

## Configuring General Host Checker Remediation (NSM Procedure)

You can specify general remediation actions that you want the Host Checker to take if an endpoint does not meet the requirements of a policy. For example, you can display a remediation page to the user that contains specific instructions and links to resources to help the user bring their endpoint into compliance with Host Checker policy requirements.

To configure general Host Checker remediation:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure general Host Checker remediation.
3. Click the **Configuration** tab. Select **system > Authentication > Endpoint Security**.
4. In the Endpoint Security screen, select **Settings > Policies** and click the **Add** icon.
5. Create new client-side policies and enable customized server-side policies.
6. 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**.
7. Add or modify settings as specified in Table 1 on page 1 to specify the remediation actions that you want Host Checker to perform if a user's computer does not meet the requirements of the current policy.
9. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 1: Configuring General Host Checker Remediation Details**

Option	Function	Your Action
<b>Remediation tab</b>		
Enable Custom Instructions	Specifies the instructions you want to display to the user on the Host Checker remediation page.	Select the <b>Enable Custom Instructions</b> option to enable this feature, and then enter the instructions.  <b>NOTE:</b> You can use the following HTML tags to format text and add links to resources such as policy servers or web sites: <code>&lt;i&gt;</code> , <code>&lt;b&gt;</code> , <code>&lt;br&gt;</code> , <code>&lt;font&gt;</code> , and <code>&lt;a href&gt;</code> .

**Table 1: Configuring General Host Checker Remediation Details** (continued)

Option	Function	Your Action
Enable Custom Actions	Allows you to select one or more alternate policies that you want Host Checker to evaluate if the user's computer does not meet the current policy requirements. The alternate policy must be either a third-party policy that uses a J.E.D.I. package or a Secure Virtual Workspace policy.	Select the <b>Enable Custom Actions</b> option to enable this feature, and then select the alternate policy and click <b>Add</b> to move from the Non-members to the Members list.
Kill Processes	Specifies the name of one or more processes you want to kill if the user's computer does not meet the policy requirements. You can include an optional MD5 checksum for the process.	Select the <b>Kill Processes</b> option to enable this feature, and then enter the name. For example, enter <code>keylogger.exe</code>
Delete Files	Specifies the names of files you want to delete if the user's computer does not meet the policy requirements. Enter one filename per line.	Select the <b>Delete Files</b> option to enable this feature, and then enter the filename. For example, enter <code>c:\temp\bad-file.txt</code> <code>/temp/bad-file.txt</code> .
Send reason strings	Displays a message to users (called a reason string) that is returned by Host Checker or integrity measurement verifier (IMV) and explains why the client machine does not meet the Host Checker policy requirements.  <b>NOTE:</b> This option applies to predefined rules, custom rules, and to third-party IMVs that use extensions in the Juniper Networks TNC SDK.	Select the <b>Send reason strings</b> option to enable this feature.

- Related Topics**
- Configuring Host Checker Third-Party Applications Using Predefined Rules (NSM Procedure)
  - Configuring the Remote Integrity Measurement Verifier Server (NSM Procedure)
  - Setting Up Secure Access Device Host Checker Options (NSM Procedure)