



Setting Up CSD for Microsoft Windows Clients

See the following sections to configure CSD for remote clients running Microsoft Windows:

- [Creating Windows Locations](#)
- [Defining Location Criteria](#)
- [Configuring the Secure Desktop for Clients that Match Location Criteria](#)

Creating Windows Locations

Windows locations let you determine how clients connect to your virtual private network, and protect it accordingly.

For example, clients connecting from within a workplace LAN on a 10.x.x.x network behind a NAT device are an unlikely risk for exposing confidential information. For these clients, you might set up a CSD Windows Location named Work that is specified by IP addresses on the 10.x.x.x network, and disable both the Cache Cleaner and the Secure Desktop function for this location.

In contrast, users' home PCs might be considered more at risk to viruses due to their mixed use. For these clients, you might set up a location named Home that is specified by a corporate-supplied certificate that employees install on their home PCs. This location would require the presence of antivirus software and specific, supported operating systems to grant full access to the network.

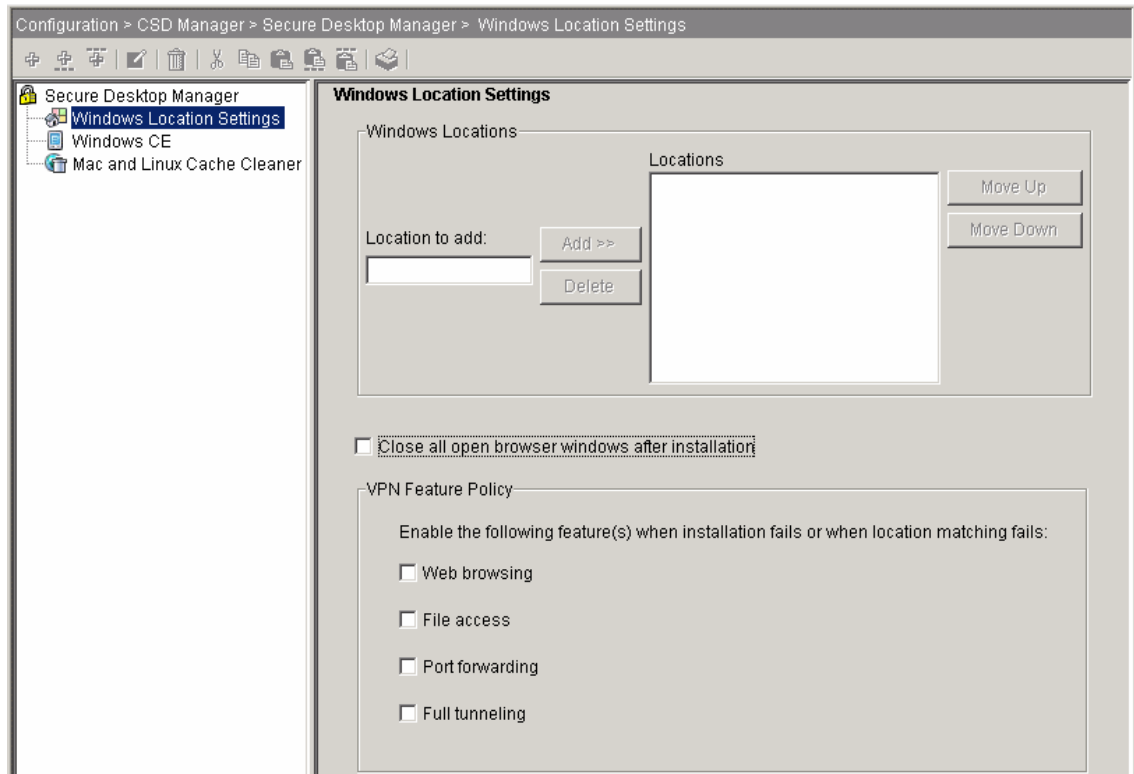
Finally, for untrusted locations such as Internet cafes, you might set up a location named "Insecure" that has no matching criteria (thus making it the default for clients that do not match other locations). This location would require full Secure Desktop functions, and include a short timeout period to prevent access by unauthorized users.

CSD evaluates remote client PCs against the locations in the order listed on the Windows Location Settings pane, and grants privileges based on the first location definition that matches.

Examine the Windows Location attribute descriptions to plan a configuration that meets the security requirements of your network.

Click **Windows Location Settings** in the menu on the left to define the location-based settings (also called adaptive policies) for CSD. [Figure 5-1](#) shows the default settings.

Figure 5-1 Windows Location Settings



The elements on this pane are as follows:

- Location to add and Add button—To add a location from which users can connect, type a new location name in the Location to add field and click Add. As you add locations, the Secure Desktop Manager adds their names to the CSD menu and to the list of “Locations” on this pane.
- Delete—Select an entry in the Locations box and click Delete to discard it.
- Locations—Lists the locations in the CSD configuration. When a remote client PC connects, the Secure Desktop Installer attempts to match it to a location in the sequence shown in this box.



Caution If you create a location and do not specify criteria, make sure it is the last entry in the “Locations” list.

- Move Up and Move Down—Select an entry in the Locations box and click one of these buttons to change its priority.
CSD evaluates clients against the locations in the order of their appearance in this list.
- Close all open browser windows upon installation—Check to remove unsecured web browser sessions from the client when CSD is installed. This option prevents confusion over whether CSD secures the data. This option applies to all Windows Locations.
- Web browsing—Check to let the remote user browse the web if the Secure Desktop installation fails or the remote client PC does not match any of the configured locations criteria. In the interest of security, we recommend that you do not check this option.

By default, this attribute is unchecked.

- **File access**—Check to let the remote user access files on a remote server if the Secure Desktop installation fails or the remote client PC does not match any of the configured locations criteria. In the interest of security, we recommend that you do not check this option.

By default, this attribute is unchecked.

- **Port forwarding**—Check to let the remote user connect a client application installed on the local PC to the TCP/IP port of a peer application on a remote server if the Secure Desktop installation fails or the remote client PC does not match any of the configured locations criteria. In the interest of security, we recommend that you do not check this option.

By default, this attribute is unchecked.

- **Full tunneling**—Check to let the remote user establish a VPN tunnel with the SSL VPN Client if the Secure Desktop installation fails or the remote client PC does not match any of the configured locations criteria. In the interest of security, we recommend that you do not check this option.

By default, this attribute is unchecked.

Defining Location Criteria

To configure the settings for a location, click the location name in the menu on the left. The Identification for <Location> pane appears (Figure 5-2).

Figure 5-2 Identification for <Location>

Identification for Work

Location Module: Secure Desktop or Cache Cleaner

Certificate Criteria

Enable identification using certificate criteria

Issued By: Issued To:

IP Criteria

Enable identification using IP criteria

IP Address Range to Add

From: . . .

To: . . .

Add >>

Delete

IP Address Range

Registry and File Criteria

Enable identification using registry or file criteria

This pane lets you specify the criteria that define the location. A location can be based on any of the following matching criteria:

- Certificate name and issuer
- IP address range
- Presence or absence of a particular file or registry key.

**Note**

To push the Secure Desktop to all remote client PCs regardless of their status, configure only one location and do not specify a certificate, IP address range, or file or registry criteria. This default location pushes the Secure Desktop to all computers from which users connect.

CSD considers the three location criteria in a logical “AND” relationship. For example, if you specify an IP address range under “Enable identification using IP criteria,” and you specify “File company_software.exe #does exist#” under “Enable identification using File or Registry criteria,” the client must meet both of these conditions to match the location.

Within each area in the pane, only one of the criteria you specify must match; that is, CSD considers the criteria in a logical “OR” relationship. For example, if you specify several files under “Enable identification using File or Registry criteria,” only one of these files must be present.

Refer to the sections that name the location criteria you want to configure:

- [Location Module](#)
- [Certificate Criteria](#)
- [IP Criteria](#)
- [Registry and File Criteria](#)

Location Module

The Location Module attribute in the Identification for <Location> pane ([Figure 5-2](#)) permits one of the following options:

- Secure Desktop—Check if you want to require the Secure Desktop to be present on the remote client as a criterion for assigning this location entry.

**Note**

If you check Secure Desktop and configure the Secure Desktop settings, you should still configure the Cache Cleaner as well. The Cache Cleaner serves as a fall-back security solution for older Windows operating systems such as Windows 98, which the full Secure Desktop functions do not support.

- Cache Cleaner—Check if you want to require the Cache Cleaner to be present on the remote client as a criterion for assigning this location entry.
- Both Secure Desktop and Cache Cleaner—Leave unchecked to let CSD apply the configured [VPN feature policy](#).

Certificate Criteria

Check **Enable identification using certificate criteria** in the Identification for <Location> pane (Figure 5-2) to specify values of a digital certificate on the remote client PC as a criterion for assigning the properties of the location to the remote client.

**Note**

For information about setting up your server to work with client certificates, see the “[Frequently Asked Questions](#)” section on page A-1.

Use one of the following instructions to examine the certificate Subject and Issuer fields to identify the values to be completed in the “Issued By” and “Issued To” fields:

- [Using a Certificate File to Specify Certificate Criteria](#)
- [Using a Signed File to Specify Certificate Criteria](#)
- [Using the Certificates in Your Store to Specify Certificate Criteria](#)

Using a Certificate File to Specify Certificate Criteria

To specify certificate criteria if you have a certificate file (for example, a *.cer or *.pfx file),

Step 1 Double-click the certificate.

The Certificate window opens.

Step 2 Click the **Details** tab.

Step 3 Complete both of the fields in the “Certificate Criteria” area of the Identification for <Location> pane (Figure 5-2), as follows:

- **Issued By**—Click **Subject** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Subject field of the certificate. The subordinate fields include such names as “CN” for common name, “O” for organization unit name, and “E” for e-mail address. Type the value of one of these subfields in the **Issued By** field on the Identification for <Location> pane to match it against the Subject field of the certificate.

**Note**

Specify the value of the subfield. For example, type the value of the “O” field, not the “O” itself.

- **Issued To**—Click **Issuer** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Issuer field of the certificate. The subordinate fields include such names as “CN” for common name, “O” for organization unit name, and “E” for e-mail address. Type the value of one of these subordinate fields in the **Issued To** field on the Identification for <Location> pane to match it against the Issuer field of the certificate.

CSD assigns the location to the client only if it has a certificate that contains *both* of the following, and only if it matches at least one criterion in each of the completed areas in the Identification for <Location> pane:

- Value in the Subject field that matches the value you specified in the “Issued By” field
- Value in the Issuer field that matches the value you specified in the “Issued To” field

Using a Signed File to Specify Certificate Criteria

To specify certificate criteria if you have a signed file (that is, the file is not a certificate file, but contains a certificate):

Step 1 Right click the file and choose **Properties**.

The Properties window opens.

Step 2 Click the **Digital Signatures** tab (which appears only if the file is signed).

Step 3 Click **Details**.

Step 4 Click **View Certificate**.

The Certificate window opens.

Step 5 Click the **Details** tab.

Step 6 Complete both of the fields in the “Certificate Criteria” area of the Identification for <Location> pane (Figure 5-2), as follows:

- **Issued By**—Click **Subject** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Subject field of the certificate. The subordinate fields include such names as “CN” for common name, “O” for organization unit name, and “E” for e-mail address. Type the value of one of these subfields in the **Issued By** field on the Identification for <Location> pane to match it against the Subject field of the certificate.



Note Specify the value of the subfield. For example, type the value of the “O” field, not the “O” itself.

- **Issued To**—Click **Issuer** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Issuer field of the certificate. The subordinate fields include such names as “CN” for common name, “O” for organization unit name, and “E” for e-mail address. Type the value of one of these subordinate fields in the **Issued To** field on the Identification for <Location> pane to match it against the Issuer field of the certificate.
-

CSD assigns the location to the client only if it has a certificate that contains *both* of the following, and only if it matches at least one criterion in each of the completed areas in the Identification for <Location> pane:

- Value in the Subject field that matches the value you specified in the “Issued By” field
- Value in the Issuer field that matches the value you specified in the “Issued To” field

Using the Certificates in Your Store to Specify Certificate Criteria

To specify certificate criteria if you have neither a certificate file nor a signed file, go to the certificates in your *store* (your computer) to retrieve the data you need, as follows:

-
- Step 1** Open the **Control Panel**.
- Step 2** Choose **Internet Options**.
- Step 3** Click the **Content** tab.
- Step 4** Click **Certificates**.
- Step 5** Choose a certificate and click **View**.
- The Certificate window opens.
- Step 6** Click the **Details** tab.
- Step 7** Complete both of the fields in the “Certificate Criteria” area of the Identification for <Location> pane (Figure 5-2), as follows:

- **Issued By**—Click **Subject** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Subject field of the certificate. The subordinate fields include such names as “CN” for common name, “O” for organization unit name, and “E” for e-mail address. Type the value of one of these subfields in the **Issued By** field on the Identification for <Location> pane to match it against the Subject field of the certificate.



Note Specify the value of the subfield. For example, type the value of the “O” field, not the “O” itself.

- **Issued To**—Click **Issuer** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Issuer field of the certificate. The subordinate fields include such names as “CN” for common name, “O” for organization unit name, and “E” for e-mail address. Type the value of one of these subordinate fields in the **Issued To** field on the Identification for <Location> pane to match it against the Issuer field of the certificate.

CSD assigns the location to the client only if it has a certificate that contains *both* of the following, and only if it matches at least one criterion in each of the completed areas in the Identification for <Location> pane:

- Value in the Subject field that matches the value you specified in the “Issued By” field
- Value in the Issuer field that matches the value you specified in the “Issued To” field

IP Criteria

Check **Enable identification using IP criteria** in the Identification for <Location> pane (Figure 5-2) to use the IP address of the remote client PC as a criterion for assigning a location to the remote client, then click **Add** to enter one or more IP address ranges.

CSD checks the IP addresses of remote client PCs trying to connect. If a client has an address within the specified range, CSD assigns the properties of the location to the remote client.

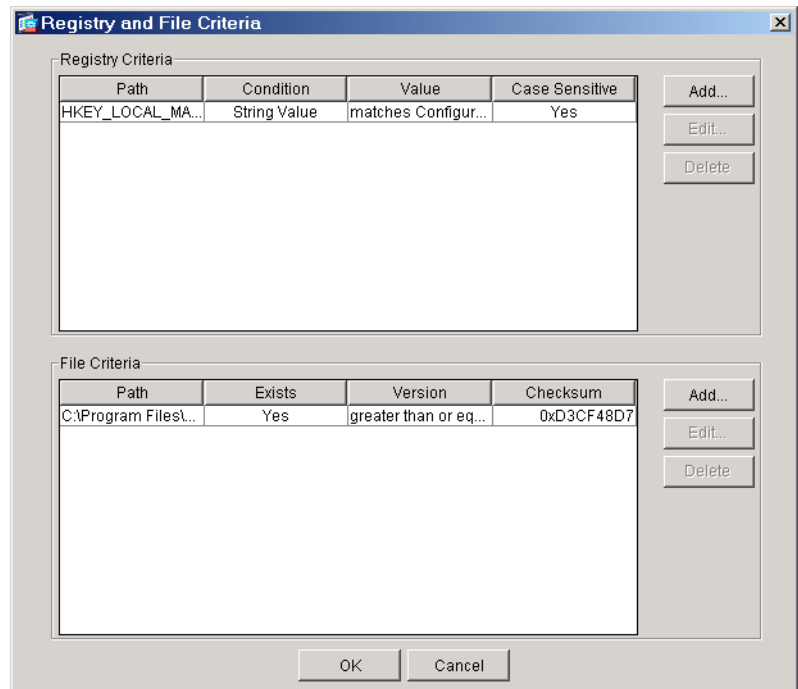
**Note**

If the client has more than one network card, CSD uses only the address of the first card detected.

Registry and File Criteria

Check **Enable identification using registry or file criteria** in the Identification for <Location> pane (Figure 5-2) if you want to specify registry key or file criteria to match to qualify a remote client PC to obtain the access rights associated with the location you are configuring, and click **Configure Criteria**. The Registry and File Criteria dialog box opens (Figure 5-3).

Figure 5-3 Registry and File Criteria



The tables in this window list any registry key and file requirements needed to qualify a remote client to obtain the access rights associated with the location you are configuring. Each entry is a logical OR operator (that is, the evaluation result for any entry must be TRUE to assign the location).

**Note**

To view details in the Registry Criteria or File Criteria tables, float the cursor over the column header divider. As you do so, it becomes a double, horizontal arrow. Drag the arrow to the left or right to expose the contents of the column.

Refer to the section that identifies the type of criteria you would like to configure:

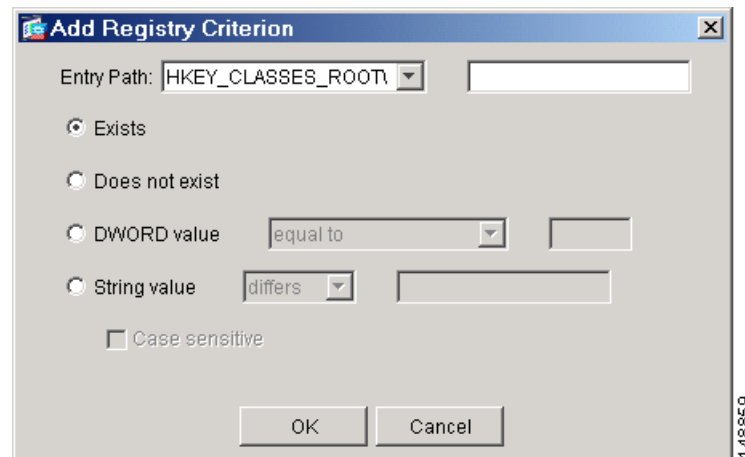
- [Registry Criteria](#)
- [File Criteria](#)

Registry Criteria

In the Registry Criteria area of the Registry and File Criteria dialog box (Figure 5-3), click **Add** if you want to confirm the presence or absence of a specific registry key as a criterion, or choose a criterion to be modified from the Registry Criteria area and click **Edit**.

The Add or Edit Registry Criterion dialog box opens. Figure 5-4 shows the Add Registry Criterion dialog box.

Figure 5-4 Add Registry Criterion



Note

You can use the value types to be specified in this window as a guide to set up one or more secret criteria within the remote client's system to match those specified for this location. For example, you can add a DWORD (double word, an unsigned 32-bit integer) value or string value to a registry key on client computers to qualify them for the location you are configuring.

Step 1

Assign values to the mandatory attributes in the Add or Edit Registry Criterion dialog box as follows:

- **Entry Path** menu—Choose the *hive*, the initial directory path of a registry key. The options are as follows:

```
HKEY_CLASSES_ROOT\  
HKEY_CURRENT_USER\  
HKEY_LOCAL_MACHINE\  
HKEY_USERS\  

```

Each string references a registry base that stores different information. The `HKEY_LOCAL_MACHINE\` path is the most commonly used one because it contains the machine-specific registry files.

- **Entry Path** field—Enter the name of the registry key required to be present on or absent from the client system.



Note Refer to the subsequent attribute descriptions for examples of Entry Path strings.

Step 2

Click one radio button from the following list and assign the associated values:

- **Exists**—Click if the mere presence of the named registry key on the remote client PC is sufficient to match the location you are configuring.

EXAMPLE Click **Exists** if you want to require the following registry key to be present to match a criterion for assigning a location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\<Protective_Software>
```

- **Does not exist**—Click if the absence of the named registry key from the remote client PC is sufficient to match the location you are configuring.

EXAMPLE Click **Does not exist** if you want to require the following registry key to be absent to match a criterion for assigning a location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\<Evil_SpyWare>
```

- **DWORD value** radio button—Click if the registry key includes a “Dword” (“double word,” a 32-bit integer) and you want to specify its value as a criterion.

“DWORD” refers to the attribute in the Add/Edit Registry Criterion dialog box. “Dword” refers to the attribute as it appears in the registry key.



Note Use the regedit application, accessed on the Windows command line, to view the Dword value of a registry key, or use it to add a Dword value to the registry key to satisfy the requirement you are configuring.

DWORD value menu—Choose one of the following options next to **DWORD value** to specify the relationship of the Dword value of the registry key to the value to be entered to the right:

- different from
- equal to
- greater than
- greater than or equal to
- less than
- less than or equal to

DWORD value field—Enter a decimal to compare with the Dword value of the registry key on the client computer.

EXAMPLE Choose **greater than or equal to** and enter an integer if you want to require that the following protective software application meet a minimum version requirement:

```
HKEY_LOCAL_MACHINE\SOFTWARE\<Protective_Software>\Version
```

- **String value** radio button—Click if the registry key includes a string and you want to specify its value as a criterion.



Note Use the regedit application, accessed on the Windows command line, to view the String value of a registry key, or use it to add a String value to the registry key to satisfy the requirement you are configuring.

String value menu—Choose one of the following options to specify the relationship of the String value of the registry key to the value to be entered to the right:

- contains
- differs
- matches

String value field—Enter a string to compare with the String value of the registry key on the client computer.

EXAMPLE Choose **matches** and enter Active if you want to ensure the following protective software application is active:

HKEY_LOCAL_MACHINE\SOFTWARE*<Protective_Software>*\Status

Case sensitive—Check to require the String value of the registry key on the client computer to match the case used in the String value field to satisfy the criterion.

Step 3 Click **OK**.

The dialog box closes and the new criterion appears as an entry in the Registry Criteria window inside the Registry and File Criteria dialog box.

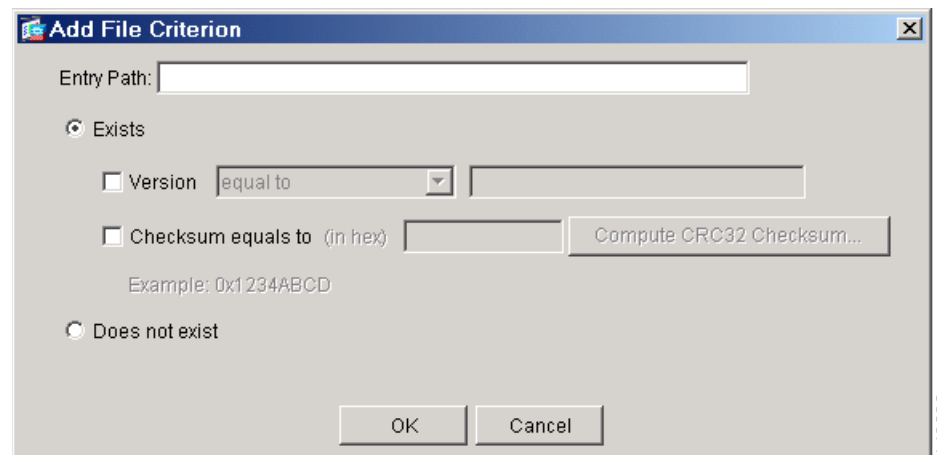
Step 4 Click **Add** if you want to specify another registry key, refer to the next section if you want to specify a file criterion, or click **OK** to return to the Identification for *<Location>* pane.

File Criteria

In the File Criteria area of the Registry and File Criteria dialog box (Figure 5-3), click **Add** if you want to confirm the presence or absence of a specific file as a criterion for assigning the location you are configuring for the remote client, or choose a criterion to be modified from the File Criteria area and click **Edit**.

The Add or Edit File Criterion dialog box opens. Figure 5-5 shows the Add File Criterion dialog box.

Figure 5-5 Add File Criterion



Configure a file criterion as follows:

Step 1 Assign a value to the following mandatory attribute:

- **Entry Path**—Enter the directory path of the file required to be present on or absent from the client system.



Note Refer to the subsequent attribute descriptions for examples File paths.

Step 2 Click one radio button from the following list and assign the associated values:

- **Exists**—Click if the file must be present on the remote client PC to assign the location you are configuring.

EXAMPLE Click **Exists** to ensure the following security application is installed:

C:\Program Files\

You can specify a version, checksum, both, or neither in conjunction with the “Exists” radio button.

(Optional) **Version** check box—Check if you want to specify the version of the file as a criterion. Use this criterion to require that a specific application is a particular version.



Note To display the version of an .exe file, use Windows Explorer to right-click the file, choose **Properties**, and click the **Version** tab.

(Optional) **Version** menu—Choose one of the following options to specify the relationship of the “Version value” of the file to the number to be entered to the right:

- less than
- less than or equal to
- equal to
- different from
- greater than
- greater than or equal to

(Optional) **Version** field—Type a string (typically in dotted decimal notation) to compare with the version of the file on the client computer.

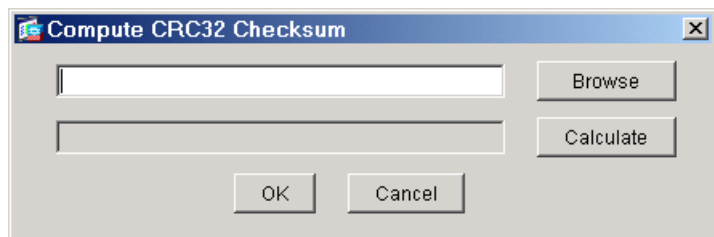
(Optional) **Checksum equals to** check box—Check to specify a checksum to authenticate the file named in the Path field.

(Optional) **Checksum equals to** field—Enter a checksum in hexadecimal format, beginning with 0x, to authenticate the file named in the Path field, or click **Compute CRC32 Checksum** to calculate and insert the value automatically.

(Optional) **Compute CRC32 Checksum**—Click to calculate the checksum of the file stored locally and insert the value in the **Checksum equals to** field.

The Compute CRC32 Checksum dialog box opens (Figure 5-6).

Figure 5-6 Compute CRC32 Checksum



Retrieve the checksum as follows:

- a. Click **Browse** and choose the file on which to calculate the checksum.

The field at the top of the Compute CRC32 Checksum dialog box displays the path to the file you chose.

- b. Click **Calculate**.

The field at the bottom of the Compute CRC32 Checksum dialog box displays the checksum in hexadecimal format.

- c. Click **OK**.

The Compute CRC32 Checksum dialog box closes and the hexadecimal value appears in the **Checksum equals to** field.

- Step 3** Click **OK** in the Add or Edit File Information dialog box.

The dialog box closes and the new criterion appears as an entry in the File Criteria window inside the Registry and File Criteria dialog box.

- Step 4** Click the associated **Add** button if you want to specify another registry or file criterion, or click **OK** to return to the Identification for <Location> pane.
-

Configuring the Secure Desktop for Clients that Match Location Criteria

Refer to the following sections to define the Secure Desktop experience for clients that match the criteria defined for a specific location:

- [Configuring a VPN Feature Policy for a Location](#)
- [Configuring Keystroke Logger for a Location](#)
- [Configuring Cache Cleaner for a Location](#)
- [Configuring Secure Desktop General for a Location](#)
- [Configuring Secure Desktop Settings for a Location](#)
- [Configuring Secure Desktop Browser for a Location](#)

Configuring a VPN Feature Policy for a Location

CSD applies the configured VPN feature policy if you choose neither the Secure Desktop nor the Cache Cleaner location modules in the Identification for <Location> pane ([Figure 5-2](#)). Use the instructions in the following sections to configure the VPN feature policy for each location for which neither option is chosen:

Configuring a Group-based Policy for a Location

Configure a group-based VPN feature-based policy as follows:

- Step 1** Click **VPN Feature Policy** under the name of the location you are configuring in the menu on the left. The Group-Based Policy tab opens ([Figure 5-7](#)).

Figure 5-7 VPN Group-based Policy under Windows Installations

VPN Feature Policy under Windows Installations

Group-Based Policy | Web browsing | File access | Port forwarding | Full tunneling

Use Failure Group-Policy
 Always use Success Group-Policy
 Use Success Group-Policy, if criteria match

The user belongs to either a Failure-Group or Success-Group policy. Select the appropriate radio button above to indicate which group. To configure group privileges, go to the WebVPN Group-Policy configuration screen. The group policy is not completely configured until you complete the configuration on that screen.

Criteria

Select one or more items from the lists below:

Location Module:
Secure Desktop

Anti-Virus:
Must have been updated in the last days

Norton Antivirus (Corp 8.0-9.0, Pro 2004-2005)
eTrust Antivirus (7.0-2005)
Panda Antivirus (Titanium 2004, Platinum 7.0-8.0)
PC-Cillin (2003-2005)
McAfee VirusScan (8.0-10.0, Enterprise 7.0-8.0)
F-Secure Antivirus (2003-2005)
AVG AntiVirus (7.0)
Avast AntiVirus (4.0)

Anti-Spyware:
Must have been updated in the last days

Microsoft Windows AntiSpyware (beta1)
Anonymizer AntiSpyware

Firewall:

Norton Personal Firewall (2003-2005)
Sygate Personal Firewall (5.0-5.6)
McAfee Personal Firewall (4.0-5.0)
ZoneAlarm Personal Firewall (4.0-5.5)
ISS BlackICE PC Protection (3.6)
Internet Connection Firewall (ICF) (XP-XPsp2)
Cisco Secure Agent (4.0-4.5)
PC-Cillin Personal Firewall (2005)

OS:

Windows XP SP2
Windows XP SP1
Windows XP no SP
Windows 2000 SP4
Windows 2000 SP3
Windows 2000 SP2
Windows 2000 SP1
Windows 2000 no SP
Windows NT4 SP6
Windows Millenium
Windows 98 Secound Edition

148853

Step 2 Click one of the following radio buttons:

- **Use Failure Group-Policy** if you want to apply the “Alternative group policy” to any remote client matched to this location.

This option lets you apply an alternative to the default group policy so you can differentiate access rights. Typically, you would use the failure group policy to apply access rights that are more limited than those associated with the success group policy.

With this option set, CSDM dims the attributes in the Criteria area. If you click this radio button, you cannot change other settings on this tab.



Note If you click this radio button, change the alternative group policy setting for the WebVPN tunnel group to a group policy that has access rights that are different than the default group policy. To do so, choose the **Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN Access > WebVPN** tab. Change the policy assigned to the **Alternative group policy** attribute to apply a policy to all clients who match this location.

- **Always use Success Group-Policy** if you want to apply the default WebVPN group policy to any remote client matched to this location.

This option is the default group-based policy setting. If you click this radio button, CSDM dims the attributes in the Criteria area; you cannot change other settings on this tab. Your configuration of a group-based policy ends with this step.

- **Use Success Group-Policy if criteria match** if you want to apply the following group policy to the remote client matched to this location:
 - WebVPN default group policy if the client PC satisfies the criteria specified on this tab.
 - WebVPN failure group policy if the client PC fails to satisfy the criteria specified on this tab.



Note If you click this radio button, choose the **Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN Access > WebVPN** tab. Change the policy assigned to the **Alternative group policy** attribute to apply a policy to clients that fail to satisfy the criteria.

If you click this radio button, CSDM activates the check boxes in the criteria area.



Note A “Use Success Group-Policy if criteria match,” setting without criteria is equivalent to “Always use Success Group-Policy.”

Continue with the following steps.

- Step 3** Check **Location Module** if you want to require the presence of Secure Desktop or Cache Cleaner as a criterion for assigning the success group policy, then choose the module to require: Secure Desktop or Cache Cleaner.



Note If the feature you choose is not active, the client fails the VPN feature policy criteria check.

- Step 4** Check **Anti-Virus, Anti-Spyware, Firewall,** and **OS** if you want to require their presence as conditions for assigning the success group policy.

If you enable more than one category, the end user's computer must pass in each category to pass the System Detection check. An “AND” relationship is present among the enabled categories.

The options within each category have an “OR” relationship. For example, you can specify that any one of a list of antivirus software programs be running, and even if you have checked all of them as possible candidates, having just one of them running is enough to satisfy the antivirus software requirement.

The security categories are as follows:

- **Anti-Virus**—Check to enable System Detection for the presence of antivirus software. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the anti-virus requirement.
- **Anti-Spyware**—Check to enable System Detection for the presence of antispyware software. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the anti-virus requirement.
- **Firewall**—Check to enable System Detection for the presence of a personal firewall that is running. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the personal firewall requirement.
- **OS**—Check to enable System Detection for the presence of a particular operating system and service pack. CSD requires one of the operating systems highlighted to be running on the remote client PC to satisfy the operating system requirement.

Step 5 (Optional) Enter an integer in the range 0 - 999999 in the **Must have been updated in the last ___ days** fields.

CSDM includes this two such fields, one above the Anti-Virus window and the other above the Anti-Spyware window.

Step 6 For each enabled security category you check, click one of the options or control-click multiple options.



Note

For the complete list of applications checked by System Detection, see [Figure 5-7](#) or refer to “[System Detection Questions](#).”

Click **Apply All** to save the running CSD configuration.

Configuring Web Browsing, File Access, Port Forwarding, and Full Tunneling VPN Policies for a Location

This section describes how to configure permissions and system detection conditions for web browsing, file access, port forwarding, and full tunneling when the remote client satisfies the configured location criteria.



Note

To configure settings when remote clients running Microsoft Windows do *not* satisfy configured location criteria, see “[Creating Windows Locations](#).”

Step 1 Click **VPN Feature Policy** under the name of the location you are configuring in the menu on the left. The VPN Feature Policy pane displays the default Group-Based Policy tab (described in “[Configuring a Group-based Policy for a Location](#)”).

Step 2 Click the tab that names the application for which you would like to configure a policy. The tabs after the Group-Based Policy tab are as follows:

- **Web browsing**—Permits the client to use the Secure Desktop to browse the web.
- **File access**—Permits the use of the Secure Desktop to access files on a remote server.
- **Port forwarding**—Permits the use of the Secure Desktop to connect a client application installed on the local PC to the TCP/IP port of a peer application on a remote server.

- Full tunneling—Lets the SSL VPN Client establish a VPN tunnel.



Note The default setting for each of these attributes is “OFF.”

Figure 5-8 shows the Web browsing tab.

Figure 5-8 VPN Web Browsing Policy under Windows Installations

VPN Feature Policy under Windows Installations

Group-Based Policy | **Web browsing** | File access | Port forwarding | Full tunneling

Disabled Always Enabled Enabled, if criteria match

Criteria

Select one or more items from the lists below:

Location Module:
Secure Desktop

Anti-Virus:
Must have been updated in the last days

Norton Antivirus (Corp 8.0-9.0, Pro 2004-2005)
eTrust Antivirus (7.0-2005)
Panda Antivirus (Titanium 2004, Platinum 7.0-8.0)
PC-Cillin (2003-2005)
McAfee VirusScan (8.0-10.0, Enterprise 7.0-8.0)
F-Secure Antivirus (2003-2005)
AVG AntiVirus (7.0)
Avast AntiVirus (4.0)

Anti-Spyware:
Must have been updated in the last days

Microsoft Windows AntiSpyware (beta1)
Anonymizer AntiSpyware

Firewall:
Norton Personal Firewall (2003-2005)
Sygate Personal Firewall (5.0-5.6)
McAfee Personal Firewall (4.0-5.0)
ZoneAlarm Personal Firewall (4.0-5.5)
ISS BlackICE PC Protection (3.6)
Internet Connection Firewall (ICF) (XP-XPsp2)
Cisco Secure Agent (4.0-4.5)
PC-Cillin Personal Firewall (2005)

OS:
Windows XP SP2
Windows XP SP1
Windows XP no SP
Windows 2000 SP4
Windows 2000 SP3
Windows 2000 SP2
Windows 2000 SP1
Windows 2000 no SP
Windows NT4 SP6
Windows Millenium
Windows 98 Secound Edition



Note Except for the tab name, the last four tabs are identical. Also, except for the row of radio buttons near the top, they are also identical to the Group-Based Policy tab (Figure 5-7).

Step 3 Click one of the following radio buttons:

- **Disabled** to make the feature unavailable to the remote client that matches the location criteria.

This option is the default VPN policy setting for web browsing, file access, port forwarding, and full tunneling. If set, CSDM dims the attributes in the Criteria area. If you click this radio button, you cannot change other settings on this tab; your configuration of a VPN policy for this feature ends at this step.

- **Always Enabled** to make the feature available to the remote client that matches the location criteria. If you click this radio button, CSDM dims the attributes in the Criteria area. If set, you cannot change other settings on this tab; your configuration of a VPN policy for this feature ends at this step.
- **Enabled if criteria match** to make the feature available to the remote client that matches the location criteria and satisfies the conditions set below. If you click this radio button, CSDM activates the check boxes in the criteria area.



Note An “Enabled if criteria match,” setting without criteria is equivalent to “Always Enabled.”

- Step 4** Check **Location Module** if you want to require the presence of Secure Desktop or Cache Cleaner as a criterion for enabling the feature identified in the tab, then choose the module to require: Secure Desktop or Cache Cleaner.



Note If the feature you choose is not active, the client fails the VPN feature policy criteria check.

- Step 5** Click one or more security categories to require their presence as a condition to enable the location module you chose in [Step 4](#).

If you enable more than one category, the end user's computer must pass in each category to pass the System Detection check. An “AND” relationship is present among the enabled categories.

The options within each category have an “OR” relationship. For example, you can specify that any one of a list of antivirus software programs be running, and even if you have checked all of them as possible candidates, having just one of them running is enough to satisfy the antivirus software requirement.

The security categories are as follows:

- **Anti-Virus**—Check to enable System Detection for the presence of antivirus software. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the anti-virus requirement.
- **Anti-Spyware**—Check to enable System Detection for the presence of antispyware software. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the anti-virus requirement.
- **Firewall**—Check to enable System Detection for the presence of a personal firewall that is running. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the personal firewall requirement.
- **OS**—Check to enable System Detection for the presence of a particular operating system and service pack. CSD requires one of the operating systems highlighted to be running on the remote client PC to satisfy the operating system requirement.

- Step 6** (Optional) Enter an integer in the range 0 - 999999 in the **Must have been updated in the last ___ days** fields.

CSDM includes this two such fields, one above the Anti-Virus window and the other above the Anti-Spyware window.

- Step 7** For each enabled security category you check, click one of the options or control-click multiple options.

**Note**

For the complete list of applications checked by System Detection, see [Figure 5-8](#) or refer to “[System Detection Questions](#).”

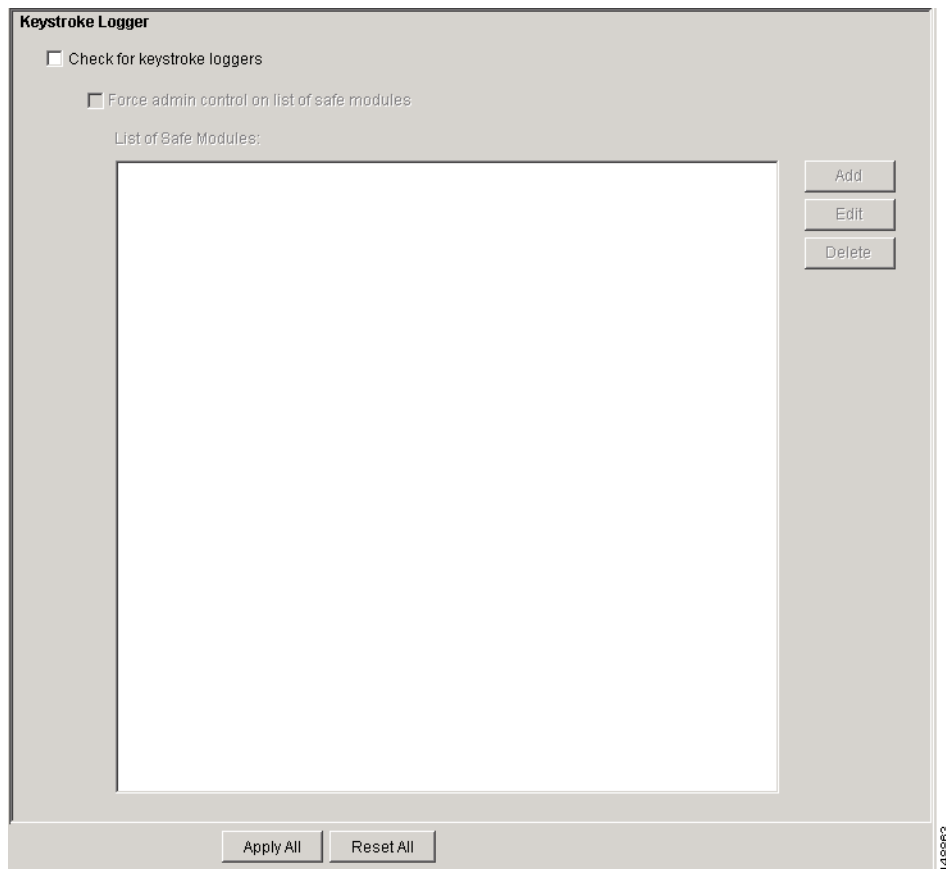
Configuring Keystroke Logger for a Location

You can configure a location type to scan for keystroke logging applications on the remote client. You can list the keystroke logging applications that are safe or let the remote user approve of the applications the scan identifies. Secure Desktop and Cache Cleaner launch only if the scan is clear, or only if you assign administrative control to the user and the user approves of the applications the scan identifies. It may not be possible for CSD to detect all keystroke loggers present, including hardware keystroke logging devices.

By default, System Detection does not scan for keystroke loggers. Configure scanning for keystroke loggers as follows:

-
- Step 1** Click **Keystroke Logger** under the name of the location you are configuring in the menu on the left. The Keystroke Logger window opens ([Figure 5-9](#)).

Figure 5-9 Keystroke Logger Window



The “List of Safe Modules” window lists the paths to program applications on the remote client that have keystroke logging capabilities, but are safe to use, as determined by the administrator. Such programs, such as Corel (previously Jasc) Paint Shop Pro, typically invoke functions when the user presses particular keystroke combinations from within another application.

- Step 2** Check **Check for keystroke loggers** to scan for a keystroke logging application on the remote client PC and make sure one is not running, before creating the Secure Desktop space on the remote client.

By default, this attribute is not checked, and the other attributes and buttons are grayed out. If you check this attribute, the “Force admin control on list of safe modules” attribute becomes active.

- Step 3** Check **Force admin control on list of safe modules** to give yourself control over which key loggers are exempt from scanning, or uncheck it to give the remote user this control.

If you check this attribute, the **Add** button become active.

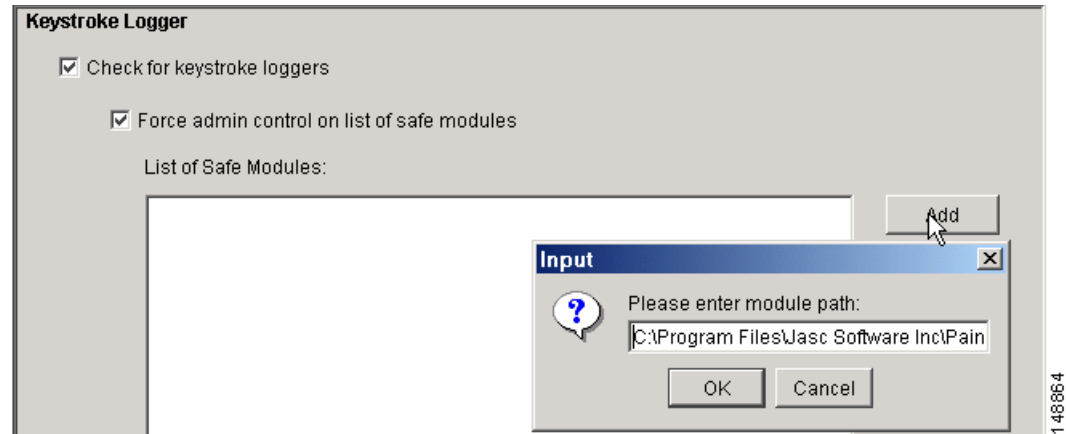
Uncheck this attribute if you want to give the remote user the right to determine if any detected keystroke logger is safe. If this attribute is unchecked, CSD lists the keystroke loggers discovered on the client computer. To access the Secure Desktop, the user must insert a check next to all of the keystroke loggers in the list to indicate they are safe. Otherwise, the user must terminate the session.



Note Unchecking this attribute deactivates but does not delete the contents of the “List of Safe Modules” window.

- Step 4** Click **Add** to specify a module as safe, or choose an entry in the List of Safe Modules window and click **Edit** if you want to modify its path.
CSDM opens the Input dialog box.

Figure 5-10 *Input (for Keystroke Logger)*



- Step 5** Type the path and name of the module or application in the **Please enter module path** field, then click **OK**.

CSDM closes the dialog box and lists the entry in the List of Safe Modules window.



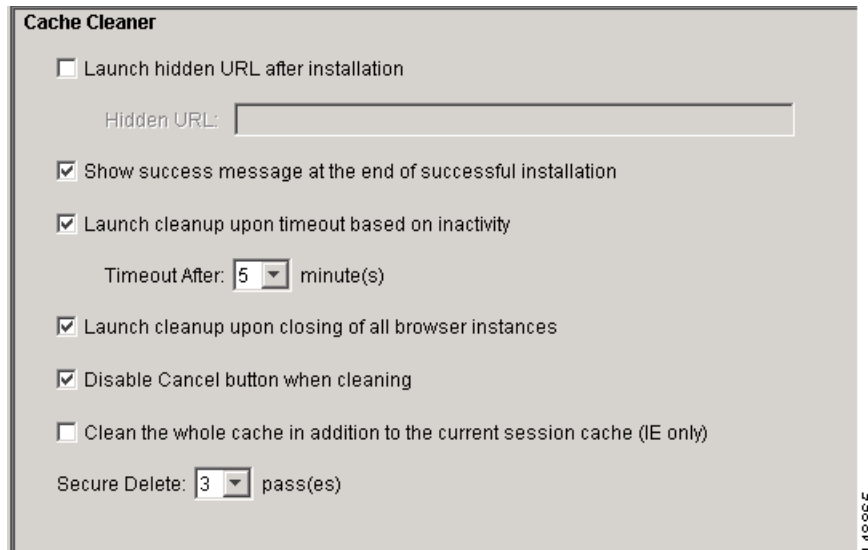
Note To remove a program from the list, click the entry in the “Path of safe modules” list, then click **Delete**.

- Step 6** Click **Apply All** to save the configuration changes.

Configuring Cache Cleaner for a Location

For each location for which the Cache Cleaner is enabled, click **Cache Cleaner** under the location you are configuring to configure Cache Cleaner for Windows. The Cache Cleaner pane appears. [Figure 5-11](#) shows the default settings.

Figure 5-11 Cache Cleaner for Windows



This window lets you configure the Cache Cleaner for the associated location only. Check the following fields as required by your security policy:

- **Launch hidden URL after installation**—Check to use a URL for administrative purposes, hidden from the remote client, so that you know that the user has the Cache Cleaner installed. For example, you could place a cookie file on the user's computer, and later check for the presence of that cookie.
- **Hidden URL**—Type the URL to use for administrative purposes, if you checked “Launch hidden URL after installation.”
- **Show success message at the end of successful installation**—Check to display a dialog box on remote client PCs informing the user when the Cache Cleaner installation is successful.
- **Launch cleanup upon timeout based on inactivity**—Check to set a specific timeout period after which the cleanup begins.
- **Timeout after**—Choose the number of minutes (1, 2, 5, 10, 15, 30, or 60) to set the timeout period if you checked the “Launch cleanup upon timeout based on inactivity” attribute. This attribute is the inactivity timer. Its default value is 5.
- **Launch cleanup upon closing of all browser instances**—Check to clean up the cache when all browser windows are closed.
- **Disable Cancel button when cleaning**—Check to prevent the remote user from canceling the deletion of the cache.
- **Clean the whole cache in addition to the current session cache (IE only)**—Check to remove data from the Internet Explorer cache upon activation, including files generated before the client's CSD session began.

- **Secure Delete**—CSD encrypts and writes the cache to the remote client’s disk. Upon termination of the Secure Desktop, CSD converts all bits occupied by the cache to all 0’s, then to all 1’s, and then to randomized 0’s and 1’s. Choose the number of times for CSD to perform this cleanup task. The default setting, 1 pass, meets the US Department of Defense (DoD) standard for securely deleting files. Following the completion of the task the number of times specified, CSD removes the pointer to the file (that is, performs a “Windows-delete”).

**Note**

Click **Apply All** to save the running CSD configuration.

Configuring Secure Desktop General for a Location

Click **Secure Desktop General** under the location name to enable or disable the Secure Desktop features and customize the user experience.

The Secure Desktop General pane appears. [Figure 5-12](#) shows the default settings.

Figure 5-12 Secure Desktop General

Check the following attributes to configure the Secure Desktop General settings for the location you are configuring, as required by your security policy:

- **Automatically switch to Secure Desktop after installation**—Check to set the Secure Desktop to load automatically after installation. This option forces users into the Secure Desktop.
- **Enable switching between Secure Desktop and Local Desktop**—We strongly recommend that you check this attribute to let users switch between Secure Desktop and the untrusted desktop. Called *desktop switching*, this feature provides users with the flexibility they might need to respond to a prompt from another application requiring an OK to let CSD continue processing. (The Cisco Secure Tunneling Client is *not* one of those applications; it is accessible on both the local desktop and the CSD.) Unchecking this attribute minimizes the potential security risk posed by a user who leaves traces on the untrusted desktop. Thus, you might choose to uncheck this option if the security

risk is a bigger issue than the deployment advantages of the alternative. Operating System limitations may prevent CSD from enforcing prevention of desktop switching, even if you disable this feature.

You can configure both the Secure Desktop component of CSD and Cisco SSL VPN Client (SVC) to run simultaneously on client PCs. If you check this attribute, the SVC connection becomes available to both.

- **Enable Vault Reuse**—Check to allow users to close the Secure Desktop and open it again at a later time. The Vault is a persistent desktop that is available from one session to the next. If you enable this option, users must enter a password (up to 127 characters in length) when CSD creates the Secure Desktop. This is useful if users are running the Secure Desktop on computers that are likely to be reused; for example, a home computer. When a user closes the Secure Desktop, CSD does not destroy the Vault. If you do not enable this option, CSD automatically destroys the Vault at the end of each Secure Desktop session.

If unchecked, this attribute activates the following two attributes.

- **Suggest application uninstall upon Secure Desktop closing**—Check to prompt the user and recommend that the Secure Desktop be uninstalled when it closes. In contrast to the option below, the user has the choice to refuse the uninstallation.



Note Leave this option disabled if you want users to be able to use the Vault. Checking this option uninstalls the Vault from the user's computer when the Secure Desktop closes.

- **Force application uninstall upon Secure Desktop closing**—Check if you do not want to leave the Secure Desktop application on untrusted computers after users are done using it. The Secure Desktop uninstalls when it closes.



Note Leave this option disabled if you want users to be able to use the Vault. Checking this option uninstalls the Vault from the user's computer when the Secure Desktop closes.

- **Enable Secure Desktop inactivity timeout**—Check to close the Secure Desktop automatically after a period of inactivity.

Because CSD runs on the client machine, it detects real inactivity and closes the Secure Desktop to avoid leaving anything behind.

If checked, this attribute activates the following attribute.

- **Timeout After**—Choose the number of minutes (1, 2, 5, 10, 15, 30, or 60) to set the timeout period if you checked the “Enable Secure Desktop inactivity timeout” attribute. This attribute is the associated inactivity timer.
- **Launch hidden URL upon Secure Desktop closing**—Check this box and enter a URL in the field to make CSD automatically open a web page when the Secure Desktop closes.
- **Secure Delete**—CSD encrypts and writes the Secure Desktop to the remote client's disk. Upon termination of the Secure Desktop, CSD converts all bits occupied by the Secure Desktop to all 0's, then to all 1's, and then to randomized 0's and 1's. Choose the number of times for CSD to perform this cleanup task. The default setting, 1 pass, meets the US Department of Defense (DoD) standard for securely deleting files. Following the completion of the task the number of times specified, CSD removes the pointer to the file (that is, performs a “Windows-delete”).

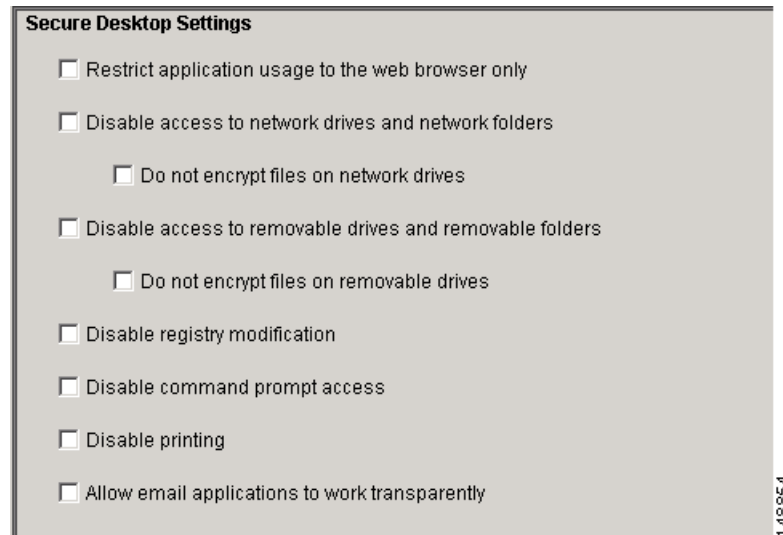


Note Click **Apply All** to save the running CSD configuration.

Configuring Secure Desktop Settings for a Location

Click **Secure Desktop Settings** under the location name to place restrictions on the Secure Desktop. The Secure Desktop Settings pane appears. [Figure 5-13](#) shows the default settings.

Figure 5-13 Secure Desktop Settings



Check the boxes to apply the associated restrictions. The restrictions are as follows:

- Restrict application usage to the web browser only—Check to let only the originating browser run on the Secure Desktop. If you choose this option, the browser that started CSD (Internet Explorer, Netscape, Firefox, etc.) is the only browser permitted to run in Secure Desktop mode. Choosing this option limits the user's ability to use other applications, but increases the level of security.
- Disable access to network drives and network folders—Check to prevent the user from accessing network resources and network drives while on the Secure Desktop. The network resources are those that use the Server Message Block (SMB) client/server, request-response protocol to share such resources as files, printers, and APIs. For maximum security, we recommend that you check this attribute. If you do, the Secure Desktop Manager dims the following attribute.
- Do not encrypt files on network drives—Check to prevent the user from saving encrypted files to drives onto the network while on the Secure Desktop. The Secure Desktop Manager dims this attribute if you check the previous attribute.
- Disable access to removable drives and removable folders—Check to prevent the user from accessing portable drives while on the Secure Desktop. Otherwise, the user can save files to a removable drive and remove the drive before closing the CSD session. After closing the CSD session, the user could forget to take the removable drive. For maximum security, we recommend that you check this attribute. If you do, the Secure Desktop Manager dims the next attribute.

This attribute applies only to the drives that Microsoft names “Removable” in the Windows Explorer “My Computer” window.

- Do not encrypt files on removable drives—Check to prevent the user from saving encrypted files onto portable drives while on the Secure Desktop. The Secure Desktop Manager dims this attribute if you check the previous attribute.

This attribute applies only to the drives that Microsoft names “Removable” in the Windows Explorer “My Computer” window.

- Disable registry modification—Check to prevent the user from modifying the registry from within the Secure Desktop. For maximum security, we recommend that you check this attribute.
- Disable command prompt access—Check to prevent the user running the DOS command prompt from within the Secure Desktop. For maximum security, we recommend that you check this attribute.
- Disable printing—Check to prevent the user from printing while using the Secure Desktop space. For maximum security of sensitive data, check this option.
- Allow email applications to work transparently—Check to let the user open e-mail while on the Secure Desktop and to prevent CSD from deleting e-mail upon the termination of the CSD session. The use of the term *transparent* means that the Secure Desktop handles e-mail the same way that the local desktop handles it. Transparent handling works for the following e-mail applications:
 - Microsoft Outlook Express
 - Microsoft Outlook
 - Eudora
 - Lotus Notes

If this attribute is checked and the remote user uses an e-mail application to save an attachment to the “My Documents” folder, it is visible from both the Secure Desktop and the local desktop. Similarly, deleting such a file from within the e-mail application running on a Secure Desktop removes the file from both desktops.



Note Deleting transparent or nontransparent files from outside of Outlook, such as from a Windows Explorer window, during a Secure Desktop session removes the file only from the Secure Desktop.

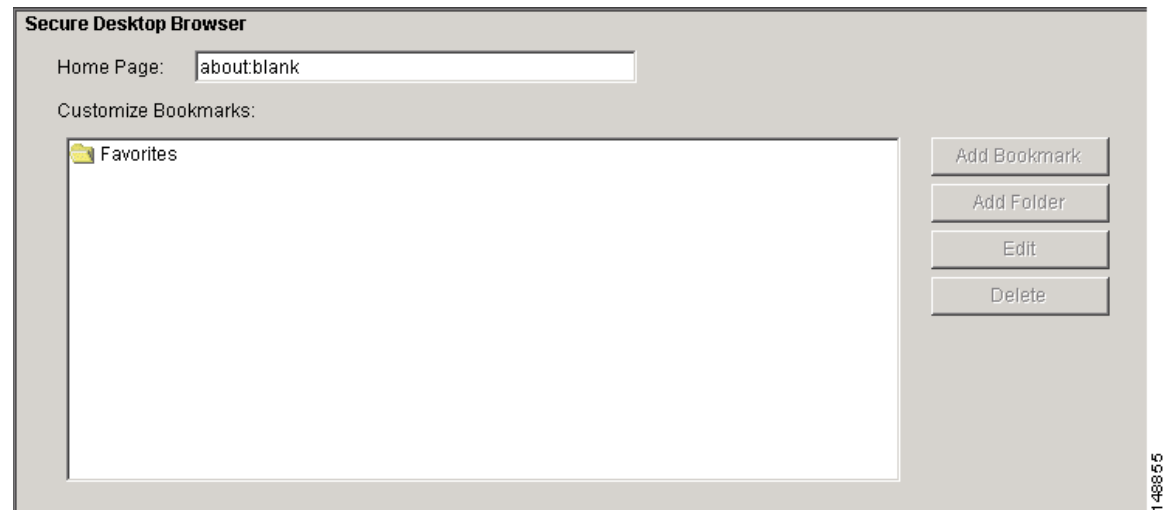
Click **Apply All** to save the running CSD configuration.

Configuring Secure Desktop Browser for a Location

Click **Secure Desktop Browser** under the location name to specify the Home Page to which the browser connects when the remote user establishes a CSD session. This option also lets you specify the folders and URLs that populate the Bookmarks or Favorites menu during the CSD session.

The Secure Desktop Browser pane appears. [Figure 5-14](#) shows the default settings.

Figure 5-14 Secure Desktop Browser



For the duration of the CSD session, the browser does not list the user's bookmarks or favorites. It lists only the ones shown in this pane.

Configure the Secure Desktop Browser as follows:

-
- Step 1** Type the URL of the page that you want to open when the remote user establishes a CSD session into the **Home Page** field.
- The Customized Bookmarks pane lists the folders and URLs that populate the browser Bookmarks or Favorites menu.
- Step 2** Use the following guidelines to add, modify, and delete entries in the Customized Bookmarks pane:
- To add a folder, choose the folder to contain it, click **Add Folder**, type the new folder in the dialog box, then click **OK**.
 - To add a bookmark to the list, choose the folder to contain it, click **Add Bookmark**, type the URL in the dialog box, then click **OK**.
 - To modify a URL, choose it, click **Edit**, type the new URL in the dialog box, then click **Edit**.
 - To remove a folder or a URL, choose it and click **Delete**.



Note

Click **Apply All** to save the running CSD configuration.

