



Tutorial

This tutorial provides an overview of the Cisco Secure Desktop configuration sequence. It does not provide detailed instructions on the attributes. The sections are as follows:

- [Tutorial Overview](#)
- [Configuring a Prelogin Assessment](#)
- [Assigning Secure Session and Cache Cleaner Settings for Each Endpoint Profile](#)
- [Assigning a DAP for Each Endpoint Profile](#)

Tutorial Overview

This tutorial describes how to configure three example prelogin policies: “Secure,” “Home,” and “Public.” “Secure” is for those connecting to the VPN from a workstation in the office, “Home” is for those working from home, and “Public” is for those who do not meet the criteria for either, such as those connecting from a cybercafé.



Note

This tutorial is only an example; we recommend that you choose profile names and configuration settings in your actual deployment that reflect your VPN security policies.

In this tutorial, “Secure” provides clients with full access, “Home” provides some flexibility, and “Public” requires restricts access. This tutorial defines the prelogin policies as follows:

- Secure
 - Assign a prelogin assessment to recognize a corporate computer attempting to establish a VPN connection by verifying the OS is Microsoft Windows, that the IP address is within a specified range, and that the computer has a specified registry entry.
 - Disable Secure Desktop (Secure Session) and Cache Cleaner.
 - Use the dynamic access policy (DAP) configuration to assign access rights.
- Home
 - Identify using a certificate given by the administrator and a file check.
 - Enable Secure Desktop (Secure Session) and Vault Reuse with no timeout.

Vault Reuse lets users close the Secure Session and open it again at a later time, creating 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) before the establishment of a Secure Session.

- Advanced features require company antivirus software, company antispysware, company firewall, and Windows 2000 Service Pack 4 or Windows XP.
- Check for keystroke logger.
- Use the DAP configuration to assign access rights.
- Public profile
 - Check for malware file.
 - Check for keystroke logger file.
 - Install Cache Cleaner.
 - Use the DAP configuration to assign access rights.

Our example includes “Secure,” “Home,” and “Public” in that order; to assign privileges to a host, Cisco Secure Desktop first determines whether it is a “Secure” host. If it is not, it determines whether it is a “Home” host. If it is not, it performs several file checks and assigns the privileges associated with the “Public” endpoint profile.

Configuring a Prelogin Assessment

These instructions assume that Secure Desktop Manager has loaded the default configuration. To reload the default configuration, rename the sdesktop/data.xml file, disable Cisco Secure Desktop, re-enable it, exit ASDM, then start a new ASDM session.

Use the following sections to configure the prelogin assessment and assign names to the prelogin policies:

- [Configuring an Endpoint Profile and Prelogin Assessment for a Secure Computer](#)
- [Configuring an Endpoint Profile and Prelogin Assessment for a Home Computer](#)
- [Configuring an Endpoint Profile and Prelogin Assessment for a Public Computer](#)

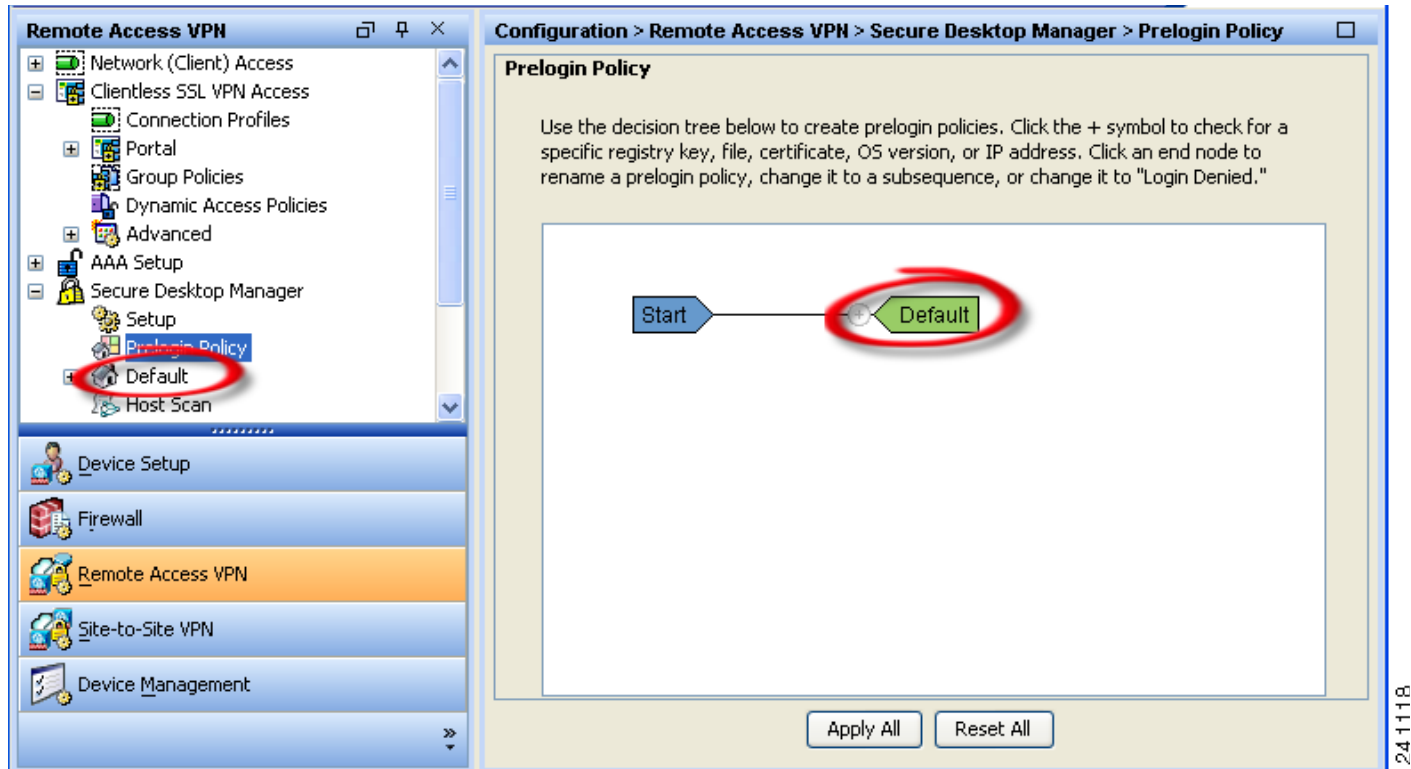
Configuring an Endpoint Profile and Prelogin Assessment for a Secure Computer

Use the following instructions to create an example endpoint profile named “Secure” and assign a prelogin assessment to qualify PCs attempting remote access VPN connections:

Step 1 Choose **Prelogin Policy**.

The Prelogin Policy pane shows the default endpoint profile named “Default.” The menu shows the same profile name, indicating the place where you assign settings to that profile ([Figure A-1](#)).

Figure A-1 Duplication of the Prelogin Policy Name in the Menu

**Tip**

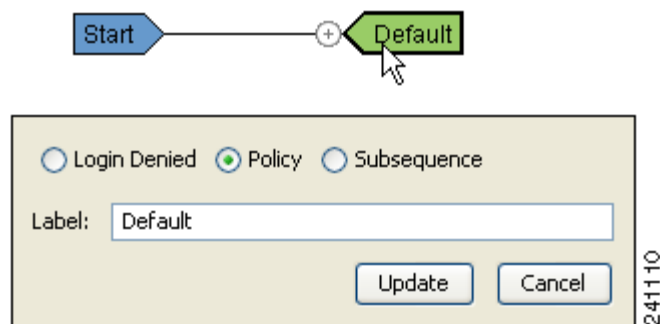
If you would like to explore the options available in the prelogin assessment sequence editor without making permanent changes to the Cisco Secure Desktop configuration file, make the changes, then choose an ASDM option outside the Secure Desktop Manager menu, and click **Discard Changes**.

Step 2 Click the end node named **Default**.

This end node represents an endpoint profile. Note that Secure Desktop Manager displays the name of this end node in its menu.

Secure Desktop Manager inserts a window that lets you change the type and name of the end node (Figure A-2).

Figure A-2 Change End Node Window



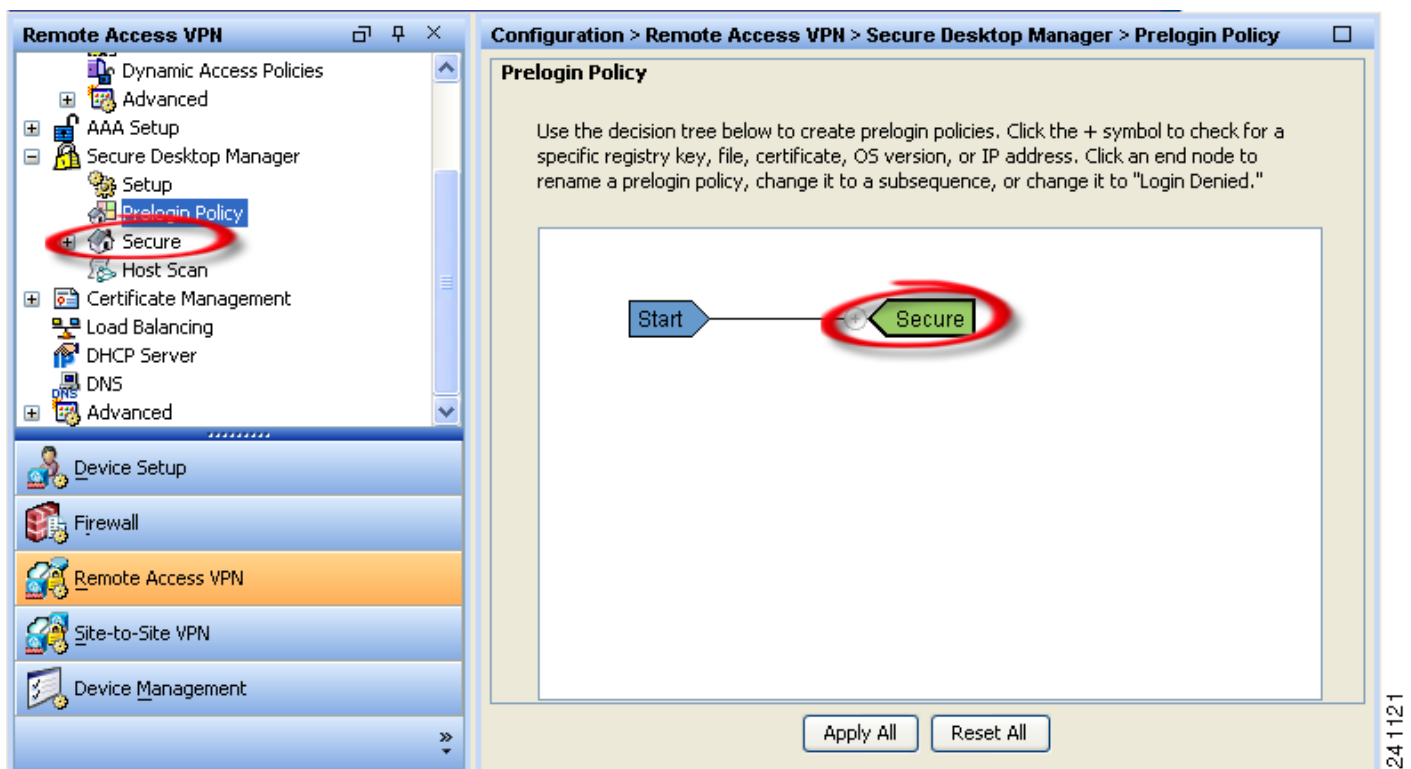
Note that the Policy option is already selected. In this case, you only need to change the name.

Step 3 Replace the name Default in the text box with the name Secure.

Step 4 Click **Update**.

Secure Desktop Manager closes the change end node window, and changes both the name of the end node and the associated menu option in the Secure Desktop Manager menu (Figure A-3).

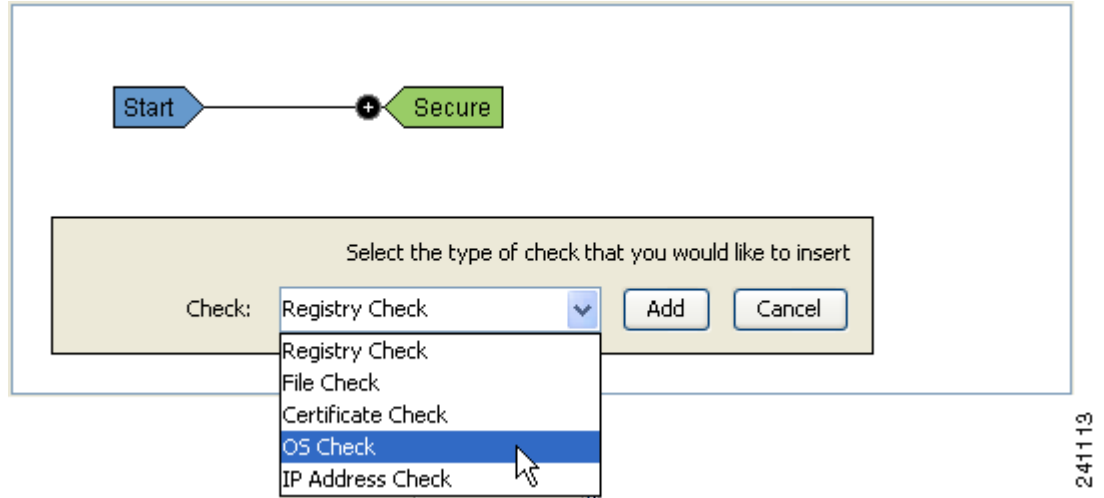
Figure A-3 Default Policy Name Changed to Secure



Step 5 Click the plus sign in the diagram.

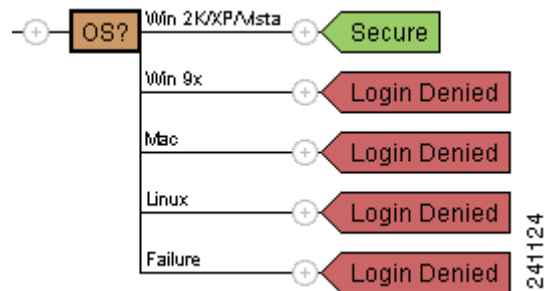
A window opens below the diagram, prompting you to select the type of check to be inserted (Figure A-4).

Figure A-4 Prelogin Assessment Options



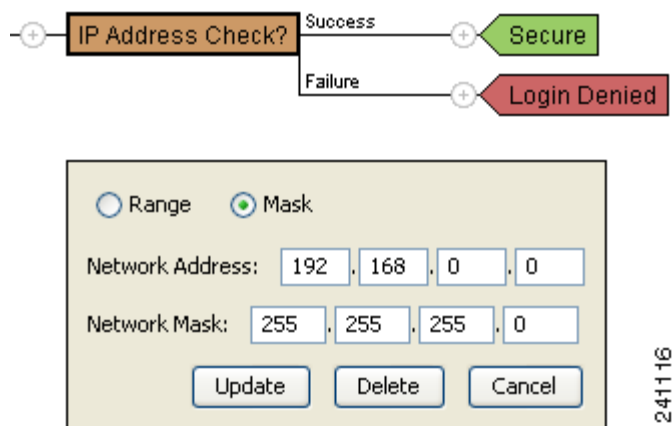
- Step 6** Choose **OS Check** and click **Add**.
Secure Desktop Manager inserts the OS check node into the diagram (Figure A-5).

Figure A-5 OS Check



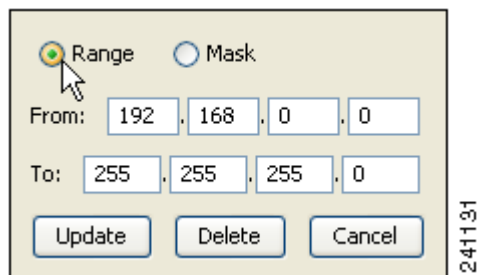
- Step 7** Click the plus sign to the left of the Secure node.
- Step 8** Select **IP Address Check** and click **Add**.
Secure Desktop Manager inserts the IP Address Check node and opens the IP address check window below the diagram. Figure A-6 shows the default Mask attributes in the IP address check window.

Figure A-6 IP Address Check (Default Mask Attributes Displayed)



- Step 9** Click **Range** to change the type of IP address check. Secure Desktop Manager changes the attributes in the IP address check window (Figure A-7).

Figure A-7 Range Attributes in the IP Address Check Window



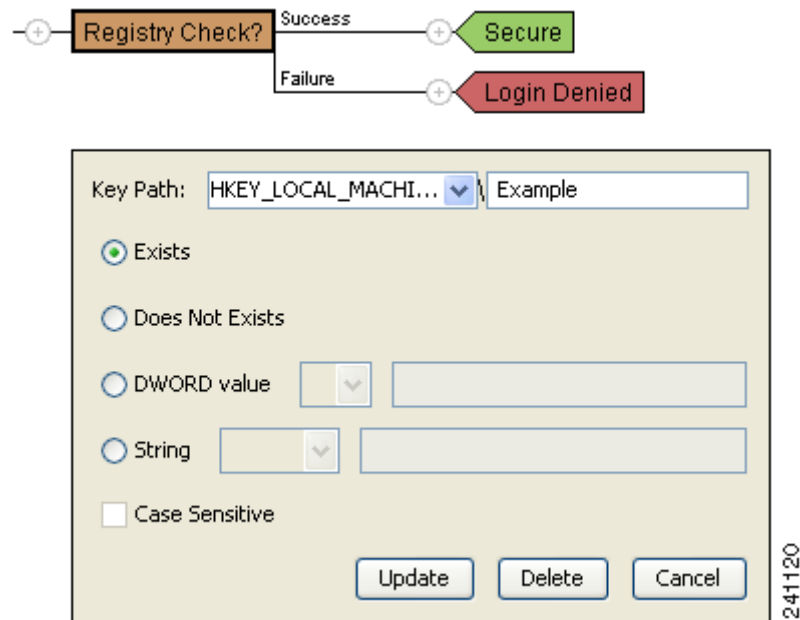
- Step 10** Enter the IP address range and subnet mask, then click **Update**.

- Step 11** Click the plus sign to the left of the Secure node.

- Step 12** Select **Registry Check** and click **Add**.

Secure Desktop Manager inserts the Registry Check node and opens the Registry check window below the diagram (Figure A-8).

Figure A-8 Registry Check



Note The prelogin assessment ignores registry checks if the computer is running Mac OS or Linux.

- Step 13** Select an option next to the Key Path drop-down menu such as HKEY_LOCAL_MACHINE,” type the string to indicate the remainder or the path such as “SOFTWARE\Company-Name,” select a radio button such as Exists, and click **Update**.

This step completes the instructions for creating checks for the example Secure node.

Configuring an Endpoint Profile and Prelogin Assessment for a Home Computer

Use the following instructions to create an example endpoint profile named “Home” and assign a prelogin assessment to qualify Windows computers for a Secure Session installation. The prelogin assessment verifies the presence of a certificate given by the administrator to users who connect from home and verifies the presence or absence of a specific file. Complete the example prelogin assessment for home computers as follows:



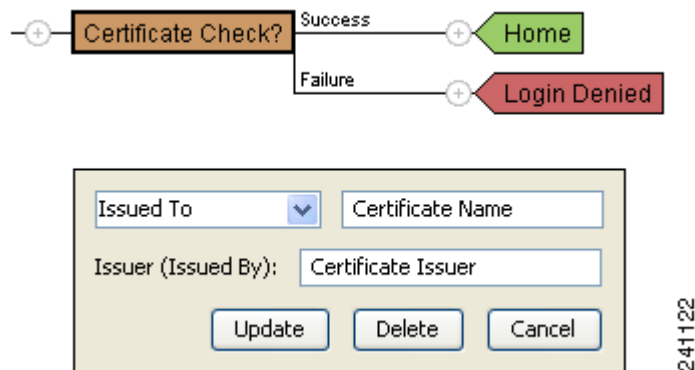
Note These instructions assume you have followed the instructions in the previous section.

- Step 1** Choose **Prelogin Policy**.
- Step 2** Click the Login Denied end node that follows the IP Address Failure branch.
Secure Desktop Manager inserts a window that lets you change the type and name of the end node.
- Step 3** Click the Subsequence radio button, replace the text in the box with the name Home Check, and click **Update**.
Secure Desktop Manager inserts a window that lets you change the type and name of the end node.

- Step 4** Scroll to the Home Check node on the left side of the diagram and click the Login Denied end node to its right.
- Step 5** Click the **Policy** radio button and replace the text in the box with the word Home.
- Step 6** Click the plus sign to the left of the end node labeled Home.
- Step 7** Select **Certificate Check**, and click **Add**.

Secure Desktop Manager inserts the Certificate Check node and opens the Certificate check window below the diagram (Figure A-9).

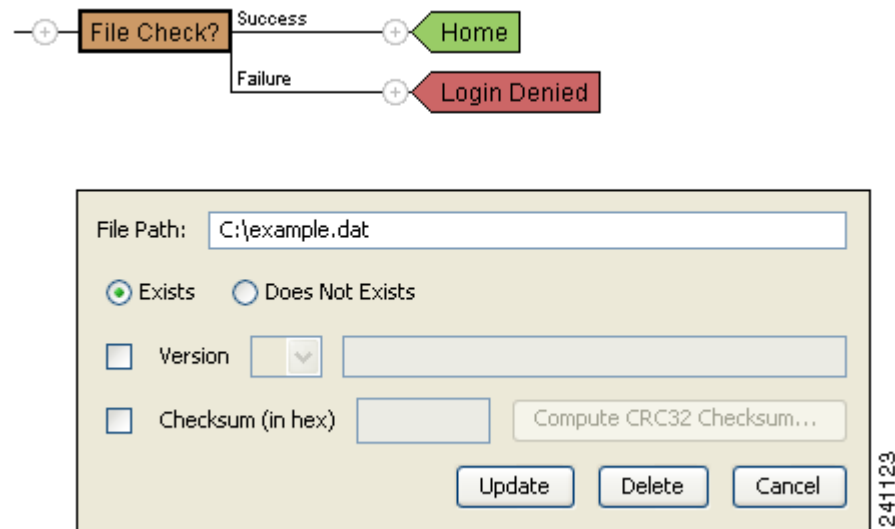
Figure A-9 Certificate Check



Note The prelogin assessment ignores certificate checks if the computer is running Mac OS or Linux.

- Step 8** Select an option from the drop-down box to specify the certificate field to be checked, enter the value of the field to match in the adjacent text box, enter the issuer of the certificate into the Issuer text field, and click **Update**.
- For each additional field of a single certificate that you want to match, create another prelogin check that specifies that field and value.
- Step 9** Click the plus sign to the left of the end node labeled Home.
- Step 10** Select **File Check** and click **Add**.
- Secure Desktop Manager inserts the File Check node and opens the File check window below the diagram (Figure A-10).

Figure A-10 File Check



- Step 11** Enter a path to the file in the drop-down box, select a radio button such as **Exists**, and click **Update**.



Note Secure Desktop Manager retains the case of the text you enter to check for a path to a file on the remote device. The match results are case-sensitive only if the devices are running Mac OS or Linux. The Microsoft Windows file system is not case-sensitive.

- Step 12** Repeat Steps 9–10 to insert an additional file check.

This step completes the instructions for creating checks for the example Secure node. Continue with the next section to create the checks for the example Home node.

Configuring an Endpoint Profile and Prelogin Assessment for a Public Computer

Use the following instructions to create an example endpoint profile named “Public” and assign a prelogin assessment to qualify Windows computers for a Cache Cleaner installation.

These instructions say to add several prelogin file checks to qualify a Windows computer for Cache Cleaner, however, you can use any prelogin checks, or replace any Login Denied end node with a “Public” end node if you do not want to require a match.



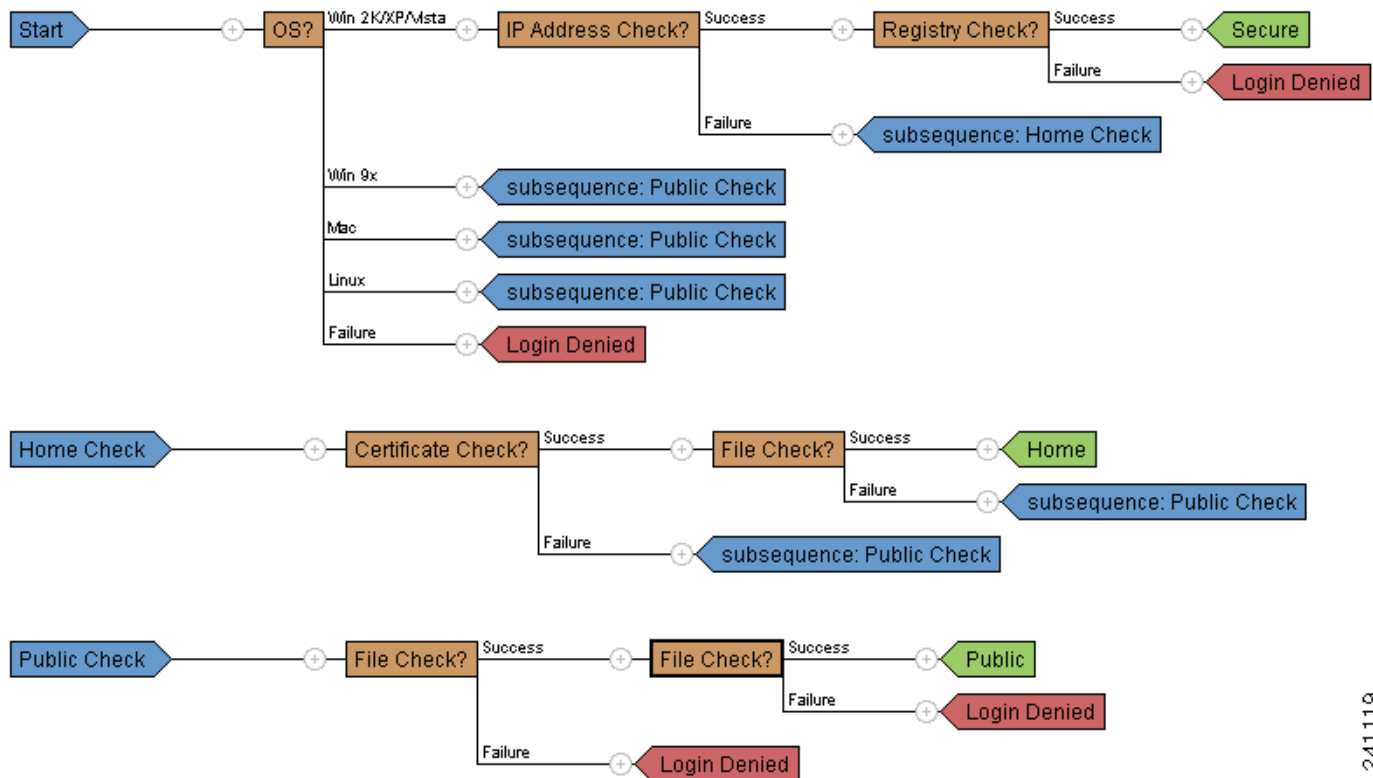
Note These instructions assume you have followed the instructions in the previous sections.

- Step 1** Choose **Prelogin Policy**.
- Step 2** Click the Login Denied end node that follows the Win 9x branch.
- Step 3** Click the Subsequence radio button, replace the text in the box with the name Public Check, and click **Update**.
- Step 4** Change the Login Denied end nodes that follow the IP Address Check, Certificate Check, and File check boxes to a subsequence end node, also named Public Check.

- Step 5** Scroll to the Public Check node on the left side of the diagram and click the Login Denied end node to its right.
- Step 6** Click the **Policy** radio button and replace the text in the box with the word Public.
- Step 7** Insert two File Checks to the left of the Public end node.

This step completes the configuration of the example prelogin assessment. The diagram of your prelogin assessment should look like the one shown in [Figure A-11](#).

Figure A-11 Example Prelogin Configuration



24119

Continue with the next section to assign the Secure Session and Cache Cleaner settings appropriate for each endpoint profile.

Assigning Secure Session and Cache Cleaner Settings for Each Endpoint Profile

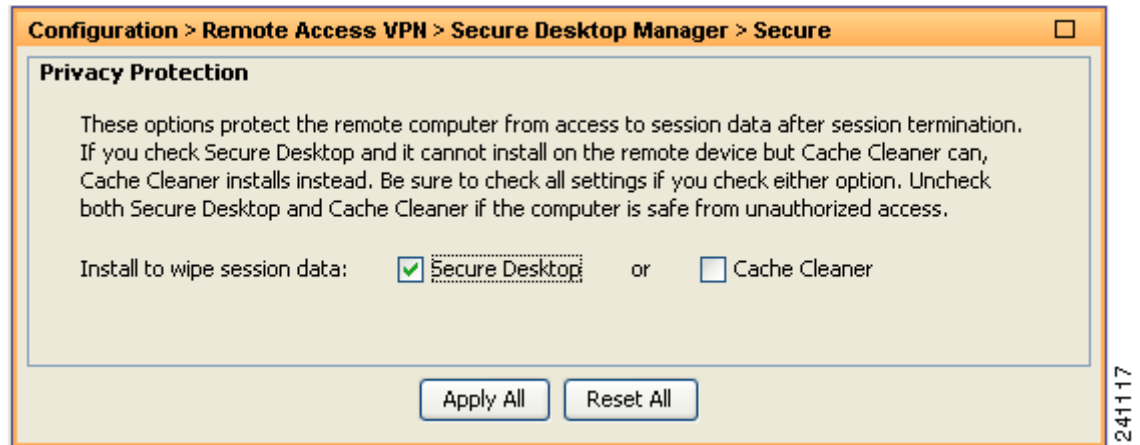
The following sections describe how to enable or disable Secure Desktop (Secure Session) and Cache Cleaner for each endpoint profile and how to configure scanning for keystroke loggers:

- [Enabling or Disabling Secure Session and Cache Cleaner](#)
- [Configuring Keystroke Logger Scanning](#)

Enabling or Disabling Secure Session and Cache Cleaner

For each endpoint profile, click the name of the endpoint profile in the Secure Desktop menu. The Privacy Protection pane opens. [Figure A-12](#) shows the default settings for each endpoint profile.

Figure A-12 Privacy Protection



This window lets you specify whether to run Secure Session or Cache Cleaner on the remote desktops of computers that match the criteria associated with the selected profile.



Note

If you check Secure Desktop, make sure that both the Secure Desktop and Cache Cleaner settings are appropriate for this policy. Cache Cleaner serves as a fall-back security solution for operating systems that Secure Session does not support.

See [Table A-1](#) to check or uncheck Secure Desktop or Cache Cleaner.

Table A-1 Privacy Protection—Sample Values

| Action and Attribute | Endpoint Profile | | |
|-----------------------|------------------|------|--------|
| | Secure | Home | Public |
| Check Secure Desktop? | No | Yes | — |
| Check Cache Cleaner? | No | — | Yes |

Configuring Keystroke Logger Scanning

By default, keystroke logger scanning is disabled. Keep it disabled for the Secure endpoint profile. Configure scanning for keystroke loggers once for the Home endpoint profile and once for the Public profile, as follows:

- Step 1** Click **Keystroke Logger & Safety Checks** under the name of the endpoint profile you are configuring in the menu on the left.

The Keystroke Logger window opens ([Figure A-13](#)).

Figure A-13 Keystroke Logger & Safety Checks

Configuration > Remote Access VPN > Secure Desktop Manager > Secure > Keystroke Logger & Safety Checks

Keystroke Logger & Safety Checks

If you check "Force admin control" and an unapproved keystroke logger is detected, the Cisco Secure Desktop module (that is, Secure Desktop, Cache Cleaner, or Host Scan) does not install on the remote device. Likewise, if you check "Always deny access" and a host emulator is detected, the Cisco Secure Desktop module does not install on the remote device.

Check for keystroke loggers

Force admin control on list of safe modules

List of Safe Modules:

Check for host emulation

Always deny access if running within emulation

Buttons: Add, Edit, Delete, Apply All, Reset All

241108

See [Table A-2](#) to check the attributes in this window.

Table A-2 Keystroke Logger & Safety Checks—Example Values

| Action and Attribute | Endpoint Profile | | |
|---|------------------|------|--------|
| | Secure | Home | Public |
| Check for keystroke loggers | No | Yes | Yes |
| Check Force Admin control on list of safe module? | — | No | Yes |
| Populate List of Save Modules? | — | — | Yes |
| Check for host emulation? | No | Yes | Yes |
| Check Always deny access if running within emulation? | — | — | Yes |

- Step 2** Check **Check for keystroke loggers** to scan for a keystroke logging application on the remote PC and make sure one is not running, before creating the Secure Session 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 specify which key loggers are exempt from scanning, or uncheck it to let the remote user decide.
- 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, the Cisco Secure Desktop installer lists the keystroke loggers discovered on the client computer. To access Secure Session, 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.
- Cisco Secure Desktop Manager opens the Input dialog box.
- Step 5** Type the path and name of the module or application in the **Please enter module path** field, then click **OK**.
- Cisco Secure Desktop Manager 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**.

Assigning a DAP for Each Endpoint Profile



Note These instructions assume you have followed the instructions in the previous sections of this tutorial.

Configure a dynamic access policy (DAP) to support an endpoint profile as follows:

- Step 1** Choose **Configuration > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies > Add** or **Edit**.
- The Add or Edit Dynamic Policy window opens ([Figure A-14](#)).

Figure A-14 Add Dynamic Access Policy

Policy Name:

Description: Priority:

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values... and the following endpoint attributes are satisfied.

| AAA Attribute | Operation/Value |
|---------------|-----------------|
| | |

| Endpoint ID | Name/Operation/Value |
|-------------|----------------------|
| | |

Advanced

Access Policy Attributes

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.

Action: Continue Terminate

Specify the message that will be displayed when this record is selected.

User Message:

241114

- Step 2** Move the mouse to the right of the Endpoint Attribute table and click **Add**.
The Add Endpoint Attribute window opens (Figure A-15).

Figure A-15 Add Endpoint Attribute

Step 3 Select **Policy** from the drop-down list next to the **Endpoint Attribute Type**.

Step 4 Select the name of the prelogin policy from the drop-down list.

Step 5 Click **OK**.

The Add or Edit Endpoint Attribute window closes, leaving the Add or Edit Dynamic Policy window open.

Step 6 For each entry in the Basic Host Scan table, click **Add** to the right of the Endpoint Attribute table. Select the type (Registry, File, or Process) next to the Endpoint Attribute Type attribute, enter the unique ID of the entry in the Endpoint ID box, and click **OK**.

Step 7 For each antispymware, antivirus, and personal firewall application you would like to require as part of the DAP, click **Add** to the right of the Endpoint Attribute table. Select the type (Antispymware, Antivirus, or Personal Firewall) next to the Endpoint Attribute Type attribute, select the company and application, and click **OK**.

Step 8 Use the Add or Edit Dynamic Policy window to name and prioritize the DAP entry, complete the configuration of any other selection criteria, and specify the access policy attributes, then click **OK**.

