has run, it might take a long time because it pulls data for the last 30 days.
- **Wait three minutes after data synchronization is complete, or refresh each monitor manually.** Click the triangle icon in the upper-left corner of each monitor, then select **Refresh** from the menu.
- **Check whether information appears in the widgets on the Dashboard page of the SecurityCenter console.** If you recently set up your SecurityCenter account and the information has not yet had time to appear in the widgets, it cannot be synchronized with the ePolicy Orchestrator software. If sufficient time has elapsed and the information still isn't displayed in the widgets, there is a problem with your SecurityCenter account. For more information, check the McAfee SaaS Endpoint Protection documentation, which is available on the **Help & Support** tab of the SecurityCenter console.

### You create a synchronization point using a SecurityCenter account that has already been registered and synchronized

Changing the synchronization point for a registered account does not cause monitors to display information for the new synchronization point automatically. If you change the synchronization point, do one of the following:

- Rename the existing synchronization point.
- Delete McAfee SaaS managed computers from the existing synchronization point before setting up the new synchronization point.

### You see duplicate data for the SaaS managed systems

Duplicate data can result from these situations:

- **You deleted a registered SecurityCenter account and did not manually delete the associated synchronization point.** Delete the synchronization point for the deleted account, then run the SaaS data synchronization task again.
- **You deleted a registered SecurityCenter account and did not manually delete the Threat Events.** This resulted in outdated Threat Events from the previous registration being pulled during data synchronization. Purge the Threat Events for the account, then run the data synchronization task again.
- **You uninstalled and re-installed the extension and did not manually delete the Threat Events.** This resulted in outdated Threat Events from the previous installation being pulled during data synchronization. Purge the Threat Events for the account, then run the data synchronization task again.

### You delete a synchronization point, then re-create it

If you delete an existing synchronization point, its associated server task no longer runs. If you re-create the synchronization point, you need to configure its server task or a new server task to synchronize data for it. Re-creating the synchronization point does not cause the server task associated with the previous instance of the synchronization point to begin synchronizing data automatically for the new instance of the synchronization point.



### Your data is not being updated

Do any or all of the following:

- From the ePolicy Orchestrator console, check the status of the SaaS Data Synchronization server task in the Server Task Log (click **Menu Automation Server Task Log**).
- From the SecurityCenter console, view the status of the synchronization (from the **Utilities** page, click the **ePO Servers** tab, then view the **ePolicy Orchestrator (McAfee ePO) Servers** list).
- If the SaaS data synchronization server task continues to fail, contact technical support (from the SecurityCenter console, click the **Help & Support** tab, then click **Get Support**).

### You nested one synchronization point under another in the System Tree, and the nested one no longer appears

When you synchronize data for the top synchronization point, any synchronization points nested within it are deleted (because those systems do not actually exist in the same registered account). Re-create the deleted synchronization point at the root level of the System Tree, link it to a SaaS data synchronization server task, and run the server task to populate the replacement synchronization point with SaaS managed systems.

### All of your systems don't appear in the System Tree

Within a single group of managed systems, only one instance of a system name can be synchronized. If you have multiple systems using the same name within the same group, you need to rename systems with unique names.

## Viewing data with dashboard monitors

### You have synchronized data, but don't see data in any Security-as-a-Service dashboard monitor

When synchronization is complete, information in your dashboard monitors refreshes automatically after three minutes. To see data immediately, click the triangle icon in the upper-left corner of each monitor, then select **Refresh** from the menu.



Clicking the **Refresh** icon in the upper-right corner of the console does not refresh the monitors in this situation.

### You have synchronized data, but the information that appears in the Security-as-a-Service monitors does not match what appears in the SecurityCenter widgets

Information that appears in the monitors should match or be very similar to what appears in the corresponding widgets on the **Dashboard** page of the SecurityCenter console. If information appears in the widgets and not in the monitors, there might be a problem with configuration or synchronization for the extension. Contact technical support.

### You have synchronized data, but don't see data in the Top Computers with Detections or Top Computers with Blocked Sites monitors

- For the length of time specified by the monitor, there haven't been any relevant detections.



Your SecurityCenter account does not have to be active during the entire 7 or 30 days for data to appear in a monitor. Account data is available for the number of days that the account has been active.

- Data synchronization was unsuccessful or hasn't yet occurred. Check the status in the Server Task Log (from the ePolicy Orchestrator console, click **Menu | Automation | Server Task Log**).
- It hasn't been three minutes since synchronization occurred. Wait for monitors to refresh automatically after three minutes, or refresh each monitor manually (click the triangle icon in the upper-left corner of each monitor, then select **Refresh** from the menu).

### You have synchronized data, but don't see all your Threat Events data

If Threat Events are missing from the SecurityCenter after you run a SaaS data synchronization task, the amount of information in your account exceeds the amount that can be pulled during a single execution of the task. Schedule the task to run multiple times each day to ensure that all Threat Events are pulled from the SecurityCenter.

## Performing risk analysis

### A McAfee Risk Advisor risk analysis indicates that McAfee SaaS managed systems are at risk

Only a subset of information relevant to calculating risk is pulled from the SecurityCenter account and synchronized with the ePolicy Orchestrator database. Therefore, the analysis cannot accurately assess the vulnerabilities for these systems. For more accurate results, we recommend that you exclude McAfee SaaS managed systems from analysis. You can do this manually in the System Tree, or create a query and server task to identify and exclude these systems automatically.

#### See also

*Exclude SaaS managed systems manually* on page 36

*Exclude SaaS managed systems with a server task* on page 36

*Delete data manually* on page 43

*Purge Threat Events* on page 34

---

## Manual deletion of files and events

Some files are not deleted automatically when you remove the extension or components from your ePolicy Orchestrator environment.

You need to delete data manually in these situations.

- **After deleting a registered SecurityCenter account.**
  - Delete the container group in the System Tree where synchronized groups and systems were placed. (The container group in the System Tree is no longer configured as a synchronization point, but it still contains the groups and systems previously synchronized with the deleted account.)
  - Purge the Threat Events. (If you do not plan to re-register the account, you can keep Threat Events for reference purposes.)
- **Before re-installing the extension.**
  - Delete these items manually before re-installing the extension:
    - The default **SaaS Data Synchronization** task.
    - **Security-as-a-Service** dashboard.
    - **Security-as-a-Service** queries.
    - Threat Events.
  - Don't delete these items. They are updated automatically during the initial SaaS data synchronization for the new installation:
    - Registered SecurityCenter accounts.
    - Computers and groups previously synchronized with the SecurityCenter.
  - Don't delete these items. They can be reused or reconfigured for the new installation:
    - Scheduled SaaS data synchronization tasks.

## Delete data manually

Delete or purge items that are not deleted automatically when you remove the extension or its components from your ePolicy Orchestrator environment.



If you plan to re-install the extension, only the Threat Events and synchronization points need to be deleted.

### Task

For option definitions, click ? in the interface.

- Delete items as needed.

To delete this...	Do these steps...
Threat Events	<ol style="list-style-type: none"> <li>1 Click <b>Menu</b>   <b>Reporting</b>   <b>Threat Event Log</b>.</li> <li>2 Click <b>Actions</b>   <b>Purge</b>.</li> <li>3 In the <b>Purge</b> dialog box next to <b>Purge records older than</b>, type a number and select a time unit.</li> <li>4 Click <b>OK</b>.</li> </ol>
Synchronization points	<ol style="list-style-type: none"> <li>1 Click <b>Menu</b>   <b>Systems</b>   <b>System Tree</b>.</li> <li>2 In the <b>System Tree</b> pane, select the synchronization point.</li> <li>3 Click <b>System Tree Actions</b>   <b>Delete Group</b>.</li> </ol>
Default dashboard	<ol style="list-style-type: none"> <li>1 Click <b>Menu</b>   <b>Reporting</b>   <b>Dashboards</b>, then select the dashboard you want to delete from the <b>Dashboard</b> drop-down list.</li> <li>2 From the <b>Dashboards</b> list, select <b>Security-as-a-Service</b>.</li> <li>3 Click <b>Dashboard Actions</b>   <b>Delete</b>.</li> <li>4 Click <b>OK</b>.</li> </ol>
Default server task	<ol style="list-style-type: none"> <li>1 Click <b>Menu</b>   <b>Automation</b>   <b>Server Tasks</b>.</li> <li>2 Select the <b>Synchronize SaaS Data</b> server task, then click <b>Actions</b>   <b>Delete</b>.</li> <li>3 Click <b>OK</b>.</li> </ol>
Queries	<ol style="list-style-type: none"> <li>1 Click <b>Menu</b>   <b>Reporting</b>   <b>Queries &amp; Reports</b>.</li> <li>2 Select a query to delete, then click <b>Actions</b>   <b>Delete</b>.</li> <li>3 Click <b>Yes</b>.</li> </ol>

### See also

[Install the product extension on page 14](#)

## Find more information

Access additional documentation to get more information about using the software.

### Task

- Do any of the following.

Product	How to access documentation
ePolicy Orchestrator software	From the ePolicy Orchestrator console: <ul style="list-style-type: none"> <li>• View the online Help: Click the ? icon in the upper-right corner of any page.</li> <li>• Download the user guide or release notes:               <ol style="list-style-type: none"> <li>1 Click <b>Menu   Software   Software Manager   Extensions</b>.</li> <li>2 In the <b>Product Categories</b> pane, click <b>Management Solutions</b>.</li> <li>3 In the right pane under <b>Software</b>, click <b>McAfee ePolicy Orchestrator</b>.</li> <li>4 In the lower-right pane, locate the document in the <b>Component</b> column, then click <b>Download</b> in the <b>Actions</b> column.</li> <li>5 In the <b>File Download</b> dialog box, save the document file to a local folder, then click <b>OK</b>.</li> </ol> </li> </ul>
Security-as-a-Service extension	From the ePolicy Orchestrator console: <ul style="list-style-type: none"> <li>• View the online Help: Click the ? icon in the upper-right corner of any page containing content specific to the extension.</li> <li>• Download the user guide or release notes:               <ol style="list-style-type: none"> <li>1 Click <b>Menu   Software   Software Manager   Extensions</b>.</li> <li>2 In the <b>Product Categories</b> pane, click <b>Management Solutions</b>.</li> <li>3 In the right pane under <b>Software</b>, click <b>McAfee SaaS &lt;version number&gt;</b>.</li> <li>4 In the lower-right pane, locate the document in the <b>Component</b> column, then click <b>Download</b> in the <b>Actions</b> column.</li> <li>5 In the <b>File Download</b> dialog box, save the document file to a local folder, then click <b>OK</b>.</li> </ol> </li> </ul>
SecurityCenter, McAfee SaaS Endpoint Protection, and McAfee SaaS services	From the SecurityCenter console: <ul style="list-style-type: none"> <li>• View the online Help: Click the ? icon in the upper-right corner of any page.</li> <li>• View the product guide or installation guide for McAfee SaaS Endpoint Protection in PDF format: Click the <b>Help &amp; Support</b> tab, then select a document link.</li> <li>• View a quick start guide or troubleshooting solutions for the extension: Select one of the links on the <b>ePO Servers</b> tab of the <b>Utilities</b> page.</li> <li>• View additional documentation for a specific McAfee SaaS service: Check the corresponding chapter in the product guide for instructions. Typically, click a link in the widget associated with the service to open the associated SaaS management portal, then click the <b>Help</b> link on the portal.</li> </ul>

# Index

## A

about this guide [5](#)

accounts

    synchronization administrator, about [26](#)

    synchronization administrator, creating [27](#)

Active Directory

    synchronization administrator account, about [26](#)

    synchronization administrator account, creating [27](#)

administrators

    data synchronization, about [26](#)

    data synchronization, creating [27](#)

## C

compatibility, Security-as-a-Service and McAfee Risk Advisor [36](#)

components for Security-as-a-Service extension

    required [8](#)

    setup [8](#)

configuration

    McAfee Risk Advisor risk analysis tasks [36](#)

    overview [13](#)

    permission sets for Security-as-a-Service [26](#)

    registered servers for Security-as-a-Service extension [16](#)

    SaaS data synchronization [22](#)

    synchronization administrator account [26](#), [27](#)

    synchronization points [20](#)

    user roles for Security-as-a-Service [26](#)

conventions and icons used in this guide [5](#)

create

    data synchronization points [20](#)

    registered servers [16](#)

    SaaS data synchronization schedule [22](#)

    synchronization administrator account [26](#), [27](#)

## D

dashboards for Security-as-a-Service

    about [31](#)

    customizing [31](#)

    default [31](#)

    deleting [43](#)

data center, selecting [16](#)

data synchronization (Active Directory)

    synchronization administrator, about [26](#)

    synchronization administrator, creating [27](#)

data synchronization (Security-as-a-Service extension)

    about [18](#)

    definition of SaaS data [19](#)

    performing [22](#)

    scheduling [22](#)

    synchronization administrator, about [26](#)

    synchronization administrator, creating [27](#)

    synchronization points, about [18](#)

    synchronization points, creating [20](#)

    synchronization points, viewing status [24](#)

    viewing synchronization status [24](#)

    viewing synchronized data [30](#)

delete

    dashboards [43](#)

    queries [43](#)

    registered SecurityCenter accounts [18](#)

    SaaS managed systems from risk analysis [36](#)

    synchronization points [43](#)

    Threat Event Log entries [34](#), [43](#)

    when to delete items manually [42](#)

documentation

    audience for this guide [5](#)

    online Help [43](#)

    product and user guides [43](#)

    product-specific, finding [6](#), [43](#)

    typographical conventions and icons [5](#)

downloads, Security-as-a-Service extension [14](#)

## E

edit

    permission sets for Security-as-a-Service [26](#)

    registered SecurityCenter accounts [17](#)

    SaaS data synchronization server tasks [22](#)

    synchronization administrator account [26](#), [27](#)

    user roles for Security-as-a-Service [26](#)

events

    Threat Event Log, contents [34](#)

    Threat Event Log, purging [34](#)

exclusion of SaaS managed systems from risk analysis [36](#)

## H

Help, online [43](#)

**I**

## installation

- deleting data from previous installations [43](#)
- installing after a previous installation [42](#)
- installing Security-as-a-Service extension [14](#)
- requirements [8](#)

**L**

## logs

- Threat Event [34](#)

**M**McAfee Risk Advisor [36](#)

## McAfee SecurityCenter, See SecurityCenter

McAfee SecurityCenter monitor [35](#)McAfee ServicePortal, accessing [6](#)

## monitor SaaS security, See SaaS security, monitoring

## monitors for Security-as-a-Service

- about [31](#)
- default [31](#)
- for System Information page [33](#)
- McAfee SecurityCenter monitor [35](#)

**O**online Help [43](#)open, SecurityCenter console [35](#)

## overview

- component setup for Security-as-a-Service extension [8](#)
- extension installation and setup process [11](#)
- feature configuration [13](#)
- how the product extension works [7](#)
- process for monitoring SaaS security [29](#)
- SaaS features added to McAfee ePO environment [12, 30](#)

**P**

## permission sets for Security-as-a-Service

- about [25](#)
- configuring [26](#)

## pull tasks, See server tasks for SaaS data synchronization

## pulling SaaS data, See data synchronization

## purge, See delete

**Q**

## queries for Security-as-a-Service

- about [32](#)
- custom [33](#)
- deleting [43](#)
- excluding systems from risk analysis [36](#)
- predefined [33](#)

Query Builder, Security-as-a-Service additions [33](#)**R**re-installation, requirements [42, 43](#)

## registered servers for Security-as-a-Service

- about [16](#)
- accessing from McAfee ePO console [31, 35](#)
- deleting [18](#)
- deleting data from previous registrations [42, 43](#)
- editing [17](#)
- re-registering after a previous registration [42](#)
- registering [16](#)
- viewing [17](#)

reports for Security-as-a-Service [33](#)requirements for Security-as-a-Service extension [8](#)

## retrieval of SaaS data, See data synchronization

risk analysis and Security-as-a-Service [36](#)

## roles, user for Security-as-a-Service

- configuring [26](#)
- defined [25](#)
- SaaS Admin [26](#)
- SaaS Reviewer [26](#)

**S**SaaS Admin role, configuring [26](#)

## SaaS data synchronization, See data synchronization

SaaS Reviewer role, configuring [26](#)

## SaaS security, monitoring

- dashboards and monitors, about [31](#)
- features overview [30](#)
- process overview [29](#)
- queries, about [32](#)
- queries, custom [33](#)
- queries, predefined [33](#)
- reports [33](#)
- System Information page [33](#)
- Threat Event Log [34](#)

scheduled, SaaS data synchronization [22](#)

## SecurityCenter

- defined [7](#)
- deleting registered ePO servers [18](#)
- documentation links [43](#)
- downloading Security-as-a-Service extension [14](#)
- opening from the McAfee ePO console [31, 35](#)
- registering with McAfee ePO software [16](#)
- unregistering with McAfee ePO software [18](#)

server tasks for excluding systems from risk analysis [36](#)

## server tasks for SaaS data synchronization

- about [18](#)
- checking status [18, 24](#)
- definition of data [19](#)
- deleting [43](#)
- editing [22](#)
- running [22](#)
- scheduling [22](#)
- viewing [22](#)

- servers, registered for Security-as-a-Service
    - about [16](#)
    - deleting [18](#)
    - editing [17](#)
    - registering [16](#)
    - viewing [17](#)
  - ServicePortal, finding product documentation [6](#)
  - setup for Security-as-a-Service extension, overview [8](#)
  - Software Manager
    - downloading documentation [43](#)
    - downloading the product extension [14](#)
  - synchronization administrator
    - about [26](#)
    - creating and updating [27](#)
  - synchronization points
    - about [18](#)
    - creating [20](#)
    - deleting [18](#), [43](#)
    - viewing status [24](#)
  - synchronization, SaaS data, See data synchronization
  - System Information page [33](#)
  - system requirements [8](#)
  - System Tree, synchronization points and [20](#), [24](#)
- T**
- Technical Support, finding product information [6](#), [43](#)
  - Threat Event Log
    - contents [34](#)
    - purging [34](#), [43](#)
    - when to purge [18](#), [42](#)
- U**
- unregistration, servers for Security-as-a-Service [18](#)
  - user roles, See roles, user for Security-as-a-Service
- V**
- view
    - registered SecurityCenter accounts [17](#)
    - SaaS data synchronization server tasks [22](#)
    - SaaS data synchronization, status [22](#)
    - SaaS data, synchronized [29](#), [30](#)
    - synchronization points, status [24](#)

