Symantec™ Posture Plug-in for Cisco® Network Admission Control (NAC) 2.0

This guide includes the following topics:

- About Symantec Posture Plug-in for Cisco Network Admission Control (NAC)
- About security attribute policies
- System requirements
- Symantec Posture Plug-in for Cisco NAC components
- How Symantec Posture Plug-in works
- Required preinstallation tasks
- Rolling out and installing Symantec Posture Plug-in for Cisco NAC
- How to view client compliancy logs
- How client compliancy status is displayed on the client

About Symantec Posture Plug-in for Cisco Network Admission Control (NAC)

Symantec Posture Plug-in for Cisco Network Admission Control (NAC) plugs into Cisco security software.
Symantec™ Posture Plug-in for Cisco® Network Admission Control (NAC) 2.0

About security attribute policies

Symantec Posture Plug-in reduces exposure to threats by working in conjunction with Cisco NAC software to prevent users with nonsecure computers from connecting to the corporate network. It ensures that computers attempting to access your corporate network meet the requirements of your approved security attribute policy for Symantec AntiVirus™ and Symantec™ Client Firewall.

Symantec Posture Plug-in provides Symantec AntiVirus and Symantec Client Firewall status information to Cisco NAC software, which uses this information to deny a computer access to your network until it is remediated with the required Symantec software or settings. Once the computer complies with your security attribute policy, Symantec Posture Plug-in forwards this information to the Cisco NAC software, which then allows the computer to access the network.

All client compliancy issues must be manually remediated before network access is allowed. For example, you can enable Auto-Protect on a client or update Symantec AntiVirus to a compliant version, and then reattempt to access the network.

About security attribute policies

A security attribute policy is created and configured from the Cisco Secure Access Control Server (ACS) server, a component of the Cisco Systems NAC solution. The policy may contain network access rules for several client applications. A security attribute policy may include the following Symantec antivirus-specific requirements:

- Symantec AntiVirus is installed.
- Auto-Protect is enabled.
- Symantec AntiVirus is the specified minimum version or later.
- The scan engine that is included in Symantec AntiVirus is the specified minimum version or later.
- Virus definitions files are at least a specified minimum version.

A security attribute policy might include the following Symantec Client Firewall requirements:

- Symantec Client Firewall is installed.
- Symantec Client Firewall is enabled.
- Symantec Client Firewall is at least a specified minimum version.
System requirements

You must meet both Cisco Systems® and Symantec requirements to implement Symantec Posture Plug-in for Cisco NAC.

Cisco Systems requirements

You must have the following Cisco Systems software installed to use Symantec Posture Plug-in for Cisco NAC:

- Cisco Secure Access Control Server (ACS) server v3.3 (1.5)
  This Authentication, Authorization, Accounting (AAA) server must be running on a Windows® 2000 server.
- Cisco IOS® router software 12.3(8)T
  This software must be installed on the network access device.
- Cisco Trust Agent v1.0 (build 49 or later)
  This software must be installed and running on the client.

Symantec requirements

You must have one of the following Symantec products installed to use Symantec Posture Plug-in for Cisco NAC:

- Symantec™ Client Security 3.0
- Symantec AntiVirus 10.0

You must have 6MB of free disk space available on each computer to which you install Symantec Posture Plug-in for Cisco NAC.

Symantec Posture Plug-in for Cisco NAC components

Symantec Posture Plug-in for Cisco NAC consists of the following Symantec components, which are described in Table 1-1.

<table>
<thead>
<tr>
<th>Component</th>
<th>Primary function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Posture Plug-in for Cisco NAC</td>
<td>Plugs in to the Cisco Trust Agent and serves as a communication bridge between the Cisco Trust Agent and Symantec VPN Sentry.</td>
</tr>
</tbody>
</table>
Symantec™ Posture Plug-in for Cisco® Network Admission Control (NAC) 2.0

Symantec Posture Plug-in for Cisco NAC components

Symantec Posture Plug-in for Cisco NAC is dependent upon the following Cisco Systems components:

- Cisco Secure Access Control Server (ACS), which creates and maintains the security policies that determine client access to network
- Cisco IOS router, which forwards client configuration settings to the Cisco ACS server and processes network access policies that determine client access to network
- Cisco Trust Agent, which serves as the single point of contact on the host client for collecting credentials and sends this information to the Cisco ACS server.

Figure 1-1 illustrates the interaction between the Symantec and Cisco Systems components.

### Table 1-1 Symantec Posture Plug-in components

<table>
<thead>
<tr>
<th>Component</th>
<th>Primary function</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPNSentry.exe</td>
<td>Collects client antivirus and firewall status and sends results through the Symantec Posture Plug-in for Cisco NAC to the Cisco Trust Agent.</td>
</tr>
</tbody>
</table>

**Figure 1-1** Symantec and Cisco Systems components
How Symantec Posture Plug-in works

Symantec Posture Plug-in for Cisco NAC works in the following way. The client that is running Symantec Posture Plug-in for Cisco NAC resides on a local access network (LAN) that is connected to a Cisco router.

- Cisco Trust Agent communicates through the Symantec Posture Plug-in for Cisco NAC and queries VPNSentry.exe for Symantec AntiVirus and Symantec Client Firewall status.
- VPN Sentry performs the following actions:
  - Collects the client validation status of Symantec AntiVirus and Symantec Client Firewall.
  - Forwards the client validation status to the Symantec Posture Plug-in for Cisco NAC.
- The Symantec Posture Plug-in for Cisco NAC passes the client validation status to Cisco Trust Agent.
- Cisco Trust Agent sends the client validation status to Cisco IOS router.
- Cisco IOS router sends the client validation status to Cisco Secure Access Control Server (ACS) server, which maintains the security attribute policy that contains network access rules for the client.
- Cisco Secure ACS server compares the client validation status to the rules in the security attribute policy and determines the network access policy.
- Cisco Secure ACS server sends the decision (network access policy) to the Cisco IOS router.
- The Cisco IOS router enforces the network access policy and either allows or restricts network access to Symantec AntiVirus and Symantec Client Firewall.

Automatic remediation is not supported for Symantec Posture Plug-in for Cisco NAC. Symantec AntiVirus and Symantec Client Firewall client computers that are denied network access must either enable or update their software to comply with the Cisco network access policy. Once updated, the client can reattempt to access the network.

Required preinstallation tasks

You must complete the following tasks before you install Symantec Posture Plug-in for Cisco NAC:

- Test your LAN environment to ensure that it is working properly.
Ensure communication from Symantec AntiVirus and Symantec Client Firewall through Cisco router to the network.

- Verify that Internet Explorer 5.5 with Service Pack 2 or later is installed on each computer running Symantec AntiVirus and Symantec Client Firewall.
- Roll out the following Cisco Systems and Symantec components to each computer running Symantec AntiVirus and Symantec Client Firewall:
  - Cisco Trust Agent (if it is not already installed).
- Configure Cisco router to work with Cisco Secure ACS server for the Cisco NAC solution.
- Configure Cisco Secure ACS server security attribute policy to include specific antivirus and firewall checks.
  For more information, see the Cisco Secure ACS server documentation.

Configuring security attribute policy from Cisco Secure ACS server

You define the client compliancy policy by activating Symantec antivirus and firewall-specific security policies (credential validation policies) within the Cisco Secure ACS server. Cisco Systems maintains the list of available antivirus and firewall-specific security policies.

For more information on configuring the security attribute policy, see the Cisco Secure ACS server documentation.

**Note:** Additional Symantec antivirus and firewall-specific security policies that are not included in the latest version of Cisco Secure ACS server may be available. See the Readme document for more information.

Rolling out and installing Symantec Posture Plug-in for Cisco NAC

You must roll out and execute the Microsoft Windows Installer file, Symantec Posture Plug-in for Cisco.msi, to every client.

You can roll out and install Symantec Posture Plug-in for Cisco NAC using the LiveUpdate™ Custom Content Publishing Application (CCPA). You can also use a variety of third-party products, including Microsoft Active Directory®, Tivoli®, and Microsoft® Systems Management Server (SMS), to roll out and install Symantec Posture Plug-in for Cisco NAC.
How to roll out Symantec Posture Plug-in for Cisco NAC using the LiveUpdate CCPA

Custom content publishing lets you use the security features of LiveUpdate to allow client computers to receive custom content. Custom content can consist of any type of file that you want your clients to receive, including service packs, installable files, documents, and spreadsheets.

Using the CCPA, you create, modify, and publish updates that are uploaded to the Central LiveUpdate server. When the LiveUpdate client runs, it looks for custom content packages, in addition to LiveUpdate virus definitions and product updates, and authenticates the packages to determine if they can be trusted.

You can install CCPA from the LiveUpdate directory on the Symantec AntiVirus or Symantec Client Security CD.

For information on using the CCPA, see the LiveUpdate Administrator’s Guide.

How to roll out Symantec Posture Plug-in for Cisco NAC using Microsoft Active Directory and Tivoli

You can install Symantec Posture Plug-in for Cisco NAC using the standard options that are provided by Active Directory and Tivoli for all Windows Installer-based installation packages.

For Active Directory and Tivoli deployment instructions, see the documentation on deploying Windows Installer (.msi) installation packages that is provided with the environment that you are using.

How to roll out Symantec Posture Plug-in for Cisco NAC using Microsoft SMS package definition files

Microsoft SMS administrators can use a package definition file (.pdf) to distribute Symantec Posture Plug-in for Cisco NAC to clients.

To distribute Symantec Posture Plug-in for Cisco NAC with SMS, you typically complete the following tasks:

- Create source directories to store Symantec Posture Plug-in for Cisco NAC.
■ Create a query to identify clients that have sufficient free disk space to install the software.
■ Create a workstation package to distribute the software.
■ Generate an SMS job to distribute and install the workstation package on clients.

In a workstation package, you define the files that comprise the software application to be distributed, and the package configuration and identification information.

The installation folder must be copied locally before you run the installation using SMS.

For more information on using SMS, see the Microsoft Systems Management Server documentation.

### Installing Symantec Posture Plug-in for Cisco NAC to a single computer

The Symantec AntiVirus or Symantec Client Security CD includes a standard setup program that you can use to install Symantec Posture Plug-in for Cisco NAC to a single computer.

**To install Symantec Posture Plug-in for Cisco NAC to a single computer**

1. Insert the Symantec AntiVirus or Symantec Client Security CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Click **SymSentry**.
4. Click **Symantec Posture Plug-in**.
5 Double-click **Setup.exe**.

6 In the Welcome panel, click **Next**.
7 In the Ready to Install the Program panel, click Install.

8 In the InstallShield Wizard Completed panel, click Finish.

Installed files

The setup program installs files in the Cisco Systems directory, which is C:\Program Files\Common Files\Cisco Systems\CiscoTrustAgent\Plugins\Install. The following files are installed:

- SYMC_PP.dll
  (When invoked, the Cisco Trust Agent automatically moves the file to C:\Program Files\Common Files\Cisco Systems\CiscoTrustAgent\Plugins.)

- SYMC_PP.inf
  (When invoked, the Cisco Trust Agent automatically moves the file to C:\Program Files\Common Files\Cisco Systems\CiscoTrustAgent\Plugins.)
Table 1-2 lists the directories and files that the setup program installs.

<table>
<thead>
<tr>
<th>Directory</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>\Program Files\Symantec\VPNSentry\</td>
<td>Installs the following files:</td>
</tr>
<tr>
<td></td>
<td>■ VPNSentry.exe</td>
</tr>
<tr>
<td></td>
<td>■ XmlUtil.dll</td>
</tr>
<tr>
<td></td>
<td>■ ComplianceEvent.dll</td>
</tr>
<tr>
<td></td>
<td>■ Notifier.exe</td>
</tr>
<tr>
<td></td>
<td>■ XSCore.dll</td>
</tr>
<tr>
<td></td>
<td>■ XSDataFiles.dll</td>
</tr>
<tr>
<td>\Program Files\Symantec\VPNSentry\Cisco</td>
<td>Installs the following files:</td>
</tr>
<tr>
<td></td>
<td>■ atl71.dll</td>
</tr>
<tr>
<td></td>
<td>■ msvcr71.dll</td>
</tr>
<tr>
<td></td>
<td>■ mfc71u.dll</td>
</tr>
<tr>
<td></td>
<td>■ mfc71.dll</td>
</tr>
<tr>
<td></td>
<td>■ msvcp71.dll</td>
</tr>
</tbody>
</table>

**Migrating Symantec Posture Plug-in for Cisco NAC**
When you install Symantec Posture Plug-in for Cisco NAC 2.0 on a client computer that includes an earlier version, the installer recognizes the previous version and automatically updates the Symantec Posture Plug-in to the newer version.

**Uninstalling Symantec Posture Plug-in for Cisco NAC**
You uninstall Symantec Posture Plug-in for Cisco NAC using the uninstallation program that is provided by Symantec. If a manual uninstallation is required, see the support Knowledge Base on the Symantec Web site.

To uninstall Symantec Posture Plug-in for Cisco NAC

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec Posture Plug-in**.
4. Click **Remove**.
How to view client compliance logs

You can review client compliance logs from the Cisco Secure ACS server. Logs can be viewed under **ACS Manager>Report Activity>Passed Logs** and **ACS Manager>Report Activity>Failed Logs**.

Cisco Trust Agent includes logging functionality for the client. See the Cisco Readme document for information on activating this feature.

A debug log is available for Symantec Posture Plug-in for Cisco NAC. Enable the log by adding a key to the registry located in **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SymSentry**.

**To create Symantec Posture Plug-in debug log**

- From **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SymSentry**, create a new String value called **DebugLogFlags** with value data of TIPSD. The debug log file, SymSentry.log, is created under **C:\Documents and Settings\All Users\Application Data\Symantec\SymSentry**.

How client compliance status is displayed on the client

Cisco Trust Agent displays a message on the client when a connection attempt succeeds or fails. The message informs the user of the current connection status. A “healthy” client signifies that the client is fully compliant with the Cisco Secure ACS server security attribute policy. An “infected” client signifies that the client does not fulfill all requirements that are outlined in the security attribute policy, therefore network connection may be denied.