

Specifying Customized Requirements Using Custom Rules (NSM Procedure)

If the predefined client-side policies and rules that come with the Infranet Controller do not meet your needs, you can create custom rules within a Host Checker policy to define requirements that your users' computers must meet.



NOTE: You can only check for registry keys, third-party DLLs, NetBIOS names, MAC addresses, and machine certificates on Windows computers.

To create a client-side Host Checker policy:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to create a client-side Host Checker policy.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker**.
4. Create a new policy or click an existing policy in the Policies area 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** or **Solaris**. In the same policy, you can specify different Host Checker requirements for each operating system.
6. Under Rule Settings, click **Add**. The Add Custom Rule page appears.
7. Add or modify settings as shown in Table 1 on page 1.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Custom Rules Configuration Details

Rule	Usage	Your Action
Remote IMV Rule	Configures 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 option.3. Click OK.

Table 1: Custom Rules Configuration Details (continued)

Rule	Usage	Your Action
NHC Rule	(Windows only)—Specifies 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 Infranet Controller 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.
Ports Rule	Controls 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 Infranet Controller.	<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 Rule	Controls 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 Infranet Controller.	<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.

Table 1: Custom Rules Configuration Details (continued)

Rule	Usage	Your Action
File Rule	Ensures that certain files are present or not present on the client machine before the user can access the Infranet Controller. 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 file name 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: Custom Rules Configuration Details (continued)

Rule	Usage	Your Action
Registry Setting Rule	(Windows only)—Controls the corporate PC images, system configurations, and software settings that a client must have to access the Infranet Controller. This rule type ensures that certain registry keys are set on the client machine before the user can access the Infranet Controller. 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 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 Minimum Version to allow the specified version or newer versions of the application. For example, you can use this option to specify version information for an antivirus application to make sure that the client antivirus software is current. The Infranet Controller uses lexical sorting to determine if the client contains the specified version or later. 9. Select the Monitor this rule for change in result check box to continuously monitor the policy compliance of endpoints. 10. Click OK.
NetBIOS Rule	(Windows only, does not include Windows Mobile)—Checks the NetBIOS name of the client machine before the user can access the Infranet Controller.	<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.

Table 1: Custom Rules Configuration Details (continued)

Rule	Usage	Your Action
MAC Address Rule	(Windows only)—Checks the MAC addresses of the client machine before the user can access the Infranet Controller.	<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.
Machine Certificate Rule	(Windows only)— Checks 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 Certificate field and Expected value to specify any additional criteria that Host Checker should use when verifying the machine certificate. 4. Click OK.

- Related Topics**
- Configuring New Client-Side Policies (NSM Procedure)
 - Remediating Infranet Controller Host Checker Policies

