

## Configuring Host Checker Third-Party Applications Using Predefined Rules (NSM Procedure)

Host Checker comes pre-equipped with a vast array of predefined rules that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. You can enable one or more of these rules within a Host Checker client-side policy to ensure that the integrated third-party applications that you specify are running on your users' computers in accordance with your specifications. For firewall and antivirus rules, you can specify remediation actions to automatically bring the endpoint into compliance.

To configure third-party applications using predefined rules:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure Host Checker third-party applications using predefined rules.
3. Click the **Configuration** tab and select **Authentication > Endpoint Security > Host Checker**. The corresponding workspace appears.
4. Create a new policy or click an existing policy in the Policies section of the page.
5. Click the tab that corresponds to the operating system for which you want to specify Host Checker options—**Windows**, **Mac**, **Linux**, **Solaris** and **Windows Mobile**. In the same policy, you can specify different Host Checker requirements for each operating system.
6. Add and modify settings as specified in Table 1 on page 1.
7. Specify the support products or vendors for a system scan check.
8. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 1: Configuring Host Checker Third-Party Applications Using Predefined Rules Details**

Option	Function	Your Action
<b>Predefined Antivirus Rules</b>		
Rule Name	Specifies the name for Antivirus rule.	Enter the rule name.

**Table 1: Configuring Host Checker Third-Party Applications Using Predefined Rules Details** (continued)

Option	Function	Your Action
Select Products	Specifies the support products or vendors for system scan check.	Select one of the following options: <ul style="list-style-type: none"> <li>■ <b>Require any supported product</b>—Specifies the software vendor's product that is supported for the system scan check.</li> <li>■ <b>Require specific products/Vendors</b>—Specifies the specific vendor for the system scan check.</li> </ul>
Require any supported product from a specific vendor	Checks for any product (rather than requiring you to select every product separately).	Select the <b>Require any supported product from a specific vendor</b> to enable this feature.
Require specific products	Checks for specific products/vendors to define compliance by allowing any product by a specific vendor (for example, any Symantec product).	Select the <b>Require specific products</b> to enable this feature.
Enable Scan period check	Enables the System scan for the product.	Select the <b>Enable Scan period check</b> to enable this feature.
Successful System Scan must have been performed in the last: (days)	Specifies the days to perform the system scan.	Enter the days.
Consider this rule as passed if 'Full System Scan' was started successfully as remediation.	Passes the rule if system full scan starts successfully as remediation.	Select the <b>Consider this rule as passed if 'Full System Scan' was started successfully as remediation.</b> to enable this feature.
Enable virus definitions update check	Checks for the viral updates.	Select the <b>Enable virus definitions update check</b> to enable this feature.
Virus Definition files should not be older than (updates)	Specifies the update of client Virus definition files the client must use.	Enter a number between 1 and 10. For example: If you enter <b>1</b> , the client must have the latest update. You must import the virus signature list for the supported vendor.
Monitor this rule for change in result	Continuously monitors the policy compliance of endpoints.	Select the <b>Monitor this rule for change in result</b> to enable this feature.
Enable Download latest virus definition files for all supported products	Allows you to download latest virus definition files for all supported products.	Select the <b>Enable Download latest virus definition files for all supported products</b> to enable this feature.

**Table 1: Configuring Host Checker Third-Party Applications Using Predefined Rules Details** (continued)

Option	Function	Your Action
Enable Turning on Real Time Protection for all supported products	Enables turning on real time protection for all supported products.	Select the <b>Enable Turning on Real Time Protection for all supported products</b> to enable this feature.
Enable Starting of Antivirus Scan for all supported products	Scans supported products with antivirus scan.	Select the <b>Enable Starting of Antivirus Scan for all supported products</b> to enable this feature.
<b>Selected Vendors tab</b>		
Selected Vendors	Allows you to select the specific vendors.	Select the vendor, and then click <b>Add</b> to move the vendor from the Non-members to the Members list.
<b>Specific Products Selected tab</b>		
Specific Products Selected	Allows you to select the specific products.	Select the product, and then click <b>Add</b> to move the product from the Non-members to the Members list.
<b>Selected Products tab</b>		
Product name	Allows you to select the product.	Select the product from the Product name drop-down list.
live-update	Allows live-update for the product.	Select the <b>live-update</b> option to enable this feature.
set-real-time-protection-on	Allows real-time protection for the product.	Select the <b>set-real-time-protection on</b> option to enable this feature.
start-scan	Starts the scanning process for the product.	Select the <b>start-scan</b> option to enable this feature.
<b>Predefined Firewall Rules</b>		
Rule Name	Specifies the name for the firewall rule.	Enter the name.
Select Products	Allows you to select your firewall vendor(s) and product(s).	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>Require any supported product</b>—Specifies the software vendor’s product that is supported for the system scan check.</li> <li>■ <b>Require specific products/vendors</b>—Specifies the specific vendor for the system scan check.</li> </ul>
Require any supported product from a specific vendor	Checks for any product (rather than requiring you to select every product separately)	Select the <b>Require any supported product from a specific vendor</b> to enable this feature.

**Table 1: Configuring Host Checker Third-Party Applications Using Predefined Rules Details** (continued)

Option	Function	Your Action
Require specific products	Specifies specific products/vendors, and defines compliance by allowing any product by a specific vendor (for example, any Symantec product).	Select the <b>Require specific products</b> to enable this feature.
Monitor this rule for change in result	Continuously monitors the policy compliance of endpoints.	Select the <b>Monitor this rule for change in result</b> to enable this feature.
Turn on firewall for all supported products	Turns on the Firewall.	Select the <b>Turn on firewall for all supported products</b> to enable this feature.
<b>Selected Vendors tab</b>		
Selected Vendors	Allows you to select the specific vendors.	Select the vendor, and then click <b>Add</b> to move the vendor from the Non-members to the Members list.
<b>Specific Products Selected tab</b>		
Specific Products Selected	Allows you to select the specific products.	Select the product, and then click <b>Add</b> to move the product from the Non-members to the Members list.
<b>Selected Products</b>		
Product name	Allows you to select the product.	Select the product from the Product name drop-down list.
turn-on-firewall	Turns on the Firewall for the product.	Select the <b>turn-on-firewall</b> option to enable this feature.
<b>Predefined Malware Rules</b>		
Rule Name	Specifies the name of the Malware rule.	Enter the Malware rule name.
Monitor this role for change in result	Continuously monitors the policy compliance of endpoints.	Select the <b>Monitor this role for change in result</b> to enable this feature.
Selected Products	Allows you to select the products.	Select the product, and then click <b>Add</b> to enable this feature.
<b>Predefined Spyware Rules</b>		
Rule Name	Enter the name for the spyware rule.	Enter the name.

**Table 1: Configuring Host Checker Third-Party Applications Using Predefined Rules Details** (continued)

Option	Function	Your Action
Select Products	Allows you to select products or vendors	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>Require any supported product</b>—Specifies the software vendor’s product that is supported for the system scan check.</li> <li>■ <b>Require specific products/vendors</b>—Specifies the specific vendor for the system scan check.</li> </ul>
Require any supported product from a specified vendor	Checks for any product (rather than requiring you to select every product separately).	Select the <b>Require any supported product from a specific vendor</b> option to enable this feature.
Require specific products	Specifies specific products/vendors, and defines compliance by allowing any product by a specific vendor (for example, any Symantec product).	Select the <b>Require specific products</b> option to enable this feature.
Monitor this rule for change in result	Continuously monitors the policy compliance of endpoints.	Select the <b>Monitor this rule for change in result</b> option to enable this feature.
<b>Selected Vendors tab</b>		
Selected Vendors	Allows you to select the vendors.	Select the vendor, and then click <b>Add</b> to move the vendor from the Non-members to the Members list.
<b>Specific Products Selected tab</b>		
Specific Products Selected	Allows you to select specific products.	Select the product, and then click <b>Add</b> to move the product from the Non-members to the Members list.
<b>Selected Products</b>		
Product name	Allows you to select the product.	Select the product from the <b>Product name</b> drop-down list.
<b>Predefined OS Checks Rules</b>		
Rule Name	Specifies the name for the OS Checks rule.	Enter the name.
OS Selections	Specifies the operating systems.	Select the operating system, and then click <b>Add</b> to move from the Non-members to the members list.

**Related Topics** ■ Configuring the Remote Integrity Measurement Verifier Server (NSM Procedure)

- Configuring Host Checker Customized Requirements Using Custom Rules (NSM Procedure)
- Configuring General Host Checker Remediation (NSM Procedure)