



Installing and Enabling Cisco Secure Desktop

This chapter describes how to perform the following tasks on the security appliance.

- [Installing or Upgrading Cisco Secure Desktop](#)
- [Enabling or Disabling Cisco Secure Desktop](#)
- [Entering an Activation Key to Support Advanced Endpoint Assessment](#)
- [Configuring CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop](#)
- [Uninstalling Cisco Secure Desktop](#)

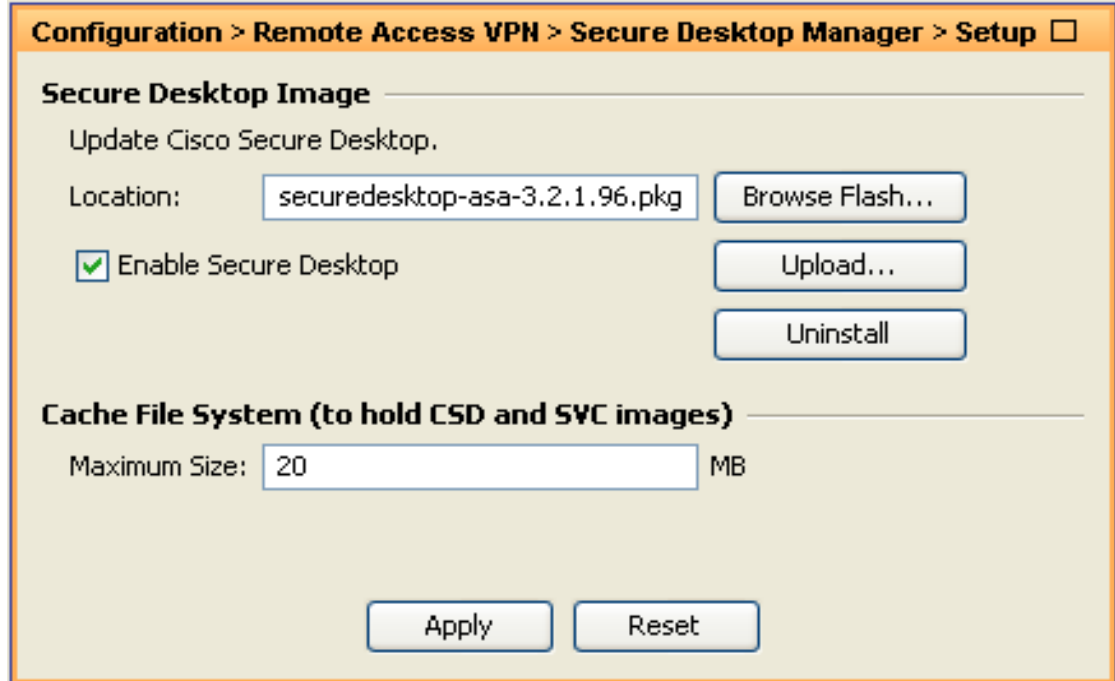
Installing or Upgrading Cisco Secure Desktop

Cisco Secure Desktop Release 3.2.1 requires ASA Release 8.0(3). You do not need to restart the security appliance after you install or upgrade Cisco Secure Desktop, however, you must exit and restart your ASDM connection to access Secure Desktop Manager.

Install or upgrade the Cisco Secure Desktop software on the security appliance as follows:

-
- Step 1** Use your Internet browser to access the following URL and download the `securedesktop_asa_<n>_<n>*.pkg` file to “My Documents” on your PC:
<http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop>
- Step 2** Establish an ASDM session with the security appliance.
- Step 3** Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**.
ASDM opens the Setup pane ([Figure 2-1](#)).

Figure 2-1 Setup



- Step 4** Click **Upload** to prepare to transfer a copy of the Cisco Secure Desktop software from your local PC to the flash card installed in the ASA 5500.
ASDM opens the Upload Image dialog box.
- Step 5** Click **Browse Local** to prepare to select the file on your local PC.
By default, the Selected File Path dialog box displays the contents of the My Documents folder.
- Step 6** Choose the `securedesktop_asa_<n>_<n>*.pkg` you downloaded in Step 1 and click **Select**.
ASDM closes the Select File Path dialog box.
- Step 7** Click **Browse Flash** and enter the name of the `securedesktop_asa_<n>_<n>*.pkg` file you are uploading in the File Name field, then click **OK**.
- Step 8** Click **Upload File**.



Caution Avoid opening other windows until you complete the remaining steps.

ASDM transfers a copy of the file to the flash card. An Information dialog box displays the following message:

```
File has been uploaded to flash successfully.
```

- Step 9** Click **OK**.
ASDM clears the fields in the Upload Image dialog box.
- Step 10** Click **Close**.
The Use Uploaded Image dialog box displays the following message:
Use disk0:/securedesktop_asa_n_n.pkg as your new current image?

Step 11 Click **OK**.

Step 12 Check **Enable Secure Desktop** if it is not already checked.

Step 13 Click **Apply**.

The Uninstall CSD dialog box opens if you upgraded from an earlier version of Cisco Secure Desktop, and displays the following message:

```
Do you want to delete disk0:securedesktop_asa_<Previous_Version>.pkg?
```

Step 14 Click **Yes** to remove the previous version from the flash memory card, and click **Proceed** in the Refresh Needed window.

If you choose to downgrade later, you can use the same method you used to upgrade (that is, upload and install it).

An ASDM Restart Confirmation window displays the following message:

```
The Secure Desktop image is successfully updated. The new features can be accessed after ASDM is restarted.
```

Step 15 Click **OK**.

Step 16 The Secure Desktop Manager menu closes.

If you reopen the menu, it shows only the Setup option.

Step 17 Click the **X** in the upper right corner of the ASDM window to exit.

A window displays the following message:

```
The configuration has been modified. Do you want to save the running configuration to flash memory?
```

Step 18 Click **Save**.

ASDM saves the configuration and closes.

Step 19 Establish a new ASDM session with the security appliance to customize the Secure Desktop Manager configuration.

Enabling or Disabling Cisco Secure Desktop

Enabling Cisco Secure Desktop loads the Cisco Secure Desktop configuration file (data.xml) from the flash device to the running configuration. If you transfer or replace the data.xml, disable and then enable Cisco Secure Desktop to load the file.

Disabling Cisco Secure Desktop does not alter the Cisco Secure Desktop configuration.

Use ASDM to enable or disable Cisco Secure Desktop as follows:

Step 1 Choose **Configuration > Clientless SSL VPN > Secure Desktop > Setup**.

ASDM opens the Setup pane (Figure 2-1).



Note The Secure Desktop Image field displays the image (and version) that is currently installed. The Enable Secure Desktop check box indicates whether Cisco Secure Desktop is enabled.

- Step 2** Check or uncheck **Enable Secure Desktop** and click **Apply**.
ASDM enables or disables Cisco Secure Desktop.
-

Entering an Activation Key to Support Advanced Endpoint Assessment

Advanced Endpoint Assessment includes all of the Endpoint Assessment features, and lets you configure an attempt to update noncompliant computers to meet version requirements. You can use ASDM to activate a key to support Advanced Endpoint Assessment after acquiring it from Cisco, as follows:

- Step 1** Choose **Device Management > System Image/Configuration > Activation Key**.
- Step 2** Enter the key in the New Activation Key field.
- Step 3** Click **Update Activation Key**.
- Step 4** Choose **File > Save Running Configuration to Flash**.
- An Advanced Endpoint Assessment entry appears and the Configure button becomes active in the Host Scan Extensions area of the **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan** pane, which is accessible only if Cisco Secure Desktop is enabled.
-

Configuring CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop

If your remote users have Cisco Security Agent (CSA) installed, you must import new CSA policies to the remote users to enable the AnyConnect VPN Client and Cisco Secure Desktop to interoperate with the security appliance.

To do this, follow these steps:

- Step 1** Retrieve the CSA policies for the AnyConnect client and Cisco Secure Desktop. You can get the files from:
- The CD shipped with the security appliance.
 - The software download page for the ASA 5500 Series Adaptive Security Appliance at <http://www.cisco.com/cgi-bin/tablebuild.pl/asa>.
- The filenames are AnyConnect-CSA.zip and CSD-for-CSA-updates.zip
- Step 2** Extract the .export files from the .zip package files.
- Step 3** Choose the correct version of the .export file to import. The Version 5.2 export files work for CSA Versions 5.2 and higher. The 5.x export files are for CSA Versions 5.0 and 5.1.
- Step 4** Import the file using the Maintenance > Export/Import tab on the CSA Management Center.

Step 5 Attach the new rule module to your VPN policy and generate rules.

For more information, see the CSA document *Using Management Center for Cisco Security Agents 5.2*. Specific information about exporting policies is located in the section *Exporting and Importing Configurations*.

Uninstalling Cisco Secure Desktop

Uninstalling Cisco Secure Desktop removes the Cisco Secure Desktop configuration file (data.xml) from the sdesktop directory on the flash card. If you want to retain the file, copy it using an alternative name or download it to your workstation before you uninstall Cisco Secure Desktop.

Uninstall Cisco Secure Desktop on the security appliance as follows:

Step 1 Establish an ASDM session with the security appliance.

Step 2 Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**.

ASDM opens the Setup pane ([Figure 2-1](#)).

Step 3 Click **Uninstall**.

A confirmation window displays the following message:

```
Do you want to delete disk0:/securedesktop_asa_3_2_0_87.pkg and all CSD data files?
```

Step 4 Click **Yes**.

ASDM removes the text from the Location text box and removes the Secure Desktop Manager menu options below Setup.
