**Microsoft System Center 2016 and above**

Guide for Microsoft System Center 2016 and above Management Pack for Windows Defender

Microsoft Corporation

Published: September 2021

Send feedback or suggestions about this document to systemcenterfeedback@microsoft.com. Please include the management pack guide name with your feedback.

The Operations Manager team encourages you to provide feedback on the monitoring pack by providing a review on the monitoring pack’s page in the [Management Pack Catalog](http://go.microsoft.com/fwlink/?LinkID=82105) .

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2013 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Bing, BizTalk, Forefront, Hyper-V, Internet Explorer, JScript, SharePoint, Silverlight, SQL Database, SQL Server, Visio, Visual Basic, Visual Studio, Win32, Windows, Windows Azure, Windows Intune, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

[Guide for Microsoft System Center 2016 and above Management Pack for Windows Defender 4](#_Toc81907190)

[Management Pack Purpose 5](#_Toc81907191)

[Monitoring Scenarios 5](#_Toc81907192)

[How Health Rolls Up 7](#_Toc81907193)

[Configuring the Management Pack for Windows Defender 7](#_Toc81907194)

[Appendix: Management Pack Contents 8](#_Toc81907195)

Guide for Microsoft System Center 2016 and above Management Pack for Windows Defender

This guide is based on the version 7.1.10128.1 of the Windows Defender Management Pack.

Guide History

|  |  |
| --- | --- |
| Release Date | Changes |
| September 2021 | MP have been verified for windows server 2016 and above operating systems and branded as version agnostic. |
| October 2016 | Re-release of guide with Windows Server 2016 RTM |
| December 2015 | Original release of this guide |

Supported Configurations

This management pack requires System Center Operations Manager 2016 and above

SCOM 2019 : [System requirements for System Center Operations Manager | Microsoft Docs](https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2019#microsoft-monitoring-agent-operating-system)

SCOM 2016 : [System requirements for System Center Operations Manager | Microsoft Docs](https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2016#software-requirements-for-operations-manager-components)

The following table details the supported configurations for the Management Pack for Windows Defender

|  |  |
| --- | --- |
| **Configuration** | **Support** |
| Windows Server 2016 and above | Yes |
| Windows Server Technical Preview | Yes |
| Windows 8.1/10 | Yes |
| Clustered servers | Not supported/not tested |
| Agentless monitoring | Not supported |
| Virtual environment | Not supported/not tested |

Management Pack Scope

This management pack supports as many agents running Windows Defender.

Prerequisites

The following requirements must be met to run this management pack:

* Installation of System Center Operations Manager and the Microsoft Windows Defender Management Pack

Files in this Management Pack

The Management Pack for Windows Defender includes the following files:

 Windows Defender Management Pack

Management Pack Purpose

In this section:

 [Monitoring Scenarios](#z5a9ff008734b4183946f840ae0464ab0)

 [How Health Rolls Up](#zb8b3e32eb8154a8da8b18b606568e65d)

For details on the discoveries, rules, monitors, views, and reports contained in this Management pack, see [Appendix: Management Pack Contents](#zf475f3cc57b84a049d89cda7b1f37ba8).

Monitoring Scenarios

The Windows Defender Management Pack monitors a few key components that are important to Windows Defender health.

|  |  |  |
| --- | --- | --- |
| Monitoring scenario | Description | Associated rules and monitors |
| Realtime Protection(RTPStatus) | This scenario checks to see if real-time protection is turned on. Realtime protection constantly monitors the agent for malicious activity | **** (non-alerting rule) Real-time protection on**** (Error alerting rule) Real-time protection off  |
| Antimalware Status (AMStatus) | This scenario checks to see if the antimalware service is running.  | **** (non-alerting rule) AM service is running**** (Error alerting rule) AM service is not running  |
| Antimalware Definitions Status (AntimalwareDefinitions) | This scenario will monitor the age of the antimalware definitions to see how up to date they are.  | **** (non-alerting rule) Antimalware definitions aren’t older than 3 days**** (warning alerting rule) Antimalware definitions are older than 3 days**** (critical alerting rule) Antimalware definitions are older than 7 days**Note:**Days are user configurable |
| Antimalware Scan Status(AntimalwareScan) | This scenario will monitor how long ago a scan occurred. This will monitor the age of both quick and full scans | **** (non-alerting rule) Quick scan has happened within 3 days**** (non-alerting rule) Full scan has happened within 7 days**** (warning alerting rule) Quick Scan hasn’t happened in more than 3 days**** (warning alerting rule) Full Scan hasn’t happened in more than 7 days**Note:**Days are user configurable |
| Malware Outbreak (OutbreakMonitor) | This scenario will monitor when Defender takes action on malware.  | **** (non-alerting rule) When there is no malware activity**** (warning alerting rule) When Defender detects and take action on malware. |
| Active Malware (ActiveMalware) | This scenario will monitor whether there is an active malware that requires additional user action.  | **** (non-alerting rule) When there is no malware activity**** (error alerting rule) When there is an active malware and it requires additional user action such as reboot, full scan, offline scan etc. |

How Health Rolls Up

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

Protected Endpoint

Malware Detection Monitor

Antimalware Scan Monitor

Antimalware Definitions Monitor

Active Malware Monitor

Real-time Protection Monitor

Antimalware Status Monitor

|  |  |
| --- | --- |
| Legend |  |
|  | Will service a critical alert |
|  | Can service critical or warning alert |
|  | Will only give a warning alert |

Configuring the Management Pack for Windows Defender

Add sections for additional configuration tasks, and let customers know whether a task is required or optional.

This section provides guidance on configuring and tuning this management pack.

 [Best Practice: Create a Management Pack for Customizations](#z2)

 [Security Configuration](#z3)

 [Tuning Performance Threshold Rules](#z4)

 [Using the &lt;name&gt; Template](#z5)

Best Practice: Create a Management Pack for Customizations

By default, Operations Manager saves all customizations such as overrides 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.

When you create a management pack for the purpose of storing customized settings for a sealed management pack, it is helpful to base the name of the new management pack on the name of the management pack that it is customizing.

Creating a new management pack for storing customizations of each sealed management pack makes it easier to export the customizations from a test environment to a production environment. It also makes it easier to delete a management pack, because you must delete any dependencies before you can delete a management pack. If customizations for all management packs are saved in the Default Management Pack and you need to delete a single management pack, you must first delete the Default Management Pack, which also deletes customizations to other management packs.

If you make a customized

Security Configuration

|  |  |  |
| --- | --- | --- |
| Run As Profile Name | Associated Rules and Monitors | Notes |
| Local System | All monitors |  |

Appendix: Management Pack Contents

Please find below separate sections based on the feature set of the Management Pack for Windows Defender.

When inventory is discovered, it is grouped into one of the following monitor groups.

|  |  |
| --- | --- |
| Monitor Group | Description |
| Protected Endpoint | Inventory will show up under this group if the endpoint **has** Windows Defender up and running and protected |
| Unprotected Endpoint | Inventory will show up under this group if the endpoint **does not have** Windows Defender up and running |
| Protected Candidate  | Inventory will show up under this group if the endpoint **has** Windows Defender up and running |