FORESCOUT

Forescout

Windows Vulnerability DB

Configuration Guide

All Versions

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-12-14 12:19

Table of Contents

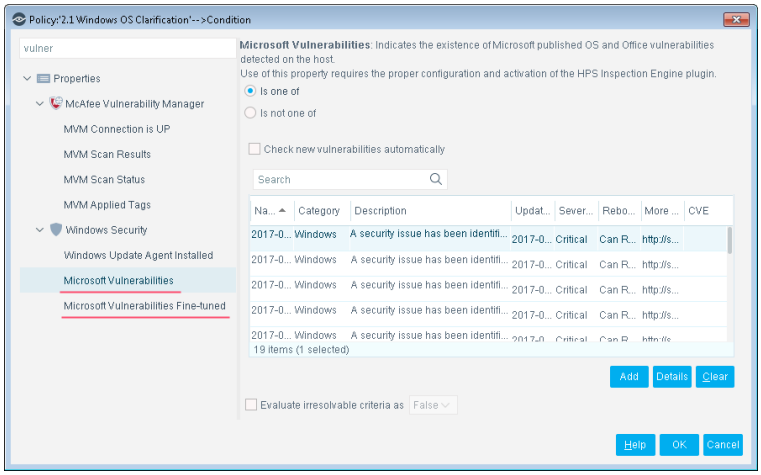
About the Windows Vulnerability DB Module

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

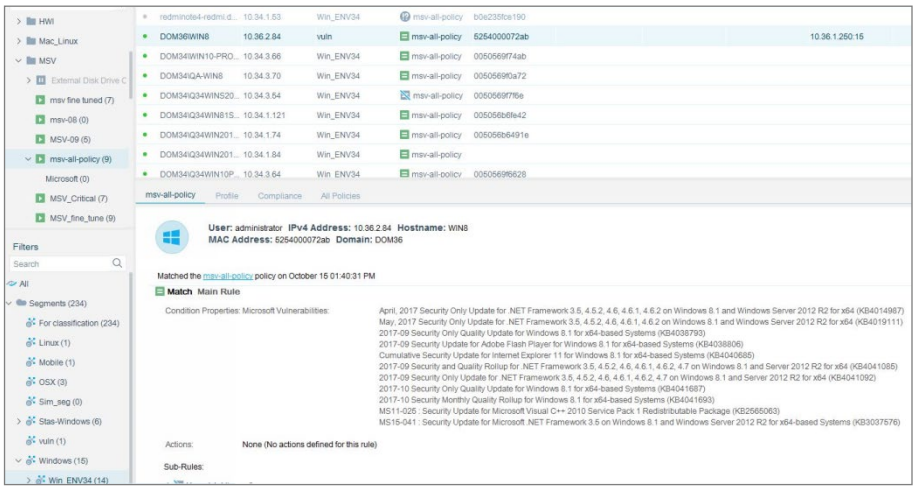
Sources and settings for Windows Updates are configured in the HPS Inspection Engine. For example, see Minimize Bandwidth During Vulnerability File Download. For more information about

See the *HPS Inspection Engine Configuration Guide* Windows Updates settings.

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.



Supported Windows Operating Systems and Other Products

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

Changes that Impact Windows Endpoints

- After installation of the Windows Vulnerability DB, the HPS Inspection Engine is restarted.
- The plugin installs the following file(s) on endpoints.

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

Windows Vulnerability DB Capabilities and Best Practices

This section describes best practices for working with the Windows Vulnerability DB content module and the Windows Update Compliance Template v2:

- Distributing Vulnerability Information to Windows Endpoints
- Minimize Bandwidth during Vulnerability File Download
- Using Vulnerability Information to Manage Endpoints
- Vulnerability Reporting

Distributing Vulnerability Information to Windows Endpoints

There are 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 from the CAB file provided by the Windows Vulnerability DB, the Forescout platform downloads its own CAB file to the endpoint.

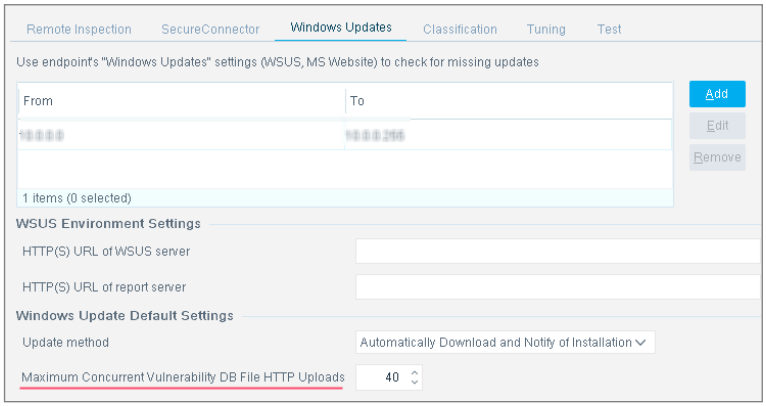
Refer to the Forescout Endpoint Module: HPS Inspection Engine Configuration Guide *for details of configuration to use WSUS or Windows Updates.*

Minimize Bandwidth during Vulnerability File Download

You can minimize bandwidth usage during Microsoft vulnerability file download 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. See Windows Update Compliance Template v2.
   - 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.

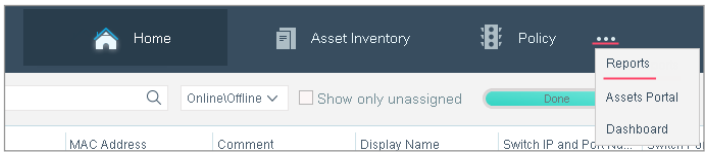
For more details, and for information on remediating vulnerabilities on MacOS/OS X endpoints, see the Control Network Vulnerabilities How-to Guide.

Vulnerability Reporting

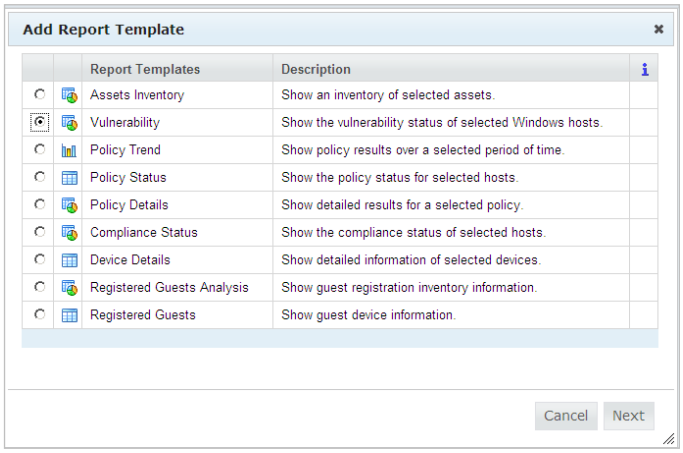
You can also generate reports that display the vulnerability status of selected Windows hosts. The report displays the number and percentage of hosts with vulnerabilities versus those that have no vulnerabilities and lists the relevant hosts.

To create a report based on vulnerability information:

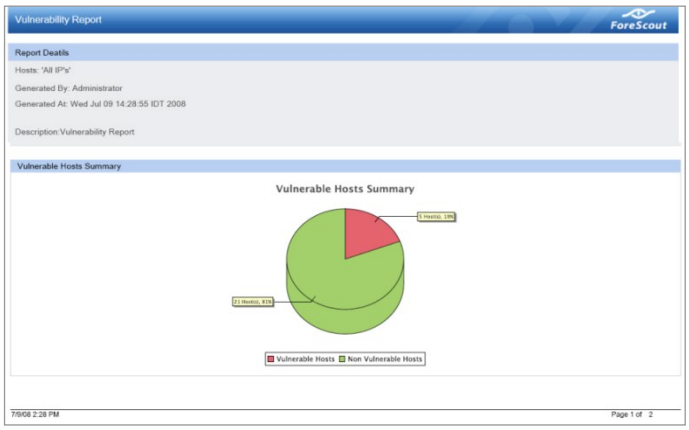
1. Select Web reports by clicking on the ellipsis icon from the Forescout platform toolbar.



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.



Windows Update Compliance Template v2

This topic describes how to use the Windows Update Compliance Template v2 and describes the main rules and sub-rules of the policy.

About Forescout Policy Templates

Forescout templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance.

Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.

The following template is available for detecting and managing endpoints:

- Windows Update Compliance Template v2

About the Windows Update Compliance Template v2

Use this policy to detect Windows endpoints that were not updated with the latest vulnerability patches published by Microsoft. The policy places endpoints in the *Windows Not Updated* group. In addition, you can use optional remediation actions (disabled by default) to:

- Install SecureConnector to manage Windows machines
- Allow endpoint users to remediate vulnerabilities from the desktop
- Allow automatic remediation of vulnerabilities

This template is a revised version of the original Windows Update Compliance Template provided with the HPS Inspection Engine. It is recommended to recreate existing policies using this newer version of the template.

This policy applies to Windows endpoints only.

How Endpoints Are Detected and Handled - Main Rule and Sub-rules

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are passed to sub-rules for detailed inspection and handling. *Endpoints that do not match the Main Rule are not inspected by sub-rules of the policy*.

Sub-rules are evaluated in the order in which they appear until an endpoint matches the condition of a rule. When a match is found, the corresponding action is applied to the endpoint. *Only* if the endpoint does not match the condition of the sub-rule, it is inspected by the next rule.

Typically, Main Rule and Sub-rules form an automated sequence that qualifies endpoints, and then applies different detection and handling scenarios.

The Windows Update Compliance Template v2 Main rule and Sub-rules

Main Rule

The main rule of this policy filters for Windows endpoints. Only Windows endpoints are passed on to evaluation by sub-rules.

Sub-Rules

The policy template provides the following sub-rules:

1. Not Corporate Hosts

   This rule matches endpoints that are not in the *Corporate Hosts* group. No action is applied. This rule matches non-corporate endpoints and excludes them from further policy evaluation.

   > *If your environment does not use Corporate/Guest user management features, disable this rule.*

2. Not Manageable

   This rule matches endpoints that are not manageable using Remote Inspection or SecureConnector. This prevents further evaluation of Windows vulnerabilities on the endpoint. Policy evaluation ends for these endpoints.

   The optional **Start SecureConnector** action installs SecureConnector, making the Windows machine manageable by the Forescout platform. This action is disabled by default.

3. Windows Updates Unavailable

   This rule matches endpoints that run versions of Windows for which updates are no longer published.

   The **Add to Group** action assigns these endpoints to the Windows Not Updated group.

   An optional **HTTP Notification** action redirects these endpoints to a web page with a customizable message. This action is disabled by default.

4. Waiting for Reboot

   This rule matches endpoints on which updates were successfully installed. The Forescout platform is now waiting for the endpoint to reboot to complete the update process. No action is applied.

5. Windows Updates Required (Custom)

   Use this rule to match endpoints that are exposed to one or more specific published vulnerabilities. In the rule condition, customize the selected items in the **Microsoft Vulnerabilities** property to detect endpoints with the vulnerabilities that interest you.

6. Windows Updates Required (Critical)

   Use this rule to match endpoints that are exposed to any published vulnerability whose Severity is *Critical*.

7. Windows Updates Required (Important)

Use this rule to match endpoints that are exposed to any published vulnerability whose Severity is *Important*.

8. Windows Updates Required (Low)

   Use this rule to match endpoints that are exposed to any published vulnerability whose Severity is *Low*.

Rules 5-8 apply the following actions to vulnerable endpoints:

The **Add to Group** action assigns endpoints with the specified vulnerabilities to the *Windows Not Updated* group.

The optional **Start Windows Updates** action to download vulnerability information to the endpoints. This action is disabled by default.

The optional **Windows Self Remediation** action sends the user links to the updates and patches that must be downloaded and installed to correct the discovered vulnerabilities. This action is disabled by default.

9. Compliant

Endpoints not matched by previous rules are assumed compliant with current Microsoft vulnerability updates. No actions are applied to matching endpoints.

Configure the Windows Update Compliance Template v2

This topic describes how to configure the Windows Update Compliance Template v2.

Prerequisites

- Detected endpoints must already be categorized by the Primary Classification policy.
- In environments that use Corporate/Guest user management features, a Corporate/Guest Control policy must identify corporate endpoints.
- For vulnerability detection and remediation, endpoints must be manageable using Remote Inspection or SecureConnector.

Configure the Template

This section describes how to use the template to create a policy.

Configure the template:

1. Log in to the Forescout Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Compliance** folder and select **Windows Update Compliance Template v2**.
4. Select **Next**. The Name pane opens.

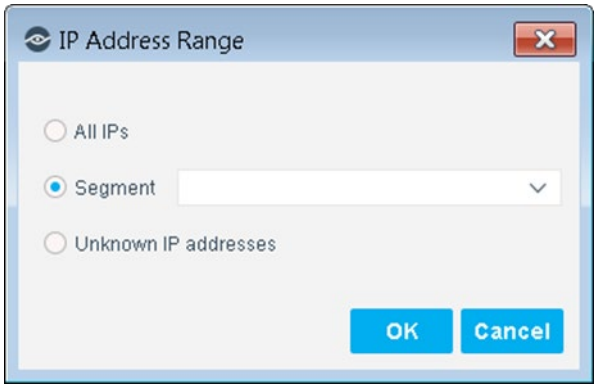
Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

1. Define a unique name for the policy you are creating based on this template and enter a description.
   - Use a name that clearly reflects what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a name that indicates what the policy verifies, and which actions will be taken.
   - Use a name that indicates whether the policy criteria must be met or not met.
   - Avoid names similar to existing policies.
2. Select **Next.** The Scope pane and IP Address Range dialog box opens.

Define Which Endpoints Will Be Inspected - Policy Scope

1. Use the IP Address Range dialog box to define which endpoints are inspected.



   The following options are available:
   - **All IPs**: Include all IP addresses in the Internal Network.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
2. Select **OK**. The added range appears in the Scope pane.
3. Select **Next**. The Sub-Rules pane opens.
4. Select **Finish** to create the policy.
5. On the Policy Manager, select **Apply** to save the policy.