

## Configuring New Client-Side Policies (NSM Procedure)

---

You can create a variety of policies through the Host Checker client that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. You can also create Host Checker policies that use third-party integrity measurement verifiers (IMVs) and third-party DLLs, or check for ports, processes, files, registry keys, and the NetBIOS name, MAC addresses, or certificate of the client machine.

When creating the policies, you must define the policy name, and either enable predefined rules or create custom rules that run the specified checks. Optionally, you can specify how Host Checker should evaluate multiple rules within a single policy.

To create a standard client-side policy:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to create a standard client-side policy.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker**.
4. Under Policies, click the **Add** button.
5. Enter a policy name and select a policy type.
6. Create one or more rules to associate with the policy.
7. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

- Related Topics**
- Specifying Customized Requirements Using Custom Rules (NSM Procedure)
  - Remediating Infranet Controller Host Checker Policies
  - Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure)

