

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

You can create custom rules within a Host Checker policy to define requirements that users' computers must meet. And creating these custom rules happens only if the predefined client-side policies and rules do not meet the needs.

To configure customized requirements using custom 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 customized requirements using custom 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, or Windows Mobile**. In the same policy, you can specify different Host Checker requirements for each operating system.
6. Configure the configure customized requirements using custom rules using the settings described in Table 1 on page 1.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Configuring Host Checker Customized Requirements Using Custom Rules Details

Option	Function	Your Action
Settings tab		
Remote IMV Rules	IMV—Use this rule type to configure integrity measurement software that a client must run to verify a particular aspect of the client's integrity, such as the client's operating system, patch level, or virus protection.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the IMV. 3. Click OK.
NHC Rules	(Windows only)—Use this rule type to specify the location of a custom DLL. Host Checker calls the DLL to perform customized client-side checks. If the DLL returns a success value to Host Checker, then the Secure Access device considers the rule met.	<ol style="list-style-type: none"> 1. Enter the rule name, vendor name, and the path to NHC DLL on client machines. 2. Select the Monitor this rule for change in result check box to continuously monitor the policy compliance of endpoints. 3. Click OK.

Table 1: Configuring Host Checker Customized Requirements Using Custom Rules Details (continued)

Option	Function	Your Action
Settings tab		
Ports Rules	Use this rule type to control the network connections that a client can generate during a session. This rule type ensures that certain ports are open or closed on the client machine before the user can access the Secure Access device.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the Required option to specify that these ports are open or closed. 3. Enter a comma delimited port list (without spaces) of ports or port ranges, such as: 1234,11000-11999,1235. 4. Click OK.
Process Rules	Use this rule type to control the software that a client may run during a session. This rule type ensures that certain processes are running or not running on the client machine before the user can access resources protected by the Secure Access device.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the Required option to specify that these ports are open or closed. 3. Enter the process name (executable file), such as: good-app.exe. 4. Enter the MD5 checksums value of each executable file to which you want the policy to apply (optional). 5. Select the Monitor this rule for change in result check box to continuously monitor the policy compliance of endpoints. 6. Click OK.
File Rules	Use this rule type to ensure that certain files are present or not present on the client machine before the user can access the Secure Access device . You may also use file checks to evaluate the age and content (through MD5 checksums) of required files and allow or deny access accordingly.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Enter the filename such as: c:\temp\bad-file.txt or /temp/bad-file.txt. 3. Select the Required option to specify that these ports are open or closed. 4. Enter the minimum version of the file (optional). For example, if you require notepad.exe to be present on the client, you can enter 5.0 in the box. Host Checker accepts version 5.0 and later, of notepad.exe. 5. Enter the maximum age of files in the File modified less than (days ago) box. 6. Enter the MD5 checksums value of each executable file to which you want the policy to apply (optional). 7. Select the Monitor this rule for change in result check box to continuously monitor the policy compliance of endpoints. 8. Click OK.

Table 1: Configuring Host Checker Customized Requirements Using Custom Rules Details (continued)

Option	Function	Your Action
Settings tab		
Registry Rules	(Windows only)—Use this rule type to control the corporate PC images, system configurations, and software settings that a client must have to access the Secure Access device. This rule type ensures that certain registry keys are set on the client machine before the user can access the Secure Access device. You may also use registry checks to evaluate the age of required files and allow or deny access accordingly.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the registry root key from the drop-down list. 3. Enter the path to the application folder for the registry subkey. 4. Enter the name of the key's value. 5. Select the key value's type (String, Binary, or DWORD) from the drop-down list (optional). 6. Enter the registry value. 7. Select the Set Registry value specified in the criteria check box. 8. Select the Monitor this rule for change in result check box to continuously monitor the policy compliance of endpoints. 9. Click OK.
NetBIOS Rules	(Windows only, does not include Windows Mobile)—Use this rule type to check the NetBIOS name of the client machine before the user can access the Secure Access device.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. Select the Required option to require that NETBIOS name of the client machine matches or does not match any one of the names you specify. 3. Enter a comma-delimited list (without spaces) of NetBIOS names. The name can be up to 15 characters in length. You can use wildcard characters in the name and it is not case-sensitive. For example: md*, m*xp and *xp all match MDXP. 4. Click OK.
MAC Address Rules	(Windows only)—Use this rule type to check the MAC addresses of the client machine before the user can access the Secure Access device.	<ol style="list-style-type: none"> 1. Enter the Rule Name. 2. Select the Required option to require that a MAC address of the client machine matches or does not match any of the addresses you specify. 3. Enter a comma-delimited list (without spaces) of MAC addresses in the form XX:XX:XX:XX:XX:XX where the X's are hexadecimal numbers. For example: 00:0e:1b:04:40:29. 4. Click OK.

Table 1: Configuring Host Checker Customized Requirements Using Custom Rules Details (continued)

Option	Function	Your Action
Settings tab		
Machine Certificate Rules	(Windows only)—Use this rule type to check that the client machine is permitted access by validating the machine certificate stored on the client machine.	<ol style="list-style-type: none"> 1. Enter the rule name. 2. From the Select Issuer Certificate list, select the certificate that you want to retrieve from the user’s machine and validate. Or, select Any Certificate to skip the issuer check and only validate the machine certificate based on the optional criteria that you specify below. 3. Enter any additional criteria that Host Checker should use when verifying the machine certificate in the Certificate field and Expected value box. 4. Click OK.
Patch Assessment Rules		
Scan for Specific products	Configures a policy based on specific products.	<ul style="list-style-type: none"> ■ Select one of the following options from the drop-down list <ul style="list-style-type: none"> ■ Enter the integrity measurement rule name. ■ All products—Host Checker checks for all of the exposed patches on the endpoint. ■ Specific products—An extensive listing of products and versions. ■ Select specific patches that you wish to ignore for all products by clicking the Add button under Ignore following patches. ■ Select the check boxes to determine the severity level of the patches that you wish to ignore. ■ Select the Enable SMS patch update check box to update patches using SMS.
Scan for specific patches	Configures a policy based on specific patches	<ul style="list-style-type: none"> ■ Enter the integrity measurement rule name. ■ Select the specific patches and then click Add to move the patches from the Non-members to the Members list. ■ Select the Enable SMS patch update check box to update patches using SMS.

- Related Topics**
- Configuring Global Cache Cleaner Options (NSM Procedure)
 - Configuring a Secure Application Manager Resource Policy (NSM Procedure)