CHAPTER 3

Deploying or Installing Cisco SSC

This chapter lists SSC installation requirements and describes how to deploy, install, and upgrade SSC. The chapter contains these sections:

Before You Begin

To install SSC 5.1.1, you must have administrative privileges on the PC running Windows 2000, Windows XP, or Windows Vista. Before beginning the installation, please observe these guidelines:

- Review your authentication server requirements:
  - Identify and prioritize the needed authentication protocols.
  - Ensure that the authentication policies are configured in the user and machine profiles of the SSC distribution package.
  - If necessary, configure the server certificate on the authentication server.
  - If personal certificates are required for user authentication, ensure that the certificate infrastructure is configured and operational.
- Ensure that the access points and switches in your network are properly configured for 802.1X authentication.
- Ensure that your user PCs are configured with the required wired and wireless network cards and drivers.
- Prior to actual user deployments:
  - Test your client distribution package on a lab PC and ensure the user and machine profiles are working properly.
  - Uninstall other client management software, such as the Odyssey Client Manager. The Cisco Aironet Client Utility (ACU) and the Cisco Aironet Desktop Utility (ADU) can coexist with SSC and do not need to be uninstalled.
  - Ensure that Microsoft Internet Explorer 5.0 or later is installed on the user's PC.

Requirements

The supported operating systems are:

- Windows Vista Business, Enterprise and Ultimate Editions—32-bit and 64-bit
  - Required Windows Hot Fixes:

    KB952613
    KB935222 or SP1
    KB932063 or SP1
- Windows XP Professional (SP2)—32-bit
- Windows 2000 (SP4)—32-bit
- Windows 2003 Server Enterprise Edition (SP2)—32-bit

Note Other Windows XP versions, such as Media Center, Tablet PC, and Professional x64 are not supported. Other Windows Vista versions, such as Home Premium and Home Basic are not supported.

Note The latest drivers should be loaded on the user's PC prior to installing SSC.

Note Cisco strongly recommends that you install Windows Vista Service Pack 1. However, SP1 is required if wired network connections are to be attempted before user logon.

Installing SSC

The system administrator normally deploys the SSC client destination package to the end user PC, and SSC is automatically installed without user intervention. Typically, the system administrator provides pre-configured enterprise network connections in the destination package.

Prior to distributing the destination package to end users, the system administrator should manually install SSC and test the configured profiles to ensure that they operate correctly.

Manually Installing an SSC Test Package

To manually install SSC on a PC, follow these instructions:

Step 1 Obtain the client destination package .msi file produced by the SSC management utility

Step 2 Place the file in a folder on a test PC.

Step 3 Double-click the client destination package .msi file.

Step 4 Click **Next** and the license agreement window appears.

Step 5 Read and accept the terms in the license agreement, then click **Next**.

Step 6 Accept the default destination folder or click **Change** and follow the prompts to the desired folder. When complete, click **Next**.

Step 7 Click **Install** and a bar appears indicating the progress of the installation.

Step 8 When the installation is complete, click **Finish** and a pop-up message appears indicating that your PC must be restarted and asks if you want to restart now.

Step 9 Click **Yes** and your PC reboots.

When you log in to the PC, the SSC icon appears in the system tray.

Deploying to a User PC

SSC does not provide mechanisms for moving files to user PCs; however, there are numerous third-party methods available for use by the system administrator. Cisco assumes that the IT Administrators already have a preferred method of moving files to user PCs, such as Microsoft's System Management Server (SMS) method.

When the SSC destination package file is placed on the user's PC, the standard Microsoft installer mechanism can be used by the system administrator to silently install the SSC destination package file. For this example, enter this command:

msiexec /i yourCisco-SSC-XP2K-5.msi /quiet

The **/quiet** parameter prevents the installation process from being visible to the user and prevents user interaction.

Note Use the **/i** parameter for fresh installations only. If you want to use the **/i** parameter, ensure that you have uninstalled any previous version of SSC.

If you want to upgrade from a previous version to a newer version, say 5.1.0 to 5.1.1, enter the following command:

msiexec /fvomusc yourCisco-SSC-XP2K-5.msi /quiet

This informs the Windows Installation program about the presence of a previous version of *yourCisco-SSC-XP2K-5.msi* and to upgrade it to the installer specified after the **/fvomusc** parameter.

In this upgrade scenario, ensure that the .msi filename of the new version matches the .msi filename of the previous version. That is, if the name of the file used in the 5.1.0 version is *yourCisco-SSC-XP2K-5.msi*, then ensure that you specify the same name for the 5.1.1 version.

Note When you are upgrading or reinstalling SSC, the new SSC destination file must have the same fileneme as the previous installation.

Upgrading SSC Running Windows 2000 or Windows XP

Migrating From SSC 5.0 to SSC 5.1.1

Previously installed SSC 5.0 software with administrator pre-deployed configurations must be uninstalled and the PC rebooted prior to installing SSC 5.1.1. The SSC 5.1.1 installation process automatically detects a previous SSC 5.0 pre-deployed package installation and displays an error message indicating *Internal error 2771 Core* and fails to install. After SSC 5.0 software is uninstalled from the user's PC and the PC rebooted, SSC 5.1.1 can be successfully installed.

Note The installation error occurs because the SSC 5.0 pre-deployed installation package functionality is not in compliance with the Windows Installer Component Rules. This prevents backwards compatibility and the normal SSC upgrade procedure, which does not require an explicit uninstall-reboot and install-reboot sequence.

If the SSC 5.0 software does not contain a pre-deployed configuration, there is no need to uninstall the SSC software prior to installing SSC 5.1.1.

After the SSC 5.1.1 installation, the PC must be rebooted for the SSC software changes to take effect.

Migrating From SSC 4.x to 5.x

The SSC installation process uninstalls SSC releases 4.1.1 to 4.2.x and converts the user configurations from the SSC 4 product to SSC 5.1.1 configuration settings.

SSC releases earlier than 4.1.1 are not converted or uninstalled. The earlier SSC release must be manually installed before you install SSC 5.1.1. Also, the SSC 5.1.1 installation process will indicate that the previous SSC release must be manually uninstalled.

Note For some configurations, it might be easier and faster to create a new destination package file using the SSC management utility.

Upgrading Administrator-Deployed Networks from SSC 4.1.x to 5.x

An administrator must have the following SSC 5.x client elements on his PC:

- SSC 5.x installation msi file (Cisco_SSC-XP2K-5.msi)
- Configuration management utility (sscMgmtToolkit_5.x.0.xxxx.zip)
- Configuration combining tool (ConfigCombiner.exe)
- Configuration conversion tool (ConfigConverter.exe)
- Administrator xslt file (configConvert_3_1_admin.xslt)—used to translate administrator-configured SSC 4.1 networks to SSC 5.x schema.
- sscPackageGen utility that generates a custom client destination package file.

Note The ConfigCombiner.exe, ConfigConverter.exe, and Convert_3_1_admin.xslt files are only available after the SSC 5.1.1 installation completes. The files are located in the C:\Documents and Settings\All Users\Application Data\Cisco Secure Services Client\Conversion Tools folder.

The administrator also must have the current SSC 4.x deployment package translated into SSC 4.1.2 internal configuration. This is the *profiles* folder found in the *Program Files\Cisco Systems\Cisco Secure Services Client* folder.

In order to deploy an SSC 5.1.1 client that is equivalently configured to your SSC 4.x destination, you must perform these operations:

1. Use the combining tool (ConfigCombiner.exe) to combine SSC 4.1 configuration files into a single file:

   Usage: ConfigCombiner.exe [options]

   Options include:

   --source *directory* or -s *directory*—specifies the source directory path. If the source directory option is not specified, the default value for the source directory is *C:\Program Files\Cisco Systems\Cisco Secure Services Client\profiles*.

   --quiet or -q—do not display the results

   --help—gives the usage of the tool

   The following illustrates a combining tool example:

   ```
   ConfigCombiner.exe -q
   ```

   The output of this operation produces a file called *configuration.xml*. The file is located in the folder where the tool was executed. The file contains the information in the multiple folders under *c:\Program Files\Cisco Systems\Cisco Secure Client Services\profiles*.

   Note SSC 4.1.x files are not modified in any way as a result of this operation.

2. Use the conversion tool (ConfigConverter.exe) with the administrator XSLT file (configConvert_3_1_admin.xslt) to convert the output of the combining tool into an SSC 5.1.1 configuration.xml file:

   Usage: ConfigConverter.exe [options]

   Options include these values:

   --quiet or -q—specifies to not display the results

   --output *filename* or -o *filename*—specifies the output XML file

   --input *filename* or -i *filename*—specifies the input XML file

   --xslt *filename* or -xslt *filename*—specifies the XSLT file

   You should specify the *--xslt* file option with the XSLT file name set to *configConvert_3_1_admin.xslt* when you are converting the administrator-deployed networks using the ConfigConverter tool. This is the same tool used with a different default xslt file to translate the end user created networks on end user systems.

   The following illustrates a conversion tool example:

```
ConfigConverter.exe -i configuration.xml -o configuration.xml
--xslt configConvert_3_1_admin.xslt
```

The output of this operation is an SSC 5.1.1 schema compatible destination package with an equivalent configuration of your SSC 4.1.x deployed networks.

3. You can now use the management utility to perform these operations:
   - Read in the SSC 5.1.1 configuration.xml (which contains the administrator-deployed SSC 4.1 networks).
   - If needed, modify the SSC 5.1.1 configuration.xml file.
   - Sign the SSC 5.1.1 configuration.xml file.
4. Run the sscPackageGen tool to bundle the signed configuration.xml file along with the SSC 5.1.1 msi file and then deploy the package.

Upgrading End User Created SSC 4.1.x Networks to 5.x

When SSC 5.1.1 is installed on a PC as an upgrade, it automatically upgrades the SSC Release 4.1.x end user created networks to SSC 5.1.1 networks. There is nothing that you, the administrator, or the end user need to do. The results of the upgrade are as follows:

- SSC 5.1.1 starts running with the deployed administrator configuration file.
- All the end user created profiles from SSC 4.1 are imported into SSC 5.1.1.
- This conversion is done once only during the upgrade.
- SSC 4.1 has multiple user xml files on an end-station, but SSC 5.1.1 has only one user XML file. The conversion tool places the contents of multiple SSC 4.1 user profile files into the single SSC 5.1.1 user XML file. Each user XML file in SSC 4.1 corresponds to a group in SSC 5.1.1. The group name is the user xml file name prefixed with *SSC 4_*. The profiles in the *allusers* file are placed in the *SSC4_allusers* group. It is the responsibility of the end user to later go through the list of available networks using the GUI and delete any networks they do not want.
- There may be multiple networks created in SSC 5.1.1 for a single network in SSC Release 4.1. This is because the SSC 5.1.1 schema allows only one EAP-method per network, whereas the SSC 4.1 schema allows multiple EAP methods per network. This means that a user network from SSC 4.1, after conversion to SSC 5.1.1, has a network name that includes both the SSC 4.1 network name and the EAP method. This is done to help avoid confusion.
- On an upgrade from SSC 4.1 to SSC 5.1.1, all static user credentials are imported into SSC 5.1.1. Also, the WEP and PSK credentials entered by the user are also imported into SSC 5.1.1. However, any 802.1X credentials are not imported, they need to be re-entered if required.

Pre-Installation of Client Certificates

If the end user SSC file uses a client-certificate-based EAP method, the client certificate used to supply the user's credentials must be independently deployed and placed in the proper Windows Certificate Store (User-Personal Store). The destination package file can be used to deploy a server certificate, an intermediate CA certificate, and/or the trusted root certificate on the user’s PC.

Upgrading SSC from Windows XP to Windows Vista

After upgrading your operating system from Windows XP to Windows Vista, the previously installed SSC software must be uninstalled. After the SSC software is uninstalled from the user's PC and the PC rebooted, SSC 5.1.1 for Windows Vista can be successfully installed.

After the SSC 5.1.1 installation, the PC must be rebooted for the SSC software changes to take effect.

Upgrading SSC Running on Windows Vista

A previous version of SSC 5.1.1 software for Windows Vista can be upgraded to a later version by reinstalling SSC using the procedures define in the "Installing SSC" section on page 3-2. The SSC 5.1.1 installation process automatically detects a previous SSC 5.1.1 installation and maintains any existing connection profiles.

After the SSC 5.1.1 installation, the PC must be rebooted for the SSC software changes to take effect.

Upgrading Only SSC Profiles in all Supported Operating Systems

After the administrator has successfully deployed SSC on the user's PC, it might become necessary from time to time to modify the deployed connection settings or policies due to an infrastructure improvement, new security policies, and so on. The administrator can modify these settings and profiles by generating an updated configuration.xml file using the SSC management utility. The administrator only needs to deploy the configuration.xml file on the user's PC and does not need to reinstall SSC.

The revised configuration.xml file must be installed in this directory location on the user's PC:

- Windows 2000 and Windows XP:

  C:\Documents and Settings\All Users\Application Data\Cisco\Cisco Secure Services Client\system

- Windows Vista:

  C:\ProgramData\Cisco\Cisco Secure Services Client\system

SSC switches to the new configuration when any one of these events occurs:

- The PC reboots.
- The current network connection is lost. Before attempting to establish the connection again, SSC switches to the new configuration.
- The user explicitly initiates the configuration switch by right-clicking the SSC tray icon and choosing **Repair**.