ForeScout

ForeScout CounterACT®

Windows Vulnerability DB

Configuration Guide

Updated February 2018

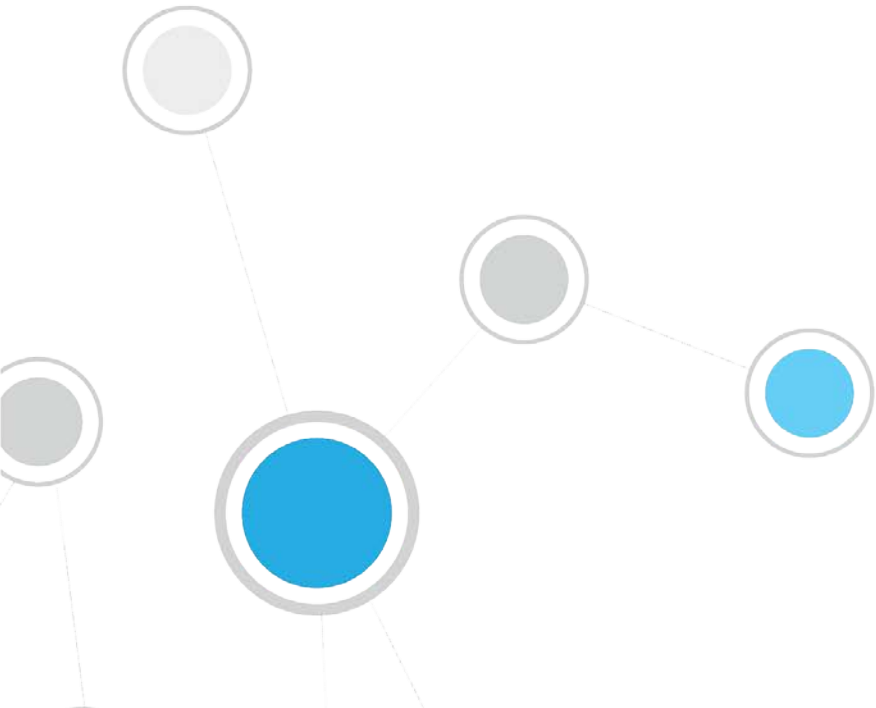
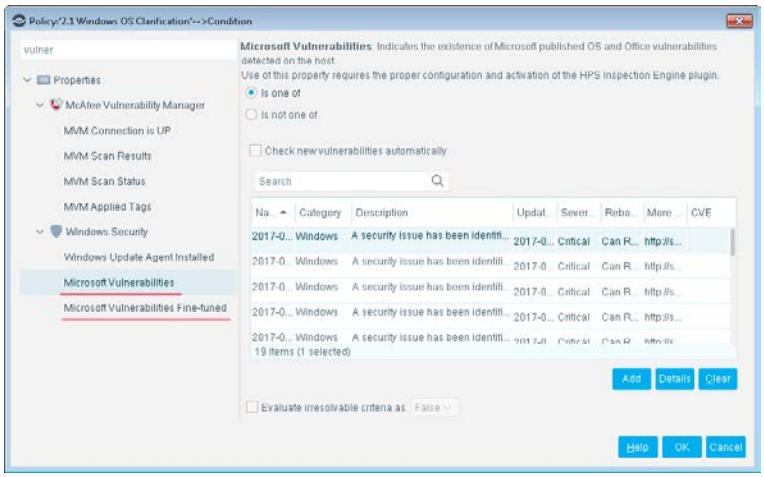


Table of Contents

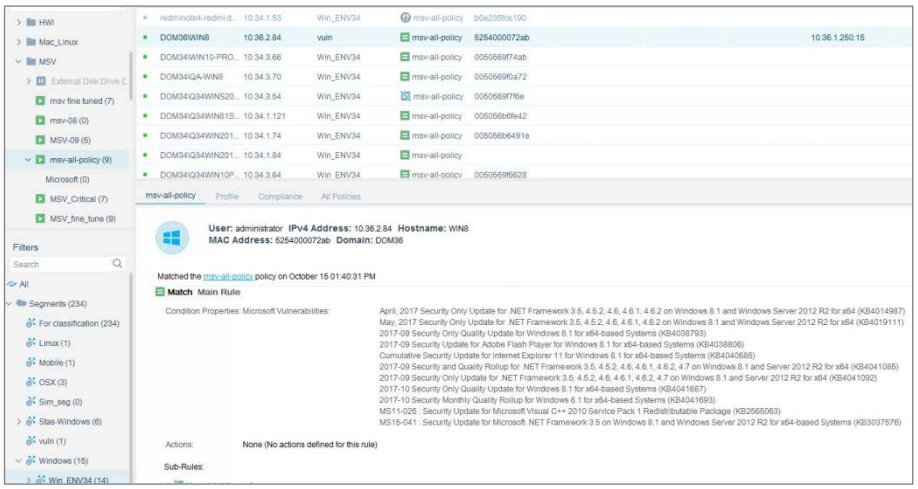
About the Windows Vulnerability DB Module

The Windows Vulnerability DB is a Content Module that delivers vulnerability updates to CounterACT soon after they are released from Microsoft. These updates are used when working with vulnerability policies.

The HPS Inspection Engine, installed on each Appliance, instructs endpoints to download the information from the Windows Vulnerability DB when the **Microsoft Vulnerabilities** or the **Microsoft Vulnerabilities fine-tuned** property is used. SecureConnector is not required to download or work with Windows Vulnerability DB information on endpoints.



Vulnerability detections appear in the Console Details pane when you select the policy used to detect vulnerabilities.



Module Requirements

The module requires CounterACT version 8.0.

Supported Windows Operating Systems and Other Products

The following Windows operating systems are supported on 32-bit and 64-bit machines.

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016

In addition, network server and productivity packages that are updated through the Windows Updates facility are supported.

Distributing Vulnerability Information to Windows Endpoints

There may be situations when it is more efficient for endpoints to retrieve vulnerability information from WSUS or Windows Updates, rather than use the information provided by the Windows Vulnerability DB.

It is recommended to continue using WSUS or Windows Update in the following situations:

- When a local WSUS instance is deployed in your network environment.
- When endpoints are connected to your network through a VPN and are physically located at a distance from the Appliance, it may be faster for the endpoint to retrieve vulnerability information directly from the Microsoft Updates website or a local WSUS.

When they are available, you may use other methods to distribute the Microsoft Vulnerability CAB file to endpoints in your environment.

The HPS Inspection Engine looks for the following file on Windows endpoints:

`%systemroot%\temp\wsusscn2.cab`

If this file is different than the CAB file provided by the Windows Vulnerability DB, CounterACT downloads its own CAB file to the endpoint.

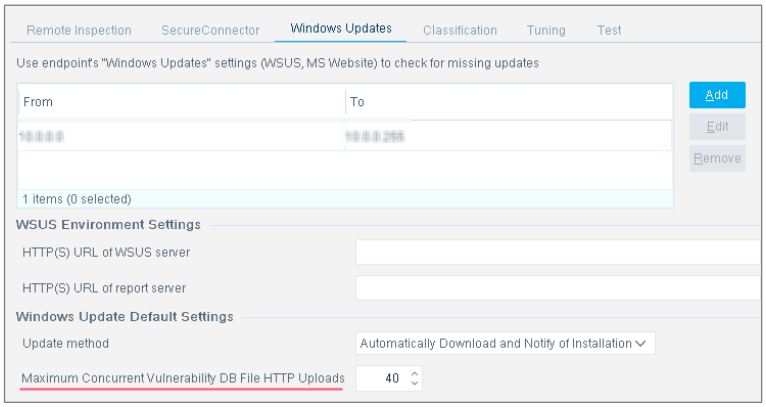
Refer to the HPS Inspection Engine Configuration Guide *for details of configuration to use WSUS or Windows Updates.*

Minimize Bandwidth During Vulnerability File Download

You can minimize bandwidth usage during Microsoft vulnerability file download processes by limiting the number of concurrent HTTP downloads to endpoints. The default is 20 endpoints simultaneously.

To customize:

1. Select **Tools>Options>HPS Inspection Engine>Windows Updates** tab.
2. Define a value in the **Maximum Concurrent Vulnerability DB File HTTP Uploads** field.



Using Vulnerability Information to Manage Endpoints

This section describes recommended best practices for detecting and remediating vulnerabilities on endpoints.

To work with vulnerability information:

1. Create a policy based on the Windows Updates Compliance policy template. This policy uses the Microsoft Vulnerabilities property to check Windows endpoints for vulnerabilities related to all Knowledge Base issues downloaded from Microsoft.
   - By default, the Check new vulnerabilities automatically option is enabled, so that the policy automatically checks for new vulnerabilities added when the Windows Vulnerability DB is updated.
   - The policy provides the Start Windows Update action to update endpoints that are missing patches for known vulnerabilities. By default, this action is disabled. It is recommended to enable this action.
2. Accept default scheduling/recheck behavior for the policy.

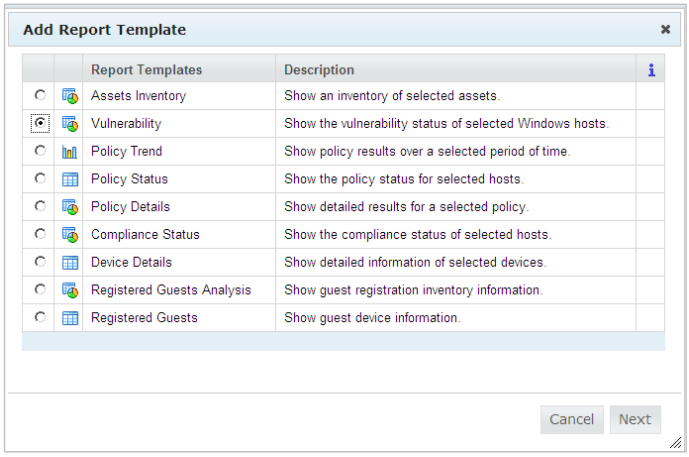
For more details, and for information on remediating vulnerabilities on Linux and MacOS/OS X endpoints, see the Control Network Vulnerabilities How-to Guide.

Vulnerability Reporting

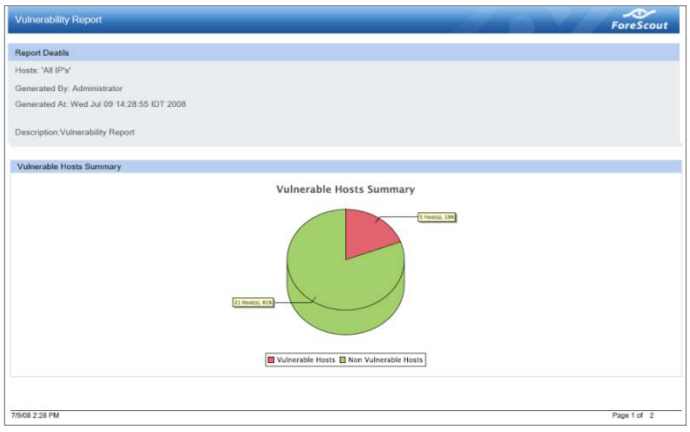
You can also generate reports that display the vulnerability status of selected Windows hosts. The report displays the number and percentage of hosts with vulnerabilities versus those that have no vulnerabilities, and lists the relevant hosts.

To create a report based on vulnerability information:

1. Select Reports by clicking on the ellipsis icon from the CounterACT toolbar.
2. The Reports portal opens.
3. Select **Add**. The Add Report template Wizard opens.
4. Select the Vulnerability Report template.



5. Follow the wizard instructions to create the report.



About Installation

After installation of the Windows Vulnerability DB Module, the HPS Inspection Engine is restarted.

Configuration

Sources and settings for Windows Updates are configured in the HPS Inspection Engine. For example, see Minimize Bandwidth During Vulnerability File Download. For more information about Windows Updates settings, see the *HPS Inspection Engine Configuration Guide*.

Changes that Impact Windows Endpoints

The plugin installs the following file(s) on endpoints.

Name	Description
fs_wua_search.vbs	Resolves *Microsoft Vulnerabilities* properties.

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

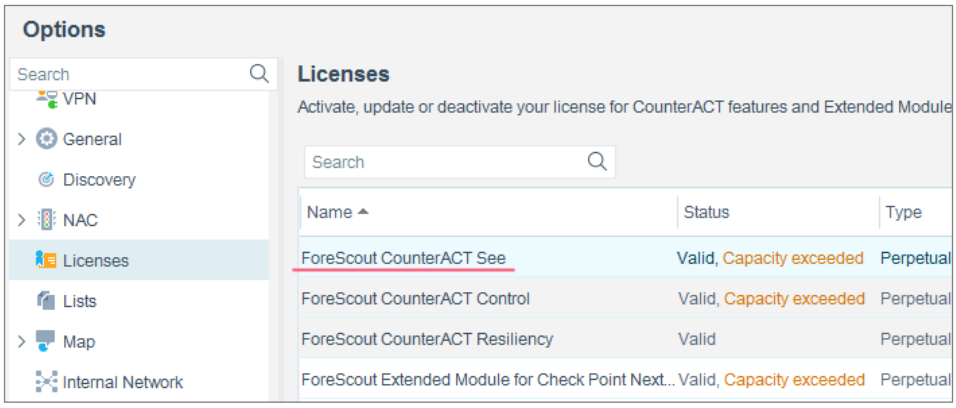
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21