

Forefront Protection 2010 for SharePoint

Management Pack Guide

Microsoft Corporation

Published: June 2010

Send suggestions and comments about this document to mpgfeed@microsoft.com. Please include the Management Pack guide name with your feedback.

Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Excel, Forefront, Internet Explorer, Outlook, PowerPoint, SharePoint, Windows, Windows NT, Windows PowerShell, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Privacy policy

Review the privacy statement at the following address: <http://go.microsoft.com/fwlink/?linkid=166227>

Contents

[Forefront Protection 2010 for SharePoint Management Pack 5](#_Toc261290080)

[Introduction to monitoring with Operations Manager 2007 5](#_Toc261290081)

[Key features 5](#_Toc261290082)

[Getting the latest FPSP Management Pack and documentation 6](#_Toc261290083)

[Supported configurations 6](#_Toc261290084)

[Getting Started 6](#_Toc261290085)

[Before you import the FPSP Management Pack 6](#_Toc261290086)

[Files in this management pack 7](#_Toc261290087)

[What this management pack monitors 8](#_Toc261290088)

[Importing the FPSP Management Pack 9](#_Toc261290089)

[Verifying system requirements for installing the management pack 10](#_Toc261290090)

[Installing the management pack 10](#_Toc261290091)

[About the folder structure 12](#_Toc261290092)

[Deploying agents 12](#_Toc261290093)

[Creating a new management pack for customizations 13](#_Toc261290094)

[Enabling performance threshold rules 13](#_Toc261290095)

[Low-Privilege Environments 14](#_Toc261290096)

[Understanding management pack operations 14](#_Toc261290097)

[Configuring notifications 14](#_Toc261290098)

[Working with monitors 14](#_Toc261290099)

[Viewing the Knowledge Base for monitors 15](#_Toc261290100)

[Monitor reference 15](#_Toc261290101)

[Antimalware engine monitors 15](#_Toc261290102)

[License monitors 18](#_Toc261290103)

[Services monitors 19](#_Toc261290104)

[Workload integration monitors 20](#_Toc261290105)

[Realtime scan monitors 20](#_Toc261290106)

[Scheduled scan monitors 22](#_Toc261290107)

[Working with rules 25](#_Toc261290108)

[Rules reference 25](#_Toc261290109)

[Working with views 26](#_Toc261290110)

[Views reference 27](#_Toc261290111)

[Common views 27](#_Toc261290112)

[Forefront Protection 2010 for SharePoint views 29](#_Toc261290113)

[Working with tasks 30](#_Toc261290114)

[Running a task 31](#_Toc261290115)

[Objects the FPSP Management Pack discovers 32](#_Toc261290116)

[Classes 33](#_Toc261290117)

[Class discoveries 34](#_Toc261290118)

[How health rolls up 35](#_Toc261290119)

[Key monitoring scenarios 35](#_Toc261290120)

[Problem types 36](#_Toc261290121)

[Engines 36](#_Toc261290122)

[SharePoint hook 36](#_Toc261290123)

[Scan Jobs 36](#_Toc261290124)

[Services 38](#_Toc261290125)

[License 38](#_Toc261290126)

[Viewing information in the Operations Manager Console 38](#_Toc261290127)

[Placing monitored objects in maintenance mode 38](#_Toc261290128)

[Troubleshooting 40](#_Toc261290129)

[Appendix: Monitors and overrides for management packs 40](#_Toc261290130)

[How to view management pack details 40](#_Toc261290131)

[How to display monitors for a management pack 41](#_Toc261290132)

[How to display overrides for a management pack 41](#_Toc261290133)

[How to display all management pack rules 41](#_Toc261290134)

[How to display monitor thresholds 42](#_Toc261290135)

[How to display performance collection rules 44](#_Toc261290136)

# Forefront Protection 2010 for SharePoint Management Pack

This guide describes the Microsoft® Forefront™ Protection 2010 for SharePoint Management Pack (FPSP Management Pack, version 11.1.301.0. The management pack is used to monitor Forefront Protection 2010 for SharePoint.

Essential features, configuration, and usage of the FPSP Management Pack for Microsoft System Center Operations Manager 2007 (Operations Manager 2007) are provided in this guide. Additional information about Operations Manager 2007 is available at the [Microsoft System Center Operations Manager TechCenter](http://go.microsoft.com/fwlink/?linkid=96668).

# Introduction to monitoring with Operations Manager 2007

Operations Manager 2007 provides a way for you to monitor important applications and to be notified when there are issues with those applications that could result in degraded performance or complete loss of functionality. You do this by installing a management pack that primarily consists of monitors for alerts and state based on events and performance counters generated by applications. It works within the Operations Manager 2007 framework to monitor your FPSP systems.

The FPSP Management Pack is a collection of monitors, rules, and scripts that work within Operations Manager 2007. These monitors, rules, and scripts assist in the centralized management of systems that have FPSP installed. Remote servers are managed by means of Operations Manager 2007 "agents." Systems that have agents installed are referred to as "agent-managed systems."

You can build a service model and health model by defining targets and creating monitors, rules, and reports. These are all contained in a management pack for that application. When imported into Operations Manager 2007, the management pack describes the application and tells Operations Manager 2007 how to discover and monitor it. Operations Manager 2007 is not aware of an application until its management pack is imported.

## Key features

The FPSP Management Pack for Operations Manager 2007 provides support for Operations Manager 2007 agent-managed systems running FPSP. It also provides support for monitoring of the "health" of your agent-managed systems, informing you when they are running smoothly and when there are problems, both actual and potential. For example, you are notified if over half of your scan engines failed to update, or if it is determined that files are not being scanned.

The FPSP Management Pack contains rules for:

* Monitoring the state of FPSP and its key features.
* Collecting statistical data about file scanning performance for each scan job (realtime and scheduled).

## Getting the latest FPSP Management Pack and documentation

You can find the FPSP Management Pack in the [System Center Operations Manager 2007 Catalog](http://go.microsoft.com/fwlink/?LinkId=82105) (<http://go.microsoft.com/fwlink/?LinkId=82105>).

# Supported configurations

The following table details the supported configurations for Forefront Protection 2010 for SharePoint:

|  |  |
| --- | --- |
| **Configuration** | **Support** |
| Windows Server 2003 | SP2 and above |
| Windows Server 2008 | Yes |
| Windows Server 2008 R2 | Yes |
| Office SharePoint Server 2007, Windows SharePoint Services version 3 | SP1 and above |
| SharePoint Server 2010, SharePoint Foundation 2010 | Yes |
| Virtual environment | Hyper-V and any SVVP-compliant virtual machine.  |

# Getting Started

This section describes the actions you should take before you import the management pack, steps you should take to install the product after you import the management pack, and information about customizing the management pack. It is assumed that since you have this guide that you have already downloaded the management pack files. If not, refer to the files listed in [Files in this management pack](#_Files_in_This).

## Before you import the FPSP Management Pack

Before you import the FPSP Management Pack, ensure the managed FPSP server has the PowerShell execution policy at least set to “RemoteSigned.”

## Files in this management pack

To monitor Forefront Protection 2010 for SharePoint, you must first download the following file or files from the Management Pack Catalog, located at <http://go.microsoft.com/fwlink/?LinkId=82105>.

|  |  |  |
| --- | --- | --- |
| **Management Pack Name** | **Contents** | **Required?** |
| Microsoft.ForefrontProtection.Library.mp | Microsoft Forefront Server Protection 2010 Core Library | This management pack is the core library for all versions of Forefront Protection Server. It defines all base classes and relationships. | Yes |
| Microsoft.ForefrontProtection.FPSP.mp | Microsoft Forefront Protection 2010 for SharePoint Management Pack | This management pack provides monitoring capabilities for Microsoft Forefront Protection 2010 for SharePoint. | Yes |
| OM2007\_MP\_refresh\_FPSP.doc | Forefront Protection 2010 for SharePoint Management Pack Guide | This user guide provides an overview to the management pack as well as how to import and install.  | No |

## What this management pack monitors

The following tables list all of the elements in this management pack.

|  |  |
| --- | --- |
| **DISCOVERIES** | **Description** |
| Microsoft.ForefrontProtection.FPSP.Server.Discovery | Discovery of FPSP server. |
| Microsoft.ForefrontProtection.FPSP.Services.Discovery | Discovery of FPSP services. |
| Microsoft.ForefrontProtection.FPSP.Licensing.Discovery | Discovery of FPSP license. |
| Microsoft.ForefrontProtection.FPSP.ScanJobs.Discovery | Discovery of FPSP scan jobs. |
| Microsoft.ForefrontProtection.FPSP.Engines.Discovery | Discovery of FPSP engines. |
| Microsoft.ForefrontProtection.FPSP.AVEngines.Discovery | Discovery of FPSP antimalware engines. |
| Microsoft.ForefrontProtection.FPSP.RealtimeScanJob.Discovery | Discovery of FPSP realtime scan job. |
| Microsoft.ForefrontProtection.FPSP.ScheduledScanJob.Discovery | Discovery of FPSP scheduled scan job. |
| Microsoft.ForefrontProtection.FPSP.WorkloadIntegration | Discovery of FPSP workload integration. |
| Microsoft.ForefrontProtection.FPSP.Services.FSSPFSCController.Discovery | Discovery of Microsoft Forefront Server Protection Controller Service |
| Microsoft.ForefrontProtection.FPSP.Services.EventingService.Discovery | Discovery of Microsoft Forefront Server Protection Eventing Service |
| Microsoft.ForefrontProtection.FPSP.Services.MailPickupService.Discovery | Discovery of Microsoft Forefront Server Protection Mail Pickup Service  |
| Microsoft.ForefrontProtection.FPSP.Services.FSSPController.Discovery | Discovery of Microsoft Forefront Server Protection Controller for SharePoint Service  |

|  |  |
| --- | --- |
| **CLASSES** | **Description** |
| Microsoft.ForefrontProtection.FPSP.Server | Microsoft Forefront Protection 2010 for SharePoint Server |
| Microsoft.ForefrontProtection.FPSP.Services | Microsoft Forefront Protection 2010 for SharePoint Service |
| Microsoft.ForefrontProtection.FPSP.Services.FSSPController | Microsoft Forefront Server Protection Controller for SharePoint Service |
| Microsoft.ForefrontProtection.FPSP.Services.FSSPFSCController | Microsoft Forefront Server Protection Controller Service |
| Microsoft.ForefrontProtection.FPSP.Services.EventingService | Microsoft Forefront Server Protection Eventing Service |
| Microsoft.ForefrontProtection.FPSP.Services.MailPickupService | Microsoft Forefront Server Protection Mail Pickup Service |
| Microsoft.ForefrontProtection.FPSP.Licensing | Microsoft Forefront Protection 2010 for SharePoint License State |
| Microsoft.ForefrontProtection.FPSP.ScanJobs | Microsoft Forefront Protection 2010 for SharePoint Scan Job |
| Microsoft.ForefrontProtection.FPSP.RealtimeScanJob | Microsoft Forefront Protection for SharePoint Realtime scan job |
| Microsoft.ForefrontProtection.FPSP.ScheduledScanJob | Microsoft Forefront Protection 2010 for SharePoint Scheduled Scan Job |
| Microsoft.ForefrontProtection.FPSP.Engines | Microsoft Forefront Protection 2010 for SharePoint Scan Engine |
| Microsoft.ForefrontProtection.FPSP.AVEngines | Microsoft Forefront Protection 2010 for SharePoint Antimalware Engine Update Status |
| Microsoft.ForefrontProtection.FPSP.WorkloadIntegration | Microsoft Forefront Protection 2010 for SharePoint Workload Integration Status |

# Importing the FPSP Management Pack

There are several steps involved in installing and configuring the FPSP Management Pack for Operations Manager 2007 on Forefront Protection 2010 for SharePoint (FPSP):

1. Ensure that the requirements are met. For information, see [Verifying system requirements for installing the management pack](#z1).
2. Install the product. For information, see [Installing the management pack](#z2).
3. Deploy agents. For information, see [Deploying agents](#z906b3d6d63164b228b5d263d18eb941e).
4. Configure notifications. For information, see [Configuring notifications](#zd2c6553f1d3a435892c48e7755eeac74).

After the FPSP Management Pack is imported and installed, follow these steps to finish your initial configuration:

1. Create a new management pack in which you store overrides and other customizations.
2. Override the parameters of the performance rules if you require performance monitoring.

## Verifying system requirements for installing the management pack

The only requirement for installing the FPSP Management Pack on Operations Manager 2007 is that you have an operational server running Operations Manager 2007. Download the management pack files (see [Installing the management pack](#z2)) to this server.

## Installing the management pack

There are two files required for the installation of the management pack: a common file and one specific to FPSP. The common file is called Microsoft.ForefrontServer.Library.mp, and the FPSP-specific file is called Microsoft.ForefrontServer.FPSP.mp. These are "sealed" files (binaries) that cannot be edited (although many parameters can be overridden).

Note:

If you have installed a previous version of either the FPSP management pack or the FPE management pack (version 11.1.0269.0 or lower), you need to remove it before installing this management pack.

You import a management pack in order to install it.

To import the management packs in pre-Operations Manager 2007 R2 systems

|  |
| --- |
| 1. Log on to the Operations Manager 2007 server with an account that is a member of the Operations Manager Administrator role.2. Select and download the setup package from the [Microsoft System Center Pack Catalog](http://go.microsoft.com/fwlink/?LinkId=71124) to the desktop. The setup package is called "Forefront Protection for SharePoint Management Pack.msi."3. Run the downloaded .msi setup package in order to extract the two .mp files: Microsoft.ForefrontServer.Library.mp, and Microsoft.ForefrontServer.FPSP.mp.4. Click Start, point to All Programs, point to System Center Operations Manager 2007, and then click Operations Console.5. In the Operations Manager 2007 Operations Console, click the Administration space.Note: If you have installed a previous version of either the FPSP management pack or the FPE management pack (version 11.1.0269.0 or lower), you need to remove it before installing this management pack.6. Right-click the Management Packs node and select Import Management Packs or click Import Management Packs in the Actions pane.7. In the Select Management Packs to import dialog box, navigate to the location of the files.8. Select the Microsoft.ForefrontServer.Library.mp and the Microsoft.ForefrontServer.FPSP.mp files, and then click Open.9. In the Import Management Packs dialog box, click Import to import the management packs.10. After the management pack has been imported, the Status changes to "Imported." Click Close. |

To import the management packs directly from the online catalog in Operations Manager 2007 R2 (or later) systems

|  |
| --- |
| 1. Log on to the Operations Manager 2007 server with an account that is a member of the Operations Manager Administrator role.2. Click Start, point to All Programs, point to System Center Operations Manager 2007, and then click Operations Console.3. In the Operations Manager 2007 Operations Console, click the Administration space.Note: If you have installed a previous version of either the FPSP management pack or the FPE management pack (version 11.1.0269.0 or lower), you need to remove it before installing this management pack.4. Right-click the Management Packs node and select Import Management Packs or click Import Management Packs in the Actions pane.5. In the Select Management Packs dialog box, click Add, and then select Add from catalog to download and install management packs directly from the online catalog.6. In the Select Management Packs from Catalog dialog, in the Find field, enter "Forefront", and then click Search to search for all Forefront management packs.7. Expand Forefront, and then, in the Forefront Protection 2010 node, select Forefront Protection 2010 for SharePoint and, if it has not yet been installed, Forefront Protection 2010 Core Library. Click Add.8. When you have selected all the required management packs, click OK.9. In the Select Management Packs dialog box, click Install to import the management packs.10. After the management pack has been imported, the Status changes to "Imported". Click Close.  |

After you have imported them, management packs appear in the Administration space, in the Management Packs list. For more information about importing management packs, refer to the product help and documentation at the [Microsoft System Center Operations Manager TechCenter](http://go.microsoft.com/fwlink/?linkid=96668).

When the management packs have been successfully installed, a folder structure is created in Operations Manager 2007. For more information, see [About the folder structure](#z3). You should now finish the installation by deploying agents (see [Deploying agents](#z906b3d6d63164b228b5d263d18eb941e)) and configuring notifications (see [Configuring notifications](#zd2c6553f1d3a435892c48e7755eeac74)).

## About the folder structure

After you install the management packs, a folder structure is created in the Operations Manager 2007 Operations Console, under the Monitoring space. All folders are views of monitored items, except for those folders that contain subfolders (that is, only the lowest level folders view monitored items).

The top level folder is called Microsoft Forefront Server Protection 2010. It contains subfolders common to all Microsoft Forefront Protection Suite products (Alerts, Task Status, and Common), plus the Forefront Protection for SharePoint folder. The Forefront Protection for SharePoint folder contains subfolders that are specific to FPSP. For more information about working with views, see [Working with views](#_Working_with_views), and Views reference.

This is the folder structure for the common elements and for FPSP. All items not labeled "(folder)" contain views.

     Microsoft Forefront Server Protection 2010 (folder)

          Alerts

          Task Status

          Common (folder)

                    Engines (folder)

                              Engine Update State

                              Engine Update Alerts

                    License (folder)

                              License Alerts

                              License State

          Forefront Protection for SharePoint (folder)

                    Alerts

                    State

                    Task Status

                    Scan Job Performance (folder)

                              Realtime Scan Performance

                              Scheduled Scan Performance

## Deploying agents

To administer remote computers that have Microsoft Forefront Protection 2010 for SharePoint installed, you must deploy Operations Manager 2007 agents to them. These agents communicate between the managed servers and Operations Manager 2007.

An agent is an Operations Manager 2007 service that runs on each computer that you want to monitor. The agent captures information from the computer on which it is running, applies predefined rules to the captured data, and performs actions as defined by the rules.

Systems that have the agents installed are referred to as "agent-managed systems."

Agents are deployed using the Discovery Wizard, which discovers all of the computers that can be managed. You deploy the agents from within the Discovery Wizard, after the computers are discovered.

The Discovery Wizard is accessed from the Administration space. At the bottom of the navigation pane, click Discovery Wizard.

For more information about deploying Operations Manager 2007 agents, refer to the product help and documentation at the [Microsoft System Center Operations Manager TechCenter](http://go.microsoft.com/fwlink/?linkid=96668).

# Creating a new management pack for customizations

Most vendor management packs are sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, Operations Manager 2007 saves all customizations to the default management pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

Creating a new management pack for storing overrides has the following advantages:

 It simplifies the process of exporting customizations that were created in your test and pre-production environments to your production environment. For example, instead of exporting a default management pack that contains customizations from multiple management packs, you can export only the management pack that contains customizations of a single management pack.

 It allows you to delete the original management pack without first needing to delete the default management pack. A management pack that contains customizations is dependent on the original management pack. This dependency requires you to delete the management pack with customizations before you can delete the original management pack. If all of your customizations are saved to the default management pack, you must delete the default management pack before you can delete an original management pack. By doing so you would lose all of your customizations.

 It is easier to track and update customizations to individual management packs.

For more information about sealed and unsealed management packs, see [Management Pack Formats](http://go.microsoft.com/fwlink/?LinkId=108355) (http://go.microsoft.com/fwlink/?LinkId=108355). For more information about management pack customizations and the default management pack, see [About Management Packs in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=108356) (http://go.microsoft.com/fwlink/?LinkId=108356).

# Enabling performance threshold rules

The following table lists the performance rules that we recommend you enable. Before you enable a performance rule, you should baseline the relevant performance counters and then apply the appropriate overrides to define and enable a suitable sampling frequency for your environment.

The following rule threshold ranges and intervals represent the recommended minimum and maximum values for most environments.

| **Rule Name** | **Rule target** |
| --- | --- |
| Realtime Scan Performance | FPSP Realtime scan jobs |
| Scheduled Scan Performance | FPSP Scheduled scan jobs |

# Low-Privilege Environments

In order to obtain full functionality, the Operations Manager agent account must be a member of the local administrators group or must be *networkservice* or *localsystem*. When running in a low-privilege environment, special privileges are required for the following functionality:

* To collect performance monitoring data, the Operations Manager agent account must be a member of the local Performance Monitor users group.
* To run tasks in the FPSP management pack, the Operations Manager agent account must be a member of the local administrators group or must be a network service or local system.

# Understanding management pack operations

Operation tasks performed by the FPSP management pack are described in the following section.

## Configuring notifications

E-mail and paging notifications can be sent when alerts occur. Microsoft System Center Operations Manager 2007 (Operations Manager 2007) supports several kinds of notifications, including e-mail, instant messages (IM), text messages (SMS), and customized commands. For more information about configuring notifications within Operations Manager 2007, refer to the product help and documentation at the [Microsoft System Center Operations Manager TechCenter](http://go.microsoft.com/fwlink/?linkid=96668).

# Working with monitors

Monitors are used to determine the health state of an application feature and are an integral part of the health model. Generally speaking, monitors are the "intelligence" of Microsoft System Center Operations Manager 2007 (Operations Manager 2007), determining whether your application is healthy.

Monitors are state machines that show a state of healthy (green), warning (yellow), or unhealthy (red). The monitor's state changes in response to the information that it receives.

In the Microsoft Forefront Server Protection Management Pack for Operations Manager 2007, monitors examine the Forefront Protection 2010 for SharePoint (FPSP) product, including engine updates, scan jobs, and services. They examine events generated by those processes to determine if alerts should be generated or if the health state should be changed. Some monitors (called performance monitors) retrieve statistics for scan jobs. There are several different kinds of monitors included with the Microsoft Forefront Server Protection Management Pack.

All monitors are stored in the Authoring space of the System Center Operations console, in the Management Packs Objects node. They monitor events specific to the particular type of server. There are several categories of monitors for FPSP.

## Viewing the Knowledge Base for monitors

All monitors contained in Operations Manager 2007 have a Knowledge Base entry containing a summary or description of the event. This entry explains the event's significance, possible causes, and possible resolutions. For a list of all event codes, see Event ID codes in the Forefront Protection 2010 for SharePoint Technical Reference Guide.

Knowledge Base entries can be viewed through the Operations Manager 2007 Operations Console.

To view a Knowledge Base entry for a monitor

|  |
| --- |
| 1. In the Monitoring space, in the Microsoft Forefront Server Protection 2010 \ Forefront Protection for SharePoint \ State node, double-click in the State column for any server.2. In the Health Explorer dialog box, click any health monitor on the left to display its Knowledge Base entry on the right. |

## Monitor reference

There are several categories of monitors for Microsoft Forefront Protection 2010 for SharePoint (FPSP).

## Antimalware engine monitors

These are the monitors that keep track of potential problems with antimalware engines.

|  |  |
| --- | --- |
| **Display name** | Antimalware Engines Update Enabled Monitor |
| **Description** | Checks if updating for the antimalware engines is enabled. |
| **Alert message** | The antimalware engines selected for scanning are disabled for updating. |
| **Causes** | There are antimalware engines selected for scanning that are not enabled for updating.  |
| **Resolution** | Change the engines selected for updating to match the ones selected for scanning. |

|  |  |
| --- | --- |
| **Display name** | Antimalware Engines Update Success Rate |
| **Description** | Checks the percentage of antimalware engines successfully updated in the last attempt |
| **Alert message** | Some antimalware engines enabled for updates were not successfully updated at the last attempt |
| **Causes** | ****** Network throughput issues. ****** Low bandwidth. ****** Issues with the server providing definition updates. |
| **Resolution** | ****** Ensure that the HTTP proxy server is configured properly. ****** Ensure that there are no network issues. ****** Ensure that the Universal Naming Convention (UNC) configuration settings are appropriate. |

|  |  |
| --- | --- |
| **Display name** | Antimalware Engines Last Update Time Monitor |
| **Description** | Checks if the antimalware engines enabled for updates have been updated in the last five days. |
| **Alert message** | Some antimalware engines enabled for updates have not been updated successfully in the last five days. |
| **Causes** | ****** Network throughput issues. ****** Low bandwidth. ****** Issues with Rapid Update Server. ****** The antivirus vendor has not provided updates in a week (very unlikely). |
| **Resolution** | ****** Ensure that the HTTP proxy server is configured properly. ****** Ensure that there are no network issues. ****** Ensure that the UNC configuration settings are appropriate. |

## License monitors

These are the monitors that keep track of potential problems with licenses.

|  |  |
| --- | --- |
| **Display name** | License State Monitor |
| **Description** | Checks if the Forefront Server Protection license is about to expire or has expired. |
| **Alert message** | The Forefront Server Protection license is about to expire or has expired. |
| **Causes** | ****** A product key has not been entered. ****** Your license has expired and a new product key has not been purchased. |
| **Resolution** | ******  Enter the product key from the Forefront Server Protection Administrator console or Forefront Management Shell.****** If you do not have a product key, contact your Microsoft sales representative or visit the [Pricing and Licensing](http://go.microsoft.com/fwlink/?LinkId=92354) site. |

## Services monitors

These are the monitors that keep track of potential problems with services.

|  |  |
| --- | --- |
| **Display name** | FSCController Service State Monitor |
| **Description** | Checks if the FSCController service is running. |
| **Alert message** | Microsoft Forefront Server Protection service is not running. |
| **Causes** | Not applicable |
| **Resolution** | Restart the SharePoint services:1. Stop all SharePoint services and make sure all the Forefront services are offline.2. Start SharePoint services. Make sure Forefront is completely started. |

|  |  |
| --- | --- |
| **Display name** | FSSPController Service State Monitor |
| **Description** | Checks if the FSSPController service is running. |
| **Alert message** | Microsoft Forefront Server Protection Controller for SharePoint service is not running. |
| **Causes** | Not applicable |
| **Resolution** | Start the Microsoft Forefront Server Protection Controller for SharePoint service. |

|  |  |
| --- | --- |
| **Display name** | Eventing Service State Monitor |
| **Description** | Checks if the FSCEventing service is running. |
| **Alert message** | Microsoft Forefront Server Protection Eventing Service is not running. |
| **Causes** | Not applicable |
| **Resolution** | Start the Microsoft Forefront Server Protection Eventing Service.  |

|  |  |
| --- | --- |
| **Display name** | FSEMailPickup Service State Monitor |
| **Description** | Checks if the FSEMailPickup service is running. |
| **Alert message** | Forefront Server Protection Mail Pickup Service is not running. |
| **Causes** | Not applicable |
| **Resolution** | Start the Microsoft Forefront Server Protection Mail Pickup Service.  |

## Workload integration monitors

These are the monitors that keep track of potential problems with hooking into SharePoint.

|  |  |
| --- | --- |
| **Display name** | Workload Integration State Monitor |
| **Description** | Checks if the w3wp service is running and the Forefront VSAPI library is registered. |
| **Alert message** | Forefront Protection 2010 for SharePoint is not hooked into SharePoint properly. |
| **Causes**  | The Forefront VSAPI library is not registered with SharePoint correctly. |
| **Resolution** | Analyze the Event Log for details regarding the error. |

## Realtime scan monitors

These are the monitors that keep track of potential problems with the Realtime scan.

|  |  |
| --- | --- |
| **Display name** | Realtime Scan Filter Engine Loading Monitor |
| Description | Checks if the filter engine is loaded correctly by the Realtime scan job. |
| Alert message | The filter engine is not loaded successfully for the Realtime scan job. |
| Causes | Damaged or inaccessible filter engine. |
| Resolution | Reinstall FPSP |

|  |  |
| --- | --- |
| Display name | Realtime Scan Engines Initialization Monitor |
| **Description** | Checks if the antimalware engines selected for the Realtime scan job have been initialized successfully. |
| **Alert message** | Some antimalware scan engines have not initialized successfully for the Realtime scan job. |
| **Causes** | It is possible that the engine subfolder has been deleted. It is recreated after a successful engine update. |
| **Resolution** | ****** Make sure the HTTP proxy server is configured properly. ****** Make sure that there are no network issues. ****** Make sure that the UNC configuration settings are appropriate. |

|  |  |
| --- | --- |
| **Display name** | Realtime Scan Enabled State Monitor |
| **Description** | Checks if the Realtime scan job is enabled properly |
| **Alert message** | Realtime scan is not enabled properly. |
| **Causes** | * The Realtime scan job is bypassed.
* VSAPI scanning on upload is disabled.
* VSAPI scanning on download is disabled.
 |
| **Resolution** | * Using the Forefront Protection 2010 for SharePoint Administrator Console or through Forefront Management Shell, check that the Realtime scan job is not bypassed.
* In “Antivirus” settings of SharePoint Central Administration, make sure that “Scan documents on upload” is enabled.
* In “Antivirus” settings of SharePoint Central Administration, make sure that “Scan documents on download” is enabled.
 |

|  |  |
| --- | --- |
| **Display name** | Realtime Scanning Processes State Monitor |
| **Description** | Checks if the Realtime scanning processes are running normally. |
| **Alert message** | There are Realtime scanning processes that did not restart properly. |
| **Causes** | It could be that the server was overloaded and could not start a new process in a timely fashion. |
| **Resolution** | Recycle w3wp services |

## Scheduled scan monitors

These are the monitors that keep track of potential problems with the scheduled scan.

|  |  |
| --- | --- |
| **Display name** |  Scheduled Scan Filter Engine Loading Monitor |
| **Description** | Checks if the filter engine is loaded correctly by the Scheduled and On-Demand scan jobs.  |
| **Alert message** | The filter engine is not loaded successfully for the Scheduled or On-Demand scan job. |
| **Causes** | Damaged or inaccessible filter engine. |
| **Resolution** | Uninstall and then reinstall FPSP. |

|  |  |
| --- | --- |
| **Display name** |  Scheduled Scan Loading Monitor |
| **Description** | Checks if the Scheduled and On-Demand scan jobs have been loaded successfully. |
| **Alert message** | The Scheduled or On-Demand scan job did not load successfully. |
| **Causes** | This may occur when FPSP is unable to access the SharePoint database because:****** The SharePoint database is offline.****** The SharePoint access account that was entered during the SharePoint installation has expired or the password has been updated. |
| **Resolution** | ****** Ensure that the SharePoint database is online. ****** Update the "Log on as" account for the "Microsoft Forefront Server Security Controller for SharePoint" service.  |

|  |  |
| --- | --- |
| **Display name** | Scheduled Scan Termination Monitor |
| **Description** | Checks if the Scheduled and On-Demand scans ended successfully.  |
| **Alert message** | The Scheduled or On-Demand scan failed to complete. |
| **Causes** | This may occur when FPSP is unable to access the SharePoint database because:****** The SharePoint database is offline.****** The SharePoint access account that was entered during the SharePoint installation has expired or the password has been updated. |
| **Resolution** | ****** Ensure that the SharePoint database is online. ****** Update the "Log on as" account for the "Microsoft Forefront Server Security Controller for SharePoint" service.  |

|  |  |
| --- | --- |
| **Display name** | Scheduled Scan Engines Initialization Monitor |
| **Description** | Checks if the antimalware engines selected for the Scheduled and On-Demand scan jobs have been initialized successfully. |
| **Alert message** | No antimalware scan engines have initialized successfully for the Scheduled or On-Demand scan job. |
| **Causes** | It could be that the engine subfolder has been deleted. |
| **Resolution** | ****** Ensure that the HTTP proxy server is configured properly. ****** Ensure that there are no network issues. ****** Ensure that the UNC configuration settings are appropriate. |

# Working with rules

There are two rules in the FPSP Management Pack that collect performance statistics data from managed FPSP servers. All rules are stored in the Authoring space of the Microsoft System Center Operations Manager 2007 Operations Console, in the Management Packs Objects node.

These are the rules for FPSP. For the properties of each rule, see OpsMgr rules reference for FSSP.

 Realtime Scan Performance. Reports the number of documents scanned, per second, by the FPSP realtime scan.

 Scheduled Scan Performance. Reports the number of documents scanned, per second, by the FPSP scheduled scan.

## Rules reference

These are the specifications for each of the rules for Microsoft Forefront Protection 2010 for SharePoint (FPSP).

| **Category** | **Value** |
| --- | --- |
| Type | FPSP Realtime Scan Job |
| Name | Realtime Scan Performance |
| Description | Number of documents scanned per second by the FPSP Realtime scan. |
| Rule category | PerformanceCollection |
| Rule target | FPSP Realtime Scan Job |
| Enabled | False |
| Data source object | Forefront SharePoint Realtime Scanner |
| Data source counter | Files Scanned/sec |
| Data source instance | \_CumulativeTotal |
| Interval | 15 minutes |
| Condition | None |
| Operates on | All objects of type: FPSP Realtime scan job |
| Response 1 | Performance data collection write action |
| Response 2 | Performance data publisher |

| **Category** | **Value** |
| --- | --- |
| Type | FPSP Scheduled Scan Job |
| Name | Scheduled Scan Performance |
| Description | Number of documents scanned per second by the FPSP scheduled scan. |
| Rule category | PerformanceCollection |
| Rule target | FPSP Scheduled Scan Job |
| Enabled | False |
| Data source object | Forefront SharePoint Scheduled Scanner |
| Data source counter | Files scanned/sec |
| Data source instance | \_CumulativeTotal |
| Interval | 15 minutes |
| Condition | None |
| Operates on | All objects of type: FPSP scheduled scan job |
| Response 1 | Performance data collection write action |
| Response 2 | Performance data publisher |

# Working with views

The FPSP Management Pack for Operations Manager 2007 provides a set of views that are accessible through the Monitoring space of the Operations Manager 2007 Operations Console. Views filter and organize the alert, task status, state, and performance data received from Operations Manager 2007 agents into a relational hierarchy.

There are both common views (views common to all Forefront products) and views for FPSP. For more information about the hierarchy, see "About the folder structure" in [Installing the management pack](#z2).

There are several view types, each displaying a different aspect of monitoring data and each with a different icon. Views include:

 Alert View

Displays alerts that meet your specific criteria, such as alert severity, resolution state, or alerts that are assigned to you.

 State View

Displays relationships between features, computers, and computer groups.

 Performance View

Customizes how you want to view performance data collected from performance objects and counters. This includes the ability to view historical and current operational data together.

 Task Status View

Displays tasks that meet criteria specified in the properties, such as only those tasks that apply to certain object types.

 Web Page View

Displays a Web page in a separate window in the Operations Console.

 Dashboard View

Allows you to arrange and view any data that Operations Manager 2007 is gathering, such as designing a view that shows two different view types side by side in one window.

## Views reference

This is a reference to each of the FPSP views included in the FPSP Management Pack for Operations Manager 2007. Note that only the lowest level folders view monitored items. For more information about the views hierarchy, see "About the folder structure" in [Installing the management pack](#z2).

## Common views

These are the views not specific to servers running a particular Forefront product. They contain summaries of all the Forefront Protection Suite (FPS) managed servers.

All of these views are contained within the structure of the top level folder called Microsoft Forefront Server Protection 2010 (Microsoft.ForefrontServer.Library.Folder).

| **View** | **Purpose** | **View Type** | **Path** |
| --- | --- | --- | --- |
| Microsoft Forefront Server Protection 2010 | Contains views of data for all managed FPS servers. | Not applicable | Microsoft Forefront Server Protection 2010 |
| Alerts | Displays alerts from all managed servers. These are the alerts generated by alert rules, which normally only show failures (because you would not choose to be alerted to the success of an update process). If an alert applies to any FPS product, it only appears in this section. If an alert applies to a specific Forefront product (for example, Microsoft Forefront Protection 2010 for SharePoint), it appears both here and in the specific section for that product (for example, Forefront Protection for SharePoint \ Alerts). | Alert | Microsoft Forefront Server Protection 2010 \ Alerts |
| Task Status | Displays the status of running or completed tasks on all managed servers. If the status applies to a task on any FPS product, it only appears in this section. If the status applies to a task for a specific Forefront product (for example, Microsoft Forefront Protection 2010 for SharePoint), it appears both here and in the specific section (for example, Forefront Protection for SharePoint \ Task Status). | Task Status | Microsoft Forefront Server Protection 2010 \ Task Status |
| Common | Contains views relating to engines and licenses on all managed FPS systems. | Not applicable | Microsoft Forefront Server Protection 2010 \ Common |
| Engines | Contains views relating to the status of engine updates and the state of the engines on all managed FPS systems. | Not applicable | Microsoft Forefront Server Protection 2010 \ Common \ Engines |
| Engine Update Alerts | Displays alerts generated when there are problems in updating engines, including warnings about engines being out of date. | Alert | Microsoft Forefront Server Protection 2010 \ Common \ Engines \ Engine Update Alerts |
| Engine Update State | Displays the state (health) of all enabled engines on all managed servers.  | State | Microsoft Forefront Server Protection 2010 \ Common \ Engines \ Engine State |
| License | Contains alerts about license expiration and the status of licenses on all managed FPS systems. | Not Applicable | Microsoft Forefront Server Protection 2010 \ Common \ License |
| License Alerts | Displays alerts associated with the licenses on all managed servers. | Alert | Microsoft Forefront Server Protection 2010 \ Common \ License \ License Alerts |
| License State | Displays the state of all licenses on all managed servers. This shows you whether a license is close to expiring or has already expired. | State | Microsoft Forefront Server Protection 2010 \ Common \ License \ License State |

## Forefront Protection 2010 for SharePoint views

These are the views that are specific to servers running FPSP.

All of these views are contained within the structure of the folder called Forefront Protection for SharePoint (Microsoft.ForefrontServer.FPSP.Folder). The data is rolled up into the Microsoft Forefront Server Protection 2010 parent folder.

| **View** | **Purpose** | **View Type** | **Path** |
| --- | --- | --- | --- |
| Forefront Protection for SharePoint | Contains views of data for all managed FPSP servers. | Not applicable | Microsoft Forefront Server Protection 2010 \ Forefront Protection for SharePoint |
| Alerts | Displays alerts (active or resolved) for each managed FPSP server. | Alert | Microsoft Forefront Server Protection 2010 \ Forefront Protection for SharePoint \ Alerts |
| State | Displays the state (health) of services, jobs, engines, and licensing for each managed FPSP server. By observing the red (unhealthy), yellow (warning), and green (healthy) icons you can instantly determine if any of your servers have problems. | State | Microsoft Forefront Server Protection 2010 \ Forefront Protection for SharePoint \ State |
| Task Status | Displays the status of running or completed tasks on each managed FPSP server. | Task Status | Microsoft Forefront Server Protection 2010 \ Forefront Protection for SharePoint \ Task Status |
| Scan Job Performance | Contains the performance counters for all managed FPSP systems, presented as graphed output. The scan rate for the jobs is shown, as is scan job failure and scan job status. | Not applicable | Microsoft Forefront Server Protection 2010 \ Forefront Protection for SharePoint \ Scan Job Performance |
| Realtime Scan Performance | Displays the realtime scan performance counters for each managed FPSP server. | Performance | Microsoft Forefront Server Protection 2010 \ Forefront Protection for SharePoint \ Scan Job Performance \ Realtime Scan Performance |
| Scheduled Scan Performance | Displays the scheduled scan performance counters for each managed FPSP server. | Performance | Microsoft Forefront Server Protection 2010 \ Forefront Protection for SharePoint \ Scan Job Performance \ Scheduled Scan Performance |

# Working with tasks

Tasks provide centralized control over some basic administrative processes that may be required to troubleshoot or correct problems with Forefront Protection 2010 for SharePoint (FPSP). These are problems that are identified through the Microsoft System Center Operations Manager 2007 (Operations Manager 2007) Operations Console.

The tasks are all optional. All tasks are stored in the Authoring space of the Operations Manager 2007 Operations Console, in the Management Packs Objects node.

You can run them manually for a selected agent-managed system; Operations Manager 2007 does not run them automatically. When you start a task from the Operations Manager 2007 Operations Console, it is scheduled to run on the agent-managed system. For information about running a task, see Running a task.

Note:

Operations Manager 2007 runs a single task at a time.

These are the tasks that you can run on agent-managed systems:

 Get Engine Versions—Retrieves the current engine versions of all scan engines on selected agent-managed systems. All the data for all the engines (not only version information) is returned.

 Restart FPSP Services—Restarts all FPSP services on selected agent-managed systems.

Note:

In some environments, services might not restart with this task. This could happen if the task takes over five minutes to stop and restart all of the services.

 Update FPSP Engines—Updates scan engines immediately on selected agent-managed systems.

Note:

This task causes the FPSP server to start updating engines. The task is considered successful if it triggers the update job. However, if this task is successful, it does not mean that the updates themselves were successful. To find out if the engines have been updated successfully, run the Get Engine Versions task and look at the UpdateStatus field for each engine in the Task Output section of the Task Status dialog box. If you closed the dialog box, the same information is available in the Monitoring space, in the Forefront Protection for SharePoint / Task Status view. Select the most recent Get Engine Versions task in the Task Status pane and look at the UpdateStatus field for each engine in the Details pane.

## Running a task

This is the procedure for running a task.

To run a task

|  |
| --- |
| 1. Select the Monitoring space on the Operations Manager 2007 Operations Console.2. Select the Forefront Protection for SharePoint / State view.3. In the State pane, select the servers on which to run the task. 4. In the Actions pane, the available tasks appear in the FPSP Server Tasks section. Click a task in order to run it.5. In the Run Task dialog box you can do any of the following: Clear one or more of the target servers.  Override the number of seconds until the task times out. Click Override, and in the Override Task Parameters dialog box, enter a different value in the New Value field. Then click Override. The default is 900 seconds (15 minutes). Change the credentials in the Task credentials section. The default is Use the predefined Run As Account, but you can select Other and enter a different User name, Password, and Domain. Choose to not see the Run Task dialog box again by checking Don't prompt when running this task in the future. To see the dialog box again, right-click the task in the Actions pane, and click **Run Task** on the options menu.6. Run the task by clicking Run. |

When the task begins, a Task Status dialog box is displayed. It shows you that the task is running and whether it completed successfully. The top of the dialog box lists the Task being run, its Status, and the Target server. The Task Output section of the dialog box shows the results. This dialog box does not need to remain open in order for the task to run. If you close the Task Status dialog box, you can check the results at any time in the Monitoring space, in the Forefront Protection for SharePoint / Task Status view. Select the task in the Task Status pane and look at the results in the Details pane.

# Objects the FPSP Management Pack discovers

When Operations Manager 2007 knows about an object type (such as the type of Forefront server), it must determine which computers actually have objects of these types. This process is called discovery. When Operations Manager 2007 discovers an object, the management pack begins monitoring it. In addition, Operations Manager 2007 discovers relationships between objects.

There are several classes that Operations Manager 2007 can discover. These include:

 Forefront Protection 2010 for SharePoint registry key

 Types of scan jobs

 Engines

 FPSP services

Note:

The Microsoft Forefront Server Protection Management Pack uses PowerShell scripts for product discoveries and tasks. If FPSP is installed on a managed server, the PowerShell Execution Policy Level must be set to "RemoteSigned." There is a timed rule ("Execution Policy Checker") in the management pack that checks and sets the Execution Policy on FPSP servers every 10 minutes. You can disable this rule by overriding it. If you change the Execution Policy Level to a higher level (AllSigned or Restricted), management pack product discoveries and tasks will not work.

 All of the objects in the FPSP Management Pack are automatically discovered. For information about discovering objects, see the "[Object Discoveries in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=108505)" topic in Operations Manager 2007 help (<http://go.microsoft.com/fwlink/?LinkId=108505>).

# Classes

The following diagram shows the classes defined in this management pack:



# Class discoveries

These are the classes that are discovered:

 Product discovery—Discovers whether FPSP is installed on a server.

 The management pack discovers servers running FPSP. Only the 2010 version is monitored by the management pack. The management pack checks whether the FPSP PowerShell snap-in is loaded. If so, the management pack checks whether FPSP is the 2010 version by running the PowerShell cmdlet Get-FsspProductInfo.

 Services discoveries—FPSP services are discovered if they are installed.

 The Microsoft Forefront Server Protection Controller for SharePoint Service (FSSPController) is installed on an FPSP server.

 The Microsoft Forefront Server Protection Controller Service (FSCController) is installed on an FPSP server.

 The Microsoft Forefront Server Protection Eventing Service (FSCEventing) is installed on an FPSP server.

 The Microsoft Forefront Server Protection Mail Pickup Service (FSEMailPickup) is installed on an FPSP server.

 Auto discovered classes—Discovers data about engines and licensing on an FPSP server.

 All installed engines.

 FPSP licensing.

For more information about class discovery, see "About class discovery" in Monitoring with Microsoft System Center Operations Manager 2007.

# How health rolls up

The following diagram shows how the health states of components roll up in this management pack.



# Key monitoring scenarios

The FPSP Management Pack for Operations Manager 2007 proactively monitors the "health" of your Forefront agent-managed systems by looking at events. Events are logged when transitions occur from one state to another. Health is indicated by a color code:

 Green (healthy) – everything is functioning properly and performing well. Green events do not trigger alerts. The symbol is a green check mark within a circle.

 Yellow (warning) – performance is poor or a problem is impairing non-critical functionality. Yellow events trigger warning alerts. The symbol is a "!" within a yellow triangle.

 Red (unhealthy) – critical functionality has been lost. Red events trigger error alerts. The symbol is a white "x" within a red circle.

## Problem types

These are the various problem types that the FPSP Management Pack tracks. For more information about monitored events, see [Monitor reference](#_Monitor_reference).

### Engines

These are the monitored engine conditions.

| **Monitored Event** | **Success (green)** | **Warning (yellow)** | **Error (red)** |
| --- | --- | --- | --- |
| Antimalware Engines Update Enabled | The engines selected to be used for the scan jobs are enabled for updating.  | The engines selected to be used for the scan jobs are not all enabled for updating. | Not applicable. |
| Antimalware Engines Update Success Rate | All engines enabled for updating were successfully updated. | At least half of the engines enabled for updating were successfully updated. | Less than half of the engines enabled for updating were successfully updated. |
| Antimalware Engines Last Update Time | All engines enabled for updating were successfully updated within the last five days. | Some of the engines enabled for updating were not updated within the last five days. | None of the engines enabled for updating were updated within the last five days. |

### SharePoint hook

These are the monitored SharePoint hook conditions.

| **Monitored Event** | **Success (green)** | **Warning (yellow)** | **Error (red)** |
| --- | --- | --- | --- |
| SharePoint hook state | The w3wp service is running and the Forefront VSAPI library is registered. | Not applicable. | The agent failed to register or is not enabled. |

### Scan Jobs

These are the monitored scan job conditions. There are separate events for realtime and scheduled scans.

| **Monitored Event** | **Success (green)** | **Warning (yellow)** | **Error (red)** |
| --- | --- | --- | --- |
| Realtime scan job enabled | The Realtime scan job is enabled. | The Realtime scan job is not scanning all files. | The Realtime scan job is disabled. |
| Realtime scan process state | The scanning processes are running. | Some processes did not restart after a timeout or exception. | No scanning processes restarted after a timeout or exception. |
| Scan filter engine loaded (for realtime and scheduled scans) | The engine that handles filtering loaded correctly. | Not applicable. | The engine that handles filtering did not load correctly. |
| Scheduled or on-demand scan loaded | The scheduled scan or the on-demand scan loaded correctly. | Not applicable. | The scheduled scan or the on-demand scan did not load correctly. |
| Scheduled or on-demand scan termination | The scheduled scan or the on-demand scan executed within the allowed time. | Not applicable. | The scheduled scan or the on-demand scan exceeded the allowed time limit. |
| Realtime scan engines have been initialized | The engines selected for the realtime scan have been initialized. | Not applicable. | The selected scanning engines were not initialized when the realtime scan was enabled. |
| Scheduled scan engines have been initialized | The engines selected for the scheduled scan have been initialized. | Not applicable. | The selected scanning engines were not initialized when the scheduled scan was enabled. |

### Services

These are the monitored services conditions.

| **Monitored Event** | **Success (green)** | **Warning (yellow)** | **Error (red)** |
| --- | --- | --- | --- |
| FSCController service | The FSCController service is running. | Not applicable. | The FSCController service has stopped. |
| Eventing service | The Eventing service is running. | Not applicable. | The Eventing service has stopped. |
| FSEMailPickup service | The FSEMailPickup service is running. | Not applicable. | The FSEMailPickup service has stopped. |
| FSSPController service | The FSSPController service is running. | Not applicable. | The FSSPController service has stopped. |

### License

These are the monitored license conditions.

| **Monitored Event** | **Success (green)** | **Warning (yellow)** | **Error (red)** |
| --- | --- | --- | --- |
| License state | The Forefront Protection 2010 for SharePoint is license. | The Forefront Protection 2010 for SharePoint license will expire soon.  | The Forefront Protection 2010 for SharePoint license has expired. |

# Viewing information in the Operations Manager Console

Alerts of all monitors in the FPSP Management Pack are located in the **Alerts** node under **Microsoft Forefront Server Protection 2010**. Task Status, State information, and Scan Job Performance data are also located under this folder. A folder also contains common views. Common components, such as engine and license health, can be viewed in a single view for both products.

# Placing monitored objects in maintenance mode

When a monitored object, such as a computer or distributed application, goes offline for maintenance, Operations Manager 2007 detects that no agent heartbeat is being received and may generate many alerts and notifications. To prevent alerts and notifications from being generated, place the monitored object into maintenance mode. In maintenance mode, alerts, notifications, rules, monitors, automatic responses, state changes, and new alerts are suppressed at the agent.

For general instructions on placing a monitored object in maintenance mode, see [How to Put a Monitored Object into Maintenance Mode in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=108358) (<http://go.microsoft.com/fwlink/?LinkId=108358>).

# Troubleshooting

1. No FPSP servers discovered after management packs are imported.

Make sure that:

1. The Operations Manager 2007 agent has been deployed to FPSP servers.
2. The FPSP version on managed server is 2010.
3. The Powershell Execution Policy level on the managed FPSP server is set at least to “RemoteSigned.”
4. Tuning the performance of FPSP server discovery.

The FPSP Management Pack discovers FPSP servers every 4 hours. You can choose to override the frequency and set a shorter time interval if you need the management pack to have a quicker response to changes of FPSP servers, or you can configure a longer frequency to decrease the performance impact to FPSP and SharePoint.

# Appendix: Monitors and overrides for management packs

This section provides detailed procedures and scripts that allow you to display rules and other information about the management packs you import.

# How to view management pack details

For more information about a monitor and the associated override values, see the knowledge for the monitor.

To view knowledge for a monitor

|  |
| --- |
| 1. In the Operations Console, click the Authoring button.2. Expand Management Pack Objects, and then click Monitors.3. In the Monitors pane, expand the targets until you reach the monitor level. Alternatively, you can use the Search box to find a particular monitor.4. Click the monitor, and in the Monitors pane, click View knowledge.5. Click the Product Knowledge tab. |

# How to display monitors for a management pack

To use the Forefront Management Shell to display a list of outputs for a management pack's monitors and overrides, use the following procedure.

To display monitors for a management pack

|  |
| --- |
| 1. In the command shell, type the following command:a. get-monitor -managementPack name.mp | export-csv filename2. A .csv file is created. The .csv file can be opened in Microsoft Excel.. noteDSDOC112778PADS  |

In Excel, you may be required to specify that the .csv file is a text file. For example, the command below retrieves data for the monitors associated with one of the core management packs:

get-monitor -managementPack System.Health.Library.mp | export-csv "C:\monitors.csv"

# How to display overrides for a management pack

To display overrides for a management pack use the following procedure.

To display overrides for a management pack

|  |
| --- |
| 1. In the command shell, type the following command:get-override -managementPack name.mp | export-csv filename2. A .csv file is created. The .csv file can be opened in Excel. |

In Excel, you may be required to specify that the .csv file is a text file. For example, this command displays the overrides for one of the core management packs:

get-override -managementPack Microsoft.SystemCenter.OperationsManager.Internal.mp | export-csv "c:\overrides.csv"

# How to display all management pack rules

Use the following procedure to display a list of rules for the management packs that you imported. The list of rules can be viewed in Excel.

To display management pack rules

|  |
| --- |
| 1. In your management server, click Programs, and then click System Center.2. Click Command Shell.3. In the command shell window, type the following command: get-rule | select-object @{Name="MP";Expression={ foreach-object {$\_.GetManagementPack().DisplayName }}},DisplayName | sort-object -property MP | export-csv "c:\rules.csv"4. A .csv file is created. The .csv file can be opened in Excel.. noteDSDOC112778PADSIn Excel, you may be required to specify that the .csv file is a text file. |

# How to display monitor thresholds

To display monitor thresholds, use the script described in this section. This script works for the majority of monitors. It creates a .csv file with the following columns and can be viewed using Excel:

| **Column** | **Description** |
| --- | --- |
| Type | The type of objects to which the monitor is targeted |
| DisplayName | The display name of the monitor |
| Threshold | The threshold used by the monitor |
| AlertOnState | Determines if the monitor generates an alert when the state changes |
| AutoResolveAlert | Determines if the generated alert will be automatically resolved when the monitor state goes back to green |
| AlertSeverity | The severity of the generated alert |

Run the following script to create the .csv file that displays the monitor thresholds:

function GetThreshold ([String] $configuration)

{

$config = [xml] ("<config>" + $configuration + "</config>")

$threshold = $config.Config.Threshold

if($threshold -eq $null)

{

$threshold = $config.Config.MemoryThreshold

}

if($threshold -eq $null)

{

$threshold = $config.Config.CPUPercentageThreshold

}

if($threshold -eq $null)

{

if($config.Config.Threshold1 -ne $null -and $config.Config.Threshold2 -ne $null)

{

$threshold = "first threshold is: " + $config.Config.Threshold1 + " second threshold is: " + $config.Config.Threshold2

}

}

if($threshold -eq $null)

{

if($config.Config.ThresholdWarnSec -ne $null -and $config.Config.ThresholdErrorSec -ne $null)

{

 $threshold = "warning threshold is: " + $config.Config.ThresholdWarnSec + " error threshold is: " + $config.Config.ThresholdErrorSec

}

}

if($threshold -eq $null)

{

if($config.Config.LearningAndBaseliningSettings -ne $null)

{

$threshold = "no threshold (baseline monitor)"

}

}

return $threshold

}

$perfMonitors = get-monitor -Criteria:"IsUnitMonitor=1 and Category='PerformanceHealth'"

$perfMonitors | select-object @{name="Target";expression={foreach-object {(Get-MonitoringClass -Id:$\_.Target.Id).DisplayName}}},DisplayName, @{name="Threshold";expression={foreach-object {GetThreshold $\_.Configuration}}}, @{name="AlertOnState";expression={foreach-object {$\_.AlertSettings.AlertOnState}}}, @{name="AutoResolveAlert";expression={foreach-object {$\_.AlertSettings.AutoResolve}}}, @{name="AlertSeverity";expression={foreach-object {$\_.AlertSettings.AlertSeverity}}} | sort Target, DisplayName | export-csv "c:\monitor\_thresholds.csv"

# How to display performance collection rules

To display performance collection rules, use the script in this section. This script works for the majority of monitors. It creates a .csv file with the following columns and can be viewed using Excel.

| **Column** | **Description** |
| --- | --- |
| WriteAction | Contains information about where the performance counter is written |
| WriteToDB or CollectionPerformanceData | Writes to the Operations Manager database |
| WriteToDW or CollectPerfDataWarehouse | Writes to the data warehouse |
| WC | Stores baseline data for a performance counter into the operational database |

 To display the performance collection rules present in the management group, run the following script:

function GetPerfCounterName ([String] $configuration)

{

$config = [xml] ("<config>" + $configuration + "</config>")

return ($config.Config.ObjectName + "\" + $config.Config.CounterName)

}

function GetFrequency ([String] $configuration)

{

$config = [xml] ("<config>" + $configuration + "</config>")

$frequency = $config.Config.Frequency;

if($frequency -eq $null)

{

$frequency = $config.Config.IntervalSeconds;

}

return ($frequency)

}

function GetDisplayName($performanceRule)

{

 if($performanceRule.DisplayName -eq $null)

 {

 return ($performanceRule.Name);

 }

 else

 {

 return ($performanceRule.DisplayName);

 }

}

function GetWriteActionNames($performanceRule)

{

 $writeActions = "";

 foreach($writeAction in $performanceRule.WriteActionCollection)

 {

 $writeActions += " " + $writeAction.Name;

 }

 return ($writeActions);

}

$perf\_collection\_rules = get-rule -criteria:"Category='PerformanceCollection'"

$perf\_collection\_rules | select-object @{name="Type";expression={foreach-object {(Get-MonitoringClass -id:$\_.Target.Id).DisplayName}}},@{name="RuleDisplayName";expression={foreach-object {GetDisplayName $\_}}} ,@{name="CounterName";expression={foreach-object {GetPerfCounterName $\_.DataSourceCollection[0].Configuration}}},@{name="Frequency";expression={foreach-object {GetFrequency $\_.DataSourceCollection[0].Configuration}}},@{name="WriteActions";expression={foreach-object {GetWriteActionNames $\_}}} | sort Type,RuleDisplayName,CounterName | export-csv "c:\perf\_collection\_rules.csv"