Managing Dynamic Access Policies for Remote Access VPNs (ASA 8.0+ Devices)

This chapter explains Dynamic Access Policies (DAP) for assigning remote access users to connection profiles (tunnel groups). You can configure these policies for remote access IKEv1 IPsec on ASA 8.0+ devices, IKEv2 IPsec on ASA 8.4(x) devices, and SSL VPNs on ASA 8.0+ (except 8.5) devices.

For information on configuring other remote access policies for ASA and PIX 7.0+ devices, see Chapter 31, "Managing Remote Access VPNs on ASA and PIX 7.0+ Devices".

This chapter contains the following topics:

Understanding Dynamic Access Policies

Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.

Dynamic access policies (DAP) on a security appliance let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session. The DAP system includes the following components that require your attention:

- DAP Selection Configuration File—A text file containing criteria that the security appliance uses for selecting and applying DAP records during session establishment. It is stored on the security appliance. You can use Security Manager to modify it and upload it to the security appliance in XML data format. DAP selection configuration files include all of the attributes that you configure. These can include AAA attributes, endpoint attributes, and access policies as configured in network and web-type ACL filter, port forwarding, and URL lists.

- DfltAccess Policy—Always the last entry in the DAP summary table, always with a priority of 0. You can configure Access Policy attributes for the default access policy, but it does not contain—and you cannot configure—AAA or endpoint attributes. You cannot delete the DfltAccessPolicy, and it must be the last entry in the summary table.

Tip Dynamic Access policies take precedence over Group policies. If a setting is not specified in a Dynamic Access policy, an ASA device checks for Group policies that specify the setting.

Integration of Cisco Secure Desktop with DAP

The security appliance integrates the Cisco Secure Desktop (CSD) features into dynamic access policies (DAPs). Depending on the configuration, the security appliance uses one or more endpoint attribute values in combination with optional, AAA attribute values as conditions for assigning a DAP. The Cisco Secure Desktop features supported by the endpoint attributes of DAPs include OS detection, prelogin policies, Basic Host Scan results, and Endpoint Assessment.

As an administrator, you can specify a single attribute or combine attributes that together form the conditions required to assign a DAP to a session. The DAP provides network access at the level that is appropriate for the endpoint AAA attribute value. The security appliance applies a DAP when all of its configured endpoint criteria are satisfied.

Related Topics

- Configuring Dynamic Access Policies, page 32-2
- Configuring DAP Attributes, page 32-7

Configuring Dynamic Access Policies

This procedure describes how to create or edit a dynamic access policy.

Related Topics

- Understanding Dynamic Access Policies, page 32-1
- Understanding DAP Attributes, page 32-4
- Configuring Cisco Secure Desktop Policies on ASA Devices, page 32-9

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > Dynamic Access** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Dynamic Access (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Dynamic Access page opens. For a description of the elements on this page, see Dynamic Access Page (ASA), page 32-11.

Step 2 Click **Create** or select a policy in the table and click **Edit**.

The Add/Edit Dynamic Access Policy dialog box opens, with the Main tab open by default. For a description of the elements in this dialog box, see Table 32-4 on page 32-13.

Step 3 Enter the name of the DAP record (up to 128 characters).

Step 4 Specify a priority for the DAP record. The security appliance applies access policies in the order you set here, highest number having the highest priority.

Step 5 Enter a description for the DAP record.

Step 6 In the **Main** tab, configure the DAP attributes and the type of remote access method supported by the DAP system on your security appliance. For a detailed description of the elements on this tab, see Table 32-5 on page 32-14.

a. Click **Create** below the table, or select a DAP entry in the table and click **Edit**. The Add/Edit DAP Entry dialog box opens. For a description of the elements on this dialog box, see Add/Edit DAP Entry Dialog Box, page 32-21.

   For a full description of the procedure to define the DAP attributes, see Configuring DAP Attributes, page 32-7.

b. Select the type of remote access permitted by the DAP system.

c. Select the **Network ACL** tab to select and configure network ACLs to apply to this DAP record. Beginning with Security Manager version 4.10, you can select Unified ACL entries in addition to Extended entries.

   This tab is available only if you selected an access method other than Web Portal.

d. Select the **WebType ACL** tab to select and configure Web-type ACLs to apply to this DAP record.

   This tab is available only if you selected an access method other than AnyConnect Client.

e. Select the **Functions** tab to configure file server entry and browsing, HTTP proxy, and URL entry for the DAP record.

   This tab is available only if you selected an access method other than AnyConnect Client.

f. Select the **Port Forwarding** tab to select and configure port forwarding lists for user sessions.

   This tab is available only if you selected an access method other than AnyConnect Client.

g. Select the **Bookmark** tab to select and configure URL lists for user sessions.

   This tab is available only if you selected an access method other than AnyConnect Client.

h. Select the **Action** tab to configure the type of remote access permitted.

   This tab is available for all types of access methods.

i. Select the **AnyConnect** tab to choose if the setting for Always-On VPN on the AnyConnect service profile remains unchanged, is disabled, or the AnyConnect Profile Setting must be used. Always-On VPN enables AnyConnnect to automatically establish a VPN session after you log onto the system.

j. Select the **Custom Attributes** tab to add AnyConnect Custom Attributes.

   This tab is available only if you selected the access method as Unchanged, AnyConnect Client, Both Default Web Portal, or Both Default Anyconnect Client. For information about how to add AnyConnect Custom Attributes, see Add/Edit AnyConnect Custom Attribute Dialog Box, page 31-70.

Step 7 Select the **Logical Operations** tab to create multiple instances of each type of endpoint attribute. For a description of the elements on this tab, see Table 32-22 on page 32-43.

Step 8 Select the **Advanced Expressions** tab to set additional attributes for the DAP using free-form LUA. For a description of the elements on this tab, see Table 32-23 on page 32-45.

Step 9 Click **OK**.

Understanding DAP Attributes

DAP records include all of the attributes that you configure. These can include AAA attributes, endpoint attributes, and access policies as configured in network and web-type ACL filter, port forwarding and URL lists.

DAP and AAA Attributes

DAP complements AAA services. It provides a limited set of authorization attributes that can override those AAA provides. The security appliance selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The security appliance can select multiple DAP records depending on this information, which it then aggregates to create DAP authorization attributes.

You can specify AAA attributes from the Cisco AAA attribute hierarchy, or from the full set of response attributes that the security appliance receives from a RADIUS or LDAP server.

AAA Attribute Definitions

Table 32-1 on page 32-4 defines the AAA selection attribute names that are available for DAP use. The Attribute Name field shows you how to enter each attribute name in a LUA logical expression, which you might do on the Advanced tab of the Add/Edit Dynamic Access Policy dialog box.

Table 32-1 AAA Attribute Definitions

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Cisco	aaa.cisco.memberof	AAA	string	128	memberof value
	aaa.cisco.username	AAA	string	64	username value
	aaa.cisco.class	AAA	string	64	class attribute value
	aaa.cisco.ipaddress	AAA	number	–	framed-ip address value
	aaa.cisco.tunnelgroup	AAA	string	64	tunnel-group name
LDAP	aaa.ldap.<label>	LDAP	string	128	LDAP attribute value pair
RADIUS	aaa.radius.<number>	RADIUS	string	128	Radius attribute value pair

DAP and Endpoint Security

The security appliance obtains endpoint security attributes by using posture assessment methods that you configure. These include Cisco Secure Desktop and NAC. You can use a match of a prelogin policy, Basic Host Scan entry, Host Scan Extension, or any combination of these and any other policy attributes to assign access rights and restrictions. At minimum, configure DAPs to assign to each prelogin policy and Basic Host Scan entry.

Endpoint Assessment, a Host Scan extension, examines the remote computer for a large collection of antivirus and antispyware applications, associated definitions updates, and firewalls. You can use this feature to combine endpoint criteria to satisfy your requirements before the security appliance assigns a specific DAP to the session.

DAP and Anti-Virus, Anti-Spyware, and Personal Firewall Programs

The security appliance uses a DAP policy when the user attributes matches the configured AAA and endpoint attributes. The Prelogin Assessment and Host Scan modules of Cisco Secure Desktop return information to the security appliance about the configured endpoint attributes, and the DAP subsystem uses that information to select a DAP record that matches the values of those attributes. Most, but not all, anti-virus, anti-spyware, and personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running. Host Scan checks to see if an endpoint has a program installed, and if it is memory-resident as follows:

- If the installed program does not support active scan, Host Scan reports the presence of the software. The DAP system selects DAP records that specify the program.
- If the installed program does support active scan, and active scan is enabled for the program, Host Scan reports the presence of the software. Again the security appliance selects DAP records that specify the program.
- If the installed program does support active scan and active scan is disabled for the program, Host Scan ignores the presence of the software. The security appliance does not select DAP records that specify the program. Further, the output of the **debug trace** command, which includes a lot of information about DAP, does not indicate the program presence, even though it is installed.

Endpoint Attribute Definitions

Table 32-2 on page 32-5 defines the endpoint selection attribute names that are available for DAP use. The Attribute Name field shows you how to enter each attribute name in a LUA logical expression, which you might do on the Advanced tab of the Add/Edit Dynamic Access Policy dialog box. The *label* variable identifies the application, filename, process, or registry entry.

Table 32-2 Endpoint Attribute Definitions

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Antispyware (Requires Cisco Secure Desktop)	endpoint.as.label.exists	Host Scan	true	–	Antispyware program exists
	endpoint.as.label.version		string	32	Antispyware description
	endpoint.as.label.description		string	128	class attribute value
	endpoint.as.label.lastupdate		integer	–	Seconds since update of antispyware definitions
Antivirus (Requires Cisco Secure Desktop)	endpoint.av.label.exists	Host Scan	true	–	Antivirus program exists
	endpoint.av.label.version		string	32	Antivirus description
	endpoint.av.label.description		string	128	class attribute value
	endpoint.av.label.lastupdate		integer	–	Seconds since update of antivirus definitions

Table 32-2 Endpoint Attribute Definitions (continued)

Application	endpoint.application.clienttype	Application	string	–	Client type: CLIENTLESS ANYCONNECT IPSEC L2TP
File	endpoint.file.label.exists	Secure Desktop	true	–	The files exists
	endpoint.file.label.last modified		integer	–	Seconds since file was last modified
	endpoint.file.label.crc.32		integer	–	CRC32 hash of the file
NAC	endpoint.nac.status	NAC	string	-	User defined status string
Operating System	endpoint.os.version	Secure Desktop	string	32	Service pack for Windows
	endpoint.os.servicepack		integer	–	Operating system
Personal firewall (Requires Secure Desktop)	endpoint.fw.label.exists	Host Scan	true	–	The personal firewall exists
	endpoint.fw.label.version		string	32	Version
	endpoint.fw.label.description		string	128	Personal firewall description
Policy	endpoint.policy.location	Secure Desktop	string	64	Location value from Cisco Secure Desktop
Process	endpoint.process.label.exists	Secure Desktop	true	–	The process exists
	endpoint.process.label.path		string	255	Full path of the process
Registry	endpoint.registry.label.type	Secure Desktop	dword string	–	dword
	endpoint.registry.label.value		string	255	Value of the registry entry
VLAN	endpoint.vlan.type	CNA	sting	–	VLAN type: ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

About Advanced Expressions for AAA or Endpoint Attributes

In the text box you enter free-form LUA text that represents AAA and/or endpoint selection logical operations. ASDM does not validate text that you enter here; it just copies this text to the DAP policy file, and the security appliance processes it, discarding any expressions it cannot parse.

This option is useful for adding selection criteria other than what is possible in the AAA and endpoint attribute areas above. For example, while you can configure the security appliance to use AAA attributes that satisfy any, all, or none of the specified criteria, endpoint attributes are cumulative, and must all be satisfied. To let the security appliance employ one endpoint attribute or another, you need to create appropriate logical expressions in LUA and enter them here.

Examples of DAP Logical Expressions

Study these examples for help in creating logical expressions in LUA.

- This AAA LUA expression tests for a match on usernames that begin with "b". It uses the string library and a regular expression:

```
not(string.find(aaa.cisco.username, "^b") == nil)
```

- This endpoint expression tests for a match on CLIENTLESS OR CVC client types:

```
endpoint.application.clienttype=="CLIENTLESS" or endpoint.application.clienttype=="CVC"
```

- This endpoint expression tests for Norton Antivirus versions 10.x but excludes 10.5.x:

```
(endpoint.av.NortonAV.version > "10" and endpoint.av.NortonAV.version < "10.5") or
endpoint.av.NortonAV.version > "10.6"
```

DAP Connection Sequence

The following sequence outlines a typical remote access connection establishment.

1. A remote client attempts a VPN connection.
2. The security appliance performs posture assessment, using configured NAC and Cisco Secure Desktop Host Scan values.
3. The security appliance authenticates the user via AAA. The AAA server also returns authorization attributes for the user.
4. The security appliance applies AAA authorization attributes to the session, and establishes the VPN tunnel.
5. The security appliance selects DAP records based on the user AAA authorization information and the session posture assessment information.
6. The security appliance aggregates DAP attributes from the selected DAP records, and they become the DAP policy.
7. The security appliance applies the DAP policy to the session.

Related Topics

- Configuring Dynamic Access Policies, page 32-2
- Understanding Dynamic Access Policies, page 32-1
- Configuring DAP Attributes, page 32-7

Configuring DAP Attributes

The attributes you must define for a DAP policy include specifying the authorization attributes and endpoint attributes. You can also configure network and webtype ACLs, file browsing, file server entry, HTTP proxy, URL entry, port forwarding lists and URL lists.

This procedure describes how to create or edit the AAA and endpoint attributes required for a DAP policy.

Related Topics

- Understanding DAP Attributes, page 32-4
- Understanding Dynamic Access Policies, page 32-1
- Configuring Dynamic Access Policies, page 32-2

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > Dynamic Access** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Dynamic Access (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Dynamic Access page opens. For a description of the elements on this page, see Dynamic Access Page (ASA), page 32-11.

Step 2 Click **Create** on the Dynamic Access policy page, or select the row of a policy in the table on the page, and click **Edit**.

The Add/Edit Dynamic Access Policy dialog box opens, displaying the Main tab. For a description of the elements on the Main tab, see Main Tab, page 32-14.

Step 3 Click **Create** below the table, or select a DAP entry in the table and click **Edit**. The Add/Edit DAP Entry dialog box opens. For a description of the elements on this dialog box, see Add/Edit DAP Entry Dialog Box, page 32-21.

Step 4 Select the attribute type from the Criterion list, then enter the appropriate values. The dialog box values vary based on your selection. Options are:

- AAA Attributes Cisco; see Table 32-6 on page 32-23.
- AAA Attributes LDAP; see Table 32-7 on page 32-25.
- AAA Attributes RADIUS; see Table 32-8 on page 32-26.
- Anti-Spyware; see Table 32-9 on page 32-27.
- Anti-Virus; see Table 32-10 on page 32-28.
- AnyConnect Identity; see Table 32-11 on page 32-29.
- Application; see Table 32-12 on page 32-30.
- Device; see Table 32-13 on page 32-31.
- File; see Table 32-14 on page 32-32.
- NAC; see Table 32-15 on page 32-33.
- Operating System; see Table 32-16 on page 32-34.
- Personal Firewall; see Table 32-17 on page 32-35.
- Policy; see Table 32-18 on page 32-36.
- Process; see Table 32-19 on page 32-36.
- Registry; see Table 32-20 on page 32-38.
- Multiple Certificate Authentication; see Table 32-21 on page 32-39

Step 5 Click **OK**.

Configuring Cisco Secure Desktop Policies on ASA Devices

Cisco Secure Desktop (CSD) provides a reliable means of eliminating all traces of sensitive data by providing a single, secure location for session activity and removal on the client system. CSD provides a session-based interface where sensitive data is shared only for the duration of an SSL VPN session. All session information is encrypted, and all traces of the session data are removed from the remote client when the session is terminated, even if the connection terminates abruptly. This ensures that cookies, browser history, temporary files, and downloaded content do not remain on a system.

When the session closes, CSD overwrites and removes all data using a U.S. Department of Defense (DoD) sanitation algorithm to provide endpoint security protection.

Note A complete explanation of the capabilities and configuration of the Cisco Secure Desktop program is beyond the scope of this document. For information about configuring CSD, and what CSD can do for you, see the materials available online at http://www.cisco.com/en/US/products/ps6742/tsd_products_support_configure.html. Select the configuration guide for the CSD version you are configuring.

This procedure describes how to configure the Cisco Secure Desktop feature on an ASA device.

Before You Begin

- Make sure a connection profile policy has been configured on the device. See Configuring Connection Profiles (ASA, PIX 7.0+), page 31-7.

Related Topics

- Understanding and Managing SSL VPN Support Files, page 30-5

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > Dynamic Access** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Dynamic Access (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Dynamic Access page opens. For a description of the elements on this page, see Dynamic Access Page (ASA), page 32-11.

Step 2 In the Cisco Secure Desktop section, select **Enable CSD** to enable CSD on the ASA device.

Note The Enable CSD option is available for devices running ASA version less than ASA 9.5(2). Beginning with Security Manager 4.10, a new check box is available to configure Hostscan (to disable CSD) only for devices running the ASA version 9.5(2) or later.

Step 3 In the **CSD Package** field, specify the name of the File Object that identifies the Cisco Secure Desktop package you want to upload to the device. Click **Select** to select an existing File Object or to create a new one. For more information, see Add and Edit File Object Dialog Boxes, page 34-36.

Note The package version must be compatible with the ASA operating system version. When you create a local policy in Device view, the **Version** field indicates the CSD package version you should select. (The version is included in the package file name. For example, securedesktop-asa_k9-3.3.0.118.pkg is CSD version 3.3.0.118.) When you create a shared policy in Policy view, the **Version** field indicates the version of the CSD file you selected. For more information on version compatibility, see Understanding and Managing SSL VPN Support Files, page 30-5.

Step 4 (Optional) In the **Hostscan Package** field, specify the name of the File Object that identifies the Host Scan package you want to upload to the device. Click **Select** to select an existing File Object or to create a new one. For more information, see Add and Edit File Object Dialog Boxes, page 34-36.

Step 5 Click **Configure** to open the Cisco Secure Desktop Manager (CSDM) Policy Editor that lets you configure CSD on the security appliance. This application is independent of Security Manager; read the CSD documentation cited above for an explanation of how to use the policy editor.

The editor contains these main items (select them in the table of contents):

- Prelogin Policies—This is a decision tree. When a user attempts a connection, the user's system is evaluated against your rules and the first rule that matches is applied. Typically, you create policies for secure locations, home locations, and insecure public locations. You can make your checks based on registry information, the presence of specific files or certificates, the workstation's operating system, or IP address.

  All editing is done through the right-click menu. Right click on boxes or + signs to activate related settings, if any.

  For end nodes, you can select these options:

  - Access Denied—Workstations that match your criteria are prevented from accessing the network.
  - Policy—You want to define a specific admission policy at this point. After naming the policy, it is added to the table of contents. Select each item in the policy and configure its settings.
  - Subsequence—You want to perform additional checks. Enter the name of the next decision tree that you want to evaluate for this workstation.
- Host scan—You can specify a set of registry entries, file names, and process names, which form a part of the basic host scan. The host scan occurs after the prelogin assessment but before the assignment of a dynamic access policy. Following the basic host scan, the security appliance uses the login credentials, the host scan results, prelogin policy, and other criteria you configure to assign a dynamic access policy. You can also enable:
  - Endpoint Assessment—The remote workstation scans for a large collection of antivirus, antispyware, and personal firewall applications, and associated updates.
  - Advanced Endpoint Assessment—Includes all of the Endpoint Assessment features, and lets you configure an attempt to update noncompliant workstations to meet the version requirements you specify. You must purchase and install a license for this feature before you can configure it.

Dynamic Access Page (ASA)

Use the Dynamic Access page to view the dynamic access policies (DAP) defined on the security appliance. From this page, you can create, edit, or delete DAPs.

Use the Cisco Secure Desktop section to enable and download the Cisco Secure Desktop (CSD) software on the selected ASA device. Cisco Secure Desktop provides a single, secure location for session activity and removal on the client system, ensuring that sensitive data is shared only for the duration of an SSL VPN session.

Note The CSD client software must be installed and activated on a device in order for an SSL VPN policy to work properly.

Tip Dynamic Access policies take precedence over Group policies. If a setting is not specified in a Dynamic Access policy, an ASA device checks for Group policies that specify the setting.

Navigation Path

- (Device View) Select an ASA device; then select **Remote Access VPN > Dynamic Access (ASA)** from the Policy selector.
- (Policy View) Select **Remote Access VPN > Dynamic Access (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

Related Topics

- Understanding Dynamic Access Policies, page 32-1
- Configuring Dynamic Access Policies, page 32-2
- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Cisco Secure Desktop Policies on ASA Devices, page 32-9

Field Reference

Table 32-3 Dynamic Access Policy Page (ASA)

Element	Description
Priority	Priority of the configured dynamic access policy record.
Name	Name of the configured dynamic access policy record.
Network ACL	Name of the firewall ACL that applies to the session.
WebType ACL	Name of the WebType VPN ACL that applies to the session.
Port Forwarding	Name of the port forwarding list that applies to the session.
Bookmark	Name of the SSL VPN Bookmark object that applies to the session.
Terminate	Indicates whether the session is terminated or not.
Description	Additional information about the configured dynamic access policy.
Create button	Click this button to create a dynamic access policy. See Add/Edit Dynamic Access Policy Dialog Box, page 32-12.

Table 32-3 Dynamic Access Policy Page (ASA) (continued)

Element	Description
Edit button	Click this button to edit the selected dynamic access policy. See Add/Edit Dynamic Access Policy Dialog Box, page 32-12.
Delete button	Click this button to delete the selected dynamic access policies.
Cisco Secure Desktop For the procedure to configure CSD on an ASA device, see Configuring Cisco Secure Desktop Policies on ASA Devices, page 32-9.	
Enable CSD	When selected, enables the CSD on the device. Enabling CSD loads the specified Cisco Secure Desktop package. If you transfer or replace the CSD package file, disable and then enable CSD to load the file.
CSD Package	Specify the name of the File Object that identifies the Cisco Secure Desktop package you want to upload to the device. Click **Select** to select an existing File Object or to create a new one. For more information, see Add and Edit File Object Dialog Boxes, page 34-36.
Hostscan Package	Specify the name of the File Object that identifies the Hostscan package you want to upload to the device. Click **Select** to select an existing File Object or to create a new one. For more information, see Add and Edit File Object Dialog Boxes, page 34-36.
Version	The package version must be compatible with the ASA operating system version. When you create a local policy in Device view, the Version field indicates the CSD package version you should select. (The version is included in the package file name. For example, securedesktop-asa_k9-3.3.0.118.pkg is CSD version 3.3.0.118.) When you create a shared policy in Policy view, the Version field indicates the version of the CSD file you selected. For more information on version compatibility, see Understanding and Managing SSL VPN Support Files, page 30-5.
Configure	Click **Configure** to open the Cisco Secure Desktop Manager (CSDM) Policy Editor that lets you configure CSD on the security appliance. For a description of the elements in this dialog box, see Cisco Secure Desktop Manager Policy Editor Dialog Box, page 32-46.

Add/Edit Dynamic Access Policy Dialog Box

Use the Add/Edit Dynamic Access Policy dialog box to configure the dynamic access policies (DAP) on your security appliance. You can specify a name for the dynamic access policy that you are adding, select the priority, specify attributes in a LUA expression, and set attributes for network and webtype ACL filters, file access, HTTP proxy, URL entry and lists, port forwarding, and clientless SSL VPN access methods.

Note For detailed information about dynamic access policy attributes, see Understanding DAP Attributes, page 32-4

These tabs are available in the Add/Edit Dynamic Access Policy dialog box:

- Main Tab, page 32-14
- Logical Operations Tab, page 32-42
- Advanced Expressions Tab, page 32-44

Navigation Path

Open the Dynamic Access Page (ASA), page 32-11, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit Dynamic Access Policy dialog box is displayed.

Related Topics

- Understanding Dynamic Access Policies, page 32-1
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-4 Add/Edit Dynamic Access Policy Dialog Box

Element	Description
Name	The name of the dynamic access policy record (up to 128 characters).
Priority	A priority for the dynamic access policy record. The security appliance applies access policies in the order you set here, highest number having the highest priority. In the case of dynamic access policy records with the same priority setting and conflicting ACL rules, the most restrictive rule applies. Priority is supported by Security Manager version 4.12 onwards for Multi-Context ASA version 9.6(2) or later devices.
Description	Additional information about the dynamic access policy record (up to 1024 characters). Description is supported by Security Manager version 4.12 onwards for Multi-Context ASA version 9.6(2) or later devices.
Main tab	Enables you to add a dynamic access policy entry and set attributes for the access policy depending on the type of remote access that you configure. For a description of the elements on this tab, see Main Tab, page 32-14.
Logical Operations tab	Enables you to create multiple instances of each type of endpoint attribute. For a description of the elements on this tab, see Logical Operations Tab, page 32-42.
Advanced Expressions tab	Enables you to configure one or more logical expressions to set AAA or endpoint attributes other than what is possible in the AAA and Endpoint areas. For a description of the elements on this tab, see Advanced Expressions Tab, page 32-44.

Main Tab

Use the Main tab of the Add/Edit Dynamic Access Policy dialog box to configure the dynamic access policy attributes and the type of remote access method supported your security appliance. You can set attributes for network and webtype ACL filters, file access, HTTP proxy, URL entry and lists, port forwarding, and clientless SSL VPN access methods.

Navigation Path

The Main tab appears when you open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12.

Related Topics

- Configuring Dynamic Access Policies, page 32-2
- Configuring DAP Attributes, page 32-7

Field Reference

Table 32-5 Add/Edit Dynamic Access Policy Dialog Box > Main Tab

Element	Description
Criteria ID	The AAA and endpoint selection attribute names that are available for dynamic access policy use.
Content	Values of the AAA and endpoint attributes criteria that the security appliance uses for selecting and applying a dynamic access policy record during session establishment. Attribute values that you configure here override authorization values in the AAA system, including those in existing group policy, tunnel group, and default group records.
Create button	Click this button to configure AAA and endpoint attributes as selection criteria for the DAP record. See Add/Edit DAP Entry Dialog Box, page 32-21.
Edit button	Click this button to edit the selected dynamic access policy. See Add/Edit DAP Entry Dialog Box, page 32-21.
Delete button	Click this button to delete the selected dynamic access policies.
Access Method	Specify the type of remote access permitted: • **Unchanged**—Continue with the current remote access method. • **AnyConnect Client**—Connect using the Cisco AnyConnect VPN Client. • **Web Portal**—Connect with clientless VPN. • **Both default Web Portal**—Connect via either clientless or the AnyConnect client, with a default of clientless. • **Both default AnyConnect Client**—Connect via either clientless or the AnyConnect client, with a default of AnyConnect.
Network ACL tab—Lets you select and configure network ACLs to apply to this dynamic access policy. An ACL for a dynamic access policy can contain permit or deny rules, but not both. If an ACL contains both permit and deny rules, the security appliance rejects it.	

Table 32-5 Add/Edit Dynamic Access Policy Dialog Box > Main Tab (continued)

Element	Description
Network ACL	Lists the Access Control Lists (ACLs) that will be used to restrict user access to the SSL†VPN. Beginning with Security Manager version 4.10, Network ACL supports IPv6 entries. Also IPv6 is supported for devices running the software version ASA 9.0 or later. This is applicable for both Network ACL and Web Type ACL. Click the **Select** button to open the Access Control Lists Selector from which you can make your selection. The ACL contains conditions that describe a traffic stream of packets, and actions that describe what should occur based on those conditions. Only ACLs having all permit or all deny rules are eligible. Network ACL is supported by Security Manager version 4.12 onwards for Multi-Context ASA version 9.6(2) or later devices.
AnyConnect tab—Lets you choose if the setting for Always-On VPN on the AnyConnect service profile remains unchanged, is disabled, or the AnyConnect Profile Setting must be used. Always-On VPN enables AnyConnnect to automatically establish a VPN session after you log onto the system.	
Custom Attributes tab—Lists the AnyConnect Custom Attribute Type and Custom Attribute Name. AnyConnect custom attributes allow for a more expeditious delivery and deployment of new endpoint features by giving the ASA the ability to generically support the addition of new client controls without the need for an ASA software upgrade. Beginning with version 4.7, Security Manager enables to add Custom Attribute Data to an existing Custom Attribute Type. This feature is supported for devices that are running the ASA software version 9.3(1) or higher.	
Attribute Type	Select the Attribute Type that you configured in Add/Edit AnyConnect Custom Attribute Dialog Box, page 31-70 page.
Attribute Name	Select the Attribute Name that you configured in Add/Edit AnyConnect Custom Attribute Data Dialog Box, page 31-71 page.
WebType ACL tab—Lets you select and configure web-type ACLs to apply to this dynamic access policy. An ACL for a dynamic access policy can contain only permit or deny rules. If an ACL contains both permit and deny rules, the security appliance rejects it.	
Web Type ACL	Specifies the WebType access control list that will be used to restrict user access to the SSL†VPN. Click the **Select** button to open the Access Control Lists Selector from which you can make your selection. Only ACLs having all permit or all deny rules are eligible. Beginning with version 4.10, you can enter IPv6 values for the Web Type ACL.
Functions tab—Lets you configure file server entry and browsing, HTTP proxy, and URL entry for the dynamic access policy.	

Table 32-5 Add/Edit Dynamic Access Policy Dialog Box > Main Tab (continued)

Element	Description
File Server Browsing	Specify the file server browsing setting to be configured on the portal page: • **Unchanged**—Uses values from the group policy that applies to this session. • **Enable**—Enables CIFS browsing for file servers or shared features. • **Disable**—Disables CIFS browsing for file servers or shared features. **Note** Browsing requires NBNS (primary browser or WINS). If that fails or is not configured, we use DNS. The CIFS browse feature does not support internationalization.
File Server Entry	Specify the file server entry setting to be configured on the portal page: • **Unchanged**—Uses values from the group policy that applies to this session. • **Enable**—Enables a user from entering file server paths and names on the portal page. When enabled, places the file server entry drawer on the portal page. Users can enter pathnames to Windows files directly. They can download, edit, delete, rename, and move files. They can also add files and folders. Shares must also be configured for user access on the applicable Windows servers. Users might have to be authenticated before accessing files, depending on network requirements. • **Disable**—Disables a user from entering file server paths and names on the portal page.

Table 32-5 Add/Edit Dynamic Access Policy Dialog Box > Main Tab (continued)

Element	Description
HTTP Proxy	Specify how you want to configure the security appliance to terminate HTTPS connections and forward HTTP/HTTPS requests to HTTP and HTTPS proxy servers: • **Unchanged**—Uses values from the group policy that applies to this session. • **Enable**—Allows the forwarding of an HTTP applet proxy to the client. The proxy is useful for technologies that interfere with proper content transformation, such as Java, ActiveX, and Flash. It bypasses mangling while ensuring the continued use of the security appliance. The forwarded proxy modifies the browser's old proxy configuration and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser it supports is Microsoft Internet Explorer. • **Disable**—Disables the forwarding of an HTTP applet proxy to the client. • **Auto-start**—Enables HTTP proxy and to have the DAP record automatically start the applets associated with these features.

Table 32-5 Add/Edit Dynamic Access Policy Dialog Box > Main Tab (continued)

Element	Description
URL Entry	Using SSL VPN does not ensure that communication with every site is secure. SSL VPN ensures the security of data transmission between the remote user's PC or workstation and the security appliance on the corporate network. If a user then accesses a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate security appliance to the destination web server is not secured. In a clientless VPN connection, the security appliance acts as a proxy between the end user web browser and target web servers. When a user connects to an SSL-enabled web server, the security appliance establishes a secure connection and validates the server SSL certificate. The end user browser never receives the presented certificate, so therefore cannot examine and validate the certificate. The current implementation of SSL VPN does not permit communication with sites that present expired certificates. Neither does the security appliance perform trusted CA certificate validation. Therefore, users cannot analyze the certificate an SSL-enabled web-server presents before communicating with it. Specify how the URL entry setting must be configured on the portal page: • **Unchanged**—Uses values from the group policy that applies to this session. • **Enable**—Allows a user from entering HTTP/HTTPS URLs on the portal page. If this feature is enabled, users can enter web addresses in the URL entry box, and use clientless SSL VPN to access those websites. • **Disable**—Disables a user from entering HTTP/HTTPS URLs on the portal page. **Note** To limit Internet access for users, select **Disable** for the URL Entry field. This prevents SSL VPN users from surfing the Web during a clientless VPN connection.

Port Forwarding tab—Lets you select and configure port forwarding lists for user sessions.

Note Port Forwarding does not work with some SSL/TLS versions.

Caution Make sure Sun Microsystems Java Runtime Environment (JRE) 1.4+ is installed on the remote computers to support port forwarding (application access) and digital certificates.

Table 32-5 Add/Edit Dynamic Access Policy Dialog Box > Main Tab (continued)

Element	Description
Port Forwarding	Select an option for the port forwarding lists that apply to this DAP record: • **Unchanged**—Removes the attributes from the running configuration. • **Enable**—Enables port forwarding on the device. • **Disable**—Disables port forwarding on the device. • **Auto-start**—Enables port forwarding, and to have the DAP record automatically start the port forwarding applets associated with its port forwarding lists.
Port Forwarding List	The Port Forwarding List, that defines the mapping of the port number on the client machine to the application's IP address and port behind the SSL VPN gateway. You can click **Select** to open the Port Forwarding List Selector from which you can select the required Port Forwarding List from a list of Port Forwarding List objects. A Port Forwarding List object defines the mappings of port numbers on the remote client to the application's IP address and port behind the SSL VPN gateway.
Bookmark tab—Lets you enable and configure SSL VPN bookmarks. When enabled, users who successfully log into the SSL VPN are presented with the portal page containing the list of defined bookmarks. These bookmarks enable users to access resources available on SSL VPN websites in Clientless access mode.	
Enable Bookmarks	Specify the file server browsing setting to be configured on the portal page: • **Unchanged**—Uses values from the group policy that applies to this session. • **Enable**—Enables bookmarks on the SSL VPN portal page. • **Disable**—Disables bookmarks on the SSL VPN portal page.
Bookmarks	A list of websites that will be displayed on the portal page as a bookmark to enable users to access the resources available on the SSL VPN websites. You can click **Select** to open the Bookmarks Selector from which you can select the required bookmark from a list or create a new bookmark, as desired.
Action tab—Specifies special processing to apply to a specific connection or session. Action Tab is supported by Security Manager version 4.12 onwards for Multi-Context ASA version 9.6(2) or later devices. Select one of the following options from the drop-down list:	
Continue	(Default) When selected, continues the session. By default, the access policy attributes are applied to the session and it is running.

Table 32-5 Add/Edit Dynamic Access Policy Dialog Box > Main Tab (continued)

Element	Description
Quarantine	When selected, quarantines the session. By selecting quarantine, you can restrict a particular client who already has an established tunnel through a VPN. Restricted ACLs are applied to a session to form a restricted group, based on the selected DAP record. When an endpoint is not compliant with an administratively defined policy, the user can still access services for remediation (such as updating the antivirus and so on), but restrictions are placed upon the user. After the remediation occurs, the user can reconnect, which invokes a new posture assessment. If this assessment passes, the user connects. **Note** This parameter requires an AnyConnect release that supports AnyConnect Secure Mobility features.
Terminate	When selected, terminates the session. By default, the access policy attributes are applied to the session and it is running.
User Message	Enter a text message to display on the portal page when this DAP record is selected. Maximum 128 characters. A user message displays as a yellow orb. When a user logs on it blinks three times to attract attention, and then it is still. If several DAP records are selected, and each of them has a user message, all user messages display. **Note** You can include in such messages URLs or other embedded text, which require that you use the correct HTML tags. For example: All contractors please read Instructions for the procedure to upgrade your antivirus software. **Note** User Message is supported from Security Manager version 4.12 for ASA devices running version 9.6(2) or later in Multi-context mode.

The supported Dynamic Access Policy CLIs in Security Manager version 4.12 onwards for Multi-Context ASA 9.6(2) devices are as follows:

- Dynamic-access-policy-record action
- description
- exit
- help
- network-acl
- no
- priority
- quit
- user-message

Add/Edit DAP Entry Dialog Box

Use the Add/Edit DAP Entry dialog box to specify the authorization attributes and endpoint attributes for a dynamic access policy. The security appliance selects the dynamic access policy based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the dynamic access policy to the user tunnel or session.

For detailed information about dynamic access policy attributes, see Understanding DAP Attributes, page 32-4.

The content of the dialog box differs based on the criterion that you select. The criterion is the authorization or endpoint attribute that serves as the selection criterion that the security appliance uses for selecting and applying dynamic access policies during session establishment. You can select from the following criteria:

- AAA Attributes Cisco—Refers to user authorization attributes that are stored in the AAA hierarchical model. See Add/Edit DAP Entry Dialog Box > AAA Attributes Cisco, page 32-22
- AAA Attributes LDAP—Sets the LDAP client stores all native LDAP response attribute value pairs in a database associated with the AAA session for the user. See Add/Edit DAP Entry Dialog Box > AAA Attributes LDAP, page 32-24.
- AAA Attributes RADIUS—Sets the RADIUS client stores all native RADIUS response attribute value pairs in a database associated with the AAA session for the user. See Add/Edit DAP Entry Dialog Box > AAA Attributes RADIUS, page 32-25.
- Anti-Spyware—Creates an endpoint attribute of type Anti-Spyware. You can use the Host Scan modules of Cisco Secure Desktop to scan for antispyware applications and updates that are running on the remote computer. See Add/Edit DAP Entry Dialog Box > Anti-Spyware, page 32-26.
- Anti-Virus—Creates an endpoint attribute of type Anti-Virus. You can use the Host Scan modules of Cisco Secure Desktop to scan for antivirus applications and updates that are running on the remote computer. See Add/Edit DAP Entry Dialog Box > Anti-Virus, page 32-27.
- AnyConnect Identity—Creates an endpoint attribute of type AnyConnect Identity. See Add/Edit DAP Entry Dialog Box > AnyConnect Identity, page 32-28.
- Application—Indicates the type of remote access connection. See Add/Edit DAP Entry Dialog Box > Application, page 32-29.
- Device—Creates an endpoint attribute of type Device. The Device Criterion lets you provide specific device information for use during the associated prelogin policy checking. See Add/Edit DAP Entry Dialog Box > Device, page 32-30.
- File—Creates an endpoint attribute of type File. Filename checking to be performed by Basic Host Scan must be explicitly configured using Cisco Secure Desktop Manager. See Add/Edit DAP Entry Dialog Box > File, page 32-31.
- NAC—Creates an endpoint attribute of type NAC. NAC protects the enterprise network from intrusion and infection from worms, viruses, and rogue applications by performing endpoint compliancy. We refer to these checks as posture†validation. See Add/Edit DAP Entry Dialog Box > NAC, page 32-32.
- Operating System—Creates an endpoint attribute of type Operating System. The prelogin assessment module of the CSD can check the remote device for the OS version, IP address, and Microsoft Windows registry keys. See Add/Edit DAP Entry Dialog Box > Operating System, page 32-33.

- Personal Firewall—Creates an endpoint attribute of type Personal Firewall. You can use the Host Scan modules of Cisco Secure Desktop to scan for personal firewall applications and updates that are running on the remote computer. For a description of the elements in the dialog box, see Add/Edit DAP Entry Dialog Box > Personal Firewall, page 32-34.
- Policy—Creates an endpoint attribute of type Policy. See Add/Edit DAP Entry Dialog Box > Policy, page 32-35.
- Process—Process name checking to be performed by Basic Host Scan must be explicitly configured using Cisco Secure Desktop Manager. See Add/Edit DAP Entry Dialog Box > Process, page 32-36.
- Registry—Creates an endpoint attribute of type Registry. Registry key scans apply only to computers running Windows Microsoft Windows operating systems. See Add/Edit DAP Entry Dialog Box > Registry, page 32-37.
- Multiple Certificate Authentication— Creates an endpoint attribute of type Multiple Certificate Authentication. You can specify the attributes for the multiple certificate authentication of remote VPN users. See Add/Edit DAP Entry Dialog Box > Multiple Certificate Authentication, page 32-38.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Add/Edit DAP Entry Dialog Box > AAA Attributes Cisco

To configure AAA attributes as selection criteria for dynamic access policies, in the Add/Edit DAP Entry dialog box, set AAA Attributes Cisco as the selection criterion to be used to select and apply the dynamic access policies during session establishment. You can set these attributes either to match or not match the value you enter. There is no limit for the number of AAA attributes for each dynamic access policy.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **AAA Attributes Cisco** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7

- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-6 Add/Edit DAP Entry Dialog Box > AAA Attributes Cisco

Element	Description
Criterion	Shows AAA Attributes Cisco as the selection criterion.
Group Policy	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and enter the name of the AAA server group associated with the user. The maximum length is 64 characters. AAA server groups represent collections of authentication servers focused on enforcing specific aspects of your overall network security policy.
IPv4 Address	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and enter the assigned IP address. Addresses are predefined network objects. You can also click **Select** to open a dialog box that lists all available network hosts, and in which you can create or edit network host objects. **Tip** If you select this option and later look at the rule in ASDM, the IP Address attribute is called Assigned IP Address.
IPv6 Address (Security Manager version 4.12 or later and ASA version 9.0 or later)	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and enter the assigned IP address. Addresses are predefined network objects. You can also click **Select** to open a dialog box that lists all available network hosts, and in which you can create or edit network host objects. **Tip** If you select this option and later look at the rule in ASDM, the IP Address attribute is called Assigned IP Address.
Member-of	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and enter a comma-separated string of group policy names that apply to the user. This attribute lets you indicate multiple group membership. The maximum length is 128 characters. **Tip** If you select this option, and later look at the rule in ASDM, this option will not appear. In general, this option is not used because it can be confused with the memberof LDAP attribute. Because this rule applies to Local authentication, you might want to use the Username attribute instead of the Member-of attribute.
Username	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and enter the username of the authenticated user. A maximum of 64 characters is allowed.
Username 2	Select the check box, select the matching criteria (*is* or *isn't*) from the drop-down list, and enter the secondary username of the authenticated user.

Table 32-6 Add/Edit DAP Entry Dialog Box > AAA Attributes Cisco (continued)

Element	Description
Connection Profiles	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and select the connection profile from a list of all the SSL VPN Connection Profile policies defined on the security appliance. An SSL VPN connection profile comprises a set of records that contain VPN tunnel connection profile policies, including the attributes that pertain to creating the tunnel itself. **Note** For a description of the procedure to configure an SSL VPN Connection Profiles policy, see Configuring Connection Profiles (ASA, PIX 7.0+), page 31-7.
SCEP Required	Select the check box, select the matching criteria (*is* or *isn't*) from the drop-down list, and select *True* or *False*. This attribute enables to match whether or not the connection fails the certificate authentication.

Add/Edit DAP Entry Dialog Box > AAA Attributes LDAP

The LDAP client stores all native LDAP response attribute value pairs in a database associated with the AAA session for the user. The LDAP client writes the response attributes to the database in the order in which it receives them. It discards all subsequent attributes with that name. This scenario might occur when a user record and a group record are both read from the LDAP server. The user record attributes are read first, and always have priority over group record attributes.

To support Active Directory group membership, the AAA LDAP client provides special handling of the LDAP memberOf response attribute. The AD memberOf attribute specifies the DN string of a group record in AD. The name of the group is the first CN value in the DN string. The LDAP client extracts the group name from the DN string and stores it as the AAA memberOf attribute, and in the response attribute database as the LDAP memberOf attribute. If there are additional memberOf attributes in the LDAP response message, then the group name is extracted from those attributes and is combined with the earlier AAA memberOf attribute to form a comma separated string of group names, also updated in the response attribute database.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **AAA Attributes LDAP** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-7 Add/Edit DAP Entry Dialog Box > AAA Attributes LDAP

Element	Description
Criterion	Shows AAA Attributes LDAP as the selection criterion.
Attribute ID	Specify the name of the LDAP attribute map in the dynamic access policy. LDAP attribute maps take the attribute names that you define and map them to Cisco-defined attributes. A maximum of 64 characters is allowed.
Value	Select the matching criteria (for example, *is*) from the drop-down list, and enter the custom map value that maps to a Cisco Map Value or enter the Cisco map value that maps to the Custom Map Value. To enter multiple values, separate each value with **;** as the delimiter. The attribute map is populated with value mappings that apply customer, user-defined attribute values to the customer attribute name and to the matching Cisco attribute name and value. Alternatively, click the **Fetch AD Groups** button to open the Fetch AD Groups dialog box. The table in the dialog box lists the UserGroup ID and UserGroup Name of the available LDAP servers that you can choose from. Select one or more rows and click the **Select** button. To search for a particular UserGroup in the list you can enter text in the Filter text box and click **Search**. The UserGroup name meeting the criteria appears in the list. **Note** To be able to view the list of available LDAP servers you must first configure the mapping of Domain to AD Server Group. To perform this task, go to **Tools >Security Manager Administration** and select **Identity Settings** from the table of contents. For more information, see Identity Settings Page, page 11-38.

Add/Edit DAP Entry Dialog Box > AAA Attributes RADIUS

The RADIUS client stores all native RADIUS response attribute value pairs in a database associated with the AAA session for the user. The RADIUS client writes the response attributes to the database in the order in which it receives them. It discards all subsequent attributes with that name. This scenario might occur when a user record and a group record are both read from the RADIUS server. The user record attributes are read first, and always have priority over group record attributes.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **AAA Attributes RADIUS** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-8 Add/Edit DAP Entry Dialog Box > AAA Attributes RADIUS

Element	Description
Criterion	Shows AAA Attributes RADIUS as the selection criterion.
Attribute ID	Specify the name of the RADIUS attribute name or number in the dynamic access policy. A maximum of 64 characters is allowed. RADIUS attribute names do not contain the cVPN3000 prefix to better reflect support for all three security appliances (VPN 3000, PIX, and the ASA). The appliances enforce the RADIUS attributes based on attribute numeric ID, not attribute name. LDAP attributes are enforced by their name, not by the ID.
Value	Select the matching criteria (for example, *is*) from the drop-down list, and enter the attribute value.

Add/Edit DAP Entry Dialog Box > Anti-Spyware

You can use the Host Scan feature of the Cisco Secure Desktop feature to enable Endpoint Assessment, a scan for antivirus, personal firewall, and antispyware applications and updates that are running on the remote computer. Following the configuration of the prelogin policies and host scan options, you can configure a match of any one or any combination of the Host Scan results to assign a dynamic access policy following the user login.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **Anti-Spyware** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-9 Add/Edit DAP Entry Dialog Box > Anti-Spyware

Element	Description
Criterion	Shows Anti-Spyware as the selection criterion.
Type	Select one of the following options and assign the associated values: • **Not Installed**—Select if the absence of the named anti-spyware from the remote PC is sufficient to match the prelogin policy you are configuring. • **Installed and enabled**—Select if the named anti-spyware must be present and enabled on the remote PC to match the prelogin policy you are configuring. • **Installed and disabled**—Select if the mere presence of the named anti-spyware on the remote PC is sufficient to match the prelogin policy you are configuring.
Vendor Name	Select the text that describes the application vendor from the list.
Product ID	Select a unique identifier for the product that is supported by the selected vendor from the list.
Product Description	Available only if you selected **Matches** as the Type. Select the check box, then select the description of the product from the list.
Version	Available only if you selected **Matches** as the Type. Identify the version of the application, and specify whether you want the endpoint attribute to be equal to/not equal to that version.
Last Update	Available only if you selected **Matches** as the Type. Specify the number of days since the last update. You might want to indicate that an update should occur in less than or greater than the number of days you enter here.

Add/Edit DAP Entry Dialog Box > Anti-Virus

You can configure a scan for antivirus applications and updates as a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connection. Following the prelogin assessment, Cisco Secure Desktop loads Endpoint Assessment checks and reports the results back to the security appliance for use in assigning a dynamic access policy.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **Anti-Virus** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-10 Add/Edit DAP Entry Dialog Box > Anti-Virus

Element	Description
Criterion	Shows Anti-Virus as the selection criterion.
Type	Select one of the following options and assign the associated values: • **Not Installed**—Select if the absence of the named anti-virus from the remote PC is sufficient to match the prelogin policy you are configuring. • **Installed and enabled**—Select if the named anti-virus must be present and enabled on the remote PC to match the prelogin policy you are configuring. • **Installed and disabled**—Select if the mere presence of the named anti-virus on the remote PC is sufficient to match the prelogin policy you are configuring.
Vendor Name	Select the text that describes the application vendor from the list.
Product ID	Select a unique identifier for the product that is supported by the selected vendor from the list.
Product Description	Available only if you selected the criteria to match the endpoint attribute for the dynamic access policy. Select the check box, then select the description of the product from the list.
Version	Available only if you selected the criteria to match the endpoint attribute for the dynamic access policy. Identify the version of the application, and specify whether you want the endpoint attribute to be equal to/not equal to that version.
Last Update	Available only if you selected the criteria to match the endpoint attribute for the dynamic access policy. Specify the number of days since the last update. You might want to indicate that an update should occur in less than or greater than the number of days you enter here.

Add/Edit DAP Entry Dialog Box > AnyConnect Identity

To configure AnyConnect Identity attributes as selection criteria for dynamic access policies, set AnyConnect Identity as the selection criterion in the Add/Edit DAP Entry dialog box. The ASA generates DAP endpoint attributes based on the AnyConnect Identification attributes received from the AnyConnect mobile client. You are not required to enable Cisco Secure Desktop to configure these specific attributes using Security Manager.

For the purposes of assigning a dynamic access policy, if you configure more than one AnyConnect Identity attribute for a particular DAP entry, the entry will be considered a match if any of the attributes values are true. There is no limit for the number of AnyConnect Identity attributes for each dynamic access policy.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **AnyConnect Identity** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-11 Add/Edit DAP Entry Dialog Box > AnyConnect Identity

Element	Description
Criterion	Shows AnyConnect Identity as the selection criterion.
Client Version	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and enter the AnyConnect Client version number.
Platform	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and select the appropriate platform from the drop-down list.
Platform Version	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and enter the appropriate version number of the platform.
Device Type	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and select the appropriate device type from the drop-down list.
Device Unique ID	Select the check box, select the matching criteria (for example, *is*) from the drop-down list, and enter the unique device ID. This ID distinguishes the device allowing you to set policies exclusive to that device.

Add/Edit DAP Entry Dialog Box > Application

Use this dialog box to indicate the type of remote access connection as the endpoint attribute for the dynamic access policy.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **Application** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-12 Add/Edit DAP Entry Dialog Box > Application

Element	Description
Criterion	Shows Application as the selection criterion.
Client Type	Select the check box, then select the matching criteria (for example, *is* or *isn't*) from the drop-down list, and specify the type of remote access connection from the list: AnyConnect, Clientless, Cut-through Proxy, IPsec, Generic IKEv2 Client, or L2TP. **Note** If you select AnyConnect as the client type, make sure to enable Cisco Secure Desktop. If it is not enabled, Security Manager generates an error.

Add/Edit DAP Entry Dialog Box > Device

The DAP Device Criterion lets you provide specific device information for use during the associated prelogin policy checking. You can provide one or more of the following attributes for a device—host name, MAC address, port number, Privacy Protection selection—and indicate whether each *is* or *isn't* to be matched.

Note that *isn't* is exclusionary. For example, if you specify the criterion `Host Name isn't zulu_2`, all devices not named `zulu_2` will match.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Choose **Device** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-13 Add/Edit DAP Entry Dialog Box > Device

Element	Description
Criterion	Shows Device as the selected Criterion.
Host Name	Select this option, choose a match criterion (*is* or *isn't*) from the related drop-down list, and then enter the device host name to be matched.
MAC Address	Select this option, choose a match criterion (*is* or *isn't*) from the related drop-down list, and then enter the device's MAC address to be matched.
BIOS Serial Number	Select this option, choose a match criterion (*is* or *isn't*) from the related drop-down list, and then enter the BIOS serial number value of the device you are matching for. The number format is manufacturer-specific. There is no format requirement.
Port Number	Select this option, choose a match criterion (*is* or *isn't*), and then enter or Select the device port to be matched.
TCP/UDP Port Number	Select this option, choose a match criterion (*is* or *isn't*), and then enter or Select the TCP/UDP port in listening state that you are matching for. In the TCP/UDP combo box, select the kind of port you are matching for: TCP (IPv4), UDP(IPv4), TCP(IPv6) or UDP(IPv6). Beginning with version 4.12, Security Manager supports IPv6 addresses for ASA devices running the version 9.0 or later. If you are matching for more than one port, make several individual endpoint attribute rules in the DAP and specify one port in each.
Privacy Protection	Select this option, choose a match criterion (*is* or *isn't*), and then choose the Privacy Protection option defined on the device: **none**, **cache cleaner**, or **secure desktop**.
CSD Version	Select this option, choose a match criterion (*is* or *isn't*) from the related drop-down list, and then enter the version of the Host Scan image running on the endpoint.
Endpoint Assessment Version	Select this option, choose a match criterion (*is* or *isn't*) from the related drop-down list, and then enter the version of endpoint assessment (OPSWAT) you are matching for.

Add/Edit DAP Entry Dialog Box > File

The file criterion prelogin check lets you specify that a certain file must or must not exist to be eligible for the associated prelogin policy. For example, you might want to use a file prelogin check to ensure a corporate file is present or one or more peer-to-peer file-sharing programs containing malware are not present before assigning a prelogin policy.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **File** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-14 Add/Edit DAP Entry Dialog Box > File

Element	Description
Criterion	Shows File as the selection criterion.
Type	Specify whether this endpoint attribute must match or not match the criteria configured for selecting and applying dynamic access policies during session establishment.
Endpoint ID	Select a string that identifies an endpoint for files. Dynamic access policies use this ID to match Cisco Secure Desktop host scan attributes for dynamic access policy selection. You must configure Host Scan before you configure this attribute. When you configure Host Scan, the configuration displays in this pane, so you can select it, reducing the possibility of errors in typing or syntax.
Filename	Specify the filename.
Last Update	Available only if you selected the criteria to match the endpoint attribute for the dynamic access policy. Specify the number of days since the last update. You might want to indicate that an update should occur in less than (<) or more than (>) the number of days you enter here.
Checksum	Available only if you selected the criteria to match the endpoint attribute for the DAP record. Select the check box to specify a checksum to authenticate the file, then enter a checksum in hexadecimal format, beginning with 0x. Beginning with version 4.7, Security Manager provides a utility to compute CRC32 checksum for a file. Click the **Compute CRC32 Checksum** button to open the Compute Checksum dialog box. Click Browse to open the File browser, select the required file and then click the Compute button. The CRC32 checksum of the file will be calculated and populated in the Checksum field. **Note** Only client-side browsing is supported for the Compute CRC32 Checksum utility. By default client-side browsing is enabled. If you have disabled it, you must enable it by selecting **Tools > Security Manager Administration** and select **Customize Desktop** from the table of contents. For more information, see Customize Desktop Page, page 11-10.

Add/Edit DAP Entry Dialog Box > NAC

NAC protects the enterprise network from intrusion and infection from worms, viruses, and rogue applications by performing endpoint compliancy and vulnerability checks as a condition for production access to the network. We refer to these checks as *posture†validation*. You can configure posture

validation to ensure that the anti-virus files, personal firewall rules, or intrusion protection software on a host with an AnyConnect or Clientless SSL VPN session are up-to-date before providing access to vulnerable hosts on the intranet. Posture validation can include the verification that the applications running on the remote hosts are updated with the latest patches. NAC occurs only after user authentication and the setup of the tunnel. NAC is especially useful for protecting the enterprise network from hosts that are not subject to automatic network policy enforcement, such as home PCs. The security appliance uses Extensible Authentication Protocol (EAP) over UDP (EAPoUDP) messaging to validate the posture of remote hosts.

The establishment of a tunnel between the endpoint and the security appliance triggers posture validation. You can configure the security appliance to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server, such as a Trend server, uses the host IP address to challenge the host directly to assess its health. For example, it may challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **NAC** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-15 Add/Edit DAP Entry Dialog Box > NAC

Element	Description
Criterion	Shows NAC as the selection criterion.
Posture Status	Select the matching criteria (for example, *is*) from the drop-down list, then enter the posture token string received from ACS.

Add/Edit DAP Entry Dialog Box > Operating System

The prelogin assessment includes a check for the OS attempting to establish a VPN connection. When the user attempts to connect, however, Cisco Secure Desktop checks for the OS, regardless of whether you insert an OS prelogin check.

If the prelogin policy assigned to the connection has Secure Desktop (Secure Session) enabled and if the remote PC is running Microsoft Windows XP or Windows 2000, it installs Secure Session, regardless of whether you insert an OS prelogin check. If the prelogin policy has Secure Desktop enabled and the operating system is Microsoft Windows Vista, Mac OS X 10.4, or Linux, Cache Cleaner runs instead. Therefore, you should make sure the Cache Cleaner settings are appropriate for a prelogin policy on

which you have configured Secure Desktop or Cache Cleaner to install. Although Cisco Secure Desktop checks for the OS, you may want to insert an OS prelogin check as a condition for applying a prelogin policy to isolate subsequent checks for each OS.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **Operating System** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-16 Add/Edit DAP Entry Dialog Box > Operating System

Element	Description
Criterion	Shows Operating System as the selection criterion.
OS Version	Select the check box, then select the matching criteria (for example, *is*) from the drop-down list, and select the OS version from the list. Select Apple Plugin for iPhones and similar devices.
Service Pack	Select the check box, then select the matching criteria (for example, *is*) from the drop-down list, and select the service pack for the operating system.

Add/Edit DAP Entry Dialog Box > Personal Firewall

You can click Host Scan in the Cisco Secure Desktop interface to enable Endpoint Assessment, a scan for personal firewalls that are running on the remote computer. Most, but not all, personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **AAA Attributes Cisco** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4

- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-17 Add/Edit DAP Entry Dialog Box > Personal Firewall

Element	Description
Criterion	Shows Personal Firewall as the selection criterion.
Type	Select one of the following options and assign the associated values: • **Not Installed**—Select if the absence of the named personal firewall from the remote PC is sufficient to match the prelogin policy you are configuring. • **Installed and enabled**—Select if the named personal firewall must be present and enabled on the remote PC to match the prelogin policy you are configuring. • **Installed and disabled**—Select if the mere presence of the named personal firewall on the remote PC is sufficient to match the prelogin policy you are configuring.
Vendor Name	Select the text that describes the application vendor from the list.
Product ID	Select a unique identifier for the product that is supported by the selected vendor from the list.
Product Description	Available only if you selected that this endpoint attribute and all its settings must be available on the remote PC. Select the check box, then select the description of the product from the list.
Version	Available only if you selected that this endpoint attribute and all its settings must be available on the remote PC. Identify the version of the application, and specify whether you want the endpoint attribute to be equal to/not equal to that version.

Add/Edit DAP Entry Dialog Box > Policy

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 Cisco Secure Desktop 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. Cisco Secure Desktop checks locations in the order listed on the Windows Location Settings window, and grants privileges to client PCs based on the first location definition they match.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **Policy** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-18 Add/Edit DAP Entry Dialog Box > Policy

Element	Description
Criterion	Shows Policy as the selection criterion.
Location	Select the matching criteria (for example, *is*) from the drop-down list, and select the Cisco Secure Desktop Microsoft Windows location profile from the list. All the locations configured in the Cisco Secure Desktop Manager are displayed in this list.

Add/Edit DAP Entry Dialog Box > Process

You can specify a set of process names, which form a part of Basic Host Scan. The host scan, which includes Basic Host Scan and Endpoint Assessment, or Advanced Endpoint Assessment; occurs after the prelogin assessment but before the assignment of a dynamic access policy. Following the Basic Host Scan, the security appliance uses the login credentials, the host scan results, prelogin policy, and other criteria you configure to assign a DAP.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **Process** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-19 Add/Edit DAP Entry Dialog Box > Process

Element	Description
Criterion	Shows Process as the selection criterion.

Table 32-19 Add/Edit DAP Entry Dialog Box > Process (continued)

Element	Description
Type	Select one of the following options and assign the associated values: • **Matches**—Select if the mere presence of the named process on the remote PC is sufficient to match the prelogin policy you are configuring. • **Doesn't Match**—Select if the absence of the named process from the remote PC is sufficient to match the prelogin policy you are configuring.
Endpoint ID	A string that identifies an endpoint for files, processes or registry entries. Dynamic access policies use this ID to match Cisco Secure Desktop host scan attributes for dynamic access policy selection. You must configure Host Scan before you configure this attribute. When you configure Host Scan, the configuration displays in this pane, so you can select it, reducing the possibility of errors in typing or syntax.
Path	Select the check box, then select the matching criteria (for example, *is*) from the drop-down list, and enter the name of the process. You can display it in Microsoft Windows by opening the Windows Task Manager window and clicking the Processes tab. Configure Host Scan before you configure this attribute. When you configure Host Scan, the configuration displays in this pane, so you can select it and specify the same index when you assign this entry as an endpoint attribute when configuring a DAP, reducing the possibility of errors in typing or syntax.

Add/Edit DAP Entry Dialog Box > Registry

Registry key scans apply only to computers running Windows Microsoft Windows operating systems. Basic Host Scan ignores registry key scans if the computer is running Mac OS or Linux.

Note Duplicate entries are not allowed. If you configure a dynamic access policy with no AAA or endpoint attributes, the security appliance always selects it since all selection criteria are satisfied.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **Registry** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-20 Add/Edit DAP Entry Dialog Box > Registry

Element	Description
Criterion	Shows Registry as the selection criterion.
Type	Select one of the following options and assign the associated values: • **Matches**—Select if the mere presence of the named registry key on the remote PC is sufficient to match the prelogin policy you are configuring. For example, select this option if you want to require the following registry key to be present to match a criterion for assigning a prelogin policy: HKEY_LOCAL_MACHINE\SOFTWARE\<Protective_Software> • **Doesn't Match**—Select if the absence of the named registry key from the remote PC is sufficient to match the prelogin policy you are configuring. For example, select this option if you want to require the following registry key to be absent to match a criterion for assigning a prelogin policy: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\<Evil_SpyWare>
Endpoint ID	A string that identifies an endpoint for files, processes or registry entries. Dynamic access policies use this ID to match Cisco Secure Desktop host scan attributes for dynamic access policy selection. You must configure Host Scan before you configure this attribute. When you configure Host Scan, the configuration displays in this pane, so you can select it, reducing the possibility of errors in typing or syntax.
Registry Name	Select the text that describes the registry name from the list.
Value	Select the value, **dword** or **string**, from the list, then select the matching criteria (whether it equals or does not equal), and enter a decimal or a string to compare with the dword or string value of the registry key on the remote PC. **Note** "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. 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.
Ignore Case	When selected, ignores the case in the registry entry if it includes a string.

Add/Edit DAP Entry Dialog Box > Multiple Certificate Authentication

The DAP multiple certificate authentication criterion allows you to provide specific certificate information for use during the associated prelogin policy checking. Cisco Security Manager supports two certificates to authenticate remote VPN users. You can provide one or more of the following attributes for the certificates—subject, issuer, subject alternate name, serial number and certificate store.

Note You can modify the DAP entry except the certificate option.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12 with the Main tab selected, then click **Create**, or select a dynamic access policy in the table and click **Edit**. The Add/Edit DAP Entry dialog box is displayed. Select **Multiple Certificate Authentication** as the Criterion.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-21 Add/Edit DAP Entry Dialog Box > Multiple Certificate Authentication

Element	Description
Criterion	Shows Multiple Certificate Authentication as the selection criterion.
Certificate	Multiple certification in 4.13 refers to two certificate authentication. Select one of the following options and assign the associated attributes: • **Cert1**—Select to provide the certificate 1 details to match the prelogin policy you are configuring. • **Cert2**—Select to provide the certificate 2 details to match the prelogin policy you are configuring. **Note** You cannot edit/modify the certificate option.

Table 32-21 Add/Edit DAP Entry Dialog Box > Multiple Certificate Authentication (continued)

Element	Description
Subject	From the drop-down list, select the domain name (DN) attribute field from subject name of the certificate: • dnq—Domain name qualifier • fulldn—Full subject-name • ser—Serial number • cn—Common name • i—Initials • ou—Organization Unit • sp—State/Province • o—Organization • n—Name • sn—Surname • t—Title • uid—User Identifier • genq—Generation Qualifier • c—Country • l—Locality • gn—Given Name • ea—E-mail address In the adjacent text box, enter the DAP entry value for the selected Subject. **Note** If you leave the text box blank, and error message appears while saving.

Table 32-21 Add/Edit DAP Entry Dialog Box > Multiple Certificate Authentication (continued)

Element	Description
Issuer	From the drop-down list, select the domain name (DN) attribute field from issuer name of the certificate: • dnq—Domain name qualifier • fulldn—Full issuer-name • ser—Serial number • cn—Common name • i—Initials • ou—Organization Unit • sp—State/Province • o—Organization • n—Name • sn—Surname • t—Title • uid—User Identifier • genq—Generation Qualifier • c—Country • l—Locality • gn—Given Name • ea—E-mail address In the adjacent text box, enter the DAP entry value for the selected issuer. **Note** If you leave the text box blank, an error message appears while saving.
Subject Alternate Name	For configuring the serial number, select upn from this drop-down list. In the adjacent text box, enter the User Principal Name from Subject Alt Name field of certificate
Serial Number	Enter the serial number of certificate to be matched. This value should be a hexadecimal number (a combination of 0 to 9, and A to F). **Note** If you enter a non-hexadecimal number, an error message appears while saving.

Table 32-21 Add/Edit DAP Entry Dialog Box > Multiple Certificate Authentication (continued)

Element	Description
Certificate Store	Select the relevant store from where the certificate can be found for authentication: • None—Choose if you are not aware of the certificate type. • Machine—Choose if the certificate pertains to machine (accessible only by privileged processes). You cannot select this option for both cert1 and cert2. • User—Choose if the certificate pertains to user log in (accessible only by processes owned by the logged-in user). **Note** For Windows, the store may be a) one machine and one user, or b) two users. For non-Windows platforms, the indication is always two user certificates.

Logical Operations Tab

Use the Logical Operations tab of the Add/Edit Dynamic Access Policy dialog box to configure multiple instances of the AAA and each type of endpoint attribute that you defined in the DAP Entry dialog box. On this tab, set each type of endpoint or AAA attribute to require only one instance of a type (Match Any = OR) or to have all instances of a type (Match All = AND).

- If you configure only one instance of an endpoint category, you do not need to set a value.
- For some endpoint attributes, it is not useful to configure multiple instances. For example, no users have more than one running OS.
- You are configuring the Match Any/Match All operation within each endpoint type. The security appliance evaluates each type of endpoint attribute, and then performs a logical AND operation on all of the configured endpoints. That is, each user must satisfy the conditions of ALL of the endpoints you configure, as well as the AAA attributes.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12, then click the **Logical Operations** tab.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-22 Add/Edit Dynamic Access Policy Dialog Box > Logical Operations Tab

Element	Description
AAA	Select one of the following options if you defined the AAA attribute in the dynamic access policy: • **Match Any**—Creates an OR relationship among the attributes. Attributes matching any of your criteria are included in the filter. The security appliance grants access to a particular user for a particular session even if any one of the attributes is matching all your criteria. • **Match All**—Creates an AND relationship among the attributes. The security appliance grants access to a particular user for a particular session only if the attributes are matching all your criteria. • **Match None**—Creates a NOT relationship among the attributes. The dynamic access policy specifies that none of the attributes of the user need to match to be granted access to a session.
Anti-Spyware	Select one of the following options if you defined Anti-Spyware as an endpoint attribute: • **Match Any**—Creates an OR relationship among the attributes. Policies matching any instance of your criteria are used to authorize users. • **Match All**—Creates an AND relationship among the attributes. Only those attributes matching all your criteria are used to authorize users.
Anti-Virus	Select one of the following options if you defined Anti-Virus as an endpoint attribute: • **Match Any**—Set to require that user authorization attributes match any of the values in the Antivirus endpoint attributes you are configuring. • **Match All**—Set to require that user authorization attributes match all of the values in the endpoint attributes you are configuring, as well as satisfying the AAA attribute.
Application	Select one of the following options if you defined Application as an endpoint attribute: • **Match Any**—Set to require that user authorization attributes match any of the values in the Antivirus endpoint attributes you are configuring. • **Match All**—Set to require that user authorization attributes match all of the values in the endpoint attributes you are configuring, as well as satisfying the AAA attribute.

Table 32-22 Add/Edit Dynamic Access Policy Dialog Box > Logical Operations Tab (continued)

Element	Description
File	Select one of the following options if you defined File as an endpoint attribute: • **Match Any**—Set to require that user authorization attributes match any of the values in the Antivirus endpoint attributes you are configuring. • **Match All**—Set to require that user authorization attributes match all of the values in the endpoint attributes you are configuring, as well as satisfying the AAA attribute.
Personal Firewall	Personal firewall rules let you specify applications and ports for the firewall to allow or block. Select one of the following options if you defined Personal Firewall as an endpoint attribute: • **Match Any**—Set to require that user authorization attributes match any of the values in the Antivirus endpoint attributes you are configuring. • **Match All**—Set to require that user authorization attributes match all of the values in the endpoint attributes you are configuring, as well as satisfying the AAA attribute.
Process	Select one of the following options if you defined Process as an endpoint attribute: • **Match Any**—Set to require that user authorization attributes match any of the values in the Antivirus endpoint attributes you are configuring. • **Match All**—Set to require that user authorization attributes match all of the values in the endpoint attributes you are configuring, as well as satisfying the AAA attribute.
Registry	Registry key scans apply only to computers running Windows Microsoft Windows operating systems. Basic Host Scan ignores registry key scans if the computer is running Mac OS or Linux. Select one of the following options if you defined Registry as an endpoint attribute: • **Match Any**—Set to require that user authorization attributes match any of the values in the Antivirus endpoint attributes you are configuring. • **Match All**—Set to require that user authorization attributes match all of the values in the endpoint attributes you are configuring, as well as satisfying the AAA attribute.

Advanced Expressions Tab

Use the Advanced Expressions tab of the Add/Edit Dynamic Access Policy dialog box to set additional attributes for the dynamic access policy. You can configure multiple instances of each type of endpoint attribute. Be aware that this is an advanced feature that requires knowledge of LUA (www.lua.org).

Note For detailed information about advanced expressions, see About Advanced Expressions for AAA or Endpoint Attributes and Examples of DAP Logical Expressions.

Navigation Path

Open the Add/Edit Dynamic Access Policy Dialog Box, page 32-12, then click the **Advanced Expressions** tab.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2

Field Reference

Table 32-23 Add/Edit Dynamic Access Policy Dialog Box > Advanced Expressions Tab

Element	Description
Basic Expressions	This text box is populated with basic expressions based on the endpoint and AAA attributes that you configured in the dynamic access policy.
Relationship Drop-down List	Specify the relationship between the basic selection rules and the logical expressions you enter on this tab, that is, whether the new attributes add to or substitute for the AAA and endpoint attributes already set. Select one of the following options: • **Basic AND Advanced**—Creates an AND relationship between the basic and advanced expressions. Both the basic and advanced expressions defined in the dynamic access policy are considered while authenticating users. By default, this option is selected. • **Basic OR Advanced**—Creates an OR relationship between the basic and advanced expressions. Users are granted access to a session if either the basic or advanced expressions in the dynamic access policy are matched with the user policy. • **Basic Only**—Only the basic expressions defined in the DAP entry are used to determine whether the security appliance grants users access to a particular session. • **Advanced Only**—Only the advanced expressions defined in the DAP entry are used to authorize users for an SSL VPN session.
Advanced Expressions	Enter one or more logical expressions to set AAA or endpoint attributes other than what is possible in the AAA and Endpoint areas above. Enter free-form LUA text that defines new AAA and/or endpoint selection attributes. Security Manager does not validate text that you enter here; it just copies this text to the dynamic access policy XML file, and the security appliance processes it, discarding any expressions it cannot parse.

Cisco Secure Desktop Manager Policy Editor Dialog Box

Using the Cisco Secure Desktop Manager (CSDM) Policy Editor dialog box, you can configure prelogin policies, specify the checks to be performed between the time the user establishes a connection with the security appliance and the time the user enters the login credentials, and configure host scans. For an explanation of configuring CSD on an ASA device, see Configuring Cisco Secure Desktop Policies on ASA Devices, page 32-9.

Note The Cisco Secure Desktop Manager Policy Editor is an independent program. For information about configuring CSD, and what CSD can do for you, see the materials available online at http://www.cisco.com/en/US/products/ps6742/tsd_products_support_configure.html. Look specifically for information on configuring prelogin policies and host scan. Select the configuration guide for the CSD version you are configuring.

Navigation Path

Open the Dynamic Access Page (ASA), page 32-11, then click **Configure** from the Cisco Secure Desktop section (you must first specify a CSD package). The CSDM Policy Editor dialog box is displayed.

Related Topics

- Understanding DAP Attributes, page 32-4
- Configuring DAP Attributes, page 32-7
- Configuring Dynamic Access Policies, page 32-2