

VPN

---

# Deploying Cisco ASA VPN Solutions

---

**Volume 3**

Version 1.0

**Student Guide**

Text Part Number: 97-2924-01




**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

**DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.**

# Table of Contents

## Volume 3

### **Deployment of Advanced Cisco ASA Adaptive Security Appliance VPN Solutions 5-1**

Overview	5-1
Module Objectives	5-1
<b><u>Deploying VPN Authorization, Access Control, and Accounting</u></b>	<b>5-3</b>
Overview	5-3
Objectives	5-3
Configuration Choices, Basic Procedures, and Required Input Parameters	5-4
Deploying Local Authorization	5-10
Deploying External Authorization	5-30
Configuring Session Accounting	5-55
Troubleshoot Authorization and Accounting of a Clientless SSL VPN	5-59
Summary	5-64
<b><u>Deploying Cisco Secure Desktop in SSL VPNs</u></b>	<b>5-65</b>
Overview	5-65
Objectives	5-65
Configuration Choices, Basic Procedures, and Required Input Parameters	5-66
Installing, Enabling, and Customizing Cisco Secure Desktop	5-79
Configuring Prelogin Criteria	5-85
Configuring Prelogin Policies	5-93
Basic Host Scan	5-97
Endpoint Assessment	5-98
Advanced Endpoint Assessment	5-98
Configuring Advanced Endpoint Assessment	5-110
Troubleshooting Cisco Secure Desktop Operation for Clientless Connections	5-118
Summary	5-122
<b><u>Deploying Dynamic Access Policies</u></b>	<b>5-123</b>
Overview	5-123
Objectives	5-123
Configuration Choices, Basic Procedures, and Required Input Parameters	5-124
Configuring DAP	5-131
Aggregating DAP Records	5-150
Integrating Cisco Secure Desktop with DAP	5-157
Using LUA Expressions in DAP	5-162
Troubleshooting DAP	5-164
Summary	5-170
References	5-170
<b><u>Deploying High Availability and High Performance in SSL and IPsec VPNs</u></b>	<b>5-171</b>
Overview	5-171
Objectives	5-171
Configuration Choices, Basic Procedures, and Required Input Parameters	5-172
Deploying Redundant Peering	5-175
Deploying Cisco ASA Adaptive Security Appliance Active/Standby Failover	5-198
Deploying Dynamic-Routing-Based VPN Failover	5-209
Deploying Cisco ASA Adaptive Security Appliance VPN Clustering	5-220
Deploying High Availability and High Performance Using Network SLB	5-235
Deploying VPN QoS	5-237
Troubleshooting Cisco ASA Adaptive Security Appliance VPN Failover and Clustering	5-251
Summary	5-254
Module Summary	5-255

<b>Deploying External Authentication in Cisco AnyConnect Full Tunnel SSL VPNs</b>	<b>A-1</b>
Overview	A-1
Objectives	A-1
Deploying Certificate-Based Client Authentication Using External CAs	A-2
LDAP Password Management	A-26
Summary	A-32

# Deployment of Advanced Cisco ASA Adaptive Security Appliance VPN Solutions

---

## Overview

This module first describes how to deploy authorization, access control, and accounting for all types of remote access virtual private networks (VPNs). The module also describes how to use Cisco Secure Desktop to additionally protect Secure Sockets Layer (SSL) VPN deployments. The module also describes dynamic access policies (DAP), which can be used to assign additional session attributes based on client authentication, authorization, and accounting (AAA) attributes and client posture assessment. The module concludes with a description of high-availability and high-performance features in SSL and IP Security (IPsec) VPNs, which are essential for scalable and reliable VPN deployments.

## Module Objectives

Upon completing this module, you will be able to implement and maintain advanced VPN solutions on the Cisco ASA adaptive security appliance VPN gateway according to policies and environmental requirements. This ability includes being able to meet these objectives:

- Deploy and manage advanced authorization, access control, and accounting features of a Cisco AnyConnect full tunnel SSL VPN
- Deploy and manage Cisco Secure Desktop features and manage related faults in a Cisco SSL VPN
- Deploy and manage DAP on the Cisco ASA adaptive security appliance
- Deploy and manage high-availability and high-performance features



## Lesson 1

---

# Deploying VPN Authorization, Access Control, and Accounting

---

## Overview

An important security aspect of virtual private networks (VPNs) that is described in this course is the ability to selectively control access to internal enterprise resources. Scalable deployments implement a centralized approach, where the access control policy is stored on an external database. From the database, it is downloaded to VPN servers on demand. Accounting is needed to collect VPN connection records that are used to analyze potential security breaches and create VPN access patterns.

This lesson discusses the supported access control methods of Secure Sockets Layer (SSL) and Cisco Easy VPN solutions. It describes authorization and accounting that complement the authentication function.

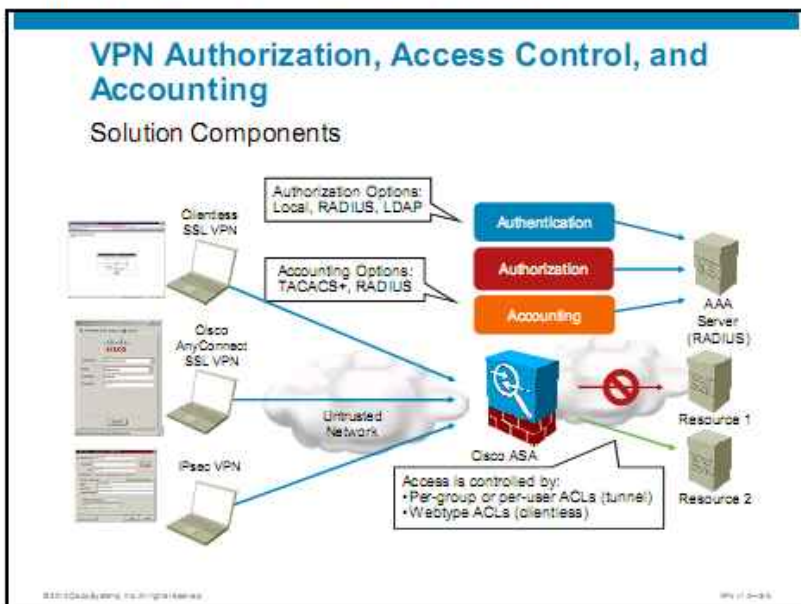
## Objectives

Upon completing this lesson, you will be able to deploy and manage advanced authorization, access control, and accounting features of a Cisco AnyConnect full tunnel SSL VPN. This ability includes being able to meet these objectives:

- Choose authorization, access control, and accounting methods in SSL and Cisco Easy VPN solutions
- Configure and verify local authorization
- Configure and verify remote authorization
- Configure and verify remote accounting
- Troubleshoot authorization, access control, and accounting features

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic introduces the access control features, authorization, and accounting in a VPN environment on the Cisco ASA adaptive security appliance.



Access control is tightly related to authorization, and in fact, both terms are often used interchangeably. Authorization specifies the actions that a user is permitted to perform. It depends on access control mechanisms, such as access control lists (ACLs) or webtype ACLs, to enforce the access policy.

The VPN implementation on the Cisco ASA adaptive security appliance supports these authorization methods:

- Local authorization uses ACLs or webtype ACLs to control access to internal resources. The policy can be applied to VPN connections for individual users or user groups.
- RADIUS or Lightweight Directory Access Protocol (LDAP) authorization can upload authorization attributes to the VPN server, which are then applied to individual user sessions.

VPN accounting is only supported with external authentication, authorization, and accounting (AAA) servers. It keeps track of VPN connections and stores the records on the external AAA database. These two AAA types are supported:

- TACACS+
- RADIUS

The most common AAA solution is RADIUS, because it supports all AAA components: authentication, authorization, and accounting.



# VPN Authorization, Access Control, and Accounting

## Access Control Methods

### Generic VPNs

- Simultaneous connections, access hours, maximum connect time, and so on

### Tunnel VPNs

- ACLs: address- and service-based

### Clientless selective portal features

- File access control: browsing, server entries, hidden share access
- Resource access control: browsing, server entries
- Application access control: port-forwarding lists, smart tunnel lists

### Clientless webtype ACLs

- Two types: URL-based, address- and service-based
- Support these URL types: ofs, citrix, citriks, ftp, http, https, imap4, nfs, pop3, smart tunnel, smtp, ssh, telnet, any

```
Permit http://10.0.0.1/
Permit ftp://*.cisco.com/
Permit http://*.cisco.com@01/
*implicit deny*
```

URL-Based ACL

```
Permit access to 10.1.1.2 TCP/2000
Permit access to 10.1.1.3 TCP/*
Permit access to * TCP/3000
*implicit deny*
```

Address- and Service-Based ACL

The security appliance offers various access control mechanisms for the supported VPN technologies:

- **Generic VPNs:** This feature suite is available for all types of SSL VPN types and remote access IP Security (IPsec) VPNs. It includes access restrictions such as the maximum number of simultaneous connections, access hours, maximum connect time, and so on.
- **Tunnel VPNs:** This family includes the Cisco AnyConnect SSL and remote access IPsec VPNs. Access control is enforced using ACLs that are defined using the classic approach that is based on addresses and services.
- **Clientless SSL VPNs:** Access control in Cisco SSL VPN solutions is enforced using selective portal features and webtype ACLs.
  - Selective portal features can control access to the following:
    - **Files:** Browsing, server entries, hidden share access
    - **Resources other than files:** Browsing, server entries
    - **Applications:** Port forwarding lists, smart tunnel lists
  - Webtype ACLs, also called webtypes, offer two types of traffic definitions:
    - **URL-based:** This ACL type consists of a number of permit or deny access control entries (ACEs) that control traffic based on the destination URL and port numbers. The syntax follows the widespread URL usage on the World Wide Web.
    - **Service-based:** This type is identical to the ACLs that are configured on Cisco IOS routers and most other Cisco devices. A service-based webtype ACL consists of a number of permit or deny ACEs that specify IP addresses, protocols, and port numbers of network services.

**Note** URL- and service-based ACEs can be mixed in the same webtype ACL. A webtype ACL has an implicit deny statement at the end, just like a normal ACL on most Cisco platforms.

## VPN Authorization, Access Control, and Accounting

### Policy Hierarchy

The security appliance applies user policies according to the following hierarchy:

1. **Dynamic access policies (DAP)** rules
2. **User profile**
3. **Group policy attached to the user profile**
4. **Group policy attached to the connection profile**
5. **DfltGrpPolicy** settings

All settings not specified in each level are automatically inherited from the lower-priority level.

Access control mechanisms can be applied at different levels in the VPN system. This precedence model determines effective access permissions (from highest to lowest precedence):

1. **Dynamic access policy (DAP):** DAP rules are built at the session connection time and can take into account temporary parameters, such as the endpoint secure posture. The precedence among multiple DAP policies is configured using a precedence value.
2. **User profile:** Parameters configured at the user level are the most granular settings that are configured statically (without considering security posture).
3. **Group policy attached to the user profile:** Parameters are defined in a group policy that is attached to the individual user.
4. **Group policy attached to the connection profile:** Parameters are defined in a group policy that is attached to the connection profile that the user connects to.
5. **DfltGrpPolicy settings:** This default group policy is preconfigured on the security appliance with default parameters. It can be modified but cannot be removed. By default, all other policy groups and users inherit the settings from the DfltGrpPolicy.

# VPN Authorization, Access Control and Accounting

## Authorization Options

Authorization Options	Benefits	Limitations
Local	Quick to deploy. Useful in very small or test environments.	Not scalable in environments with more than one VPN gateway.
External Radius/LDAP selects local group policy	Semicentralized policy configuration. AAA server authenticates users and authorizes them by selecting a local group policy.	Requires an external AAA server. Group policies configured locally on Cisco ASA adaptive security appliance.
External Radius/LDAP pushes authorization parameters	Centralized policy configuration. Local group policy can be selected as baseline for unspecified parameters.	Requires an external AAA server. Not all settings configurable on AAA server. Many parameters, such as port forwarding or smart tunnel lists configured locally and referenced by AAA server.

VPN authorization defines what actions a user is allowed to perform within the VPN connection. The authentication phase must be completed before authorization can be completed.

Authorization of VPN users can be configured locally on the security appliance, or using an external AAA database. RADIUS and LDAP are the only two supported remote authorization protocols.

You can take one of three general approaches when deploying VPN authorization:

- **Local:** With this approach, the entire ruleset, consisting of VPN access restrictions, ACLs, selective portal features, and webtype ACLs, must be configured locally on the VPN server. This approach is quick to deploy and often used in small networks. However, it does not scale to larger environments with multiple VPN servers providing high availability and load balancing.
- **External AAA server selects local group policy:** This method offers a semicentralized policy configuration, in which the external AAA server authenticates users and authorizes them by applying a locally configured group policy to the user session. The group policies still need to be configured locally on each security appliance in the network.
- **External AAA server applies authorization parameters:** This technique provides the most centralized policy configuration. The AAA server applies authorization settings to the user sessions by applying parameters that are stored in the AAA database. Not all settings are configurable on the AAA server. Some parameters, such as port forwarding or smart tunnel lists must be configured locally on the appliance and are then referenced by the AAA server. Optionally, the AAA server can reference a local policy group (defined on Cisco ASA adaptive security appliance), to provision a baseline for unspecified parameters. This method is used by the second approach (external AAA server selects local group policy).

## VPN Authorization, Access Control, and Accounting

### Accounting

- Accounting generates records about client activity.
  - Including start and stop of VPN sessions
- Cisco ASA does not support local accounting.
- Accounting does not require authentication to be performed against the same database.

Accounting	Use
RADIUS	Can use the same AAA server that is used for authentication and authorization. Does not require that authentication be performed on the same RADIUS AAA server.
TACACS+	Entire session is encrypted. Less common, because authorization cannot be performed on the same TACACS+ server.

Accounting of VPN sessions generates records about per-user session activity. It includes the start and stop time of each session.

The security appliance supports accounting using these AAA protocols.

- **RADIUS:** This option provides for simplified deployment by allowing the same AAA server to be used for authentication, authorization, and accounting. The protocol is widely used due to its extensible, standards-based blueprint.
- **TACACS+:** This method is less common, because authorization cannot be performed using the same TACACS+ server. In comparison to RADIUS, TACACS+ is more secure because it encrypts entire packet payloads instead of encrypting only passwords. This option is mostly used in environments consisting of only Cisco equipment with an existing TACACS+ infrastructure.

Local accounting on the security appliance is not supported.

Accounting does not require that authentication or authorization be performed against the same database. For example, a user can be authenticated using an LDAP server and accounting information can be sent to a TACACS+ server.

## VPN Authorization, Access Control, and Accounting

### AAA Server Chaining

- Some supported authentication servers do not provide authorization and accounting.
- AAA servers can be daisy-chained to offer all three features.

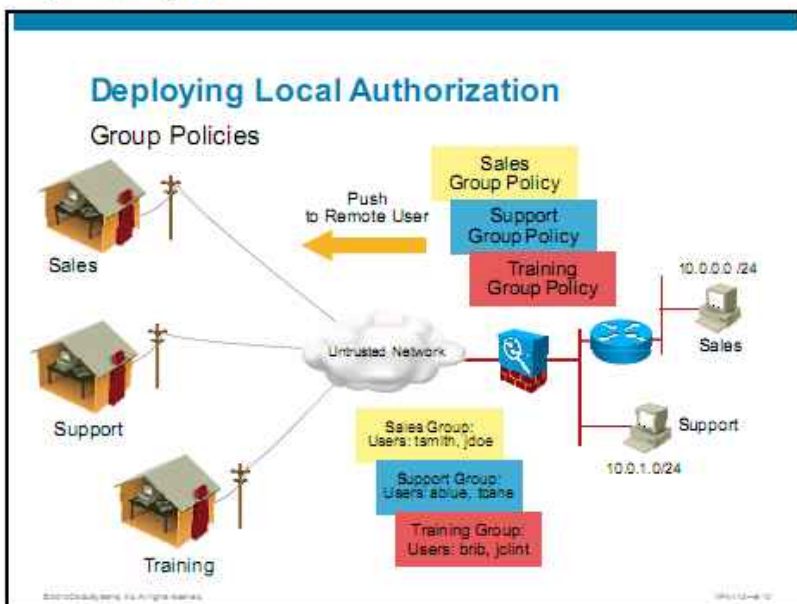


For the most flexibility, you can design the AAA system as a chain of two servers: the AAA front-end, and AAA back-end servers. The AAA servers play different roles in the AAA operations:

- **AAA front end** acts as the authentication proxy between the SSL VPN server and the back end. The front end typically does not contain user records and is therefore not used for authentication. Instead, it supports a wide set of authorization options and accounting. Because the users do not exist in the database of the front end, the authorization settings are configured on a group basis. This approach ensures scalable policy enforcement. In this figure, the front end uses RADIUS. It supports authentication, authorization, and accounting.
- **AAA back end** stores the user database but is typically not capable of providing authorization and accounting features. It can employ sophisticated one-time password (OTP) algorithms. An example of such a back-end approach is the RSA SDI server that is shown in the figure.

# Deploying Local Authorization

This topic describes how to configure local group policy authorization on the Cisco ASA adaptive security appliance.



Within a corporation, not everyone has the same access requirements. Customer service engineers may require 7-day, 24-hour access; sales entry personnel need 5-day, 8-hour access; and contractors might need access from 9 a.m. to 5 p.m. (0900 to 1700), with restricted server access. The security appliance can accommodate different access and usage requirements. By using group policies, you can define different rights and privileges on a group basis. A customer service engineer, sales entry person, and contractor can be assigned to different groups. Within each group, you can configure different access hours, access protocols, idle timeouts, and server restrictions.

A group policy is a set of user-oriented attribute and value pairs that are stored either internally on the security appliance or externally on a RADIUS server. The connection profile refers to a group policy that sets terms for user connections after the connection is established. Group policies enable you to apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user. Each remote VPN user belongs to a specific VPN group. As users connect to the VPN Server, the server identifies the group to which they belong. It then pushes the appropriate VPN group policy to the remote user.

If you decide to grant identical rights to all VPN users, you do not need to configure specific group policies; however, VPNs seldom work that way. For example, you might allow a finance group to access one part of a private network, a customer support group to access another part, and a sales group to access other parts. In addition, you might allow specific users within sales group to access systems that other sales users cannot access. Group policies provide the flexibility to do so securely.

The security appliance includes a default group policy named `DfltGrpPolicy`. This group policy always exists on the security appliance, but it does not take effect unless you configure the security appliance to use it. When you configure other group policies, any attribute that you do not explicitly specify takes its value from the default group policy. You cannot delete the default group policy, but you can modify it. You can also create one or more group policies specific to your environment. You can configure internal and external group policies. Internal groups are configured on the internal database of the security appliance. External groups are configured on an external authentication server, such as RADIUS.

Group policies include the following attributes:

- Identity
- Server definitions
- Tunneling protocols
- Filters
- Client configuration settings
- Connection settings
- Cisco AnyConnect-, clientless SSL VPN-, and IPsec-specific parameters

In the figure, there are three VPN group policies configured: Sales, Support, and Training. Each user belongs to one group. As the users establish VPN connections, the central site security appliance pushes a specific policy to each remote user.

To view the default group policy, enter the **show running-config all group-policy DfltGrpPolicy** command at the security appliance CLI.

By default, users inherit all user attributes from the assigned group policy. The security appliance also lets you assign individual attributes at the user level, overriding values in the group policy that apply to that user. For example, you can specify a group policy giving all users access during business hours, but give a specific user 24-hour access.

To assign attributes to an individual user, the user account must exist on the security appliance. For an existing user account, you can use the **username attributes** command to enter the configuration mode for username attributes and configure the attributes. Any attributes that you do not specify are inherited from the group policy. User-specific attributes always take precedence over group-specific attributes. By default, VPN users that you add with the **username** command have no attributes or group policy association. You must explicitly configure all values.

## Deploying Local Authorization

### Configuration Tasks

1. Configure ACL (full tunnel VPN).
2. Configure webtype ACL (clientless SSL VPN).
3. Configure group policy with required restrictions.
  - Single group policy can accommodate both full tunnel and clientless parameters.
  - Edit policy in appropriate menu to configure the relevant settings.
4. Apply group policy to connection profiles, users, or both.
  - User setting has precedence over connection profile.

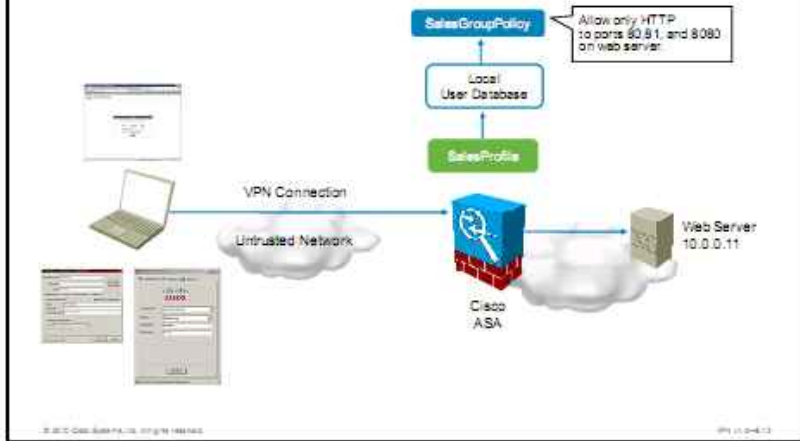
To configure local VPN authorization, you will perform these configuration tasks:

1. Configure an ACL (full tunnel VPN).
2. Configure a webtype ACL (clientless SSL VPN).
3. Configure a group policy with required restrictions using one of two possible approaches:
  - Define separate group policies for clientless and full tunnel users. This approach is more difficult to manage if the users are allowed multiple access types.
  - Define one group policy for a set of users with similar privileges. Enable multiple access types and configure the appropriate parameters through the respective configuration menu.
6. Apply the group policy to the connection profile, users, or both. The user setting has precedence over the connection profile.



## Deploying Local Authorization

### Configuration Scenario



In this scenario, you will authorize Sales users to access only common World Wide Web ports on the web server (10.0.0.11). This authorization will be achieved by applying appropriate ACLs to the Sales users who are connecting either via full tunnel VPNs (Cisco AnyConnect or IPsec), or clientless SSL VPNs. In addition, you will configure two generic parameters: a banner warning and idle timeout. These settings will be applied to all VPN types.

This example uses an already configured connection profile. Configuration of a connection profile is not discussed in this topic. The users are allowed to select a connection profile when they establish a connection. In this scenario, they will select the SalesProfile connection profile that will start local user authentication. The authorization parameters will be configured in local group policy SalesGroupPolicy, which will be assigned to local users on the ASA.

## Deploying Local Authorization

### Task 1: Configure ACL

The screenshot displays the Cisco ASA ACL Manager interface. The main window shows a table of ACLs under the heading 'COMMON\_WEB\_PORTS'. Three ACEs are listed:

#	Enabled	Source	Destination	Service	Action
1	<input checked="" type="checkbox"/>	any	10.0.0.11	3000	Permit
2	<input checked="" type="checkbox"/>	any	10.0.0.11	81	Permit
3	<input checked="" type="checkbox"/>	any	10.0.0.11	Http	Permit

Annotations in the image include:

- A callout box pointing to the three ACEs: "Three permit ACEs: permit tcp any host 10.0.0.11 3000, permit tcp any host 10.0.0.11 81, permit tcp any host 10.0.0.11 80, implicit deny at end".
- A dialog box titled 'Rename ACL' with 'ACL Name: COMMON\_WEB\_PORTS' and a callout: "Specify ACL name".
- A dialog box titled 'Add ACE' with fields for Source, Destination, Service, and Action, and a callout: "Specify ACE parameters".

Configuration > Remote Access VPN > Network (Client) Access > Advanced > ACL Manager

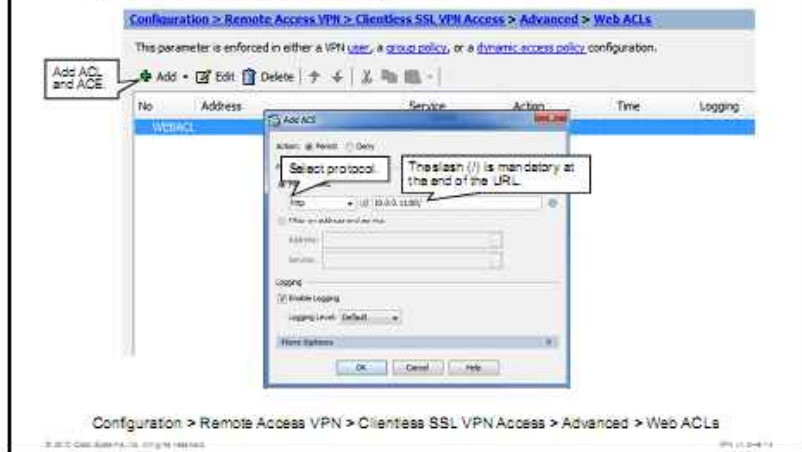
To locally authorize access through full tunnel VPNs (Cisco AnyConnect or IPsec), you need to define ACLs by completing the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > ACL Manager**.
- Step 2** Click **Add > ACL** to create an ACL and enter its name. Click **OK**. In the example, COMMON\_WEB\_PORTS ACL is created.
- Step 3** Select the previously created ACL and click **Add > ACE** to create the required ACEs that define the traffic filter. Click **OK**. Repeat this step to add all required ACEs.
- Step 4** Click **Apply** to apply the configuration.

**Note** An ACL has an implicit deny any statement at the end. This deny statement is not applied when the ACL is selected by a DAP record. DAP records support concatenated ACLs, and the implicit deny is applied at the end of the ACL chain. An ACL must consist of only permit or only deny statements to be applied to a DAP record. DAP is covered in a later lesson.

## Deploying Local Authorization

### Task 2: Configure Webtype ACL



To authorize access through clientless SSL VPNs, you need to define webtype ACLs by completing the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.
- Step 2** Click **Add** to create a new ACL.
- Step 3** Enter a name for the webtype ACL. In this example, the name is **WEBACL**. Click **OK** (not shown in the example).
- Step 4** Select the created ACL and click **Add** to create an ACE that is a member of the ACL.
- Step 5** Choose the desired ACE action: permit or deny.
- Step 6** If you want to configure a URL-based ACE, click the **Filter on URL** radio button and choose the required protocol from the drop-down list. Enter the URI in the adjacent field. The URL may contain a port number and must end with a slash (/).
- Step 7** If you want to configure a service-based ACE, make the appropriate selection, and enter the destination IP address and port number or service name.
- Step 8** Click **OK** and repeat the described procedure to add the required number of ACEs to the webtype ACL.
- Step 9** Click **Apply** to apply the configuration.

**Note** A webtype ACL can contain a mix of URL- and service-based ACEs. Every webtype ACL has an implicit deny any statement at the end that prevents all other unspecified access methods.

As with an ACL, the implicit deny at the end of the webtype ACL is not applied when the webtype ACL is selected by a DAP record.

## Deploying Local Authorization

### Task 2: Configure Webtype ACL (Cont.)

The screenshot shows the configuration page for Webtype ACLs. The breadcrumb path is Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs. A note states: "This parameter is enforced in either a VPN user, a group policy, or a dynamic access policy configuration." Below this are controls for Add, Edit, Delete, and a search icon. The main table lists three ACL entries:

No.	Address	Service	Action	Time	Logging
1	http://30.0.0.1:80/		Permit		
2	http://20.0.0.1:81/		Permit		
3	http://30.0.0.1:8080/		Permit		

Below the table, two callouts are present: "URL Notation" pointing to the address column and "Implicit Deny at the End" pointing to the bottom of the table.

Expression	Description	Example
*	Matches none or any number of characters	http://*.cisco.com/ - any servers in cisco.com domain
?	Matches any single character	http://ww?.cisco.com/ - for example www.cisco.com and ww1.cisco.com
Range []	Matches any character in the range	http://www.cisco.com:8[01]/ - www.cisco.com:80 and www.cisco.com:81

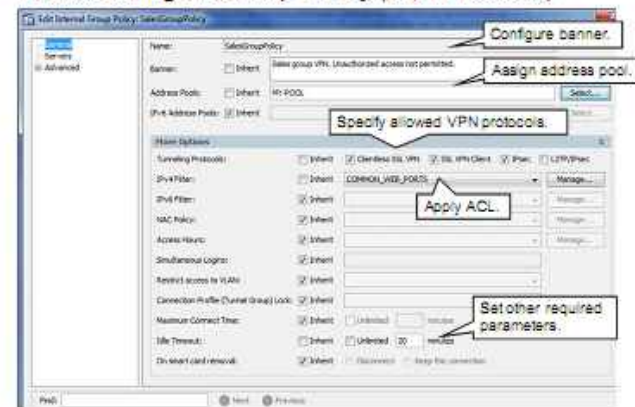
You can use regular expressions to match multiple URIs with a single ACE. These are the most common supported regular expressions:

- Asterisk (\*) is used as a wildcard to match none or any number of characters. An example is `http://*.cisco.com/`. This expression matches any servers in domain `cisco.com`.
- Question mark (?) matches any single character. An example is `http://ww?.cisco.com/`. This expression matches multiple servers, such as `www.cisco.com` and `ww1.cisco.com`.
- Range [] matches any character in the range. An example is `http://www.cisco.com:8[01]/`. This expression matches `www.cisco.com:80` and `www.cisco.com:81`.

The pane in at the top portion of the figure illustrates the webtype ACL that will be applied to the group policy in the current scenario. It allows access to the common ports (80, 81, and 8080) of the web service that is running on the host `Insrv1`.

## Deploying Local Authorization

### Task 3: Configure Group Policy (Client Access)



Next, you create a local group policy. The group policy can be created and modified using two Cisco Adaptive Security Device Manager (Cisco ASDM) menus:

- **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**
- **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**

You may define a group policy in one menu and then edit it through the other menu, the difference being in the list of displayed parameters. This figure displays the full tunnel settings of the SalesGroupPolicy.

To configure a group policy using Cisco ASDM, complete the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
- Step 2** Select a group policy that you want to configure from the table and click **Edit**. To add the new group policy, click the **Add** button.
- Step 3** Uncheck the **Inherit** check box near the Banner keyword and specify banner in the field next to the check box.
- Step 4** Uncheck the **Inherit** check box near the Tunneling Protocols keyword and specify which VPN protocols can be used by clicking the proper check boxes. In the example, Clientless SSL VPN, SSL VPN Client, and IPsec are allowed inside the policy group.
- Step 5** Uncheck the **Inherit** check box near the IPv4 Filter keyword and select the previously configured ACL from the drop-down menu. In the example, the COMMON\_WEB\_PORTS ACL is selected.
- Step 6** Uncheck the **Inherit** check box near the Idle Timeout keyword and specify idle timeout by entering a number into the Minutes field. In the example, idle timeout is set to 20 minutes.


- Step 7** Click **OK**.
- Step 8** Click **Apply** to apply the configuration.

**Note** In addition to internal group policies, you can also configure external group policies. External group policies are used in IPsec remote access VPNs, where they correspond to user groups, which are actually Internet Key Exchange (IKE) identity names. An external group policy requires the configuration of a pre-shared key (PSK) that is needed for IKE Phase 1 authentication. External group policies are not applicable to SSL VPNs.

## Deploying Local Authorization

### Task 3: Configure Group Policy (Clientless Access)

- Common options configured in Network (Client) Access menu are:



Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

Next, you configure authorization settings for the clientless SSL VPN users. To configure a group policy for clientless access using Cisco ASDM, complete the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**.
- Step 2** Uncheck the **Inherit** check box near the Web ACL keyword and select the previously configured wectype ACL from the drop-down menu. In the example, the wectype ACL named WEBACL is selected.
- Step 3** Click **OK**.
- Step 4** Click **Apply** to apply the configuration.

This figure displays the clientless SSL VPN settings of the SalesGroupPolicy. The generic settings, such as banner, and idle timeout have already been set and can be verified here. The settings that apply to the full tunnel, such as IP version 4 (IPv4) and IP version (IPv6) filters, and Network Admission Control (NAC) policy are omitted.

## Deploying Local Authorization

### Task 4: Apply Group Policy

- Group policy can be applied to connection profiles or local users



Configuration > Remote Access VPN > AAA/Local Users

Configuration > Device Management > Users/AAA

The group policy needs to be applied either to the connection profile or to individual user. The user setting takes precedence over the connection profile setting. In this example, the group policy SalesGroupPolicy is applied at the user level.

To apply a group policy to a user profile on the Cisco ASA adaptive security appliance, complete the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > AAA/Local Users**.
- Step 2** Choose the **VPN Policy** option from the menu on the left.
- Step 3** Uncheck the **Inherit** check box near the Group Policy keyword and select the previously configured group policy from the drop-down menu. In the example, the SalesGroupPolicy is selected.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration.

# Configuring Local VPN Authorization

## CLI Configuration

```
access-list COMMON_WEB_PORTS extended permit tcp any host 10.0.0.11
eq 8080
access-list COMMON_WEB_PORTS extended permit tcp any host 10.0.0.11
eq 81
access-list COMMON_WEB_PORTS extended permit tcp any host 10.0.0.11
eq www
!
access-list WEBACL webtype permit url http://10.0.0.11:80/
access-list WEBACL webtype permit url http://10.0.0.11:81/
access-list WEBACL webtype permit url http://10.0.0.11:8080/
```

Configure  
access list

Configure  
webtype  
access list

To configure the access list and web access list using the command line interface (CLI), use the **access list extended** and **access-list webtype** commands respectively.

### access-list extended

To add an ACE, use the **access-list extended** command in global configuration mode. An ACL is made up of one or more ACEs with the same access list ID. ACLs are used to control network access or to specify traffic for many features to act upon. To remove an ACE, use the **no** form of this command. To remove the entire ACL, use the **clear configure access-list** command.

```
access-list id [line line-number] [extended] {deny | permit} {protocol | object-group protocol_obj_grp_id} {src_ip mask | interface ifc_name | object-group network_obj_grp_id} [operator port | object-group service_obj_grp_id] {dest_ip mask | interface ifc_name | object-group network_obj_grp_id} [operator port | object-group service_obj_grp_id] object-group icmp_type_obj_grp_id] [log [[level] [interval secs] | disable | default]] [inactive | time-range time_range_name]
```

### access-list extended Parameters

Parameter	Description
<b>default</b>	(Optional) Sets logging to the default method, which is to generate system log message 106023 for each denied packet.
<b>deny</b>	Denies a packet if the conditions are matched. In the case of network access (the <b>access-group</b> command), this keyword prevents the packet from passing through the adaptive security appliance. In the case of applying application inspection to a class map (the <b>class-map</b> and <b>inspect</b> commands), this keyword exempts the traffic from inspection. Some features do not allow ACEs to be used, such as NAT. See the command documentation for each feature that uses an access list for more information.



Parameter	Description
<code>dest_ip</code>	Specifies the IP address of the network or host to which the packet is being sent. Enter the <b>host</b> keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the <b>any</b> keyword instead of the address and mask to specify any address.
<code>disable</code>	(Optional) Disables logging for this ACE.
<code>extended</code>	(Optional) Adds an ACE.
<code>icmp_type</code>	(Optional) If the protocol is Internet Control Message Protocol (ICMP), specifies the ICMP type.
<code>id</code>	Specifies the access list ID, as a string or integer up to 241 characters in length. The ID is case-sensitive.  <b>Tip</b> Use all capital letters to see the access list ID better in your configuration.
<code>inactive</code>	(Optional) Disables an ACE. To re-enable it, enter the entire ACE without the <b>inactive</b> keyword. This feature lets you keep a record of an inactive ACE in your configuration to make re-enabling easier.
<code>interface ifc_name</code>	Specifies the interface address as the source or destination address.  <b>Note</b> You must specify the <b>interface</b> keyword instead of specifying the actual IP address in the access list when the traffic destination is a device interface.
<code>interval secs</code>	(Optional) Specifies the log interval at which to generate system log message 106100. Valid values are from 1 to 600 sec. The default is 300.
<code>level</code>	(Optional) Sets the system log message 106100 severity level from 0 to 7. The default level is 6 (informational).
<code>line line-num</code>	(Optional) Specifies the line number at which to insert the ACE. If you do not specify a line number, the ACE is added to the end of the access list. The line number is not saved in the configuration; it only specifies where to insert the ACE.
<code>log</code>	(Optional) Sets logging options when an ACE matches a packet for network access (an access list that is applied with the <b>access-group</b> command). If you enter the <b>log</b> keyword without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 sec). If you do not enter the <b>log</b> keyword, then the default system log message 106023 is generated.
<code>mask</code>	The subnet mask for the IP address. When you specify a network mask, the method is different from the Cisco IOS Software <b>access-list</b> command. The adaptive security appliance uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
<code>object-group icmp_type_obj_grp_id</code>	(Optional) If the protocol is ICMP, specifies the identifier of an ICMP-type object group.
<code>object-group network_obj_grp_id</code>	Specifies the identifier of a network object group.
<code>object-group protocol_obj_grp_id</code>	Specifies the identifier of a protocol object group.

Parameter	Description
<code>object-group</code> <code>service_obj_grp_id</code>	(Optional) If you set the protocol to TCP or User Datagram Protocol (UDP), specifies the identifier of a service object group.
<code>operator</code>	(Optional) Matches the port numbers that are used by the source or destination. The permitted operators are as follows: <ul style="list-style-type: none"> <li>■ <b>lt</b>: less than</li> <li>■ <b>gt</b>: greater than</li> <li>■ <b>eq</b>: equal to</li> <li>■ <b>neq</b>: not equal to</li> <li>■ <b>range</b>: an inclusive range of values. When you use this operator, specify 2 port numbers, for example: <code>range 100 200</code></li> </ul>
<code>permit</code>	Permits a packet if the conditions are matched. In the case of network access (the <b>access-group</b> command), this keyword lets the packet pass through the adaptive security appliance. In the case of applying application inspection to a class map (the <b>class-map</b> and <b>inspect</b> commands), this keyword applies inspection to the packet.
<code>port</code>	(Optional) If you set the protocol to TCP or UDP, specifies the integer or name of a TCP or UDP port. Domain Name System (DNS), Discard, Echo, Ident, Network Time Protocol (NTP), remote procedure call (RPC), Sun Remote Procedure Call (SunRPC), and Talk each require one definition for TCP and one for UDP. TACACS+ requires one definition for port 49 on TCP.
<code>protocol</code>	Specifies the IP protocol name or number. For example, UDP is 17, TCP is 6, and exterior gateway protocol (EGP) is 47.
<code>src_ip</code>	Specifies the IP address of the network or host from which the packet is being sent. Enter the <b>host</b> keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the <b>any</b> keyword instead of the address and mask to specify any address.
<code>time-range</code> <code>time_range_name</code>	(Optional) Schedules each ACE to be activated at specific times of the day and week by applying a time range to the ACE.

## access-list webtype

To add an ACL to the configuration that supports filtering for clientless SSL VPN, use the **access-list webtype** command in global configuration mode. To remove the access list, use the **no** form of this command.

```
access-list id webtype {deny | permit} url [url_string | anyU] [log [[disable | default] | level]
[interval secs] [time_range name]]
```

```
access-list id webtype {deny | permit} tcp [host ip_address | ip_address subnet_mask
| anyA] [oper port [port]] [log [[disable | default] | level] [interval secs] [time_range name]]
```

### access-list webtype Parameters

Parameter	Description
<code>anyA</code>	Specifies all IP addresses
<code>anyU</code>	(Optional) Specifies all URLs
<code>deny</code>	Denies access if the conditions are matched
<code>host ip_address</code>	Specifies a host IP address
<code>id</code>	Name or number of an access list

Parameter	Description
<code>interval secs</code>	(Optional) Specifies the time interval at which to generate system log message 106100; valid values are from 1 to 600 sec
<code>ip_address ip_mask</code>	Specifies a specific IP address and subnet mask
<code>log [[disable   default]   level]</code>	(Optional) Specifies that system log message 106100 is generated for the ACE
<code>oper</code>	Compares <code>ip_address</code> ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range)
<code>permit</code>	Permits access if the conditions are matched
<code>port</code>	Specifies the decimal number or name of a TCP or UDP port
<code>time_range name</code>	(Optional) Specifies a keyword for attaching the time-range option to this access list element
<code>url</code>	Specifies that a URL should be used for filtering
<code>url_string</code>	(Optional) Specifies the URL that is to be filtered

## Configuring Local VPN Authorization

### CLI Configuration (Cont.)

```

group-policy SalesGroupPolicy internal
group-policy SalesGroupPolicy attributes
  banner value Sales group VPN. Unauthorized access not permitted.
  vpn-idle-timeout 20
  vpn-filter value COMMON_WEB_PORTS
  vpn-tunnel-protocol IPSec svc webvpn
  webvpn
  filter value WEBACL
!
username LocalSalesUser password lMjKvt0e3k4/gglj encrypted
username LocalSalesUser attributes
  vpn-group-policy SalesGroupPolicy

```

Annotations in the diagram:

- Callout for `group-policy SalesGroupPolicy internal`: Create local group policy.
- Callout for `vpn-filter value COMMON_WEB_PORTS`: Specify group policy attributes.
- Callout for `vpn-group-policy SalesGroupPolicy`: Assign a group policy to a user.

To configure local VPN authorization using the CLI, use the following commands. Use the **group-policy internal** command to create a group policy. Use the **group-policy attributes** command to enter group-policy configuration mode. Use the **banner** command to configure a banner. Use the **vpn-idle-timeout** command to specify the VPN idle timeout. Use the **vpn-filter** command to specify the ACL to use for VPN connections. Use the **vpn-tunnel-protocol** command to select allowed VPN protocols inside the group policy. Finally, enter clientless VPN attributes configuration mode using the **webvpn** command and use the **filter** command to specify webtype ACL to use for clientless VPN connections.

To assign group policy to a user, enter user configuration mode using the **username attributes** command and use the **vpn-group-policy** command.

## group-policy

To create or edit a group policy, use the **group-policy** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

```
group-policy name { internal [from group-policy_name] | external server-  
group server_group password server_password }
```

### group-policy Parameters

Parameter	Description
<b>external server-group</b> <i>server_group</i>	Specifies the group policy as external and identifies the AAA server group for the adaptive security appliance to query for attributes.
<b>from</b> <i>group-policy_name</i>	Initializes the attributes of this internal group policy to the values of a preexisting group policy.
<b>internal</b>	Identifies the group policy as internal.
<i>name</i>	Specifies the name of the group policy. The name can be up to 64 characters long and can contain spaces. Group names with spaces must be enclosed in double quotes, for example, "Sales Group."
<b>password</b> <i>server_password</i>	Provides the password to use when retrieving attributes from the external AAA server group. The password can be up to 128 characters long and cannot contain spaces.

## group-policy attributes

To enter group-policy configuration mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, use the **no** version of this command. In group-policy configuration mode, you can configure attribute-value pairs for a specified group policy or enter group-policy webvpn configuration mode to configure WebVPN attributes for the group.

```
group-policy name attributes
```

### group-policy attributes Parameters

Parameter	Description
<i>name</i>	Specifies the name of the group policy

## banner (group-policy)

To display a banner, or welcome text, on remote clients when they connect, use the **banner** command in group-policy configuration mode. To delete a banner, use the **no** form of this command. This option allows inheritance of a banner from another group policy. To prevent inheriting a banner, use the **banner none** command.

```
banner { value banner_string | none }
```

---

**Note** If you configure multiple banners under a VPN group policy, and you delete any one of the banners, all banners will be deleted.

---

## banner (group-policy) Parameters

Parameter	Description
<code>none</code>	Sets a banner with a null value, which disallows a banner. Prevents inheriting a banner from a default or specified group policy.
<code>value banner_string</code>	Constitutes the banner text. Maximum string size is 500 characters. Use the "\n" sequence to insert a carriage return.

## vpn-idle-timeout

To configure a user timeout period, use the **vpn-idle-timeout** command in group-policy configuration mode or in username configuration mode. If there is no communication activity on the connection in this period, the adaptive security appliance terminates the connection.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a timeout value from another group policy. To prevent inheriting a value, use the **vpn-idle-timeout none** command.

**vpn-idle-timeout** {minutes | none}

### vpn-idle-timeout Parameters

Parameter	Description
<code>minutes</code>	Specifies the number of minutes in the timeout period. Use an integer between 1 and 35,791,394.
<code>none</code>	Uses the global WebVPN default-idle-timeout value (seconds) from the command: <code>hostname (config-webvpn) #default-idle-timeout</code> The range for this value in the WebVPN <b>default-idle-timeout</b> command is 60–86,400 sec. The default Global WebVPN Idle timeout in seconds—default is 1800 sec (30 min).

## vpn-tunnel-protocol

To configure a VPN tunnel type (IPsec, L2TP over IPsec, SVC, or WebVPN), use the **vpn-tunnel-protocol** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

**vpn-tunnel-protocol** {ipsec | l2tp-ipsec | svc | webvpn}

### vpn-tunnel-protocol Parameters

Parameter	Description
<code>ipsec</code>	Negotiates an IPsec tunnel between two peers (a remote access client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
<code>l2tp-ipsec</code>	Negotiates an IPsec tunnel for a Layer 2 Tunneling Protocol (L2TP) connection.
<code>svc</code>	Negotiates an SSL VPN tunnel with an SSL VPN client.
<code>webvpn</code>	Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client.

## webvpn (group-policy and username modes)

To enter this webvpn mode, use the **webvpn** command in group-policy configuration mode or in username configuration mode. To remove all commands that are entered in webvpn mode, use the **no** form of this command. These **webvpn** commands apply to the username or group policy from which you configure them.

The **webvpn** commands for group policies and usernames define access to files, Messaging Application Programming Interface (MAPI) proxy, URLs, and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter.

### webvpn

## filter

To specify the name of the access list to use for WebVPN connections for this group policy or username, use the **filter** command in webvpn configuration mode. To remove the access list, including a null value that is created by issuing the **filter none** command, use the **no** form of this command.

**filter** {value *ACLname* | none}

### filter Parameters

Parameter	Description
<b>none</b>	Indicates that there is no webtype ACL. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
<b>value</b> <i>ACLname</i>	Provides the name of the previously configured ACL.

## vpn-filter

To specify the name of the ACL to use for VPN connections, use the **vpn-filter** command in group policy or username mode. To remove the ACL, including a null value that is created by issuing the **vpn-filter none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **vpn-filter none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **vpn-filter** command to apply those ACLs.

**vpn-filter** {value *ACLname* | none}

### vpn-filter Parameters

Parameter	Description
<b>none</b>	Indicates that there is no access list. Sets a null value, which disallows an access list. Prevents inheriting an access list from another group policy.
<b>value</b> <i>ACLname</i>	Provides the name of the previously configured access list.

## username attributes

To enter username attributes mode, use the **username attributes** command in username configuration mode. To remove all attributes for a particular user, use the **no** form of this command and append the username. To remove all attributes for all users, use the **no** form of this command without appending a username. The attributes mode lets you configure attribute-value pairs for a specified user.

username {name} attributes

### username attributes Parameters

Parameter	Description
name	Provides the name of the user

### vpn-group-policy

To have a user inherit attributes from a configured group policy, use the **vpn-group-policy** command in username configuration mode. To remove a group policy from a user configuration, use the **no** version of this command. Using this command lets users inherit attributes that you have not configured at the username level.

vpn-group-policy {group-policy name}

### vpn-group-policy Parameters

Parameter	Description
group-policy name	Provides the name of the group policy

**Verifying Local Authorization**  
Cisco AnyConnect User-Side Verification

1. Cisco AnyConnect VPN Client login screen. Username: LocalSalesUser. Callout: Username Case-Sensitive.

2. Cisco AnyConnect VPN Client showing a Banner message. Buttons: Accept, Disconnect.

3. Windows Command Prompt showing a failed ping to 10.0.0.111. Callout: Ping to web server fails.

4. Windows Internet Explorer showing a successful HTTP connection to http://10.0.0.11:80 works. Displaying IIS7 welcome page.

The user-side verification of local authorization for full tunnel access is performed in this order:

- Step 1** Connect to SSL VPN via the sales profile (alias of the Sales-Profile connection profile) and log in as a local user (LocalSalesUser). The username and password are case-sensitive.
- Step 2** View the banner message and click **Accept**.
- Step 3** Verify that unauthorized traffic is blocked (ICMP in this example).
- Step 4** Verify that authorized traffic is permitted (HTTP access to the Web Server on ports 80/81/8080).

## Verifying Local Authorization

### Clientless SSL VPN User-Side Verification

1 Login

Please enter your username and password.

GROUP sales-profile

USERNAME LocalSalesUser

PASSWORD

Login

Username Case-Sensitive

2 SSL VPN Service

Banner

Sales group VPN. Unauthorized access not permitted.

Cancel Continue

Proceed

3 SSL VPN Service

Address http:// [insert 2002] Browse

Unauthorized Port

4 Connection failed

Access to this resource has been denied.

Back

Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

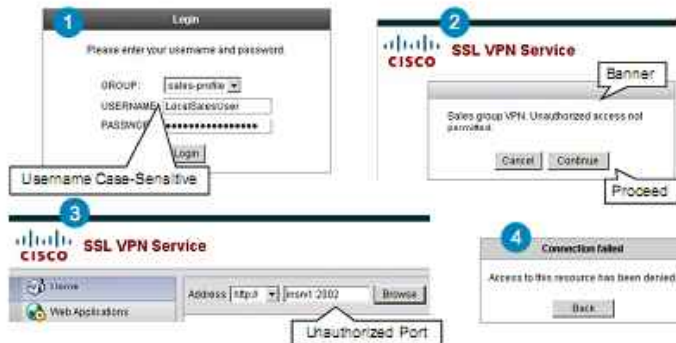
The user-side verification of local authorization for clientless SSL VPN access is performed in this order:

- Step 1** Connect to SSL VPN via the sales-profile (alias of the Sales-Profile connection profile) and log in as a local user (LocalSalesUser). The username and password are case-sensitive.
- Step 2** View the banner message and click **Continue**.
- Step 3** Attempt to access unauthorized resources (HTTP to port 2002 in this example).
- Step 4** View the message that informs you that the traffic is blocked.



## Verifying Local Authorization

### Clientless SSL VPN User-Side Verification



Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

The server-side verification of local authorization can be performed by browsing to the Monitoring > VPN > VPN Statistics > Sessions menu and viewing the details of the respective connection.

You verify both full tunnel users and clientless users are connected via the Sales-Profile and that the local group policy SalesGroupPolicy has been applied to the sessions.

# Deploying External Authorization

This topic describes how to deploy external authorization of VPN sessions on the Cisco ASA adaptive security appliance.

Attribute	VPN Type	Values	Example
primary-dns secondary-dns	Generic	IP_address	webvpn:primary-dns=10.0.0.20
wins-server-primary wins-server-secondary	Generic	IP_address	webvpn:wins-server- primary=10.0.0.20
addr	Full tunnel VPN	IP_address	webvpn:addr=10.10.10.1
addr-pool	Full tunnel VPN	name	webvpn:addr-pool=pool1
file-access	Clientless SSL VPN	0 (disable), 1 (enable)	webvpn:file-access=1
file-browse	Clientless SSL VPN	0 (disable), 1 (enable)	webvpn:file-browse=1
file-entry	Clientless SSL VPN	0 (disable), 1 (enable)	webvpn:file-entry=1
home-page	Clientless SSL VPN	URL	webvpn:home-page=osoo.com
port-forward-name	Clientless SSL VPN	name	webvpn:port-forward- name=PortForwarderSQL
port-forward-list	Clientless SSL VPN	name	webvpn:port-forward- list=PortForwardList1

The table lists some VPN authorization attributes. Some attributes define generic parameters, and may describe the network infrastructure, such as DNS, or Microsoft Windows Internet Name Service (WINS) servers. Some attributes refer some to tunnel VPNs, and others relate to selective portal features that are available through the portal.

## VPN Authorization Attributes

Attribute	Type of Value	Values	Default
addr (Framed-IP-Address <sup>1</sup> )	ipaddr	IP_address	—
addr-pool	string	name	—
auto-applet-download	integer	0 (disable) 1 (enable)	0
banner	string	—	—
default-domain	string	—	—
dns-servers	ipaddr	IP_address	—
dpd-client-timeout	integer (seconds)	0 (disabled)–3600	300
dpd-gateway-timeout	integer (seconds)	0 (disabled)–3600	300
file-access	integer	0 (disable) 1 (enable) <sup>1</sup>	0
file-browse	integer	0 (disable) 1 (enable) <sup>2</sup>	0
file-entry	integer	0 (disable) 1 (enable) <sup>3</sup>	0
hide-uribar	integer	0 (disable) 1 (enable) <sup>4</sup>	0
home-page	string	—	—
idletime (Idle-Timeout <sup>5</sup> )	integer (seconds)	0–3600	2100
ie-proxy-exception	string	DNS_name	—
	ipaddr	IP_address	—
ie-proxy-server	ipaddr	IP_address	—
nbnslst-name	string	name	—
port-forward-name	string	name	—
primary-dns	ipaddr	IP_address	—
secondary-dns	ipaddr	IP_address	—
timeout (Session-Timeout <sup>6</sup> )	integer (seconds)	1–1,209,600	43,200
urllst-name	string	name	—
wins-server-primary	ipaddr	IP_address	—
wins-server-secondary	ipaddr	IP_address	—
wins-servers	ipaddr	IP_address	—

<sup>1</sup> Any integer other than 0 enables this feature.

<sup>2</sup> Any integer other than 0 enables this feature.

<sup>3</sup> Any integer other than 0 enables this feature.

<sup>4</sup> Any integer other than 0 enables this feature.

<sup>5</sup> Standard Internet Engineering Task Force (IETF) RADIUS attribute.

<sup>6</sup> Standard IETF RADIUS attribute.

## External VPN Authorization

### Input Parameters

Parameter	Description
RADIUS connectivity parameters	Cisco ASA interface connecting to server Server name or IP address Encryption password Radius ports (1812/1813 or 1645/1646)
LDAP connectivity parameters	Cisco ASA interface connecting to server Server name or IP address Connection port and type [389/636(SSL)] Server type (Generic/Microsoft/Novell/OpenLDAP/Sun)
LDAP directory parameters	Base DN, login DN, group base DN Login password Scope Attribute names used by the LDAP host Mapping of LDAP attributes to SSL VPN attributes

To implement external authorization of clientless SSL VPN sessions, you need to gather input parameters pertaining to these areas:

1. **Settings necessary to establish RADIUS communications:** These parameters include the RADIUS server name or IP address, the ASA interface connecting to the RADIUS server, encryption password, and the ports on which the authentication and accounting services are running. (The ports are typically 1812/1813 or 1645/1646, or both.)
2. **Settings necessary to establish LDAP communications:** These parameters include the LDAP server name or IP address, the Cisco ASA adaptive security appliance interface connecting to the LDAP server, connection port and type (389/636-SSL), and the server type (generic, Microsoft, Novell, OpenLDAP, Sun).
3. **Necessary parameters to access the LDAP database and map its records to SSL VPN elements:** These parameters include the Base distinguished name (DN), Login DN, Group Base DN, Login password, scope, attribute names that are used by the LDAP host, and the mapping of LDAP attributes to SSL VPN attributes.

## Configuring External Authorization

### Configuration Tasks

#### VPN Gateway

1. Add external AAA server (RADIUS or LDAP).
2. (Optional) Configure LDAP attribute map.
3. Assign external AAA server to connection profile.
4. (Optional) Create baseline group policies that are referenced by external AAA server.

#### Authorization Server

1. Configure AAA client.
2. Create users and user groups.
3. (Optional) Define IETF Attribute 25 to reference a baseline group policy.
4. (Optional) Prepare authorization interface.
5. (Optional) Configure specific authorization parameters.

To configure external authorization, you will need to configure two components: the VPN gateway, and the authorization server.

To enable external authorization on the security appliance, perform the following configuration tasks:

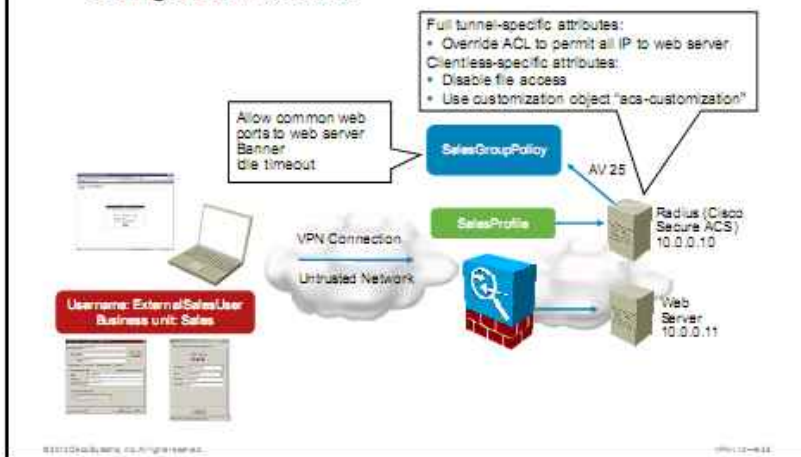
1. Add an external AAA server (RADIUS or LDAP).
2. Optionally, configure an LDAP attribute map.
3. Assign the external AAA server to a connection profile.
4. Optionally, create baseline group policies that are referenced by the external AAA server.

To configure authorization functionality on the AAA server, perform the following configuration tasks:

1. Configure an AAA association.
2. Create users and user groups.
3. Optionally, define IETF Attribute 25 to reference a baseline group policy.
4. Optionally, prepare the authorization interface and configure specific authorization parameters.

## Configuring External VPN Authorization

### Configuration Scenario



This figure presents the configuration scenario that is used in upcoming configuration tasks. You will configure the Cisco ASA adaptive security appliance to authenticate and authorize clientless SSL VPN users on the external RADIUS server. The security appliance has a local group policy named "SalesGroupPolicy" that will be referenced by the RADIUS server when the appliance is authorizing users belonging to the sales group. The group policy SalesGroupPolicy has been configured in the previous example. In addition to selecting the local group policy, the AAA server will override some parameters of that local group policy, such as disabling file access, and using customization object.

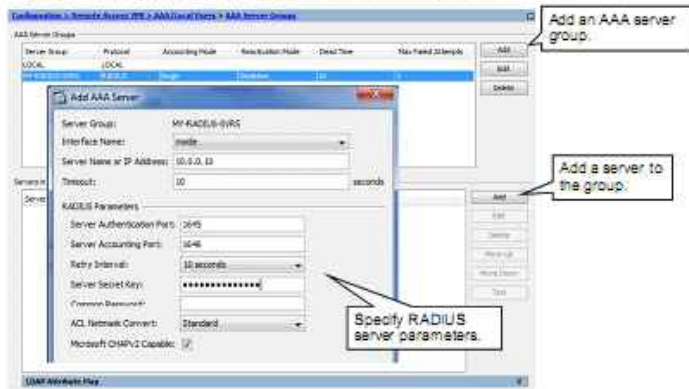
Because of this configuration, when a member of the Sales department with username ExternalSalesUser connects to the VPN, the RADIUS server authenticates and authorizes the session.

The AAA server will authorize access in this way:

- If the user connects via a full tunnel VPN (Cisco AnyConnect or IPsec), the banner, and idle timeout that is configured in the SalesGroupPolicy will be applied. Additionally, the RADIUS server will push a downloadable ACL to override the local ACL defined in the SalesGroupPolicy policy. The downloadable ACL permits all IP traffic to the internal web server.
- If the user connects via the clientless SSL VPN, the banner, idle timeout, and the webtype ACL that is configured in the SalesGroupPolicy will be applied. The Radius server will override these two parameters:
  - File access will be disabled.
  - The portal design will be obtained from the locally configured aca-customization object.

## Configuring External VPN Authorization

### Task 1: [Cisco ASA] Add RADIUS Server



Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

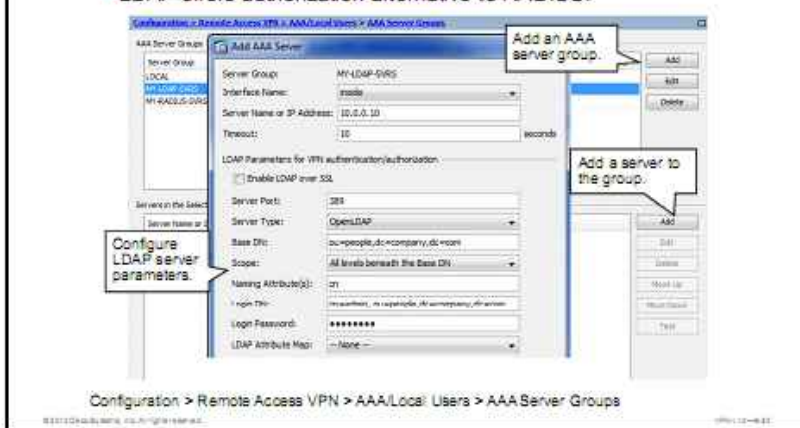
In the first configuration task of the configuration sequence on the Cisco ASA adaptive security appliance, create the RADIUS server group and configure a member of that group. Complete the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**.
- Step 2** Click **Add** in the upper section to create an AAA server group (not shown in the figure).
- Step 3** Select RADIUS as the AAA protocol. Optionally, configure other parameters. Click **OK** (not shown in the figure).
- Step 4** Select the RADIUS server group and click **Add** in the lower section to configure a member of that group.
- Step 5** Select the appropriate local Cisco ASA adaptive security appliance interface. Then choose the hostname or IP address of the AAA server and, optionally, choose other parameters that are required to establish communications with the RADIUS server.
- Step 6** Click **OK**.
- Step 7** Click **Apply** to apply the configuration.

## Configuring External VPN Authorization

### Task 1: [Cisco ASA] Add LDAP Server

- LDAP offers authorization alternative to RADIUS.



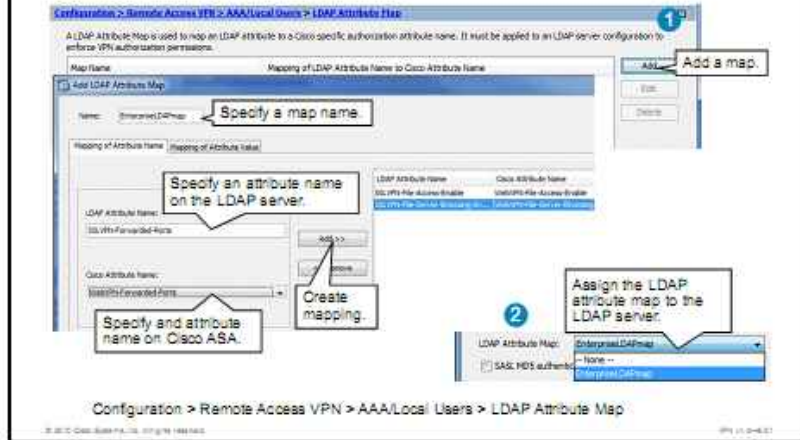
As an alternative to the RADIUS server, you can use an LDAP database to authorize clientless SSL VPN sessions. Complete these steps to create an LDAP server group and configure a member of that group:

- Step 1** Choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**.
- Step 2** Click **Add** in the upper section to create an AAA server group (not shown in the figure).
- Step 3** Select LDAP as the AAA protocol. Optionally, configure other parameters. Click **OK** (not shown in the figure).
- Step 4** Select the LDAP server group and click **Add** in the lower section to configure a member of that group.
- Step 5** Select the appropriate local Cisco ASA adaptive security appliance interface, and the hostname or IP address of the LDAP server. Enter LDAP-specific parameters, such as Base DN, Login DN, Group Base DN, Login password, scope, and naming attributes. The mapping of LDAP attributes to SSL VPN attributes will be applied in the next task.
- Step 6** Click **OK**.
- Step 7** Click **Apply** to apply the configuration.



## Configuring External VPN Authorization

### Task 2: [Cisco ASA] Define a LDAP Attribute Map



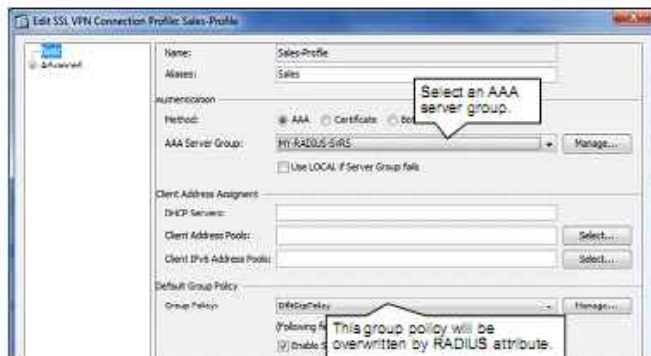
In the second, optional task, you may define the mapping of LDAP attributes to Cisco ASA adaptive security appliance attributes. This task is required when the attribute names that are used by the LDAP database are different from the ones that are used on the SSL VPN server. Complete these steps to create an LDAP attribute map and apply the map to an LDAP server entry:

- Step 1** Choose **Configuration > Remote Access VPN > AAA/Local Users > LDAP Attribute Map** and click **Add** to create an attribute map. The Add LDAP Attribute Map window appears.
- Step 2** Enter the map name.
- Step 3** Enter an LDAP attribute name and the corresponding Cisco attribute name and click **Add** to move the mapping to the configured list.
- Step 4** Repeat the previous step for any additional required mappings.
- Step 5** Click **OK**.
- Step 6** Choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**.
- Step 7** Select an LDAP server group and a specific LDAP server and click **Edit** to modify its settings.
- Step 8** Choose the appropriate map from the LDAP Attribute Map drop-down menu and click **OK**.
- Step 9** Click **Apply** to apply the configuration.

In the figure, the LDAP attribute map EnterpriseLDAPmap maps two LDAP attributes (SSLVPN-File-Access-Enable and SSLVPN-File-Server-Browsing-Enable) to the respective Cisco attributes (WebVPN-File-Access-Enable and WebVPN-File-Server-Browsing-Enable).

## Configuring External VPN Authorization

### Task 3: [Cisco ASA] Enable Authentication in Connection Profile



Configuration > Remote Access > Clientless SSL VPN Access > Connection Profiles

In the third task, you configure a connection profile for authentication using an external database. Complete these steps to configure a connection profile for external authentication:

- Step 1** Choose **Configuration > Remote Access VPN > Connection Profiles**.
- Step 2** Select the required connection profile and click **Edit**.
- Step 3** Locate the Authentication area in the Basic pane, choose appropriate authentication method, and select the required AAA server group from the AAA Server Group drop-down menu. In the example, MY-RADIUS-SVRS is selected.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration.

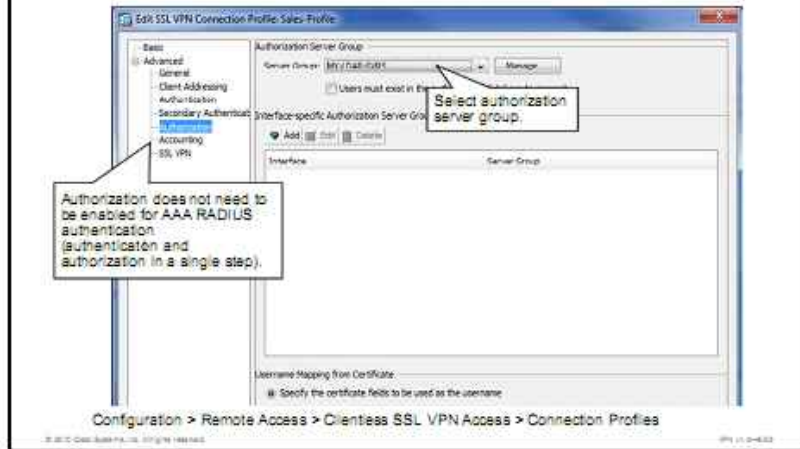
---

**Note** The connection profile points to a default group policy. In this scenario, the default group policy will not be applied to the users, because the RADIUS server will apply the SalesGroupPolicy to them.

---

## Configuring External VPN Authorization

### Task 3: [Cisco ASA] Enable Authorization in Connection Profile



Optionally, you may enable external authorization within the connection profile. It is not required if the same RADIUS server is configured for authentication, because RADIUS performs the authentication and authorization in a single step. External authorization is needed for certificate-based client authentication or when another authentication database was used.

Complete these steps to configure a connection profile for external authorization:

- Step 1** Choose **Configuration > Remote Access VPN > Connection Profiles**.
- Step 2** Select the required connection profile and choose **Edit**.
- Step 3** Expand the **Advanced** option from the menu on the left and choose the **Authorization** option. Choose the AAA server group from the Server Group drop-down menu. In the example, MY-LDAP-SVRS is selected.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration.

If you use a certificate to authenticate SSL VPN users, you can define which certificate fields are used as a username (not shown in the example).

## Configuring External VPN Authorization

### Tasks 1: [Cisco Secure ACS] Basic Settings

- Configuration depends on the AAA server implementation.

The screenshot shows the 'Network Configuration' section of the Cisco Secure ACS web interface. The main window is titled 'Add AAA Client'. On the left is a navigation tree with categories like System, Network, and Administration. The main form contains the following fields and options:

- AAA Client Hostname:** asa
- AAA Client IP Address:** 10.10.10.1
- Shared Secret:** 12345
- RADIUS Key Wrap:** Includes fields for Key Encryption Key, Message Authentication Code Key, and Key Digest Format (with a checked option for 'ASCI IP Headers').
- Authenticate Using:** RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)
- Additional Options:** Single Connect TACACS+ AAA Client (Record stop in accounting on failure) and Log Update/Watchdog Packets from the AAA Client.

Annotations in the image include a callout box pointing to the Hostname and IP fields with the text 'Configure Cisco ASA as an AAA client', and another callout box pointing to the 'Authenticate Using' dropdown with the text 'Use RADIUS'. The breadcrumb at the bottom reads 'Network Configuration > Add Entry'.

The configuration procedure involves several tasks that are performed on the authorization server. In the first task, you will define the parameters that enable RADIUS communications with the Cisco ASA adaptive security appliance, which acts in this scenario as the AAA client. The figure illustrates the AAA client entry that is created on a Cisco Secure Access Control Server (Cisco Secure ACS). This entry defines the AAA client IP address, the used protocol—RADIUS (Cisco VPN 3000/ASA/PIX 7.x+), and the secret key.

---

**Note** Screenshots of Cisco Secure ACS in this lesson apply to version 4.2.

---

## Configuring External VPN Authorization

### Tasks 2: [Cisco Secure ACS] Configure Users and User Groups

- Authorization can be performed on per-user or per-group basis.
- Consider using per-group authorization.

The screenshot displays two side-by-side configuration windows from the Cisco Secure ACS management console. The left window, titled 'User Setup', shows the configuration for a new user named 'ExternalSalesUser'. It includes fields for 'Account Enabled', 'Expiration/Validity over time', 'Full Name', and 'Description'. Below these is the 'User Setup' section with 'Password Authentication' set to 'ACTIVE\_DIRECTORY' and fields for 'Password', 'Confirm Password', and 'Enter a password.' (indicated by a callout box). The right window, titled 'Group Setup', shows the configuration for a group. It includes a 'Group' dropdown menu, 'Users in Group', 'Edit Settings', and 'Rename Group' buttons. Callout boxes point to 'Edit settings for a group.' and 'Rename a group.' The bottom of the screenshot shows the navigation path 'User Setup > Add/Edit' and 'Group Setup'.

In the second task, you will create user accounts and assign them to user groups. Managing user groups rather than individual users guarantees less configuration and more scalable maintenance. If you use per-group authorization, you configure authorization in individual group settings and then you assign individual users into the group.

## Configuring External VPN Authorization

### Task 3: [Cisco Secure ACS] (Optional) Reference Group Policy

- IETF attribute-value pair 25 can be used to reference an internal group policy
- Fallback to DfltGroupPolicy if group policy is not set.

The image shows two screenshots from Cisco configuration tools. The left screenshot, titled "Interface Configuration", shows a list of RADIUS attributes. A callout box labeled "IETF 25 Attribute" points to the "Class" attribute (ID 0025). Below the list, the breadcrumb "Interface Configuration > RADIUS (IETF)" is visible. The right screenshot, titled "Group Setup", shows the "Jump To" dropdown menu set to "Access Restrictions". Below it, the "Class" field (ID 0025) is set to "SalesGroupPolicy". A callout box points to this field with the text "Configurable per-Group or per-User. Reference to Internal Group Policy. Case-Sensitive". Below this screenshot, the breadcrumb "Group Setup > Edit Settings" is visible. At the bottom left of the overall image is the text "© 2010 Cisco Systems, Inc." and at the bottom right is "VPN-10-6-14".

In the third optional task that is performed on the AAA server, you may configure the IETF Attribute 25 to reference a local group policy.

The right half of the figure illustrates how the attribute 25 inside a group is set to the value SalesGroupPolicy. The notation is case-sensitive. This configuration has been performed for the user group vpngroup and will be applied to all members of that group.

## Configuring External VPN Authorization

### Task 4: [Cisco ACS] Prepare Authorization Interface

#### Interface Configuration

<input checked="" type="checkbox"/> [026/3076/065] Authorization-Type	<input checked="" type="checkbox"/> [026/3076/093] WebVPN-URL-Entry-Enable
<input checked="" type="checkbox"/> [026/3076/066] Authorization-Required	<input checked="" type="checkbox"/> [026/3076/094] WebVPN-File-Access-Enable
<input checked="" type="checkbox"/> [026/3076/067] Authorization-Off-Field	<input checked="" type="checkbox"/> [026/3076/095] WebVPN-File-Server-Entry-Enable
<input type="checkbox"/> [026/3076/068] IKE-Keepalive-Confidence-Interval	<input checked="" type="checkbox"/> [026/3076/096] WebVPN-File-Server-Browsing-Enable
<input checked="" type="checkbox"/> [026/3076/069] WebVPN-Content-Fike-Parameters	<input checked="" type="checkbox"/> [026/3076/097] WebVPN-Port-Forwarding-Enable
<input checked="" type="checkbox"/> [026/3076/071] WebVPN-Url-List	<input checked="" type="checkbox"/> [026/3076/098] WebVPN-Outlook-Exchange-Proxy-Enable
<input checked="" type="checkbox"/> [026/3076/072] WebVPN-Port-Forward-List	<input checked="" type="checkbox"/> [026/3076/099] WebVPN-Port-Forwarding-HTTP-Proxy
<input checked="" type="checkbox"/> [026/3076/073] WebVPN-Access-List	<input type="checkbox"/> [026/3076/100] WebVPN-Auto-Applet-Download-Enable
<input type="checkbox"/> [026/3076/075] Cisco-LEAP-Bypass	<input type="checkbox"/> [026/3076/101] WebVPN-Cisco-MetaFrame-Enable
<input checked="" type="checkbox"/> [026/3076/076] WebVPN-Homepage	<input checked="" type="checkbox"/> [026/3076/102] WebVPN-Apply-ACL
<input checked="" type="checkbox"/> [026/3076/077] Client-Type-Version-Listing	<input type="checkbox"/> [026/3076/103] WebVPN-SSL-VPN-Client-Enable
<input checked="" type="checkbox"/> [026/3076/079] WebVPN-Port-Forwarding-Name	<input type="checkbox"/> [026/3076/104] WebVPN-SSL-VPN-Client-Required
<input type="checkbox"/> [026/3076/080] IP-Proxy-Server	<input checked="" type="checkbox"/> [026/3076/105] WebVPN-SSL-VPN-Client-Keep-Installation
<input type="checkbox"/> [026/3076/081] IP-Proxy-Server-Policy	
<input type="checkbox"/> [026/3076/082] IP-Proxy-Encryption-Mode	
<input type="checkbox"/> [026/3076/083] IP-Proxy-Bypass-Local	
<input type="checkbox"/> [026/3076/094] IKE-Keepalive-Retry-Interval	
<input checked="" type="checkbox"/> [026/3076/085] Tunnel-Group-Lock	

Enable desired attributes.

Interface Configuration > RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

External authorization can be used to apply a large number of attributes to the clientless SSL VPN user sessions. These attributes may have to be explicitly added to the administration interface of individual users or user groups.

This figure illustrates an example of adding several attributes that are relevant for a clientless SSL VPN in Cisco Secure ACS. The list that is shown in the figure is not complete.

Each listed attribute is a vendor-specific attribute (VSA). It contains two parameters: the attribute identifier and the attribute name. An example of such an entry is [026/3076/071] WebVPN-Url-List. The attribute identifiers result from this convention:

- IETF Attribute 26 (vendor-specific) encapsulates vendor-specific attributes, which allows vendors to support their own extended attributes otherwise not suitable for general use. Attribute 26 contains the following three elements: Type, Length, and String (also known as data). The String includes Vendor-Id, Vendor-Type, Vendor-Length, and Vendor-Data.
- Vendor ID 3076 is the vendor ID for the implementation of Cisco VPN 3000/ASA/PIX 7.x+ RADIUS VSAs that were selected when you added the AAA client to the ACS database.
- The 071 is the individual identifier for the WebVPN-Url-List feature. Each feature has a different identifier in this last position.

## Configuring External VPN Authorization

### Task 5: [Cisco ACS] Configure Authorization Parameters

The screenshot displays the Cisco ACS configuration interface for Shared Profile Components. The top section is titled "Downloadable IP ACLs" and shows a form for creating a new ACL. The "Name" field is set to "AllowToInsrvt" and the "Description" field is empty. A callout box points to the "Name" field with the text "Create a downloadable ACL". Below the form, the "ACL Contents" section shows the rule "PermitAllToInsrvt" selected, with a callout box pointing to it that says "Network Access Filtering (All-AAA-Clients)". The "ACL Definitions" section shows the rule "Permit ip any host 10.0.0.11".

The bottom section is titled "Group Setup" and shows the "Downloadable ACLs" section. The "Assign IP ACL" checkbox is checked, and the "AllowToInsrvt" ACL is selected. A callout box points to this section with the text "Assign the downloadable ACL to a user or group profile. This ACL will overwrite the ACL specified in the local group policy."

Full tunnel VPN authorization is primarily based on ACLs that are applied to the VPN user sessions or user groups. Instead of using a local ACL defined on the security appliance, you may create a downloadable ACL on the external AAA server and push it to VPN users. If you use local ACLs and downloadable ACLs concurrently, the downloadable ACLs will override the local ACL configuration.

The downloadable ACLs are configured in the Cisco ACS in the Shared Profile Components menu. The syntax of a downloadable ACL resembles the ACL that is used on security appliances and Cisco IOS routers. In this example, the downloadable ACL permits all IP traffic to the web server (10.0.0.11), using the notation **permit ip any host 10.0.0.11**.

The downloadable ACLs can be applied either to user groups or to individual users. The first approach ensures better manageability and scalability.



## Configuring External VPN Authorization

### Task 5: [Cisco ACS] Configure Authorization Parameters (Cont.)

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes

[3076/001] Access-Hours

[3076/002] Simultaneous-Logins

[3076/006] Secondary-DNS

[3076/007] Primary-WINS: 0.0.0.0

[3076/008] Secondary-WINS: 0.0.0.0

[3076/011] Tunneling-Protocols: WebVPN

[3076/005] Authorization-Type: RADIUS

Less Granularity Than Local (Tunnel vs. Clientless)

Group Setup > Edit Settings

[3076/093] WebVPN-URL-Entry-Enable: Yes

[3076/094] WebVPN-File-Access-Enable: No (Disable file access.)

[3076/095] WebVPN-File-Server-Entry-Enable: No (Disable file server entry.)

[3076/096] WebVPN-File-Server-Browsing-Enable: No (Disable file server browsing.)

[3076/097] WebVPN-Port-Forwarding-Enable: Yes

[3076/098] WebVPN-Outlook-Exchange-Proxy-Enable: No

[3076/099] WebVPN-Port-Forwarding-HTTP-Proxy: No

[3076/102] WebVPN-Apply-ACL: Yes

[3076/113] WebVPN-Customization: acs-customization

Apply customization.

In the optional Task 4, you may set the VSAs to the required values. The precedence order that specifies which values are used in the SSL VPN session is defined as follows (from highest to lowest precedence):

1. Individual authorization attributes sent by the AAA server
2. Parameters that are defined by the nondefault group policy that is configured locally on the Cisco ASA adaptive security appliance and is referenced by the AAA server using IETF Attribute 25
3. Settings that are included in the DfltGroupPolicy that exists on the Cisco ASA adaptive security appliance, if the AAA server does not send IETF Attribute 25 to the Cisco ASA adaptive security appliance

The figure illustrates how to restrict the permitted VPN protocols to SSL VPN. It also shows how to disable file access, disable file server entry, disable file server browsing, and apply a given customization object that is called acs-customization inside group settings. The customization object must exist on the security appliance to be applied to the SSL VPN session.

## Configuring External VPN Authorization

### CLI Configuration

```
aaa-server MY-RADIUS-SVRS protocol radius
aaa-server MY-RADIUS-SVRS (inside) host 10.0.0.10
key *****
|
ldap attribute-map EnterpriseLDAPmap
map-name SSLVPN-Forwarded-Ports WebVPN-Forwarded-Ports
map-name SSLVPN-File-Server-Browsing-Enable
WebVPN-File-Server-Browsing-Enable
map-name SSLVPN-File-Access-Enable WebVPN-File-Access-Enable
|
aaa-server MY-LDAP-SVRS protocol ldap
aaa-server MY-LDAP-SVRS (inside) host 10.0.0.10
ldap-base-dn ou=people,dc=company,dc=com
ldap-login-dn cn=admin,ou=people,dc=company,dc=com
ldap-login-password *****
ldap-naming-attribute cn
ldap-scope subtree
server-type openldap
ldap-attribute-map EnterpriseLDAPmap
|
tunnel-group Sales-Profile general-attributes
authentication-server-group MY-RADIUS-SVRS
authorization-server-group MY-LDAP-SVRS
```

Configure the RADIUS server.

Configure an LDAP attribute map.

Configure the LDAP server.

Enable authentication and authorization in a connection profile.

This figure shows the CLI commands that are needed to enable external VPN authorization.

To create an AAA server group, use the **aaa-server** command, followed by a server group name and authentication protocol. To add a server to the server group, use the **aaa-server** command. Follow the command with a server group name, interface through which the server is reachable, and IP address of the server. To configure a shared key that is used for communication between the Cisco ASA adaptive security appliance and the RADIUS server, use the **key** command in the AAA server configuration mode.

To configure mappings between LDAP and VPN attributes, first create an LDAP map using the **ldap attribute-map** command. Then create individual mappings using the **map-name** command.

To configure parameters inside the LDAP server group, use the following commands in the server group configuration mode. Use the **ldap-base-dn** command to specify where the server should begin searching when it receives an authentication request. Use the **ldap-scope** command to specify extent of the search in the LDAP hierarchy. Use the **ldap-naming-attribute** command to specify the Relative Distinguished Name attribute. Use the **ldap-login-dn** and **ldap-login-password** commands to specify the name and password the Cisco ASA adaptive security appliance will use to search the LDAP directory. Use the **server-type** command to specify the type of LDAP server. Use the **ldap-attribute-map** command to bind an LDAP map to LDAP server.

To enable AAA authentication for a connection profile (tunnel group) using the CLI, use the **authentication-server-group** command. Follow the command with the AAA server group name, in tunnel group configuration mode. To enable authorization, use the **authorization-server-group** command, followed by AAA server group name, in tunnel group configuration mode.

### aaa-server

To create an AAA server group and configure AAA server parameters that are group-specific and common to all group hosts, use the **aaa-server** command in global configuration mode. To remove the designated group, use the **no** form of this command.

```
aaa-server server-tag protocol server-protocol
```

## aaa-server Parameters

Parameter	Description
<code>server-tag</code>	Specifies the server group name, which is matched by the name that is specified by the <b>aaa-server host</b> commands. Other AAA commands make reference to the AAA server group name.
<code>protocol</code> <code>server-protocol</code>	Specifies the AAA protocol that the servers in the group support: <ul style="list-style-type: none"><li>■ http-form</li><li>■ kerberos</li><li>■ ldap</li><li>■ nt</li><li>■ radius</li><li>■ sdi</li><li>■ tacacs+</li></ul>

## aaa-server host

To configure an AAA server as part of an AAA server group and to configure AAA server parameters that are host-specific, use the **aaa-server host** command in global configuration mode. When you use the **aaa-server host** command, you enter the aaa-server host configuration mode, from which you can specify and manage host-specific AAA server connection data. To remove a host configuration, use the **no** form of this command.

**aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

## aaa-server host Parameters

Parameter	Description
( <i>interface-name</i> )	(Optional) Specifies the network interface where the authentication server resides. The parentheses are required in this parameter. If you do not specify an interface, the default is <b>inside</b> , if available.
<i>key</i>	(Optional) Specifies a case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the RADIUS or TACACS+ server. Any characters that are entered past 127 are ignored. The key is used between the adaptive security appliance and the server for encrypting data between them. The key must be the same on both the adaptive security appliance and server systems. Spaces are not permitted in the key, but other special characters are allowed. You can add or modify the key using the <b>key</b> command in host mode.
<b>name</b>	Specifies the name of the server using either a name that is assigned locally using the <b>name</b> command or a DNS name. The maximum number of characters is 128 for DNS names and 63 characters for names that are assigned using the <b>name</b> command.
<i>server-ip</i>	Specifies the IP address of the AAA server.
<i>server-tag</i>	Specifies a symbolic name of the server group, which is matched by the name that is specified by the <b>aaa-server</b> command.
<b>timeout</b> <i>seconds</i>	(Optional) The timeout interval for the request. This is the time after which the adaptive security appliance gives up on the request to the primary AAA server. If there is a standby AAA server, the adaptive security appliance sends the request to the backup server. You can modify the timeout interval using the <b>timeout</b> command in host mode.

## ldap attribute-map

To create and name an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names, use the **ldap attribute-map** command in global configuration mode. To remove the map, use the **no** form of this command.

**ldap attribute-map** *map-name*

### Parameters

Parameter	Description
<i>map-name</i>	Specifies a user-defined name for an LDAP attribute map

## map-name

To map a user-defined attribute name to a Cisco attribute name, use the **map-name** command in ldap-attribute-map configuration mode. To remove this mapping, use the **no** form of this command.

**map-name** *user-attribute-name Cisco-attribute-name*

### map-name Parameters

Parameter	Description
<i>user-attribute-name</i>	Specifies the user-defined attribute name that you are mapping to the Cisco attribute
<i>Cisco-attribute-name</i>	Specifies the Cisco attribute name that you are mapping to the user-defined name

## ldap-base-dn

To specify the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request, use the **ldap-base-dn** command in the aaa-server host configuration mode. The aaa-server host configuration mode is accessible from the aaa-server protocol configuration mode. To remove this specification, thus resetting the search to start at the top of the list, use the **no** form of this command.

**ldap-base-dn** *string*

### ldap-base-dn Parameters

Parameter	Description
<i>string</i>	A case-sensitive string of up to 128 characters that specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request. An example of such a string is OU=Cisco. Spaces are not permitted in the string, but other special characters are allowed.

## ldap-scope

To specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request, use the **ldap-scope** command in the aaa-server host configuration mode. To remove this specification, use the **no** form of this command.

**ldap-scope** *scope*

## ldap-scope Parameters

Parameter	Description
<i>scope</i>	The number of levels in the LDAP hierarchy for the server to search when it receives an authorization request. Valid values include the following two rules: <ul style="list-style-type: none"><li>■ <b>onelevel</b>: Search only one level beneath the Base DN.</li><li>■ <b>subtree</b>: Search all levels beneath the Base DN.</li></ul>

## ldap-naming-attribute

To specify the Relative Distinguished Name attribute, use the **ldap-naming-attribute** command in the aaa-server host configuration mode. To remove this specification, use the **no** form of this command.

**ldap-naming-attribute** *string*

### ldap-naming-attribute Parameters

Parameter	Description
<i>string</i>	The case-sensitive, alphanumeric Relative Distinguished Name attribute, consisting of up to 128 characters, that uniquely identifies an entry on the LDAP server. Spaces are not permitted in the string, but other special characters are allowed.

## ldap-login-dn

To specify the name of the directory object that the system should bind this as, use the **ldap-login-dn** command in the aaa-server host configuration mode. To remove this specification, use the **no** form of this command.

**ldap-login-dn** *string*

### ldap-login-dn Parameters

Parameter	Description
<i>string</i>	A case-sensitive string of up to 128 characters that specifies the name of the directory object in the LDAP hierarchy. Spaces are not permitted in the string, but other special characters are allowed.

## ldap-login-password

To specify the login password for the LDAP server, use the **ldap-login-password** command in the aaa-server host configuration mode. To remove this password specification, use the **no** form of this command.

**ldap-login-password** *string*

### ldap-login-password Parameters

Parameter	Description
<i>string</i>	A case-sensitive, alphanumeric password, up to 64 characters long. The password cannot contain space characters.

## server-type

To manually configure the LDAP server model, use the **server-type** command in `aaa-server` host configuration mode. The adaptive security appliance supports the following server models:

- Microsoft Active Directory
- Sun Microsystems Java System Directory Server, formerly named the Sun ONE Directory Server
- Generic LDAP directory servers that comply with LDAP version 3 (LDAPv3) (no password management)

To disable this command, use the **no** form of this command.

**server-type** {*auto-detect* | *microsoft* | *sun* | *generic* | *openldap* | *novell*}

### server-type Parameters

Parameter	Description
<b>auto-detect</b>	Specifies that the adaptive security appliance determines the LDAP server type through autodetection.
<b>generic</b>	Specifies LDAPv3-compliant directory servers other than Sun and Microsoft LDAP directory servers. Password management is not supported with generic LDAP servers.
<b>microsoft</b>	Specifies that the LDAP server is a Microsoft Active Directory.
<b>openldap</b>	Specifies that the LDAP server is an OpenLDAP server.
<b>novell</b>	Specifies that the LDAP server is a Novell server.
<b>sun</b>	Specifies that the LDAP server is a Sun Microsystems Java System Directory Server.

## ldap-attribute-map (aaa-server host mode)

To bind an existing mapping configuration to an LDAP host, use the **ldap-attribute-map** command in `aaa-server` host configuration mode. To remove the binding, use the **no** form of this command.

**ldap-attribute-map** *map-name*

### ldap-attribute-map (aaa-server host mode) Parameters

Parameter	Description
<i>map-name</i>	Specifies an LDAP attribute mapping configuration

## authentication-server-group (tunnel-group general-attributes)

To specify the AAA server group to use for user authentication for a tunnel group, use the **authentication-server-group** command in `tunnel-group general-attributes` configuration mode. To return this attribute to the default, use the **no** form of this command.

**authentication-server-group** [(*interface\_name*)] *server\_group* [LOCAL | NONE]

### authentication-server-group (tunnel-group general-attributes) Parameters

Parameter	Description
<i>interface_name</i>	(Optional) Specifies the interface where the IPsec tunnel terminates.
<b>LOCAL</b>	(Optional) Requires authentication against the local user database if all of the servers in the server group have been deactivated because of communication failures. If the server group name is either <b>LOCAL</b> or <b>NONE</b> , do not use the <b>LOCAL</b> keyword here.
<b>NONE</b>	(Optional) Specifies the server group name as <b>NONE</b> , indicating that authentication is not required.
<i>server_group</i>	Identifies the previously configured authentication server or group of servers.

### authorization-server-group (tunnel-group general-attributes)

To specify the set of authorization servers for user authorization for a tunnel group, use the **authorization-server-group** command in tunnel-group general-attributes configuration mode. To remove authorization servers from the configuration, use the **no** form of this command. The adaptive security appliance uses authorization to verify the level of access to network resources that users are permitted.

**authorization-server-group** *group\_tag*

### authorization-server-group (tunnel-group general-attributes) Parameters

Parameter	Description
<i>group_tag</i>	Identifies the previously configured authorization server or group of servers. Use the <b>aaa-server</b> command to configure authorization servers.

## Verifying External Authorization

### Cisco AnyConnect User-Side Verification

The image illustrates the user-side verification process for Cisco AnyConnect. It is divided into four numbered steps:

- Step 1:** The Cisco AnyConnect VPN Client interface. The 'Connect to' field is set to 'asa'. The 'Group' dropdown is set to 'remote sales profile'. The 'Username' field contains 'EXTERNALSalesUser' and the 'Password' field is masked. A callout box indicates: "Username is not case-sensitive (depends on AAA server)".
- Step 2:** A dialog box titled "Sales group VPN. Unauthorized access not permitted." with a "Banner" message and "Accept" and "Disconnect" buttons.
- Step 3:** A Command Prompt window showing the execution of a ping command to 10.0.0.11. The output shows successful replies from 10.0.0.11 with 32 bytes of data, 0% loss, and a TTL of 128. The statistics are: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
- Step 4:** A browser window showing a "Welcome" page for "IIS7". The address bar shows "http://10.0.0.11:80 works".

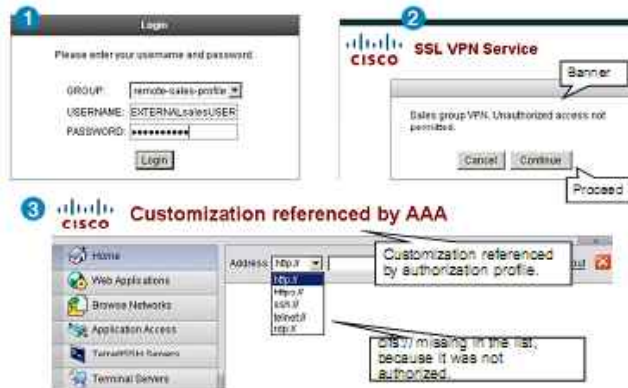
To verify external authorization for full tunnel access from the user perspective, you may complete these steps:

- Step 1** Connect to SSL VPN using the sales profile and login as a remote user (ExternalSalesUser). The username and password may be case-sensitive, depending on the type of the external database.
- Step 2** View the banner message and choose **Accept**.
- Step 3** Verify that authorized traffic is permitted, although it would be blocked by the local ACL (ICMP in this example).
- Step 4** Verify that other authorized traffic is permitted (HTTP access to the web server on ports 80/81/8080).



## Verifying External Authorization

### Clientless SSL VPN User-Side Verification



To verify external authorization for clientless SSL VPN access from the user perspective, you may complete these steps:

- Step 1** Connect to SSL VPN using the sales profile and log in as a remote user (ExternalSalesUser).
- Step 2** View the banner message and choose **Continue**.
- Step 3** Verify that the customization object has been applied to the portal. Verify that CIFS is missing from the list of available URL types.

## Verifying External Authorization

### Server-Side Verification

Monitoring > VPN > VPN Statistics > Sessions

Full Client	Site-to-Site	Clientless	With Client	Inactive	Total	Email Proxy	VPN Load Balancing	Total
0	0	0	1	0	1	0	0	0

Filter By: Full Client

Username	Group Policy	Protocol	Login Time	Bytes Tx
ID Address	Connection Profile	Encryption	Duration	Bytes Rx
RemoteSalesProf	RemoteSalesProf	Clientless SSL	Wed Aug 25 20:10	128
10.10.10.10	RemoteSalesProf	128	10:10:10	128

Monitoring > VPN > VPN Statistics > Sessions

Clientless	Site-to-Site	Clientless	With Client	Inactive	Total	Email Proxy	VPN Load Balancing	Total
0	0	1	0	0	1	0	0	0

Filter By: Clientless SSL VPN

Username	Group Policy	Protocol	Login Time	Bytes Tx
ID Address	Connection Profile	Encryption	Duration	Bytes Rx
RemoteSalesProf	RemoteSalesProf	Clientless	Wed Aug 25 20:10	128
10.10.10.10	RemoteSalesProf	128	10:10:10	128

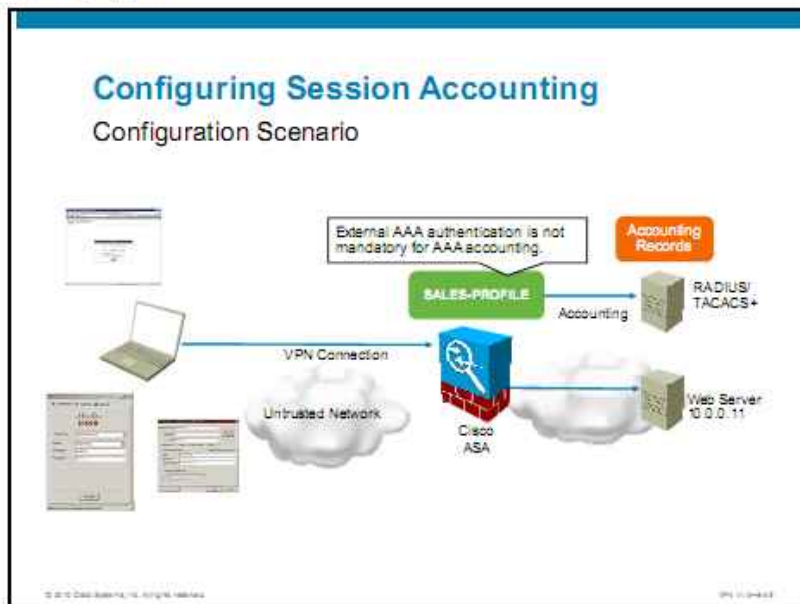
Monitoring > VPN > VPN Statistics > Sessions

The server-side verification of external authorization can be performed by browsing to the Monitoring > VPN > VPN Statistics > Sessions menu and the details of the respective connection.

You will verify that full tunnel users and clientless users are connected via the RemoteSalesProfile profile and that the local group policy SalesGroupPolicy has been applied to the sessions.

# Configuring Session Accounting

This topic describes how to implement accounting of VPN sessions on the Cisco ASA adaptive security appliance.



This figure illustrates the scenario that is used in the upcoming configuration. The security appliance has a connection profile that is configured for accounting. The accounting information will be sent to a RADIUS server that has been previously configured for authentication and authorization purposes.

## Configuring Session Accounting

### Configuration Tasks

1. Add a RADIUS or TACACS+ server.
2. Enable accounting in a connection profile.

To configure session accounting, you will complete these tasks:

1. Create a RADIUS or TACACS+ association. This task is not presented in this sequence, because it has been discussed in the previous topic.
2. Enable accounting in a connection profile.

## Configuring Session Accounting

### Task 2: Enable Accounting in a Connection Profile

The screenshot shows the 'Edit SSL VPN Connection Profile: Sales-Profile' window. The 'Advanced' tab is selected, and the 'Accounting' option is highlighted in the left-hand menu. The 'Server Group' dropdown menu is set to 'MY-RADIUS-SVRS'. A callout box points to this dropdown with the text 'Select an AAA server group.' Below the window, a terminal window shows the following configuration commands:

```
tunnel-group Sales-Profile general-attributes
accounting-server-group MY-RADIUS-SVRS
```

Navigation paths are listed at the bottom:

- Configuration > Remote Access VPN > Network (Client) Access > Connection Profiles
- Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

In the second configuration task, enable a connection profile for session accounting using these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles** or **Configuration > Remote Access VPN > Network (Client) Access > Connection Profiles**.
- Step 2** Select a desired connection profile and click **Edit** to edit the connection profile. Alternatively, click **Add** to create new connection profile.
- Step 3** Expand the **Advanced** option from the menu on the left and select the **Accounting** option. Choose the appropriate AAA server group from the Server Group drop-down menu. Since RADIUS and TACACS+ are the only supported accounting methods, you will choose one of these server groups. In the example, MY-RADIUS-SVRS is selected.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration.

To enable accounting using CLI, use the **accounting-server-group** command, followed by AAA server group name, in tunnel group configuration mode.

#### accounting-server-group

To specify the AAA server group for sending accounting records, use the **accounting-server-group** command in various modes. To remove accounting servers from the configuration, use the **no** form of this command. The adaptive security appliance uses accounting to keep track of the network resources that users access.

**accounting-server-group** *group\_tag*

## accounting-server-group Parameters

Parameter	Description
<code>group_tag</code>	Identifies the previously configured accounting server or group of servers. Use the <code>aaa-server</code> command to configure accounting servers.

### Verifying Session Accounting

#### AAA Server Verification

**Reports and Activity**

Select

RADIUS Accounting active.csv [Refresh](#) [Download](#)

Regular Expression:  Start Date & Time:  End Date & Time:  Rows per Page:

Apply Filter:

Filtering is not applied.

Date	Time	User-Name	Group-Name	User-Start	User-Stop	AAA-Session-Id	AAA-Session-Time	Service-Type	Framed-Protocol	Acct-Input-Octets	Acct-Output-Octets
07/02/2010	13:51:51	externalSalesUser	vpngroup	10.0.1.11	Stop	66500002	11	Framed	PPP	3499	11949
07/02/2010	13:51:41	externalSalesUser	vpngroup	10.0.1.11	Start	66500002	...	Framed	PPP	...	...
07/02/2010	13:49:42	LocalSalesUser	Default Group	10.0.1.11	Stop	66500001	98	Framed	PPP	4255	11709
07/02/2010	13:49:42	LocalSalesUser	Default Group	10.0.1.11	Start	66500001	...	Framed	PPP	...	...

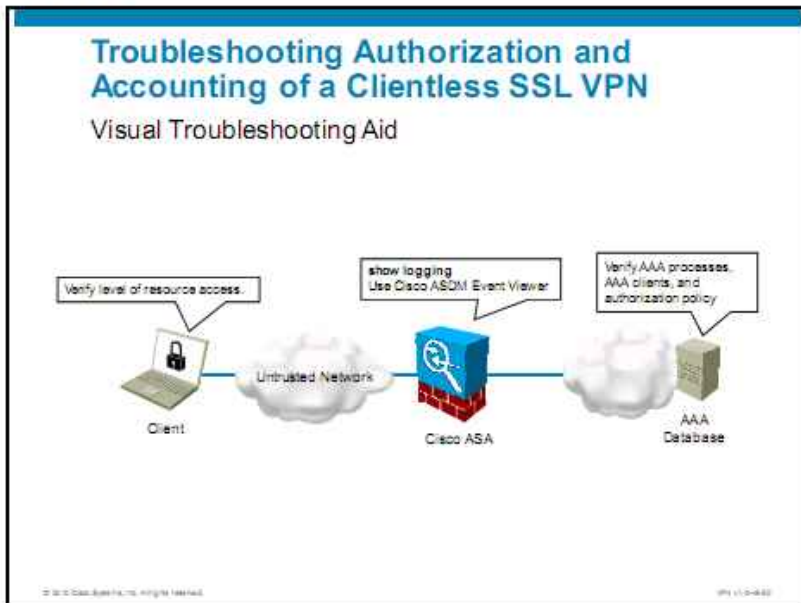
ACS > Reports and Activity > RADIUS Accounting > Active

Session accounting generates session records on the AAA server. The figure illustrates a start and stop session that is generated for two types of users. The two types of users are LocalSalesUser, who exists in the ASA local database, and ExternalSalesUser, who exists in the RADIUS database. This example has been taken on a Cisco ACS server. The users who exist in the Cisco ASA database appear as members of the Default Group. The users who exist in the RADIUS database appear along with the user group to which they belong. In this example, the user ExternalSalesUser belongs to group vpngroup.

Each session has two entries that are associated with it: the Start and Stop entry. Both indicate the time and date when the sessions started or stopped. The Stop entry contains statistics about the exchanged traffic.

# Troubleshoot Authorization and Accounting of a Clientless SSL VPN

This topic provides guidelines on how to troubleshoot authorization and accounting in a VPN environment.



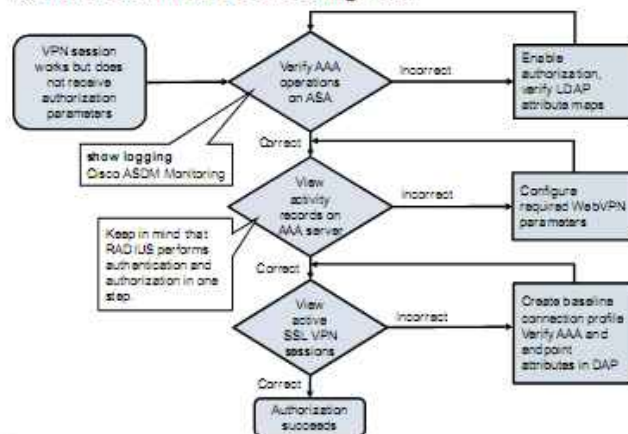
When troubleshooting VPN authorization and accounting, you should perform troubleshooting tasks on both the security appliance, and on the external AAA server. This figure shows some most useful troubleshooting commands and actions that you can use on involved components.

Note that the security appliance will extensively log all issues into its syslog subsystem. Debug commands are generally not required, except for in-depth troubleshooting of complex issues.

The troubleshooting tasks that are performed on the AAA server are not described here, because they vary depending on the deployed product.

## Troubleshooting Authorization and Accounting of a Clientless SSL VPN

### Authorization Troubleshooting Flow



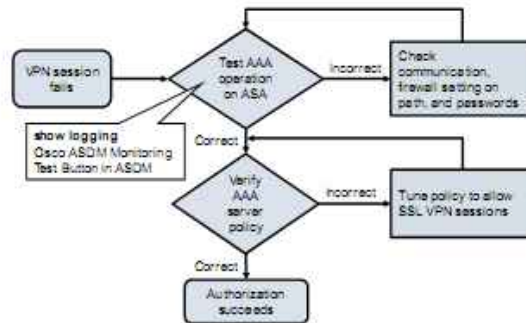
If your VPN session works but the authorization profile is not applied to it, you may follow these steps to troubleshoot the issue:

- Step 1** First, verify AAA operations on the security appliance. Verify that authorization is enabled in the required connection profiles and verify that your LDAP attribute maps are correct if you are using LDAP. Browse through the configuration pages and view the logging information to verify this step.
- Step 2** View the activity records on the external AAA server. Browse through the configuration pages on your AAA server. Investigate the granted and failed access attempts to validate that the AAA server is authorizing the sessions.
- Step 3** View the active sessions on the security appliance. The detailed information displays the group policy that is attached to the session. Verify that the actual group policy corresponds to your requirements.



## Troubleshooting Authorization and Accounting of a Clientless SSL VPN

### Authorization Troubleshooting Flow (Cont.)



If your VPN connection fails, follow these steps to troubleshoot the issue:

- Step 1** Test AAA operation on Cisco ASA adaptive security appliance. Verify the communications with the AAA server. If the connectivity is broken, check for firewall settings on the path. Ensure that the same encryption password and communication ports are used on both sides.
- Step 2** Verify AAA server policy. Browse through the configuration pages on your AAA server and investigate the granted and failed access attempts to validate that the AAA server is correctly authorizing the sessions.

## Troubleshooting Authorization and Accounting in Clientless SSL VPN

### Authorization Does Not Permit SSL VPN Sessions

```
ASA(config)# logging console 7
ASA(config)# logging enable
%ASA-6-113004: AAA user authentication Successful : server =
Insrv : user = ExternalSalesUser
%ASA-6-113003: AAA group policy for user ExternalSalesUser is
being set to SalesGroupPolicy
%ASA-6-113011: AAA retrieved user specific group policy
(SalesGroupPolicy) for user = ExternalSalesUser
%ASA-6-113005: AAA user authorization Rejected : reason = AAA
failure : server = Insrv : user = ExternalSalesUser
%ASA-7-734003: DAP: User ExternalSalesUser, Addr Inetsrv: Session
Attribute aaa.radius["4098"]["1"] = 3
%ASA-7-734003: DAP: User ExternalSalesUser, Addr Inetsrv: Session
Attribute aaa.radius["4103"]["1"] = 167772231
%ASA-7-734003: DAP: User ExternalSalesUser, Addr Inetsrv: Session
Attribute aaa.radius["4107"]["1"] = 4
...
%ASA-6-716002: Group <SalesGroupPolicy> User < ExternalSalesUser>
IP <Inetsrv> WebVPN session terminated: Client type not supported.
```

This figure illustrates the security appliance logging output when the received authorization profile does not allow SSL VPN sessions. A similar problem with not authorized IPsec connections could be also easily detected. Logging must be enabled to receive the presented information.

The reason for the failed authorization is explained in the two messages that are marked in the figure.

## Troubleshooting Authorization and Accounting in Clientless SSL VPN

### Incorrect Name of Referenced Group Policy

The session attribute aaa.radius["25"]["1"] = SalesGroupPolicy is not set for the user (case type).

```
ASA(config)# logging console 7
ASA(config)# logging enable
%ASA-6-113004: AAA user authentication Successful : server = Insrv
: user = ExternalSalesUser
%ASA-6-113009: AAA retrieved default group policy (DfltGrpPolicy)
for user = ExternalSalesUser
%ASA-6-113008: AAA transaction status ACCEPT:user=ExternalSalesUser
...
%ASA-7-734003: DAP: User ExternalSalesUser, Addr Inetsrv: Session
Attribute aaa.radius["25"]["1"] = sAlesGroupPolicy;
...
%ASA-6-716001: Group <DfltGrpPolicy> User < ExternalSalesUser> IP
<Inetsrv> WebVPN session started.
%ASA-6-716038: Group <DfltGrpPolicy> User < ExternalSalesUser> IP
<Inetsrv> Authentication: successful, Session Type: WebVPN.
```

In this example, the AAA server sends the IETF RADIUS Attribute 25 with the value of sAlesGroupPolicy;. This attribute instructs the security appliance to apply the specified group policy to the user session. However, such a group policy does not exist in the local configuration. The problem is with the letter case. Therefore, the appliance falls back to the DfltGrpPolicy.

## Troubleshooting Authorization and Accounting in Clientless SSL VPN

### Correct Name of Referenced Group Policy

The session attribute aaa.radius["25"]["1"] = SalesGroupPolicy is set for the user

```
%ASA-6-113004: AAA user authentication Successful : server = Insrv
: user = ExternalSalesUser
%ASA-6-113003: AAA group policy for user ExternalSalesUser is being
set to SalesGroupPolicy
%ASA-6-113011: AAA retrieved user specific group policy (acc-sales-
groupolicy) for user = ExternalSalesUser
%ASA-6-113009: AAA retrieved default group policy (DfltGrpPolicy)
for user = ExternalSalesUser
%ASA-6-113008: AAA status ACCEPT : user = ExternalSalesUser
...
%ASA-7-734003: DAP: User ExternalSalesUser, Addr Inetsrv: Session
Attribute aaa.radius["25"]["1"] = SalesGroupPolicy
...
%ASA-6-716001: Group < SalesGroupPolicy> User < ExternalSalesUser>
IP <Inetsrv> WebVPN session started.
%ASA-6-716038: Group <SalesGroupPolicy> User <ExternalSalesUser> IP
<Inetsrv> Authentication: successful, Session Type: WebVPN.
```

To contrast the previous problem description with a successful policy group reference, this figure displays the notifications about the correct match. In this scenario, the group policy SalesGroupPolicy is applied to the user session.

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- Scalable VPNs use external RADIUS or LDAP authorization.
- VPN internal authorization uses group policies for modularity.
- VPN external AAA authorization can activate a local group policy or apply selective VPN parameters.
- VPN accounting can be performed on an external RADIUS or TACACS+ server and does not require that the users are authenticated against the same AAA database.
- Troubleshooting of VPN access control, authorization, and accounting is based on AAA-related monitoring tools in the Cisco ASA CLI, Cisco ASDM, and the external AAA servers.

© 2010 Cisco Systems, Inc.

© 2010 Cisco

# Deploying Cisco Secure Desktop in SSL VPNs

---

## Overview

Cisco Secure Sockets Layer (SSL) virtual private network (VPN) solutions provide organizations with robust and flexible products for protecting their security and privacy of information, and they can play an important part in the compliance strategies of an organization. Cisco Secure Desktop technology interoperates with the endpoint operating system and can ensure the removal of all data, especially from an untrusted system with potentially malicious third-party software installed.

Cisco Secure Desktop can be deployed to reduce the risks that are posed by untrusted endpoints that connect to an enterprise network via a clientless SSL VPN or Cisco AnyConnect client session. Cisco Secure Desktop provides a number of features that you can configure to work independently or together.

Cisco Secure Desktop helps, in combination with other security controls and mechanisms, reduce risks that are associated with using such technologies.

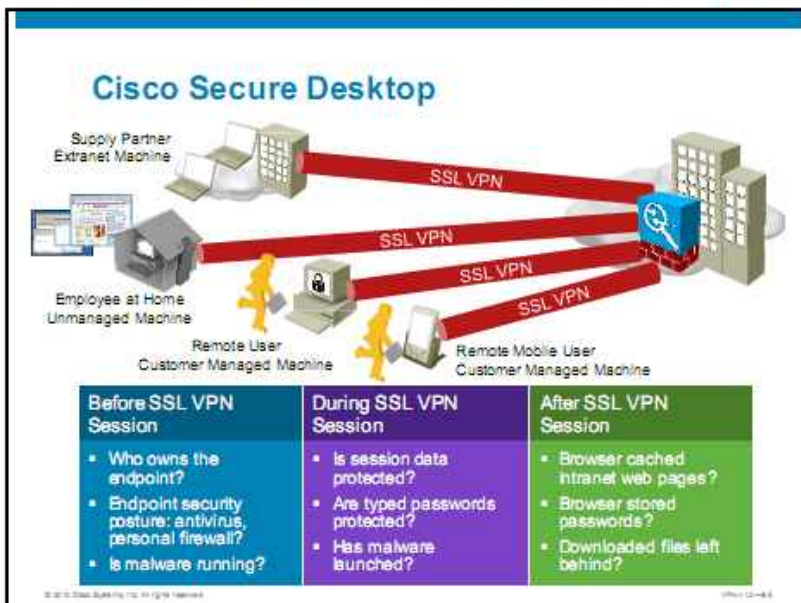
## Objectives

Upon completing this lesson, you will be able to deploy and manage Cisco Secure Desktop features and manage related faults in a Cisco SSL VPN. This ability includes being able to meet these objectives:

- Plan how to deploy the Cisco Secure Desktop in SSL VPNs
- Install, enable, and customize Cisco Secure Desktop in SSL VPNs
- Configure and verify Cisco Secure Desktop prelogin criteria for SSL VPN connections
- Configure and verify Cisco Secure Desktop policies for SSL VPN connections
- Configure and verify basic Cisco Secure Desktop Advanced Endpoint Assessment features for SSL VPN
- Troubleshoot Cisco Secure Desktop operations for SSL VPN connections

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic will discuss the security risks that are facing companies that deploy remote access VPNs, as well as the Cisco Secure Desktop operation and features that mitigate these risks.



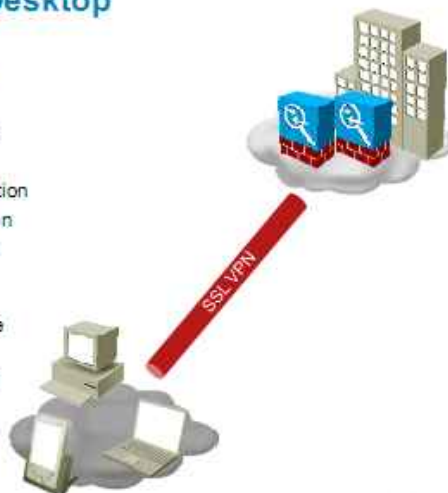
SSL VPNs provide the flexibility to deploy secured remote access to corporate resources from any location that can provide a compliant web browser with the proper SSL support. These deployments include access for customers, partners, and employees from systems that are not necessarily corporate-managed. Additional security threats are introduced without direct control over the systems that are used to access corporate resources.

- Before the SSL VPN session
  - Who owns the endpoint?
  - Endpoint security posture: Does the system have antivirus or a personal firewall?
  - Is the system already running malware?
- During the SSL VPN session
  - Is the session data protected?
  - Are locally typed passwords protected?
  - Has malware been launched during the session?
- After the SSL VPN session
  - Has the browser cached intranet web pages?
  - Has the browser stored any passwords?
- Are there any downloaded files left behind on the system?

## Cisco Secure Desktop

### Features Overview

- Prelogin assessment
- Host Scan
- Secure Desktop (Vault)
- Cache Cleaner
- Keystroke logger detection
- Host emulation detection
- Cisco Secure Desktop policies
- Integration with DAP
- Windows Mobile Device Management
- Standalone installation packages
- Cisco Secure Desktop Manual Launch



Cisco Secure Desktop seeks to minimize the risks that are posed by the use of remote devices to establish a Cisco clientless SSL VPN or Cisco AnyConnect client session. Cisco Secure Desktop provides a number of features that you can configure to work independently or together. Cisco Secure Desktop offers these features:

- **Prelogin assessment:** The prelogin assessment module installs itself after the user connects to the security appliance, but before the user logs in. This module can check the remote device for files, digital certificates, the operating system, IP address, and Microsoft Windows registry keys.
- **Host Scan:** Host Scan consists of any combination of the following modules (Basic Host Scan, Endpoint Assessment, and Advanced Endpoint Assessment). This program installs on the remote device after the user connects to the security appliance, before the user logs in, and performs a scan of the user computer.
- **Secure Desktop (Vault):** Secure Desktop encrypts the data and files that are associated with or downloaded during the remote session into a secure desktop partition. It presents a graphical representation of a desktop that includes an image of a lock to signify a safe environment for the remote user to work in. Upon session termination, it removes the partition in a secure fashion.
- **Cache Cleaner:** An alternative to Secure Desktop, it is functionally more limited, but has the flexibility to support more operating systems. It cleans the browser cache at the end of a VPN session. This information includes entered passwords, autocompleted text, files that are cached by the browser, and cookies.
- **Keystroke logger detection:** This function scans for processes or modules that record keystrokes that are entered by the user and deny VPN access if a suspected keystroke logging application is present.
- **Cisco Secure Desktop policies:** Cisco Secure Desktop policies specify the remote user experience, rights, and restrictions. Depending on the results of the prelogin assessment module, a particular policy is assigned to a user session or the session is denied.

- **Integration with DAP:** The security appliance may use one or more endpoint attribute values in combination with optional, authentication, authorization, and accounting (AAA) attribute values as conditions for assigning dynamic access policies (DAP). The Cisco Secure Desktop features that are supported by the endpoint attributes of DAP include operating system detection, Cisco Secure Desktop policies, Basic Host Scan results, and Endpoint Assessment.
- **Host emulation detection:** This additional feature of prelogin policies, determines whether a remote Microsoft Windows operating system is running over virtualization software.
- **Windows Mobile Device Management:** A feature of the Host Scan module that allows posture checks that are specific to mobile devices. This feature requires installment of Cisco AnyConnect client to on the mobile device and therefore does not apply to clientless SSL VPN sessions.
- **Standalone installation packages:** This feature offers an additional Cisco Secure Desktop installation option, in addition to being distributed to the endpoint by the Cisco ASA adaptive security appliance. Standalone packages can be deployed by enterprise-wide software distribution tools.
- **Cisco Secure Desktop Manual Launch:** This feature allows users to start a clientless SSL VPN connection by launching Cisco Secure Desktop from their computer. This benefits users who do not have permission to run ActiveX or Java, or do not have ActiveX or Java installed.



## Cisco Secure Desktop

### Prelogin Assessment

- Step 1. A remote user connects via Cisco AnyConnect client or clientless SSL VPN.
- Step 2. Operating system detection module downloaded and running.
- Step 3. Prelogin assessment module downloaded and running.
- Step 4. Based on prelogin assessment module result, login denied or Cisco Secure Desktop policies are applied.



The first phase of Cisco Secure Desktop operation includes all the tasks leading up to user login and assessment of the system of the user. Prelogin assessment occurs in these steps:

- Step 1** A remote user connects to the security appliance using the Cisco AnyConnect client or clientless SSL VPN.
- Step 2** The operating system detection module is downloaded and runs.
- Step 3** The prelogin assessment module is downloaded and runs.
- Step 4** Based on prelogin assessment module result, login is denied or Cisco Secure Desktop policies are applied.

If the remote computer passes a prelogin assessment that is associated with a particular prelogin policy that is configured on the security appliance, a scan of the antivirus, antispyware, personal firewall, and other optional keystroke logger, file, registry, and process checks occurs. This scan can be turned on or off by the system administrator.

Secure Desktop (Vault) or Cache Cleaner installs only if the prelogin assessment that is associated with a particular prelogin policy passes, and only if the Secure Desktop or Cache Cleaner parameters are enabled for the matched prelogin policy.

If both the prelogin assessment for a particular prelogin policy and the Host Scan checks pass, and the prelogin policy has both Secure Desktop (Vault) and Cache Cleaner disabled (typically for a corporate computer login), only the DAP determines the user experience after authentication.

---

**Note** DAP is covered in the other lessons within this course.

---

## Cisco Secure Desktop

### Login, Postlogin, and Session Cleanup

- Step 5. Check for **keystroke logger** and **host emulation**.
- Step 6. **Secure Desktop (Vault)** or **Cache Cleaner** downloaded and running.
- Step 7. User authenticated and VPN session initiated.
- Step 8. **DAP checks** applied.
- Step 9. VPN connection becomes active.
- Step 10. **Postsession cleanup** occurs.



After the prelogin assessment is complete, the Cisco Secure Desktop application lets the user begin the network authentication process. During the user authentication process, a secured session desktop is created for the user to switch to in order to provide a secured workspace during the VPN session. The Login phase encompasses these evaluation steps:

- Step 1** Application checks for keystroke logger and host emulation.
- Step 2** Host Scan with Secure Desktop (Vault) or Cache Cleaner is downloaded and runs.
- Step 3** The user is authenticated and a VPN session is initiated.

After the user has logged into the network and has an actively managed SSL VPN network session, the user is allowed to access network resources, based on the configured policy for that user. After the user terminates the SSL VPN connection (or the idle timeout expires), the Secure Desktop postsession cleanup initiates. The postlogin and session cleanup phase encompasses these steps:

- Step 1** DAP checks are applied.
- Step 2** A VPN connection becomes active.
- Step 3** Postsession cleanup occurs.

## Cisco Secure Desktop

### Solution Components

Before deploying Cisco Secure Desktop, analyze your current system and network architecture. It should meet these requirements:

1. Supported operating systems
2. User privileges
3. Supported Internet browsers (clientless SSL VPN)
4. Internet browser settings (clientless SSL VPN)



To deploy Cisco Secure Desktop in the SSL VPN, you must ensure that your solution components meet these requirements:

- **Supported operating systems:** The VPN users must run supported operating systems on their remote computers.
- **User privileges:** The users connecting to the SSL VPN must have sufficient privileges to install, update, or operate the Cisco Secure Desktop modules.
- **Supported Internet browsers:** The users must use a supported browser to start the SSL VPN connections. This requirement applies only to clientless SSL VPNs.
- **Internet browser settings:** The browser must be configured with parameters that allow the execution of required ActiveX controls, plug-ins, Java applets, and file downloads. These permissions are needed for clientless SSL VPNs.

## Cisco Secure Desktop

### Supported Operating Systems (Cisco Secure Desktop 3.5 x)

Operating System	Prelogin Assessment	Host Scan	Vault	Cache Cleaner	Keystroke Logger Detection	Host Emulation Detection
Windows 7	X	X		X		
Windows Vista	X	X	X*	X	X*	X*
Windows XP	X	X	X*	X	X*	X*
Windows Mobile Professional 6.0/6.1	X	X		X		
Apple Macintosh OS X 10.6	X	X		X		
Linux	X	X		X		

\*Only for 32-bit systems

This table provides the information on the interoperability of Cisco Secure Desktop.

### Operating System Interoperability

Operating System	Prelogin Assessment	Host Scan	Vault	Cache Cleaner	Keystroke Logger Detection	Host Emulation Detection
Microsoft Windows 7	Yes	Yes	—	Yes	—	—
Microsoft Windows Vista	Yes	Yes	32-bit systems only	Yes	32-bit systems only	32-bit systems only
Microsoft Windows XP	Yes	Yes	32-bit systems only	Yes	32-bit systems only	32-bit systems only
Microsoft Windows Mobile Professional 6.0/6.1	Yes	Yes	—	Yes	—	—
Apple Macintosh OS X 10.4 (PowerPC or Intel)	Yes	Yes	—	Yes	—	—
Linux	Yes	Yes	—	Yes	—	—

## Deploying Cisco Secure Desktop

### User Privileges

Cisco Secure Desktop can be installed on the client computer:

- Cisco AnyConnect SSL VPN:
  - After Cisco AnyConnect client is installed: No administrative privileges
  - Together with Cisco AnyConnect install: Requires administrative privileges
  - Executable File: Requires administrative privileges (not used)
- Clientless SSL VPN:
  - ActiveX: Requires administrative privileges
  - Microsoft JVM: Requires administrative privileges
  - Sun JVM: Does not require administrative privileges
  - Executable file: Requires administrative privileges

To enable Cisco Secure Desktop functions, the users must install the software on their computers. The software can be installed in several ways:

- Cisco AnyConnect SSL VPNs:
  - **After Cisco AnyConnect client is installed:** No administrative privileges are required. Installation of the Cisco Secure Desktop or Host Scan is performed in a similar fashion to updating the Cisco AnyConnect client, which also does not require any privileges.
  - **Together with Cisco AnyConnect install:** This method requires administrative privileges to install the Cisco AnyConnect client along with Cisco Secure Desktop.
  - **Executable file:** This method requires administrative privileges. This option is not used, because Cisco Secure Desktop alone, without Cisco AnyConnect client, cannot be used in full tunneling scenarios.
- Clientless SSL VPNs:
  - **ActiveX:** This method is used when the Cisco Secure Desktop software is being distributed to the endpoint by the Cisco ASA adaptive security appliance. The user must have administrative privileges to install the Cisco Secure Desktop using ActiveX controls.
  - **Microsoft Java Virtual Machine (JVM):** This option is used when the Cisco ASA adaptive security appliance distributes the Cisco Secure Desktop software. The user must have administrative privileges to install the Cisco Secure Desktop using Microsoft JVM.
  - **Sun Java Virtual Machine:** This method is also used when the Cisco ASA adaptive security appliance distributes the Cisco Secure Desktop software. When the security appliance distributes the software, the user does not need administrative privileges, but Sun JVM must be installed and enabled in the browser.

- **Executable file:** This installation option is related to the Cisco Secure Desktop Manual Launch feature. It allows users to install the Cisco Secure Desktop and then create a Clientless SSL VPN connection to their Cisco ASA adaptive security appliance by manually launching Cisco Secure Desktop from their computers. This option is primarily intended for users who do not have permission to run ActiveX or Java, or do not have ActiveX or Java installed. File-based installation and startup are supported by Windows, Linux, and Mac OS X desktops. They are not used by Windows Mobile Device users. The user must have administrative privileges to install the Cisco Secure Desktop software using the installation file.

## Deploying Cisco Secure Desktop

### Internet Browsers Supported by Clientless SSL VPN

Web Browser	Prelogin Assessment	Host Scan
Internet Explorer 6.0	x	x
Internet Explorer 7.0	x	x
Mozilla Firefox 3.0	x	x
Safari 3.2.1	x	x

Note: Host Scan and Cache Cleaner do not support 64-bit versions of Internet Explorer.

© 2010 Cisco Systems, Inc. All rights reserved. VPN-11-949-01

Cisco Secure Desktop works in clientless SSL VPNs with many of the mainstream web browsers that are available on the market. The table lists the supported web browsers for the prelogin assessment and Host Scan modules.

### Web Browser Interoperability

Web Browser	Prelogin Assessment	Host Scan
Microsoft Internet Explorer 6.0	Yes	Yes
Microsoft Internet Explorer 7.0	Yes	Yes
Mozilla Firefox 3.0	Yes	Yes
Safari 3.2.1	Yes	Yes

**Note** Host Scan and Cache Cleaner do not support 64-bit versions of Microsoft Internet Explorer.

## Deploying Cisco Secure Desktop

### Clientless SSL VPN Internet Browser Settings

Attribute	Setting
ActiveX controls and plug-ins > Download signed ActiveX controls	Enable
ActiveX controls and plug-ins > Run ActiveX controls and plug-ins	Enable
Downloads > File download	Enable
Scripting > Active scripting	Enable
Scripting > Scripting of Java applets	Enable
Microsoft VM > Java permissions	High, medium, or low safety

Note: Host Scan and Cache Cleaner do not support 64-bit versions of Internet Explorer.

This table illustrates the internet browser parameters that enable all three installation methods for clientless SSL VPNs, in which the security appliance distributes the installation package:

- ActiveX
- Microsoft Java Virtual Machine
- Sun Java Virtual Machine

The installation that is based on the executable file is not affected by any of these settings. The table describes the required browser settings that affect a given installation method.

#### Required Web Browser Settings

Attribute	Installation Method	Required Setting
ActiveX controls and plug-ins > Download signed ActiveX controls	ActiveX	Enable
ActiveX controls and plug-ins > Run ActiveX controls and plug-ins	ActiveX	Enable
Downloads > File download	ActiveX, Microsoft Java Virtual Machine, Sun Java Virtual Machine	Enable
Scripting > Active scripting	ActiveX	Enable
Scripting > Scripting of Java applets	Sun Java Virtual Machine	Enable
Microsoft VM > Java permissions	Microsoft Java Virtual Machine	High, medium, or low safety

## Deploying Cisco Secure Desktop

### Deployment Tasks

1. Install and enable Cisco Secure Desktop on the Cisco ASA adaptive security appliance.
2. Configure prelogin criteria.
3. Configure prelogin policies.
4. Configure Advanced Endpoint Assessment.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-11-0-4-0

The deployment of Cisco Secure Desktop consists of five overall configuration tasks:

1. Install and enable Cisco Secure Desktop on the Cisco ASA adaptive security appliance.
2. Configure prelogin criteria.
3. Configure prelogin policies.
4. Configure Advanced Endpoint Assessment.



## Deploying Cisco Secure Desktop

### Input Parameters

Parameter	Description
Operating system on endpoints	Required to choose proper version of Cisco Secure Desktop
Required prelogin policy	Required to create a prelogin policy to check endpoints Required to correctly configure: <ul style="list-style-type: none"><li>• Host Scan</li><li>• Secure Desktop (Vault)</li><li>• Cache Cleaner</li><li>• Advanced Endpoint Assessment</li><li>• Keystroke Logger Detection</li><li>• Host Emulation Detection</li></ul>

To deploy Cisco Secure Desktop in the Cisco AnyConnect SSL VPN, you must ensure that your solution components meet these requirements:

- **Operating systems running on endpoints:** Needed to select a proper version of Cisco Secure Desktop.
- **Required prelogin policy:** Needed to configure prelogin policy to check endpoints and to enable the Cache Cleaner or Secure Desktop (Vault) with proper parameters. Needed to optionally enable Host Scan, Advanced Endpoint Assessment, keystroke logger detection, and host emulation detection.

## Deploying Cisco Secure Desktop

### Deployment Guidelines

- Cisco Secure Desktop is supported in SSL VPN only (no IPsec).
- Consider using Cisco Secure Desktop in environments with very strict security policy.
- Use a prelogin policy to determine whether an endpoint connecting to the SSL VPN is enterprise-owned or unmanaged.
- Use Cisco Secure Desktop if the endpoint is unmanaged.

Consider the following general deployment guidelines when you deploy Cisco Secure Desktop in SSL VPN Cisco AnyConnect environments:

1. Cisco Secure Desktop is supported only in SSL VPNs. It cannot be deployed in IPsec VPNs.
2. Consider using Cisco Secure Desktop in environments with a very strict security policy.
3. Use a prelogin policy to determine whether an endpoint connecting to the SSL VPN policy is enterprise-owned or -managed.
4. Use Cisco Secure Desktop if the endpoints are unmanaged.

# Installing, Enabling, and Customizing Cisco Secure Desktop

This topic describes how to install, enable, and customize Cisco Secure Desktop on the Cisco ASA adaptive security appliance.

## Installing, Enabling, and Customizing Cisco Secure Desktop

### Configuration Tasks

1. Install Cisco Secure Desktop and enable it globally on the Cisco ASA.
2. (Optional) Disable Cisco Secure Desktop per the connection profile.\*
3. Customize Cisco Secure Desktop to display custom banners and backgrounds.\*\*

\* Available in Cisco ASA software 8.2(1) and later

\*\* Supported only on 32-bit Windows Vista and 32-bit Windows XP SP2 or SP3

To install, enable, and customize Cisco Secure Desktop on the Cisco ASA adaptive security appliance, complete the following configuration tasks:

- Step 1** Install Cisco Secure Desktop and enable Cisco Secure Desktop globally on the Cisco ASA adaptive security appliance.
- Step 2** Optionally, disable Cisco Secure Desktop per connection profile.
- Step 3** Customize Cisco Secure Desktop to display custom banners and backgrounds.

The figure shows an example that will serve as configuration scenario for ongoing configuration tasks. You will upload and globally enable Cisco Secure Desktop on the Cisco ASA adaptive security appliance. Then you will disable Cisco Secure Desktop for the ENGINEERING connection profile. You will also customize the Cisco Secure Desktop text color that is shown in the Cisco Secure Desktop.

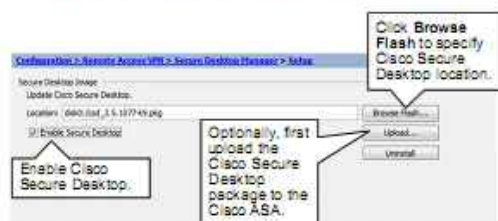
**Note** Disabling of Cisco Secure Desktop per connection profile is available in Cisco ASA software version 8.2(1) and later.

Customizing Cisco Secure Desktop to display custom banners and backgrounds is available only with 32-bit Windows Vista and 32-bit Windows XP SP 2 or SP3.

## Installing, Enabling, and Customizing Cisco Secure Desktop

### Task 1: Install and Enable Cisco Secure Desktop on the Cisco ASA.

- Download Cisco Secure Desktop web deployment package from Cisco.com.
- Upload the Cisco Secure Desktop package to the Cisco ASA.



Configuration > Remote Access VPN > Secure Desktop Manager > Setup

When enabling the Cisco Secure Desktop on the Cisco ASA adaptive security appliance, you first have to download a web deployment package from Cisco.com to the PC that is running Cisco Adaptive Security Device Manager (Cisco ASDM). Then you have to upload the package to the Cisco ASA adaptive security appliance and enable Cisco Secure Desktop globally. To perform these tasks using Cisco ASDM, complete the following configuration steps:

- Step 1** Inside the Cisco ASDM, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup** (not shown in the figure). The **Setup** panel appears.
- Step 2** Click **Upload** to prepare to transfer a copy of the Cisco Secure Desktop software from your local PC to the flash card in the Cisco ASA adaptive security appliance. Cisco ASDM opens the Upload Image dialog box (not shown in the figure).
- Step 3** Click **Browse Local Files** to prepare to select the file on your local PC (not shown in the figure).
- Step 4** Select the Cisco Secure Desktop file by navigating to the proper folder where the file is stored and click **Select** (not shown in the figure).
- Step 5** Click **Upload File**. Cisco ASDM will transfer a copy of the file to the flash card.

**Note** If Cisco Secure Desktop had been previously uploaded to the Cisco ASA adaptive security appliance, specify the location of the Cisco Secure Desktop web deployment file by entering the location into the Location field. You can also click the **Browse Flash** button and select the Cisco Secure Desktop file from the Browse Flash window (not shown in the figure).

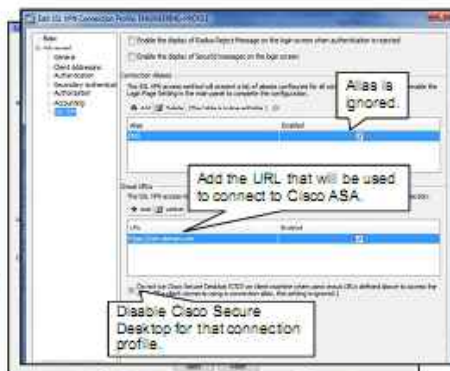
- Step 6** Check the **Enable Secure Desktop** check box.
- Step 7** Click **Apply** to apply the configuration.

## Installing, Enabling, and Customizing Cisco Secure Desktop

### Task 2: (Optional) Disable Cisco Secure Desktop per Connection Profile

You can disable Cisco Secure Desktop per specific connection profile:

- You have to manually map a URL that a user uses to connect the Cisco ASA to a connection profile.
- Then you can disable Cisco Secure Desktop for that specific connection profile.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

After you enable Cisco Secure Desktop globally, the Cisco Secure Desktop will be enabled for all SSL VPN connections that are made to the Cisco ASA adaptive security appliance, regardless of a connection profile. However, you can optionally disable the Cisco Secure Desktop for a specific connection profile. To disable Cisco Secure Desktop for a specific connection profile using Cisco ASDM, complete the following steps:

- Step 1** Inside the Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** (not shown in the figure). The **AnyConnection Profiles** panel appears.
- Step 2** From the Connection Profiles table, select a connection profile for which you would like to disable Cisco Secure Desktop. Click **Edit**. The Edit SSL VPN Connection Profile window appears.
- Step 3** Expand the **Advanced** option from the menu on the left and click the **SSL VPN** option.
- Step 4** Click **Add** in the Group URLs area of the window and enter a group URL or IP address into the URL window (not shown in the figure). This step will enable the Cisco ASA adaptive security appliance to select automatically the proper connection profile when a user makes a connection to the specified URL.
- Step 5** Click **OK** (not shown in the figure).
- Step 6** Check the **Do Not Run Cisco Secure Desktop (CSD)** check box. In the example, Cisco Secure Desktop has been disabled for the ENGINEERING-PROFILE.
- Step 7** Click **OK**.
- Step 8** Click **Apply** to apply the configuration.

## Installing, Enabling, and Customizing Cisco Secure Desktop

### Task 3: Customize Cisco Secure Desktop

You can customize the following elements:

- Text color, background image, and banner images



When running Cisco Secure Desktop on Windows Vista and XP SP2 or SP3 (32 bit only), you can customize text color, background image, and banner images that are displayed by the Cisco Secure Desktop. To customize Cisco Secure Desktop using Cisco ASDM, complete the following steps:

- Step 1** Inside the Cisco ASDM, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Secure Desktop Customization** (not shown in the figure). The **Secure Desktop Customization** pane appears.
- Step 2** Click the **Choose Color** button to invoke the color chooser to change the color of text that is displayed by Cisco Secure Desktop. Select a color from the Secure Desktop Text Color window and click **OK**.
- Step 3** To change the background or banner images, first upload a new image to the Cisco ASA adaptive security appliance by clicking the **Import** button. Choose a desired image from the **Import Local File** window and click **Import Local File** button.
- Step 4** Then choose the banner for which you would like to replace the image from the table and specify that new image should be used by clicking the—Default—table cell.
- Step 5** Repeat Steps 1 through 4 to change images for other banners and for a Cisco Secure Desktop background also.
- Step 6** Click **Apply** to apply the configuration.

# Installing, Enabling, and Customizing Cisco Secure Desktop

## CLI Commands

```
webvpn
csd image disk0:/csd 3.5.1077-k9.pkg
csd enable
|
tunnel-group ENGINEERING-PROFILE webvpn-attributes
group-url https://vpn.domain.com enable
without-csd
```

Enable Cisco Secure Desktop

Disable Cisco Secure Desktop for a connection profile.

To enable Cisco Secure Desktop using the command line interface (CLI), use the following commands. First enter webvpn configuration mode using the **webvpn** command. Then specify the location of the Cisco Secure Desktop web deployment file using the **csd image** command. Then enable Cisco Secure Desktop globally using the **csd enable** command.

To disable Cisco Secure Desktop for a specific connection profile, first enter profile (tunnel-group) configuration mode using the **tunnel-group** command, followed by tunnel group name and **webvpn-attributes** keyword. Then specify the incoming URL or IP address for the connection profile using the **group-url** command. This configuration will enable the Cisco ASA adaptive security appliance to use the proper connection profile when users connect to the specified URL or IP address. Finally, disable Cisco Secure Desktop for the connection profile using the **without-csd** command.

### webvpn

To enter webvpn mode, in global configuration mode, enter the **webvpn** command. To remove any commands that are entered with this command, use the **no webvpn** command. These **webvpn** commands apply to all WebVPN users.

These **webvpn** commands let you configure AAA servers, default group policies, default idle timeout, HTTP and HTTPS proxies, and NetBIOS Name Server (NBNS) servers for WebVPN, as well as the appearance of WebVPN screens that end users see.

### webvpn

### csd image

To validate the Cisco Secure Desktop distribution package and add it to the running configuration, effectively installing Cisco Secure Desktop, use the **csd image** command in webvpn configuration mode. To remove the Cisco Secure Desktop distribution package from the running configuration, use the **no** form of the command:

**csd image** *path*

## csd image Parameters

Parameter	Description
<code>path</code>	Specifies the path and filename of the Cisco Secure Desktop package, up to 255 characters

## csd enable

To enable Cisco Secure Desktop for management and remote user access, use the **csd enable** command in `webvpn` configuration mode. To disable Cisco Secure Desktop, use the **no** form of this command.

**csd enable**

## tunnel-group webvpn-attributes

To enter the `webvpn-attributes` configuration mode, use the **tunnel-group webvpn-attributes** command in global configuration mode. This mode configures settings that are common to WebVPN tunneling.

To remove all WebVPN attributes, use the **no** form of this command.

**tunnel-group** *name* **webvpn-attributes**

## tunnel-group webvpn-attributes Parameters

Parameter	Description
<code>webvpn-attributes</code>	Specifies WebVPN attributes for this tunnel-group
<code>name</code>	Specifies the name of the tunnel-group

## group-url

To specify incoming URLs or IP addresses for the group, use the **group-url** command in `tunnel-group webvpn` configuration mode. To remove a URL from the list, use the **no** form of this command.

**group-url** *url* [**enable** | **disable**]

## group-url Parameters

Parameter	Description
<code>disable</code>	Disables the URL, but does not remove it from the list
<code>enable</code>	Enables the URL
<code>url</code>	Specifies a URL or IP address for this tunnel group

## without-csd

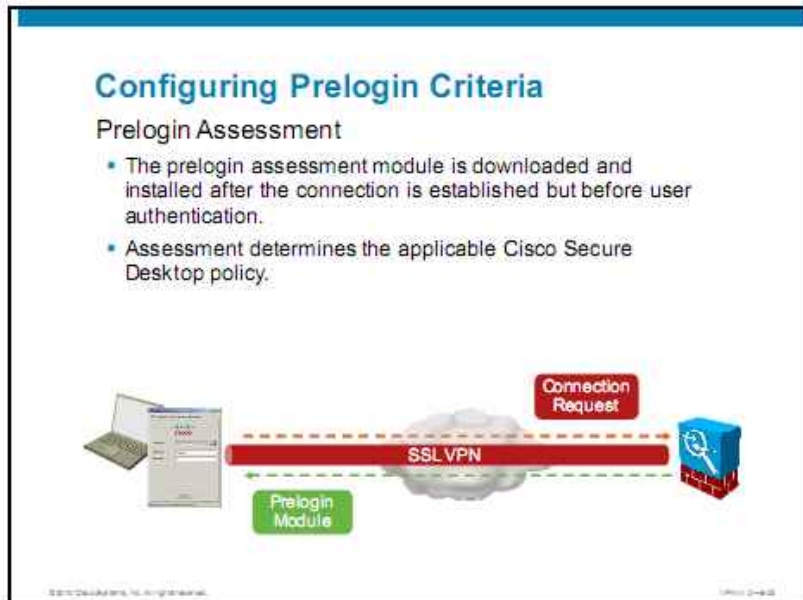
To exempt certain users from running Cisco Secure Desktop on a per-connection profile basis if they enter one of the entries in the `group-url` table to establish the VPN session, use the **without-csd** command in `tunnel webvpn` configuration mode. To remove this command from the configuration, use the **no** form of the command.

**without-csd**



# Configuring Prelogin Criteria

This topic describes how to configure prelogin criteria on the Cisco ASA adaptive security appliance.



Secure Desktop Manager lets you 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. These checks determine whether to assign a prelogin policy or whether to display a “Login Denied” message for the remote user. The settings of the matched prelogin policy determine whether Secure Desktop (Vault) or Cache Cleaner loads. The application of a prelogin policy to dynamic access policies (DAP) determines the access rights and restrictions that are placed on the connection, and determines the behavior of the Cisco Secure Desktop component before, during, and after the user logs in. For example, it determines whether to check for keystroke loggers or whether to apply an inactivity timeout.

## Configuring Prelogin Criteria

### Prelogin Assessment Capabilities

This module can check for:

- Presence and integrity of files
- Presence of digital certificates
- Type of operating system
- Network interface card IP address
- Microsoft Windows registry keys



The prelogin criteria allow you to define a set of conditions, based on which you may deny the connection, load the Secure Desktop (Vault), or load the Cache Cleaner. These criteria can be evaluated during the prelogin assessment:

- **Existence and integrity of specified files:** Lets you specify the presence or absence of a particular file, its version, and its checksum.
- **Digital certificates:** Lets you specify the issuer of a certificate and one certificate attribute and value to match.
- **OS version:** Lets you configure checks for Microsoft Windows 2000, Windows XP, and Windows Vista; Win 9x (for Windows 98), Mac (for Apple Mac OS X 10.4), and Linux.
- **IP address:** Lets you specify an IP address range, or network address and subnet mask.
- **Microsoft Windows Registry:** Lets you detect the presence or absence of a registry key. This criterion is available only for Microsoft Windows and is ignored for other operating systems.

## Configuring Prelogin Criteria

### Configuration Scenario



This figure illustrates the network scenario that will be used on the upcoming configuration tasks. You will configure a prelogin policy to determine whether endpoints are enterprise-owned or unmanaged. You will use the following criteria to categorize endpoints:

- **Enterprise-managed computers:** Employees use these endpoints in their home offices to connect to the corporate VPN. These computers run Windows operating systems.
- **Unmanaged PCs:** Users use these endpoints to connect to the VPN from public places, such as Internet kiosks.

## Configuring Prelogin Criteria

### Task 1: Configure Prelogin Criteria

- Prelogin criteria are configured in the form of a sequence.
- By default, the Default prelogin policy is configured.



The Cisco ASDM provides an intuitive tool to define the prelogin policies in the form of a graph. This graph is built as a tree of “if-then” conditions. The if-then conditions, also called checking criteria, are represented in the tree as circles with a plus (+) sign. The if-then conditions are junctions where multiple branches emerge from the tree trunk for the different results of the if-then condition.

The top of the tree is the Start field. To define the first checking criteria, click the circle with the + sign to open the Check dialog box. In the Check drop-down list, choose the if-then condition that you want to use at the top of the decision tree.

## Configuring Prelogin Criteria

### Task 1: Configure Prelogin Criteria (Cont.)

- Created policy will appear in the navigation pane.

The screenshot shows the configuration interface for Prelogin Policy. On the left is a navigation pane with the following structure:

- Remote Access VPN
  - Production
    - Remote Desktop Access
    - Remote SSL VPN Access
    - Remote Users
    - Secure Desktop Manager
      - Setup
      - Initial Action
      - Prelogin Policy
        - Unmanaged\_PCs
        - Secure Desktop Customization
      - Win9x
    - Endpoint Management
    - Endpoint Location
    - Endpoint Learning
    - Endpoint Server
    - Endpoint
    - Endpoint

The main window displays the Prelogin Policy configuration. It shows a decision tree with a root node 'Root' leading to a 'Win9x' condition node, which then branches into four end nodes: 'Default', 'Login Denied', 'Login Denied', and 'Login Denied'. A callout box points to the 'Login Denied' end node for Win9x, stating: "Click the end node to change the prelogin policy." Below the tree is a configuration dialog box with radio buttons for 'Login Denied', 'Policy', and 'Subsequent'. The 'Policy' option is selected. The 'Label' field contains 'unmanaged\_pcs'. A callout box points to this field: "Selects policy type and specify a name." At the bottom of the dialog are 'Update' and 'Cancel' buttons. A callout box points to the 'Update' button: "Update the current endpoint profile." At the bottom of the configuration window, the breadcrumb path is: Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy.

This example illustrates how the first check condition evaluates the operating system of the endpoint. This type of criteria has five different results that effectively create five branches of the decision tree.

Each branch leads to an end node. The end nodes in this example are one “Default” and four “Login Denied.” You may configure multiple if-then conditions before an end node is defined in the tree. Each end node can be edited to select one of three end-node types:

- **Login Denied:** This action effectively cuts off any further processing of this particular branch. If the defined combinations of conditions are met, access will be blocked.
- **Policy:** This option defines an endpoint profile. An endpoint profile represents the state that is achieved by the endpoint after it reaches this point in the tree. For each endpoint profile, a policy is automatically created in the Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy submenu. You will access that policy to edit the actions that will be applied to the endpoint.
- **Subsequence:** This option allows you to terminate the branch and continue it in another place in the graph. This linkage is a graphical aid that allows you to draw the entire tree in a more compact area.

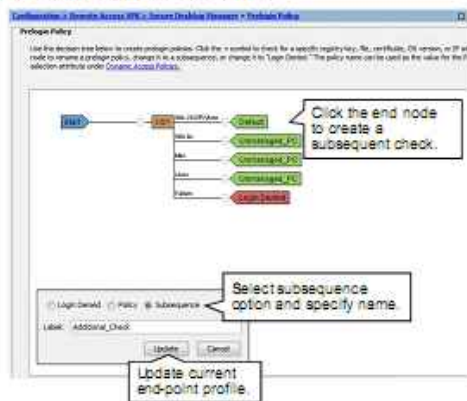
In this example, the first endpoint profile is named “Default,” and it has been created automatically in the tree. You will click the Login Denied end node for Win 9x endpoints, change its type to Policy, and enter the new policy name “Unmanaged\_PCs.” This policy is automatically created in the system and will be then applied to the matched endpoints.

## Configuring Prelogin Criteria

### Task 1: Configure Prelogin Criteria (Cont.)

To perform additional checks you can:

- Continue from the existing plus sign
- Create a new subsequence for better visibility



Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy

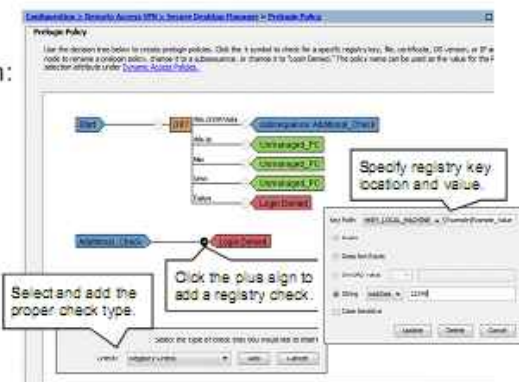
After setting three end nodes to the Unmanaged\_PC policy, you may change the Default end node to a subsequence. In this example, the subsequence is named "Additional\_Check" and will allow you to continue the endpoint evaluation at another place.

## Configuring Prelogin Criteria

### Task 1: Configure Prelogin Criteria (Cont.)

To perform additional checks you can:

- Continue from the existing plus sign
- Create a new subsequence for better visibility



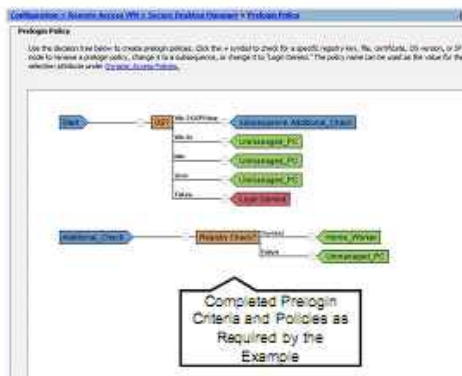
Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy

This figure illustrates how you can continue the endpoint evaluation process. The Additional\_Check subsequence identifies endpoints that run Windows 2000, XP, and Vista. In this example, you add an additional if-then condition that checks for a defined string in a specific registry key.

## Configuring Prelogin Criteria

### Task 1: Configure Prelogin Criteria (Cont.)

- Change end node policies as required.
- Another policy should appear in the navigation pane.



Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy

The registry check creates two branches for the Windows 2000, Windows XP, and Windows Vista computers; each branch representing a “then” (success or failure) in the if-then condition.

In this example, you will change the end nodes in each branch to policies named “Home\_Worker” and “Unmanaged\_PCs.” They represent the two endpoint profiles in your environment. The Home\_Worker policy is automatically added in the Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy submenu.

## Verifying Prelogin Criteria

The screenshot displays the Windows Event Viewer interface. On the left, a flowchart illustrates the prelogin process: 'Start' leads to 'Initial Checks', which then branches into 'Successful Checks' and 'Failed Checks'. 'Successful Checks' leads to 'Home\_Worker', and 'Failed Checks' leads to 'Utmanger\_PC'. 'Initial Checks' also leads to 'Subsequent Additional Check', which then branches into 'Utmanger\_PC', 'Utmanger\_PC', 'Utmanger\_PC', and 'Login Failed'. On the right, the 'Event Properties' window shows the following details:

Event
Date: 5/20/2010
Time: 1:07:20 PM
Type: None
User: N/A
Computer: VM-932

Description:

```
endpoint.os.version = "Win7x64 SP1"
endpoint.os.servicepack = "2"
endpoint.policy.location = "Home_Worker"
endpoint.device.protection = "secure desktop"
endpoint.device.protection_extension = "3.4.10.1"
endpoint.os.family = "X86_64"
endpoint.os.family = "true"
endpoint.os.family = "true"
```

Start > Programs > Administrative Tools > Event Viewer

On a Windows PC, the VPN user can verify the received prelogin assessment data by viewing the logs that are available in the Event Viewer. The Event Viewer can be accessed using the Start > Programs > Administrative Tools > Event Viewer menu. The information is recorded in the Application log and contains entries such as:

- **endpoint.os.version:** Result of the operating system-related Host Scan
- **endpoint.os.servicepack:** Result of the service pack-related Host Scan
- **endpoint.policy.location:** The prelogin policy that is identified for the endpoint; in this example, "Home\_Worker"
- **endpoint.device.protection:** The downloaded Cisco Secure Desktop module; in this example, "secure desktop"



# Configuring Prelogin Policies

This topic describes how to configure Cisco Secure Desktop policies.

## Configuring Policies

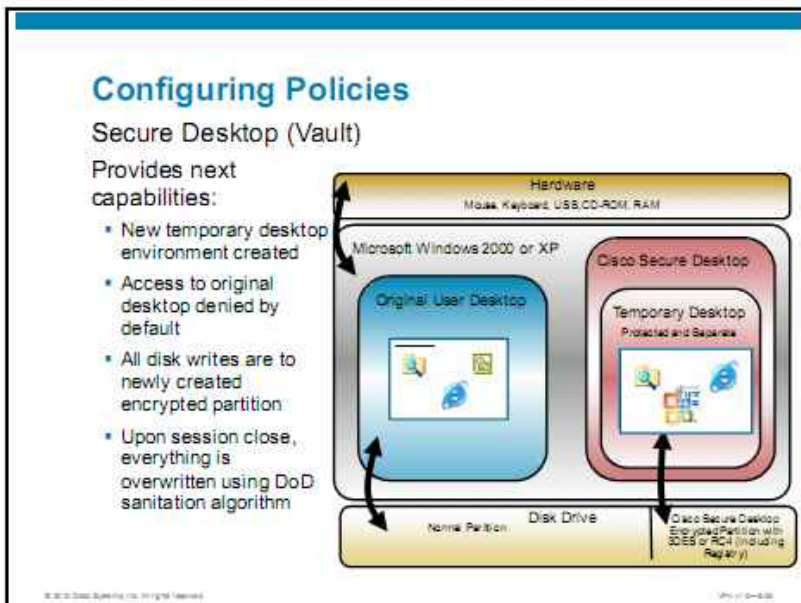
### Prelogin Policies Overview

- Based on prelogin criteria (assessment) you can assign a Cisco Secure Desktop policy to a host.
- Under Cisco Secure Desktop policies you can enable:
  - Secure Desktop (Vault)
  - Cache Cleaner
  - Detect Host Emulation
  - Detect Keystroke Logger
- Host Scan can be configured here.

When the prelogin policies have been created, you can apply actions to them. The major configuration blocks include these policies:

- **Secure Desktop (Vault):** Vault encrypts the data and files that are associated with the remote session into a secure desktop partition. It presents a graphical representation of a desktop that includes an image of a lock to signify a safe environment for the remote user to work in. Upon session termination, it uses a sanitation algorithm to remove the partition. Typically used during clientless SSL VPN sessions, Secure Desktop attempts to reduce the possibility that cookies, browser history, temporary files, and downloaded content remain after a remote user logs out, the session times out, or after an abrupt termination occurs. Secure Desktop runs only on 32-bit Microsoft Windows operating systems. If a prelogin policy is configured to install Secure Desktop, but the operating system on the remote computer does not support it, Cache Cleaner attempts to install instead.
- **Cache Cleaner:** This is a more limited alternative to Secure Desktop (Vault) that is available for a wider operating system range. In addition to Microsoft Windows, the Cache Cleaner works also on Apple Mac OS and Linux.
- **Detect Host Emulation:** This module determines whether an endpoint is running over virtualization software. Host emulation detection runs on the same operating systems as Secure Desktop (Vault), that is, only on 32-bit Microsoft Windows operating systems.
- **Detect Keystroke Logger:** You can configure selected prelogin policies to scan for processes or modules that record keystrokes that are entered by the user, and deny VPN access if a suspected keystroke logging application is present. Keystroke logger detection runs on the same operating systems as Secure Desktop (Vault), that is, on 32-bit Microsoft Windows operating systems.

- **Host Scan:** You can enable the Host Scan to scan for endpoints posture and remediation. Host Scan consists of Basic Host Scan, Endpoint Assessment, and Advanced Endpoint Assessment.



Secure Desktop (Vault) creates a new temporary desktop environment. As an administrator, you can control the Vault access to the registry, command window, network drives and folders, and removable drives. By default, the Vault provides visibility only to the Documents and Settings, WINDOWS, and Program Files directories on Microsoft Windows. It offers access only to applications that are installed in these directories.

Secure Desktop (Vault) does not encrypt or clean system memory information, including that which may be left on the disk by the operating system in the Microsoft Windows virtual memory file, commonly referred to as the paging file. Secure Desktop Manager provides an option that seeks to disable printing from within a user session. If local printing is permitted, there may be instances when data can remain in the local system print spool.

Secure Desktop (Vault) is highly configurable. It has a rich set of features that provide cooperative security for users trying to work in a secure manner. These features govern the relationship of the secure partition to the host, the network on which the host runs, and the Internet.

Secure Desktop (Vault) does not isolate the secure partition from the rest of the host; it prevents information in the secure partition from passing to the local drives. Vault does not prevent information from passing from the host to the secure partition. If the user is working on a host that is already infected with malware, that malware can pass from the host to the secure partition.

Secure Desktop (Vault) does not prevent access from the secure partition to the network on which the host runs nor does it restrict access to the file system of the host. Users can launch a browser from within the secure partition and they can have access to the Internet.

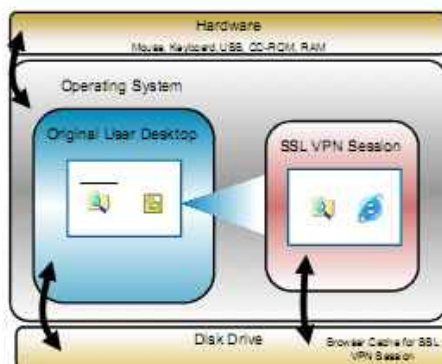
Browser plug-ins, shell extensions, and a cluttered registry can greatly extend the time that is needed for Secure Desktop (Vault) to perform read and write operations on the registry. It can therefore take a longer period than one would expect for the clientless SSL VPN login page to open Vault if the remote computer is slow or is cluttered.

## Configuring Policies

Cache Cleaner

Cache Cleaner provides next capabilities:

- Removes local browser data (downloaded, input, or created) using DoD sanitation algorithm
- Monitors one browser application per SSL VPN session



Cache Cleaner is functionally more limited than Secure Desktop, but it has the flexibility to support more operating systems. It attempts to eliminate the information from the browser cache at the end of a clientless SSL VPN or Cisco AnyConnect client session. This information includes entered passwords, autocompleted text, files that are cached by the browser, browser configuration changes made during the session, and cookies.

Cache Cleaner monitors only one browser application per SSL VPN session.

## Configuring Policies

### Keystroke Logger and Host Emulation Detection

- Keystroke logger detection
  - Detection for keystroke loggers running as a process or kernel module
  - You can specify the keystroke logging applications that are safe or let the remote user interactively approve the applications
  - Does not detect hardware-based keystroke loggers
- Host emulation detection
  - Detection host emulation or virtualization of the connecting SSL VPN client
  - Configurable to disallow virtualized host from connecting



© 2010 Cisco Systems, Inc. All rights reserved.

VPN 11.0-4.08

By default, keystroke logger detection and host emulation detection are disabled for each prelogin policy. If you enable them, they download along with Secure Desktop (Vault), Cache Cleaner, or Host Scan onto the remote computer. The associated module runs only if the scan is clear, or only if you assign administrative control to the user and the user approves of the applications or host emulator the scan identifies. Keystroke logger detection and host emulation detection are available for supported versions of Windows operating systems. The modules provide these features:

- Keystroke logger, if enabled in a policy, runs only if the operating system is Windows and the user login has administrator privileges. If the user does not, keystroke logger detection does not run. You can configure each prelogin policy to scan for keystroke logging applications and deny access if a suspected keystroke logging application is present. You can specify the keystroke logging applications that are safe or let the remote user interactively approve the applications that the scan identifies.
- Host emulation detection determines whether a remote Microsoft Windows operating system is running over virtualization software. You can enable or disable this feature to deny access if a host emulator is present or report the detection to the user and let the user decide whether to continue or terminate the session.

## Configuring Policies

### Host Scan

- Host Scan installs on a remote device and runs periodically during SSL VPN session to determine if changes have occurred.
- Host Scan consists of three modules.
  - **Basic Host Scan**
    - Enables prelogin assessment
    - Detects operating system, files, registry, IP address, certificates
  - **Endpoint Assessment**
    - Scans for personal firewall, antivirus, and antispysware software
    - Does not perform remediation, but provides information to DAP
  - **Advanced Endpoint Assessment**
    - Scans for personal firewall, antivirus, and antispysware software
    - Performs remediation (rules, updates)

The Host Scan functionality offers three deployment methods.

## Basic Host Scan

Basic Host Scan automatically identifies operating systems and service packs on connecting computers. It also lets you configure inspections for specified processes, files, and registry keys. Thus, you can use this feature to configure checks for watermarks on remote computers to determine whether they are corporate-owned. You can use the results that are returned by Basic Host Scan when you configure different dynamic access policies (DAP) to distinguish corporate computers, home computers, and public computers.

Basic Host Scan attempts to run on any remote device that is establishing an SSL VPN, if Cisco Secure Desktop is enabled on the security appliance. The operating system detection is performed automatically. Process name, filename, and registry key checking to be performed by Basic Host Scan must be explicitly configured using Secure Desktop Manager. Basic Host Scan returns the name of the operating system and service pack and the results of any configured checks to the security appliance.

Basic Host Scan automatically returns the following additional values for evaluation against configured DAP endpoint criteria:

- Microsoft Windows, Mac OS, and Linux builds
- Listening ports active on a connecting host running Microsoft Windows
- Cisco Secure Desktop components that are installed on the connecting host
- Microsoft Knowledge Base numbers (KBs)

## Endpoint Assessment

Endpoint Assessment, a Host Scan extension, examines the remote computer for 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. Endpoint Assessment does not perform any remediation but provides input that can be evaluated by DAP records.

## Advanced Endpoint Assessment

With the purchase of an Advanced Endpoint Assessment license that is installed on the Cisco ASA adaptive security appliance, you can enable features that check for personal firewall, antivirus, and antispyware and can enforce updates for these products. Thus, Advanced Endpoint Assessment is capable of performing active remediation by applying firewall rules, activating modules, and providing updates to the personal firewall, antivirus, and antispyware software.

### Configuring Policies

#### Configuration Tasks

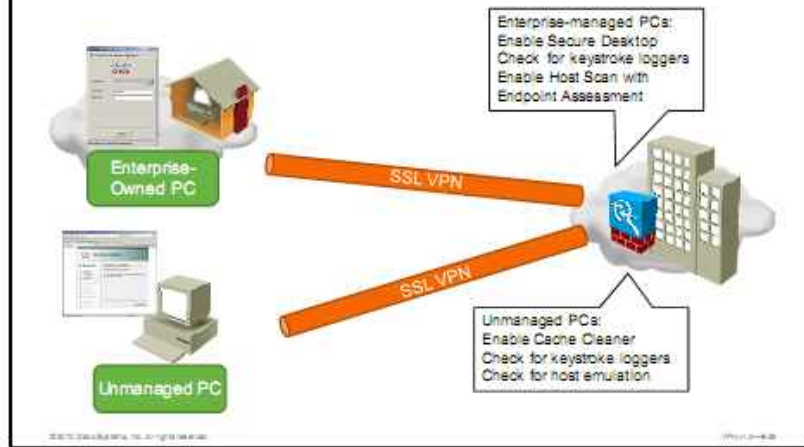
1. Enable Secure Desktop (Vault) or Cache Cleaner.
2. Configure Secure Desktop (Vault) parameters.
3. Alternatively, configure Cache Cleaner parameters.
4. Enable keystroke logger detection.
5. Enable host emulation detection.
6. Enable Host Scan.

To configure the prelogin policies, you have to complete the following configuration tasks:

1. Enable Secure Desktop (Vault) or Cache Cleaner.
2. Configure Secure Desktop (Vault) parameters.
3. Alternatively, configure Cache Cleaner parameters.
4. Enable keystroke logger detection.
5. Enable host emulation detection.
6. Enable Host Scan.

## Configuring Policies

### Configuration Scenario



In this configuration scenario, the respective policies are defined as follows:

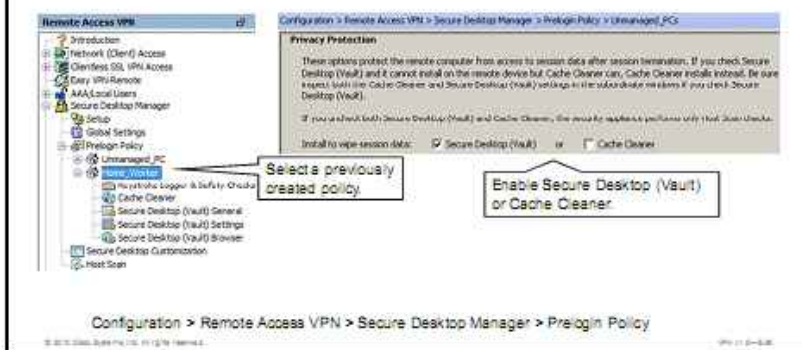
- The Home\_Worker policy, which is applied to enterprise-managed PCs, activates these modules:
  - Secure Desktop
  - Keystroke logger detection
- The Unmanaged\_PCs policy, which is applied to unmanaged PCs, applies these modules to the user sessions:
  - Cache Cleaner
  - Keystroke logger detection
  - Host emulation detection

You will also enable Host Scan with Endpoint Assessment. The respective Cisco Secure Desktop modules will be downloaded and executed by the endpoints that have been assigned to the respective policy through the prelogin assessment.

## Configuring Policies

### Task 1: Enable Secure Desktop (Vault) or Cache Cleaner.

- Enable Secure Desktop (Vault) for the Home\_Worker policy.
- Enable Cache Cleaner for the Unmanaged\_PC policy.



To configure the privacy protection setting of a prelogin policy, complete these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy**.
- Step 2** Select the required policy.
- Step 3** Locate the privacy protection section and check one of the available options: **Secure Desktop (Vault)** or **Cache Cleaner**. If you uncheck both boxes, the security appliance performs Host Scan checks only. In this configuration example, Secure Desktop (Vault) is activated for the Home\_Worker policy.
- Step 4** Click **Apply All** to apply the configuration.



## Configuring Policies

### Task 2: Configure Secure Desktop (Vault) Parameters

Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy > Home\_Worker > Secure Desktop (Vault) General

Secure Desktop (Vault) General

- Enable switching between Secure Desktop (Vault) and local desktop
- Enable Vault Reuse (User chooses a password)
- Suggest application uninstall upon Secure Desktop (Vault) closing
- Force application uninstall upon Secure Desktop (Vault) closing
- Enable Secure Desktop (Vault) inactivity timeout

Timeout After: 300 (seconds)

- Enable Secure Desktop (Vault) inactivity timeout audio alert
- Open following web page after Secure Desktop (Vault) closes

URL: \_\_\_\_\_

Secure Desktop: 3 (pages)

- Launch the following application after installation:

Program Name: \_\_\_\_\_

Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy > Home\_Worker > Secure Desktop (Vault) General

To configure the Secure Desktop general attributes, complete these steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy > Secure Desktop (Vault) General**.
- Step 2** Optionally, choose **Enable Switching Between Secure Desktop and Local Desktop**. Called desktop switching, this feature provides users with the flexibility to respond to a prompt from another application requiring an OK to let Secure Desktop continue processing. The recommended setting is to allow desktop switching. Unchecking this attribute minimizes the potential security risk that is posed by a user who leaves traces on the untrusted desktop. You might choose to uncheck this option if the deployment advantages outweigh the security risk.
- Step 3** Optionally, choose **Enable Vault Reuse**. This option allows users to close Secure Desktop and open it again at a later time. Secure Desktop becomes a persistent desktop that is available from one session to the next. If you enable this option, users must enter a password (up to 127 characters in length) to restart Secure Desktop. This option is useful if users are running Secure Desktop on PCs that are likely to be reused; for example, a home PC. When a user closes Secure Desktop, it does not self-destruct. If you do not enable this option, Secure Desktop automatically self-destructs upon termination. If unchecked, this attribute activates the following two attributes:
  - **Suggest Application Uninstall upon Secure Desktop (Vault) Closing**. This option prompts the user and recommends that the user uninstall Secure Desktop when it closes. In contrast to the next option below, the user has the choice to refuse the uninstallation.
  - **Force Application Uninstall Upon Secure Desktop (Vault) Closing**. This option is useful if you do not want to leave Secure Desktop on untrusted PCs after users finish using it. Secure Desktop uninstalls when it closes.

- Step 4** Optionally, choose **Launch Cleanup Upon Timeout Based on Inactivity**. This parameter starts Cache Cleaner automatically after a period of mouse inactivity. It applies only to Microsoft Windows. Cache Cleaner ignores it if the operating system is Mac OS or Linux.
- Step 5** Optionally, choose **Enable Secure Desktop Inactivity Timeout**. Check this check box to close Secure Desktop automatically after a period of mouse inactivity. Checking this attribute activates the following attribute:
- **Timeout After**. This field enables you to set the inactivity timer to a number of minutes (1, 2, 5, 10, 15, 30, or 60).
- Step 6** Optionally, choose **Open Following Web Page After Secure Desktop Closes**. You can check this box and enter a URL in the field to make Secure Desktop automatically open a web page when it closes.
- Step 7** Optionally, choose **Perform Secure Delete**. With this option, Secure Desktop encrypts and writes itself to the remote PC disk. Upon termination, it performs a U.S. Department of Defense (DoD) sanitation algorithm. Choose the number of times to perform this cleanup task. The default setting is three passes. Following the completion of the task the number of times that were specified, Secure Desktop removes the pointer to the file.
- Step 8** Optionally, choose **Launch the Following Application after Installation**. This option lets you start an application automatically after Secure Desktop installs on the remote PC. Enter only the path to the application that follows the C:\Program Files\ portion. The application must be in the Program Files directory.
- Step 9** Click **Apply All** to apply the configuration.

## Configuring Policies

### Task 2: Configure Secure Desktop (Vault) Parameters (Cont.)



To configure the Secure Desktop setting attributes, complete these steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy > Secure Desktop (Vault) Settings**.
- Step 2** Optionally, choose **Restrict Application Usage to the Web Browser Only**. You can check this check box to let only the originating browser and any browser helpers you specify run on Secure Desktop. Choosing this option limits the ability of the user to use other applications. This option does not control all browser behavior, such as opening additional browser windows or new browser tabs. It is meant to be used with other security settings that can be configured through the browser. This option does not prevent access from the secure partition to the network on which the host runs nor does it restrict access to the file system of the host. If you check this attribute, Secure Desktop Manager inserts a text box under it. To specify browser helpers that can run on Secure Desktop, click **Add Browser Helpers** and select them from a preconfigured list.

---

**Note** If you check **Restrict application usage**, but want to provide users with access to Java applets on the web pages they open, you must add the following entries to the browser list: `c:\program; java.exe; jp2launcher.exe`.

---

- Step 3** Optionally, choose **Disable Access to Network Drives and Network Folders**. Leave checked to attempt to prevent user access to network resources and network drives while the user is running Secure Desktop. The network resources are those that use the Server Message Block (SMB) client or server, request-response protocol to share such resources as files, printers, and APIs. Because Cisco Secure Desktop does not clean up files that are written to mapped network drives, the recommended setting of this attribute is disabled (default).

- Step 4** Optionally, choose **Disable Access to Removable Drives and Removable Folders**. Check to prevent the user from accessing portable drives while running Secure Desktop. Otherwise, the user can save files to a removable drive and remove the drive before closing the session. After closing the session, the user could forget to take the removable drive. This attribute should be checked for maximum security.
- Step 5** **Disable Registry Modification**. Check this option to prevent the user from modifying the registry from within Secure Desktop. This attribute should be checked for maximum security.
- Step 6** **Disable Command Prompt Access**. Check this option to prevent the user from running the DOS command prompt from within Secure Desktop. This attribute should be checked for maximum security.
- Step 7** **Disable Printing**. Check this option to prevent the user from printing while using Secure Desktop. This attribute should be checked for maximum security of sensitive data.
- Step 8** **Allow Email Applications to Work Transparently**. Check this option to let the user open email while on Secure Desktop and to prevent Secure Desktop from deleting email upon the termination of the session. The use of the term transparent means that Secure Desktop processes email the same way that the local desktop processes it. Transparent handling works for the following email applications: Microsoft Outlook Express, Microsoft Outlook, Eudora, Lotus Notes.
- Step 9** Click **Apply All** to apply the configuration.

## Configuring Policies

### Task 2: Configure Secure Desktop (Vault) Parameters (Cont.)

- In Secure Desktop (Vault), browsers do not show user bookmarks or favorites.
- Only Cisco Secure Desktop browser bookmarks are displayed.

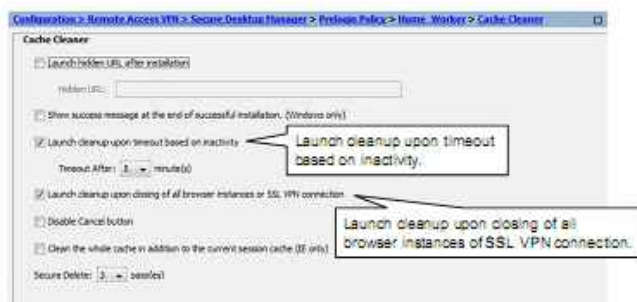


For the duration of the Secure Desktop session, the browser does not list the bookmarks or favorites of the user. It lists only the bookmarks or favorites that are configured in the Secure Desktop browser attributes. To configure the Cisco Secure Desktop browser attributes, complete these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy** (not shown in the figure).
- Step 2** Click **Secure Desktop (Vault) Browser** under the prelogin policy name to customize the Secure Desktop (Vault) Browser settings.
- Step 3** Optionally, type into the Home Page field the URL of the page that you want to open when the remote user clicks Home.
- Step 4** Use the following guidelines to add, modify, and delete entries in the Customized Bookmarks pane:
  - To add a folder, select the folder to contain it, click **Add Folder**, type the new folder name in the dialog box, then click **OK**.
  - To add a bookmark to the list, select the folder to contain it, click **Add Bookmark**, type the URL in the dialog box, then click **OK**.
  - To modify a URL, select it, click **Edit**, type the new URL in the dialog box, then click **OK**.
  - To remove a folder or a URL, select it and click **Delete**.
- Step 5** Click **Apply All** to apply the configuration.

## Configuring Policies

### Task 3: Configure Cache Cleaner Parameters



To configure Cache Cleaner parameters, complete the following steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy > Cache Cleaner**.
- Step 2** Check the **Launch Hidden URL After Installation** check box to use a hidden URL for administrative purposes that identifies the remote host as having Cache Cleaner installed. One possible way to use this attribute is to place a cookie on the remote system. Later on in the session, the Host Scan module could check for the presence of the cookie to let the administrators know who is using Cache Cleaner.
- Step 3** Check the **Show Success Message at the End of Successful Installation** check box to display a dialog box on the remote PC informing the user when the Cache Cleaner installation is successful. This option is not selected.
- Step 4** Check the **Launch Cleanup upon Timeout Based on Inactivity** check box to set a specific timeout period after which the cleanup begins. This option is selected.
- Step 5** With the **Launch Cleanup upon Timeout Based on Inactivity** check box checked, select the time from the **Timeout After** drop-down list. The available choices are 1, 2, 5, 10, 15, 30, or 60 minutes. This attribute is the inactivity timer. Its default value is 5. In this example, the time value is set to 15 minutes.
- Step 6** Check the **Launch Cleanup upon Closing of All Browser Instances or SSL VPN Connection** check box to clean up the cache when all browser windows are closed.
- Step 7** Check the **Clean the Whole Cache in Addition to the Current Session Cache (IE Only)** check box to remove data from the Internet Explorer cache. Upon activation, Cache Cleaner attempts to remove the files that are generated, browsing history, and typed fields and passwords that were retained before the session began.
- Step 8** Choose the number of passes that the DoD sanitation algorithm will use in the **Secure Delete** drop-down list for cache cleanup. The default setting is three passes. Following the completion of the task the number of times specified, Secure Desktop removes the pointer to the file. In this example, the number of passes is set to five.

**Step 9** Click **Apply All** to apply the configuration.

## Configuring Policies

### Task 4-5: Enable Detection of Keystroke Loggers and Host Emulation

- List of legitimate processes that interact with I/O interface

Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy > Unmanaged\_PC > Keystroke Logger & Safety Checks

**Keystroke Logger & Safety Checks**

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

Check for keystroke loggers

Force admin control on list of safe modules

List of Safe Modules

Check for host emulation

Always deny access if running within emulated host

Apply All Reset All

Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy > Unmanaged\_PC > Keystroke Logger & Safety Checks

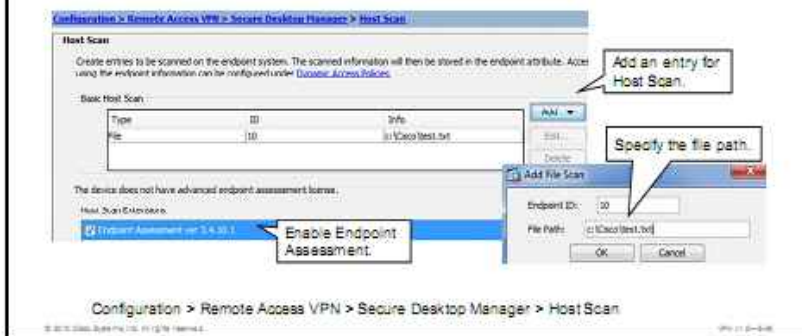
In the next task, you will configure the operations of the keystroke logger detection and host emulation detection. In the current scenario, keystroke logger detection is applied to both Home\_Worker and Unmanaged\_PCs policies, while the host emulation detection is activated only in the Unmanaged\_PCs policy. To configure the attributes of keystroke logger detection and host emulation detection, complete these steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy > Keystroke Logger & Safety Checks**.
- Step 2** Check the **Check for Keystroke Loggers** check box to scan for a keystroke logging application on the remote PC. By default, this attribute is not checked, and the other attributes and buttons are grayed out. If you check this attribute, the **Force Admin Control on List of Safe Modules** attribute becomes active.
- Step 3** Check the **Force Admin Control on List of Safe Modules** check box to specify which keystroke loggers are exempt from scanning, or uncheck it to let the remote user decide. If you check this attribute, the **Add** button becomes active and you can specify the safe modules whose presence on the remote endpoint will not be reported.
- Step 4** Check the **Check for Host Emulation** check box if you want to determine whether the operating system is running over virtualization software, such as VMware.
- Step 5** Check the **Always Deny Access if Running Within Emulation** check box to prevent the module (Secure Desktop, Cache Cleaner, or Host Scan) from running if Cisco Secure Desktop detects that the operating system is running over virtualization software. Uncheck this attribute to alert the user about the host emulation software and let the user choose whether to terminate the session.
- Step 6** Click **Apply All** to apply the configuration.

## Configuring Policies

### Task 6: Configure Host Scan

- Inside Host Scan you can enable:
  - Registry scan, file scan, process scan
- Results of these scans can be used in DAP.



To enable host scan, complete the following steps:

**Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**.

**Step 2** Click the **Add** button to add an entry for a host scan. Using host scan, you can perform the following scans:

- Registry scan
- File scan
- Process scan

In the example, file scan is being added.

**Step 3** Enter a unique and meaningful string to serve as an index into the Endpoint ID field. After completing the Host Scan configuration, specify the same index when you assign this entry as an endpoint attribute when configuring a DAP. The string is case-sensitive. In the example, 10 is entered as endpoint ID.

**Step 4** Enter a file path and filename for which you would like to check, into the File Path input field. In the example, c:\Cisco\test.txt is entered.

---

**Note** Registry, files, and process scans that are defined here can be used later when you are configuring DAP. DAP will be discussed later in the lesson.

---

**Step 5** Click **OK**.

**Step 6** Check the **Endpoint Assessment** check box to enable Endpoint Assessment. Remote PCs will be scanned for a large collection of antivirus, antispyware, and personal firewall applications, and associated updates.

---

**Note** Further configuration of Endpoint Assessment is done when you configure DAP.

---



**Step 7** Click **Apply All** to apply the configuration.

## Verifying Policies

### User Experience

The diagram illustrates the user experience of the Cisco AnyConnect client during VPN connection. It is divided into two main stages:

- Stage 1:** The client prompts the user to wait while the computer is inspected for keystroke logging. A callout states: "Cisco Secure Desktop loads and inspects computer." Below this, there are two buttons: "Switch to the Secure Desktop" and "Close the Secure Desktop".
- Stage 2:** The client prompts the user to enter their username and password. A callout states: "Cisco Secure Desktop is operational before VPN login." Below this, there are three buttons: "Launch Login Page", "Switch Desktop", and "Close Desktop Record". A callout at the bottom right states: "Close Desktop terminates the VPN."

You can verify the operations of the prelogin policy by starting the Cisco AnyConnect client and connecting to the SSL VPN. Verify if these settings are correctly applied to the session:

- Verify that the user is assigned to the correct prelogin policy.
- Verify that Cache Cleaner or Secure Desktop (Vault) installs. If the Cisco Secure Desktop is enabled, Secure Desktop (Vault) should run after the Cisco AnyConnect client connects to the Cisco ASA adaptive security appliance. After that, Cisco AnyConnect should run in the Secure Desktop, where a user can authenticate.
- Verify that keystroke logger detection is started.
- Verify that emulation detection is started.

# Configuring Advanced Endpoint Assessment

This topic describes the Advanced Endpoint Assessment feature on the Cisco ASA adaptive security appliance.

## Configuring Advanced Endpoint Assessment

### Overview

- Part of Host Scan functionality
- Requires an Advanced Endpoint Assessment license
- Can be used to remediate with the following actions:
  - Enable antivirus software if it has been disabled
  - Update signature definition files for antivirus and antispysware software if they have not been updated for a defined number of days
  - Apply firewall rules to supported personal firewalls if they have not met requirements

Advanced Endpoint Assessment offers these four advanced features of Cisco Secure Desktop:

- **Remediation:** On Windows, Mac OS X, and Linux desktops, Advanced Endpoint Assessment can attempt to initiate remediation of various aspects of antivirus, antispysware, and personal firewall protection if that software allows a separate application to initiate remediation.
- **Antivirus:** Advanced Endpoint Assessment can attempt to remediate these components of antivirus software:
  - **Force File System Protection:** If the antivirus software is disabled, Advanced Endpoint Assessment can enable it.
  - **Force Virus Definitions Update:** If the antivirus definitions have not been updated in the number of days that are defined by the Advanced Endpoint Assessment configuration, Advanced Endpoint Assessment can attempt to initiate an update of virus definitions.
- **Antispysware:** Advanced Endpoint Assessment can attempt to force an update of antispysware definitions. If the antispysware definitions have not been updated in the number of days that are defined by the Advanced Endpoint Assessment configuration, Advanced Endpoint Assessment can attempt to initiate an update of antispysware definitions.
- **Personal firewall:** The Advanced Endpoint Assessment module can attempt to reconfigure firewall settings and rules if they do not meet the requirements that are defined in the Advanced Endpoint Assessment configuration.
  - The firewall can be enabled or disabled.
  - Applications can be prevented from running or allowed to run.
  - Ports can be blocked or opened.

## Configuring Advanced Endpoint Assessment

### Configuration Tasks

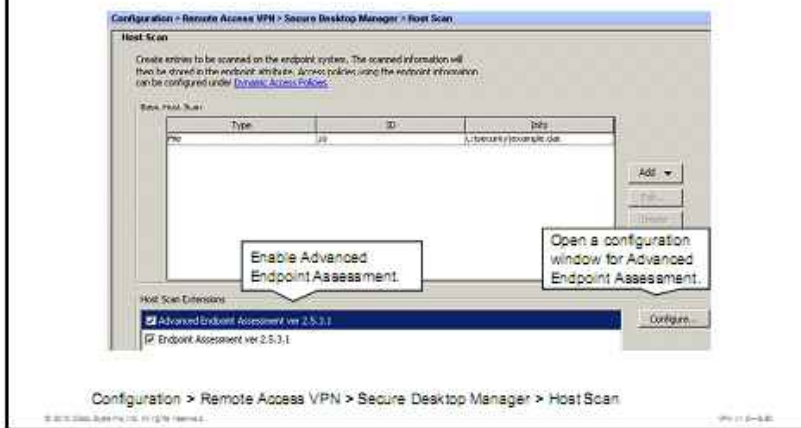
1. Enable Advanced Endpoint Assessment.
2. Configure antivirus software assessment.
3. Configure antivirus software remediation.
4. Configure personal firewall software assessment.
5. Configure personal firewall software remediation.
6. Configure antispymware software assessment.
7. Configure antispymware software remediation.

To configure Advanced Endpoint Assessment, you have to perform these configuration tasks:

1. Enable Advanced Endpoint Assessment.
2. Configure antivirus software assessment.
3. Configure antivirus software remediation.
4. Configure personal firewall software assessment.
5. Configure personal firewall software remediation.
6. Configure antispymware software assessment.
7. Configure antispymware software remediation.

## Configuring Advanced Endpoint Assessment

### Task 1: Enable Advanced Endpoint Assessment



To configure the Advanced Endpoint Assessment option, you must enable it first. Complete the following steps to enable Advanced Endpoint Assessment using Cisco ASDM:

- Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**.
- Step 2** Check the **Advanced Endpoint Assessment** check box.
- Step 3** Click **Apply All** to apply the configuration.
- Step 4** Click the **Configure** button to configure antivirus, personal firewall, and antispyware policies.

# Configuring Advanced Endpoint Assessment

## Task 2: Configure Antivirus Software Assessment

The screenshot shows the 'Advanced Endpoint Assessment' configuration window. It has three tabs: 'Windows', 'Mac OS', and 'Linux'. The 'Windows' tab is selected. Below the tabs are three checkboxes: 'Include Host Scan', 'Include File Integrity', and 'Include File Hashing'. A callout '1' points to these tabs with the text 'Select an operating system.' An 'Add...' button is visible on the right side of the main window. A callout '2' points to this button with the text 'Add a product or products.' The 'Add Products' dialog box is open, displaying a list of products. A callout '3' points to the 'Trend Micro OfficeScan Client 8.0' product in the list with the text 'Select a required antivirus product.' The dialog box has 'OK' and 'Cancel' buttons at the bottom.

Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan

In the second task of this configuration sequence, you configure the antivirus software requirements of the remote endpoints. Complete these steps:

**Step 1** When the Advanced Endpoint Assessment window opens (after you clicked Configure in the previous task), choose the appropriate operating system tab: Windows, Mac OS, or Linux.

**Note** The Windows, Mac OS, and Linux tabs let you specify remediation for each respective operating system. The three tabs are the same; only the vendors and applications differ. By default, Host Scan does not attempt to remediate.

**Step 2** Locate the Antivirus area and click **Add** to open a window with the antivirus product list.

**Step 3** Select one or more vendor and product options from the dialog box and click **OK**.

## Configuring Advanced Endpoint Assessment

### Task 3: Configure Antivirus Software Remediation



In the third task of this configuration sequence, you configure the enforcement policy of antivirus software. Complete these steps:

- Step 1** Make sure that you are in the Antivirus area of the Advanced Endpoint Assessment.
- Step 2** Optionally, check the **Force File System Protection** check box. This setting effectively turns on ongoing background scanning by the installed antivirus application. The application checks files as they are received and blocks access to files that are likely to contain viruses. This option can be enabled only if the selected antivirus application supports this feature.

---

**Note** When multiple antivirus products have been selected, one product from the list must be installed on the SSL VPN endpoint.

---

- Step 3** Optionally, check the **Force Virus Definitions Update** check box and select a number of days from the If Not Updated in Last Days field to enforce regular virus definition updates.

---

**Note** Any action and rules that you configure persist on the end-user device even after the VPN session ends. They should be applied with discretion.

---

## Configuring Advanced Endpoint Assessment

### Task 4: Configure Personal Firewall Software Assessment

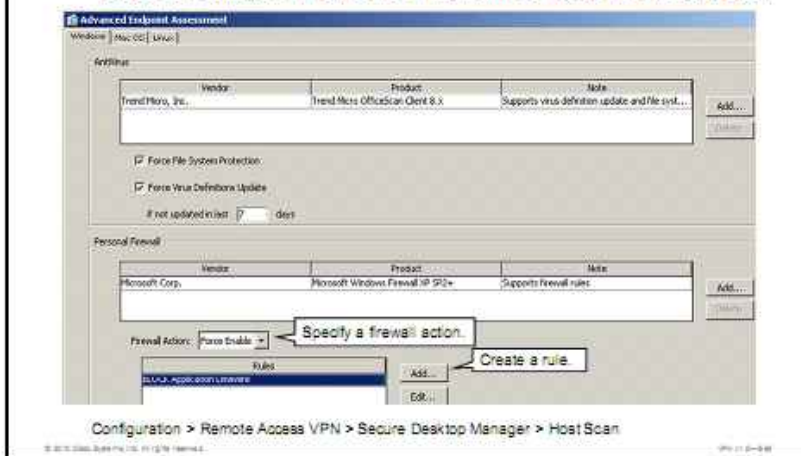


In the next task of this configuration sequence, you will configure the personal firewall requirements for the remote endpoints. Complete these steps:

- Step 1** Make sure that you are in the Advanced Endpoint Assessment configuration window, under the appropriate operating system tab: Windows, Mac OS, or Linux.
- Step 2** Locate the Personal Firewall area and click **Add** to open a window with the product list.
- Step 3** Choose the required row indicating the vendor and product you want in the Vendor and Product columns, and click **OK**.

## Configuring Advanced Endpoint Assessment

### Task 5: Configure Personal Firewall Software Remediation



After you enable checking for a specific personal firewall, you configure the enforcement policy of personal firewall software. Complete these steps:

- Step 1** Make sure that you are in the Personal Firewall area of the Advanced Endpoint Assessment.
- Step 2** Optionally, choose **Force Enable** from the Firewall Action drop-down menu.
- Step 3** Optionally, click **Add** to create a firewall rule. A rule specifies applications and ports for which the firewall allows or blocks ports or applications. Follow this procedure to configure a rule:
  - Choose the action of this rule. The options are ALLOW Application, BLOCK Application, ALLOW Port, and Block Port.
  - Go to the Application area and set the following attributes if you selected ALLOW Application or BLOCK Application.
    - Enter the complete filename and extension of the application to be allowed or blocked.
    - Enter the entire path to the application file.
  - Go to the Port area and set the following attributes if you selected ALLOW Port or BLOCK Port.
    - Select the protocols to be allowed or blocked. The options are Any, UDP, and TCP.
    - Enter the port number to be allowed or blocked.
  - Click **OK**.
- Step 4** Repeat this procedure for each personal firewall rule you want to configure.

---

**Note** Firewall rules are available only if the selected personal firewall supports them.

---



## Configuring Advanced Endpoint Assessment

### Tasks 6-7: Configure Antispyware Software Assessment and Remediation



In the final two tasks of this configuration sequence, you configure the Antispyware requirements for the remote endpoints. Complete these steps:

- Step 1** Make sure that you are in the Advanced Endpoint Assessment configuration window, under the appropriate operating system tab: Windows, Mac OS, or Linux.
- Step 2** Locate the Antispyware area and click **Add** to open a window with the product list.
- Step 3** Select one or more Vendor or Product options from the dialog box and click **OK**.

Then you configure the update policy of antivirus software. Complete these steps:

- Step 1** Make sure that you are in the Antispyware section of the Advanced Endpoint Assessment.
- Step 2** Optionally, check the **Force Spyware Definitions Update** check box and select a number of days from the If Not Updated in Last Days field to enforce regular spyware definition updates.
- Step 3** Click **OK**.
- Step 4** Click **Apply All** to apply the configuration.

You can review the policies that are defined for Advanced Endpoint Assessment by selecting the appropriate operating system tab and browsing through the three functional areas of Advanced Endpoint Assessment: Antivirus, Personal Firewall, and Antispyware.

---

**Note** DAP obtains endpoint security attributes from Cisco Secure Desktop Host Scan and Endpoint Assessment modules and applies appropriate policies to them. DAP is covered in the next lesson.

---

# Troubleshooting Cisco Secure Desktop Operation for Clientless Connections

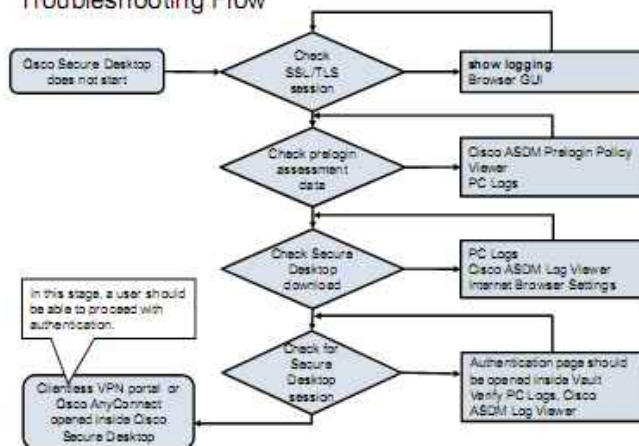
This topic describes how to troubleshoot Cisco Secure Desktop functionality in SSL VPNs.



The troubleshooting of clientless SSL VPNs is performed on both involved devices: on the remote computer and the security appliance. The tools that are available on the endpoint include connectivity tools such as ping, traceroute, nslookup, and the logs that are generated by software components. The Cisco ASA adaptive security appliance provides the logging output and Cisco ASDM Event Viewer.

## Troubleshooting Cisco Secure Desktop Operation

### Troubleshooting Flow



Troubleshooting Cisco Secure Desktop operations is required when the Cisco Secure Desktop module does not operate properly. It involves these steps:

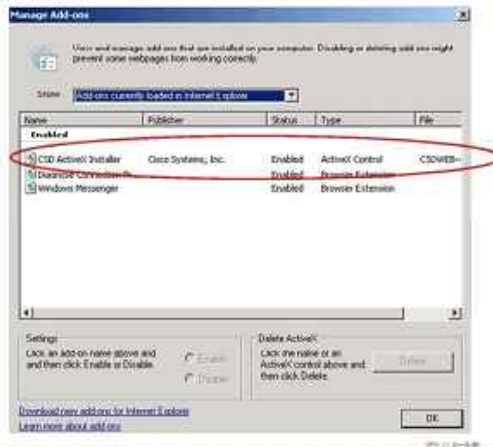
- Step 1 Check Secure Sockets Layer or Transport Layer Security (SSL/TLS) session:** In this step, use the logging output and the information that is provided in the browser GUI to verify cipher suite agreement and server certificate validation on the client.
- Step 2 Check prelogin assessment data:** In this step, use the Cisco ASDM Prelogin Policy Viewer and PC logs to verify the prelogin assessment phase.
- Step 3 Check that Cisco Secure Desktop is downloaded:** If the download does not start, verify PC logs and browser settings.
- Step 4 Check for creation of secure desktop session:** The authentication page should open inside the secured session. If it does not, check the PC logs and Cisco ASDM Log Viewer for potential issues. If it does, the user should be able to log in and access the SSL VPN portal.

## Troubleshooting Cisco Secure Desktop Operation

### Cisco Secure Desktop Download and Installation

Cisco Secure Desktop download and install options:

- ActiveX
- Java
- Standalone



To enable the Cisco Secure Desktop download and installation, you must enable one of the supported options:

- **ActiveX:** The user must have administrative privileges to install the Cisco Secure Desktop using ActiveX controls.
- **Microsoft Java Virtual Machine:** The user must have administrative privileges to install the Cisco Secure Desktop using Microsoft JVM.
- **Sun Java Virtual Machine:** The user does not need administrative privileges, but Sun JVM must be installed and enabled in the browser.
- **Executable File:** The user does not need the permission to run ActiveX or Java, or does not have ActiveX or Java installed. The user must have administrative privileges to install the Cisco Secure Desktop software using the installation file.

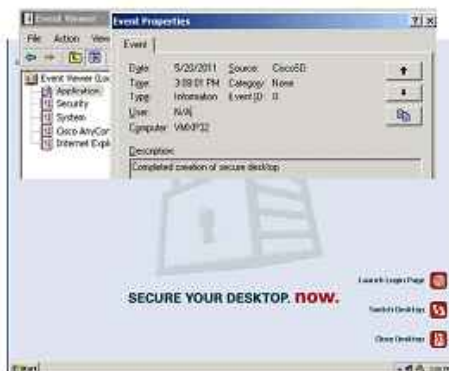
## Troubleshooting Cisco Secure Desktop Operation

### Vault Creation

When Vault is created, client will be moved into it.

### Verify:

- Analyze PC logs:
  - Completed creation of Secure Desktop
  - Spawned Explorer in Secure Desktop



In the final verification task, the user should see that the Vault environment is created and that the user is moved into that environment. These options are available to the user:

- Launch Login Page
- Switch Desktop
- Close Desktop

To verify this phase, examine the logs on the user computer for information on completed creation of Secure Desktop and on a spawned instance of Internet Explorer in the Secure Desktop.

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- Cisco Secure Desktop, when configured, downloads and runs modules to assess the remote system that is attempting SSL VPN connections to the Cisco ASA security appliance.
- Prelogin assessment evaluates VPN endpoints before the users authenticate to the SSL VPN server.
- Prelogin policies result from prelogin assessment.
- The Secure Desktop (Vault) and Cache Cleaner modules assist in securing data that is downloaded to remote systems during SSL VPN connections.
- The Advanced Endpoint Assessment extension of the Host Scan module allows the administrator to assess and remediate antivirus, personal firewall, and antispyware applications.
- Troubleshooting of clientless SSL VPNs is performed on both devices: the remote computer and the security appliance.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-10-34-900

# Deploying Dynamic Access Policies

---

## Overview

Remote-access virtual private networks (VPNs) operate in dynamic environments. Multiple variables can affect each VPN connection, such as intranet configurations that frequently change, the various roles each user can inhabit within an organization, and logins from remote-access sites with different configurations and levels of security.

Dynamic access policies (DAP) on the Cisco ASA adaptive security appliance allow for configuration of the authorization that addresses many variables that are found in various remote-access VPNs. This lesson explains configuration and troubleshooting of DAP and integration of DAP with Cisco Secure Desktop.

## Objectives

Upon completing this lesson, you will be able to deploy and manage DAP on the Cisco ASA adaptive security appliance. This ability includes being able to meet these objectives:

- Describe DAP on the Cisco ASA adaptive security appliance
- Configure and verify DAP on the Cisco ASA adaptive security appliance
- Configure aggregated DAP policies on the Cisco ASA adaptive security appliance
- Integrate DAP policies with Cisco Secure Desktop
- Use LUA expressions to provide additional flexibility when configuring matching criteria for DAP
- Troubleshoot DAP on the Cisco ASA adaptive security appliance


# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic introduces DAP on the Cisco ASA adaptive security appliance.

## Dynamic Access Policy

### Overview

- Defined as a collection of access control attributes
- Dynamically generated by aggregating attributes from one or more DAP records
- Generated and then applied to the user tunnel or session
- Available for remote access VPNs (Cisco AnyConnect VPN, clientless SSL VPN, Cisco Easy VPN)



The diagram shows a 'Remote User' on the left, connected to a 'Cisco ASA' on the right via a 'VPN Tunnel'. A box labeled 'DAP' is connected to the tunnel, containing fields for 'Role', 'Engineer', and 'Engineer'. A speech bubble from the user says 'Hi, so you get...'. The Cisco ASA has a box labeled 'DAP' with fields for 'Role', 'Engineer', and 'Engineer'. The diagram is titled 'Dynamic Access Policy' and includes an 'Overview' section with four bullet points.

DAP on the Cisco ASA security appliance allows for configuration of the authorization that addresses many variables that are found in various remote access VPNs. Setting a collection of access control attributes that are associated with a specific user tunnel or session can create a DAP. These attributes address issues of multiple group membership and endpoint security. By doing this, the security appliance can grant access to a particular user for a particular session, based on the configured policies. It generates a DAP at the time that the user connects by selecting 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 authentication, authorization, and accounting (AAA) information for the authenticated user. It then applies the DAP record to the user tunnel or session.

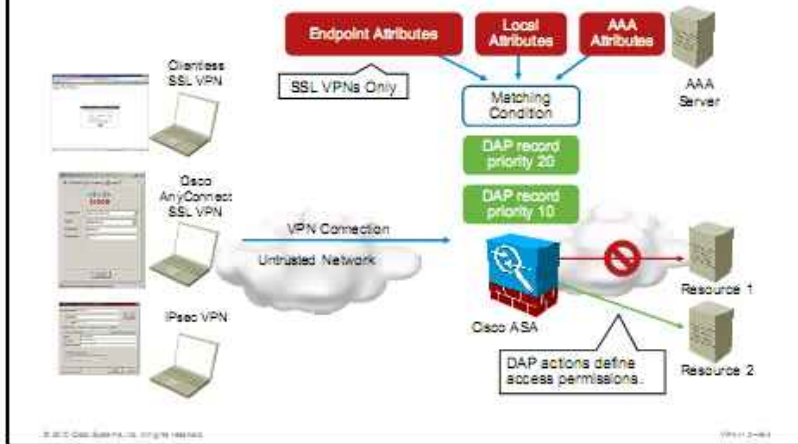
The DAP system includes two components that require administrator attention. DAP Selection Configuration File is a text file containing criteria that the Cisco ASA security appliance uses for selecting and applying DAP records during session establishment. The files are stored on the Cisco ASA security appliance. Cisco Adaptive Security Device Manager (Cisco ASDM) can be used to modify it and upload it to the security appliance in extended mark-up language (XML) data format. DAP selection configuration files include all of the attributes that are configured. These attributes can include AAA attributes, endpoint attributes, and access policies as configured in network and webtype access control list (ACL) filter, port-forwarding, and URL lists. The DfltAccessPolicy policy is 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 DfltAccessPolicy, and it must be the last entry in the summary table.

DAP applies to both IP Security (IPsec) and Secure Sockets Layer (SSL) VPNs. In this section, DAP is discussed as it applies to SSL VPN connections.



# Dynamic Access Policy

## Solution Components



Solution components of DAP are as follows:

- **One or more DAP records:** DAP records define a limited set of VPN authorization attributes that can override authorization attributes that are defined locally or provided by an AAA server. One or more DAP records are selected based on AAA attributes of a user or endpoint attributes. Authorization attributes from DAP records are then combined into a DAP policy and assigned to a VPN session. Each DAP record is identified using a name and each record has a priority. The security appliance uses this value to logically sequence the access lists when it aggregates the network and webtype ACLs from multiple DAP records.
- **Local and AAA attributes:** DAP records can be selected based on AAA information that is provided locally or by an AAA server when users authenticate to a VPN session.
- **Endpoint attributes of connecting VPN clients:** DAP records also can be selected based on endpoint attributes of connecting clients. These endpoint attributes can be determined from type of VPN connection or using Cisco Secure Desktop, for example.

## Dynamic Access Policy

### Policy Hierarchy

The security appliance applies user policies according to the following hierarchy:

1. **Dynamic Access Policies (DAP) rules**
2. **User profile**
3. **Group policy attached to the user profile**
4. **Group policy attached to the connection profile**
5. **DfltGrpPolicy settings**

All settings not specified in each level are automatically inherited from the lower-priority level.

Access control mechanisms can be applied at different levels in the VPN system. This precedence model determines effective access permissions (from highest to lowest precedence):

1. **DAP:** DAP rules are built at the session connection time and can take into account temporary parameters, such as the endpoint security posture. The precedence among multiple DAP policies is configured using a precedence value.
2. **User profile:** Parameters that are configured at the user level are the most granular settings that are configured statically (without considering security posture).
3. **Group policy attached to the user profile:** Parameters are defined in a group policy that is attached to the individual user.
4. **Group policy attached to the connection profile:** Parameters are defined in a group policy that is attached to the connection profile that the user connects to.
5. **DfltGrpPolicy settings:** This default group policy is preconfigured on the security appliance with default parameters. It can be modified but cannot be removed. By default all other policy groups and users inherit the settings from the DfltGrpPolicy.

## Dynamic Access Policy

### Operations

- Created at session connection time
- Evaluates data obtained from:
  - Local group policy or AAA authorization parameters
  - Posture of the remote endpoint device
  - DfltGrpPolicy (default parameters)
- Overrides session parameters:
  - Action (continue, terminate)
  - Network ACLs (full tunnel)
  - Webtype ACLs (clientless SSL VPN)
  - Clientless SSL VPN selective features
    - Functions (file access, HTTP proxy, URL entry)
    - Port-forwarding lists
    - Bookmarks
  - Access method (clientless, tunnel, both)

DAP is created at session connection time, based on multiple DAP records. DAP records, from where DAP is created, are selected based on parameters that are obtained from a local group or an AAA authorization parameters and posture of remote endpoint devices.

DAP overrides authorization parameters that are obtained from a local group policy or from an AAA server. Authorization parameters that can be provided by DAP are as follows:

- **Action:** An action can be as follows:
  - **Continue:** Continues with session and specifies special processing to apply to specific connection.
  - **Terminate:** Terminates a session.
- **Access control lists (ACLs):** Specifies already configured network ACLs to add to a DAP record. This parameter applies to full tunnel VPN sessions.
- **Web-Type ACLs:** Specifies already configured webtype ACLs to add to a DAP record. This parameter applies to clientless SSL VPN sessions.
- **Functions:** Enables file server entry and browsing, HTTP proxy, and URL entry for the DAP record:
  - **File Server Browsing:** Enables or disables Common Internet File System (CIFS) browsing for file servers or shared features.
  - **File Server Entry:** Lets or prohibits a user from entering file server paths and names on the portal page. When enabled, this feature 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.

- **HTTP Proxy:** Affects 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 old proxy configuration of the browser automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client-side technologies, including HTML, Cascading Style Sheets (CSS), JavaScript, Visual Basic Scripting Edition (VBScript), ActiveX, and Java. The only browser that it supports is Microsoft Internet Explorer.
- **URL Entry:** Allows or prevents a user from entering HTTP and 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.
- **Port Forwarding Lists:** Selects port-forwarding lists for user sessions.
- **Bookmarks:** Selects port-forwarding lists for user sessions.
- **Access Method:** Configures the type of remote access that is 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 Cisco AnyConnect VPN client, with a default of clientless.
  - **Both-Default-AnyConnect Client:** Connect via either clientless or the Cisco AnyConnect client, with a default of Cisco AnyConnect.

## Dynamic Access Policy

### Factors Affecting DAP

Factor	Description
AAA	DAP complements AAA services. DAP provides a limited set of authorization attributes that can override attributes provided by AAA. Selection of DAP records is based on the AAA authorization information for the user and posture assessment information for the session.
Endpoint security	Endpoint security attributes are obtained from the configured posture assessment using Cisco Secure Desktop. Clientless SSL VPN sessions are supported by Cisco Secure Desktop and Host Scan. Cisco Secure Desktop returns file information, registry key values, running processes, and operating system information. Cisco Secure Desktop Host Scan returns antivirus, antispyware, and personal firewall software information.

DAP complements AAA services. It provides a limited set of authorization attributes that can override those that AAA provides. The adaptive security appliance selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The adaptive 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 adaptive security appliance receives from a RADIUS or Lightweight Directory Access Protocol (LDAP) server.

The adaptive security appliance obtains endpoint security attributes by using a posture assessment that is performed by Cisco Secure Desktop.

The table describes the scope of the security posture that is offered by the given components and their applicability to various remote access protocols supported by the security appliance.

### Scope of Security Posture

Remote Access Protocol	Cisco Secure Desktop	Host Scan
	Returns file information, registry key values, running processes, and operating system	Returns antivirus, antispyware, and personal firewall software information
IPsec VPN	No	No
Cisco AnyConnect VPN	Yes	Yes
Clientless VPN	Yes	Yes

## Dynamic Access Policy

### DAP Connection Sequence

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

© 2010 Cisco Systems, Inc. All rights reserved.

VPN 11-20-09

DAP is applied in the following sequence:

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

# Configuring DAP

This topic describes how to configure DAP on the Cisco ASA adaptive security appliance.

## Configuring DAP

### Configuration Tasks

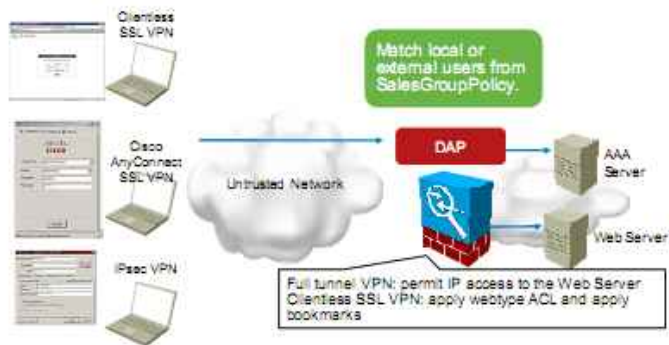
1. Create a DAP policy.
2. Specify AAA attributes matching criteria.
3. Specify endpoint attributes matching criteria.
4. Configure authorization parameters.
5. Configure an action for DfltAccessPolicy.

Complete the following tasks to configure DAP on the Cisco ASA adaptive security appliance:

1. Create a DAP policy.
2. Specify AAA attributes matching criteria.
3. Specify endpoint attributes matching criteria.
4. Configure authorization parameters.
5. Configure an action for DfltAccessPolicy.

## Configuring DAP

### Configuration Scenario



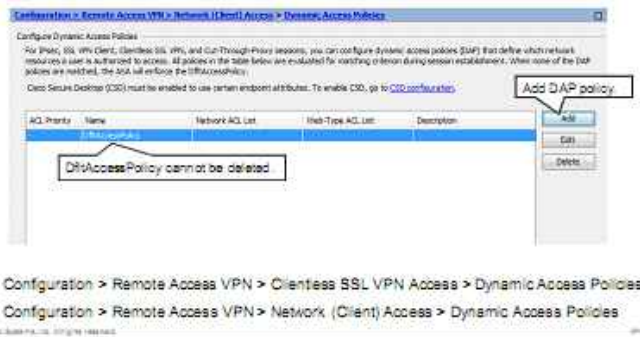
The figure shows an example, which will serve as configuration scenario for ongoing configuration tasks. You will configure a DAP policy, which will apply additional network ACLs for full tunnel VPNs and webtype ACLs and bookmark lists for clientless SSL VPNs. This DAP policy will be applied to users belonging to SalesGroupPolicy.



## Configuring DAP

### Task 1: Create DAP Policy

- **DfltAccessPolicy:**
  - Mandatory policy
  - Lowest priority (0)



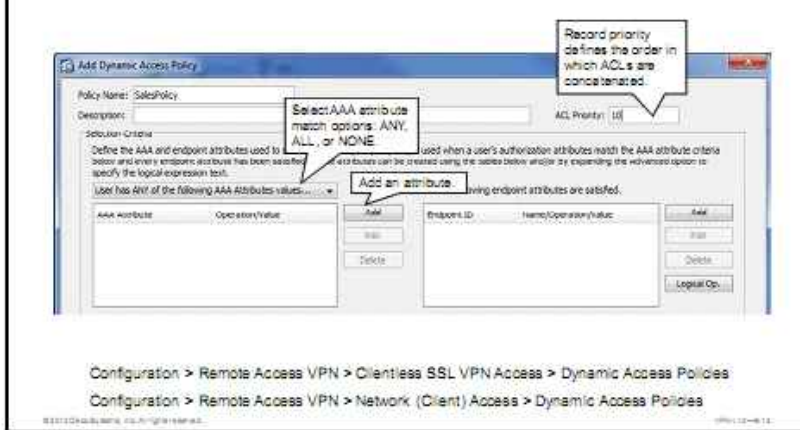
To configure DAP, you have to first create a new DAP policy. DfltAccessPolicy already exists and cannot be deleted. DfltAccessPolicy is applied to VPN sessions when other DAP policies are not configured. By default, DfltAccessPolicy does not apply any authorization attributes to VPN sessions.

To create a DAP policy using Cisco ASDM, complete the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** or **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies**.
- Step 2** Click the **Add** button. The Add Dynamic Access Policy window appears.

## Configuring DAP

### Task 2: Specify AAA Attributes Matching Criteria



In this example, DAP settings are configured by the following steps:

- Step 1** Enter the name of the policy in the Policy Name field. In this example, the policy name “SalesPolicy” is entered.
- Step 2** Optionally, enter a description for the policy in the Description field.
- Step 3** Enter a priority in the ACL Priority field. This sets a priority for the DAP. The security appliance applies access policies in the order that you set here, the highest number having the highest priority. If DAP records have the same priority setting and conflicting ACL rules, the most restrictive rule applies. In this example, the priority of 10 is set.
- Step 4** In the Selection Criteria area of the window, choose the AAA match criteria from the drop-down list. These are the options:
  - User Has ANY of the Following AAA Attributes Values Configured
  - User Has ALL of the Following AAA Attributes Values Configured
  - User Has NONE of the Following AAA Attributes Values Configured
- Step 5** Click the **Add** button to add AAA attributes. The Add AAA Attributes window appears.

## Configuring DAP

### Task 2: Specify AAA Attributes Matching Criteria (Cont.)



Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies  
Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

The following AAA attribute options are configurable for each AAA attribute type:

- **Cisco:** Refers to user authorization attributes that are stored in the AAA hierarchical model. You can specify a small subset of these attributes for the AAA selection attributes in the DAP record, including these:
  - **Group Policy:** The group policy that is associated with the user, to a maximum of 64 characters
  - **Assigned IP Address:** The assigned IP address
  - **Connection Profile:** The connection name, to a maximum of 64 characters
  - **Username:** The username of the authenticated user, to a maximum of 64 characters
- **LDAP:** The Lightweight Directory Access Protocol (LDAP) client stores all native LDAP response attribute-value pairs in a database that is 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 Microsoft Active Directory group membership, the AAA LDAP client provides special handling of the LDAP memberOf response attribute. The Active Directory memberOf attribute specifies the distinguished name (DN) string of a group record in Active Directory. The name of the group is the first common name 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 attributes to form a comma-separated string of group names. The group name is also updated in the response attribute database.

LDAP attributes consist of an attribute name and attribute-value pair in the DAP record. LDAP attributes include these:

- **Attribute ID:** Names and numbers of the attribute; maximum 64 characters
- **Value:** The value of the attribute ID
- **=/= :** Equal to/Not equal to
- **RADIUS:** The RADIUS client stores all native RADIUS response attribute-value pairs in a database that is 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.

RADIUS attributes consist of an attribute number and attribute-value pair in the DAP record. LDAP attributes include these:

- **Attribute ID:** Names or numbers for the attribute; maximum 64 characters.
- **Value:** The value of the attribute ID
- **=/= :** Equal to/Not equal to

Complete the following steps to configure AAA matching criteria for a DAP record:

- Step 1** Select an attribute type from the AAA Attribute Type drop-down menu.
- Step 2** For Cisco AAA attributes, check the appropriate attribute check box and specify attribute value.
- Step 3** For RADIUS and LDAP attributes, specify attribute ID and specify value.
- Step 4** Click **OK** in the Add AAA Attribute window.

## Configuring DAP

### Task 3: Specify Endpoint Attributes Matching Criteria

The screenshot shows the 'Add Dynamic Access Policy' configuration window. It includes a 'Policy Name' field set to 'SalesPolicy', a 'Description' field, and 'ACL Priority' and 'ID' fields. Below is the 'Selection Criteria' section, which defines the AAA and endpoint attributes used for policy selection. A table lists AAA attributes (e.g., 'aaa\_group' with value 'SalesGroup') and endpoint attributes (e.g., 'application' with value 'Clientless'). An 'Add Endpoint Attribute' dialog box is open, showing 'Application' selected for the 'Endpoint Attribute Type' and 'IPsec' selected for the 'Client Type'. Callouts indicate that the 'Add' button is used to add attributes and that the 'Application' type does not require Cisco Secure Desktop.

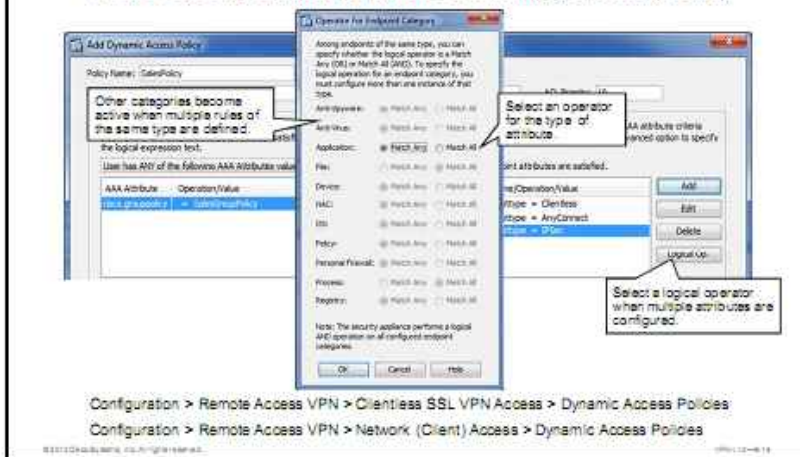
Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies  
Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

In this example, the administrator is defining the endpoint attributes that must be satisfied. DAP endpoint attributes are configured by the following steps:

- Step 1** Click the **Add** button to add endpoint attributes. The Add Endpoint Attribute window appears.
- Step 2** Choose the endpoint attribute type from the Endpoint Attribute Type drop-down list. The options include Antispyware, Antivirus, Application, File, NAC, Operating System, Personal Firewall, Process, Registry, VLAN, and Priority. In the example, Application is selected.
- Step 3** Choose the appropriate options for the endpoint attribute type chosen. In the example, IPsec is selected to match IPsec VPN session.
- Step 4** Repeat Step 3 to add other types of VPNs to apply this DAP record to.
- Step 5** Click **OK**.

## Configuring DAP

### Task 3: Specify Endpoint Attributes Matching Criteria (Cont.)



When you specify multiple attributes of the same type, you can select a logical operator to assess these multiple attributes. Complete the following steps to select a logical operator when you have multiple attributes of the same type:

- Step 1** Click the **Logical Op.** button. The Operator For Endpoint Category window appears.
- Step 2** Select a logical operator for a specific type of attribute. You can click the appropriate radio button next to the attribute to choose Match Any, where any attribute of the same type has to be met, or Match All, where all attributes of the same type have to be met. In the example, the Match Any type is selected for the Applications attribute type.
- Step 3** Click **OK**.

## Configuring DAP

### Task 4: Configure Authorization Parameters

Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies  
Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

In the fourth task, you configure authorization parameters that are applied by DAP policy. DAP Policy Attributes are used to configure a specific policy for a user or group of users that match the selection criteria that are defined in the previous steps. DAP policy attributes can be obtained from an external AAA server, in which case the attributes that are defined in Cisco ASDM override those from the AAA server. DAP policy attributes can also be defined from within Cisco ASDM. Ultimately, DAP policy attributes from your remote-access VPN users are dictated and defined based on the network security policy of your company. In this example, DAP settings are configured from within Cisco ASDM, using the following steps:

- Step 1** From the Access/Authorization Policy Attributes area of the window, click the **Action** tab.
- Step 2** Choose the action to take. The options are Continue or Terminate. Continue applies the access policy attributes to the session. Terminate terminates the session. In this example, the continue action is chosen.
- Step 3** In the User Message field, enter a message that will be displayed when the record is chosen. A user message displays as a yellow orb. When a user logs in, the orb blinks three times to attract attention, and then it is still. If several DAP records are chosen and each of them has a user message, all of the user messages display.

## Configuring DAP

### Task 4: Configure Authorization Parameters (Cont.)

- Authorization of full tunnel access (Cisco AnyConnect or Cisco Easy VPN)
- Can include only one statement type
  - Permit or deny
  - Due to aggregation functionality
  - Mixed ACLs do not appear in the drop-down list



Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Confidential

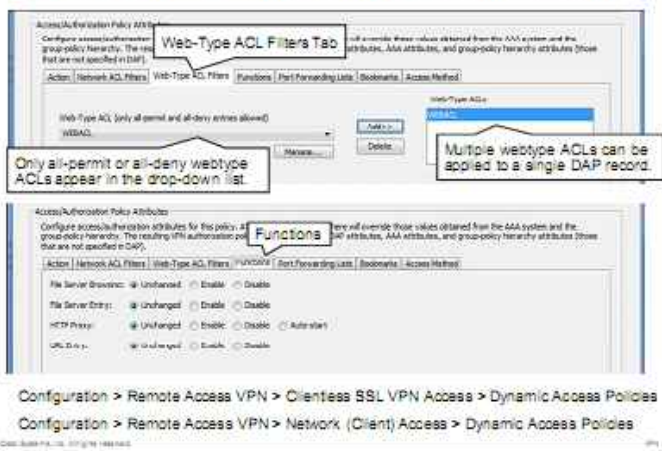
In this example, DAP settings for the Network ACL Filters tab are configured by the following steps:

- Step 4** From the Access/Authorization Policy Attributes area of the window, click the Network ACL Filters tab. This tab allows the selection and configuration of network ACLs to apply to this DAP record. An ACL for DAP can contain permit or deny rules, but not both. If an ACL contains both permit and deny rules, the security appliance rejects it.
- Step 5** Choose a preconfigured network ACL from the Network ACL drop-down list. If the ACL does not exist, click the **Manage** button to open a window to add, edit, or delete the ACLs.
- Step 6** Click the **Add** button to add the selected network ACL to the list. In this example, the previously configured network ACL SALES-ACL is selected.



## Configuring DAP

### Task 4: Configure Authorization Parameters (Cont.)



In this example, DAP settings for the Web-Type ACL Filters tab are configured by the following steps:

- Step 7** From the Access/Authorization Policy Attributes area of the window, click the **Web-Type ACL Filters** tab. This tab allows the selection and configuration of webtype ACLs to apply to this DAP record. An ACL for DAP can contain permit or deny rules, but not both. If an ACL contains both permit and deny rules, the security appliance rejects it.
- Step 8** Choose a preconfigured webtype ACL from the Web-Type ACL drop-down list. If the ACL does not exist, click the **Manage** button to open a window to add, edit, or delete the ACLs.
- Step 9** Click the **Add** button to add the selected webtype ACL to the list. In this example, the previously configured webtype ACL WEBACL is selected.

This example also shows DAP settings for the Functions tab:

- Step 10** Click the **Functions** tab from the Access/Authorization Policy Attributes area of the window. This tab allows for the configuration of file server entry and browsing, HTTP proxy, and URL entry for the DAP record.
- Step 11** Click the **File Server Browsing** radio button. This enables or disables Common Internet File System (CIFS) browsing for file servers or shared features. Browsing requires NetBIOS Name Service (NBNS) (Master Browser or Windows Internet Name Service [WINS]). If that fails or is not configured, use Domain Name System (DNS).
- Step 12** Click the **File Server Entry** radio button. This allows or prohibits a user from entering file server paths and names on the portal page. When enabled, it 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. In this example, the File Server Entry value is Unchanged.

- Step 13** Click the appropriate **HTTP Proxy** radio button. This affects 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 old proxy configuration of the browser automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client-side technologies, including HTML, cascading style sheets (CSS), JavaScript, VBScript, ActiveX, and Java. The only browser that it supports is Microsoft Internet Explorer.
- Step 14** Click the appropriate **URL Entry** radio button. This allows or prevents a user from entering HTTP or 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.

“Unchanged” is the default setting for these function settings from the group policy that applies to this session.

## Configuring DAP

### Task 4: Configure Authorization Parameters (Cont.)

**Port Forwarding Lists**

Configure access/authorization attributes for the policy. Attribute values specified here are aggregated with those obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP, AAA, and group-policy hierarchy attributes (those that are not specified in DAP).

Actions: Network ACL Filters | Web-Type ACL Filters | Functions | **Port Forwarding Lists** | Bookmarks | Access Method

Port Forwarding:  Unchanged  Enable  Disable  Auto-Set  Auto-Set

Enable port forwarding

Port Forwarding List:

Multiple lists can be applied.

**Bookmarks**

Configure access/authorization attributes for the policy. Attribute values specified here are aggregated with those obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP, AAA, and group-policy hierarchy attributes (those that are not specified in DAP).

Actions: Network ACL Filters | Web-Type ACL Filters | Functions | Port Forwarding Lists | **Bookmarks** | Access Method

Enable bookmarks

Bookmarks:

Multiple bookmarks can be applied.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies  
 Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

In this example, DAP settings for the Port Forwarding Lists tab are configured by the following steps:

- Step 15** Click the **Port Forwarding Lists** tab from the Access/Authorization Policy Attributes area of the window. This allows the selection and configuration of port-forwarding lists for user sessions. Port forwarding provides access for remote users in the group to client or server applications that communicate over known, fixed TCP/IP ports. Remote users can use client applications that are installed on their local PC and securely access a remote server that supports that application. Cisco has tested the following applications: Windows Terminal Services, Telnet, Secure FTP (FTP over Secure Shell [SSH]), Perforce, Outlook Express, and Lotus Notes. Other TCP-based applications may also work, but they have not been tested.

- Step 16** Choose the appropriate option for port forwarding. The other attributes in this field are enabled only when you set port forwarding to Enable or Auto-start.

The following options are available for the Port Forwarding Lists tab:

- **Unchanged:** Click to remove the attributes from the running configuration.
- **Enable:** Click to enable port forwarding.
- **Disable:** Click to disable port forwarding.
- **Auto-start:** Click to enable port forwarding and to have the DAP record automatically start the port-forwarding applets that are associated with its port-forwarding lists.

In this example, port forwarding is enabled.

- Step 17** Select a port-forwarding list from the drop-down menu and click the **Add** button. You can also create a new port-forwarding list by clicking the Manage button.

In this example, DAP settings for the Bookmarks tab are configured by the following steps:

- Step 18** Click the **Bookmarks** tab from the Access/Authorization Policy Attributes area of the window. This allows for the selection and configuration of bookmarks for user sessions.
- Step 19** Check the **Enable bookmarks** check box.
- Step 20** Choose a preconfigured bookmarks list from the drop-down box. If the list does not exist, click the **Manage** button to add, import, export, and delete bookmark lists.
- Step 21** Click the **Add** button.

## Configuring DAP

### Task 4: Configure Authorization Parameters (Cont.)

Access/Authorization Policy Attributes

Configure access/authorization attributes for the policy. Attribute values specified here will override those values obtained from the AAA system and the group policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group policy hierarchy attributes (those that are not specified in DAP).

Access Method:  Unchanged

- AnyConnect Client
- Web Portal
- Both default Web Portal
- Both default AnyConnect Client

Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies  
Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

© 2010 Cisco Systems, Inc. All rights reserved. SPN-10-4-01

In this example, DAP settings for the Access Method tab are configured by the following steps:

- Step 22** Click the **Access Method** tab from the Access/Authorization Policy Attributes area of the window. This allows configuration of the types of remote access that are permitted.

**Step 23** Select the appropriate Access Method from the list. In this example, the access method is unchanged.

The follow access methods are available:

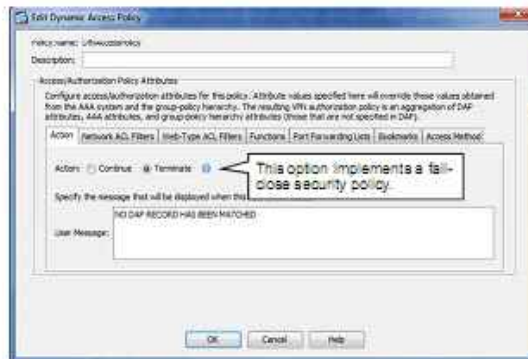
- **Unchanged:** Continue with the current remote-access method.
- **AnyConnect Client:** Connect, using the Cisco AnyConnect VPN Client.
- **Web-Portal:** Connect with clientless VPN.
- **Both-Default-Web-Portal:** Connect through either clientless or the AnyConnect client, with a default of clientless.
- **Both-Default-AnyConnect Client:** Connect through either clientless or the AnyConnect client, with a default of AnyConnect.

**Step 24** Click **OK** in the Add Dynamic Access Policy window.

**Step 25** Click **Apply** in the Dynamic Access Policies pane.

## Configuring DAP

### Task 5: Configure Action for DfltAccessPolicy



Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

In the last task, you change the action for the DfltAccessPolicy policy to terminate the other session that does not match any other DAP policy.

Complete the following steps to change action for DfltAccessPolicy:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** or **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies**.
- Step 2** Select the DfltAccessPolicy policy and click the **Edit** button. The Edit Dynamic Access Policy window appears.
- Step 3** Make sure that the **Action** tab is selected.
- Step 4** Check the **Terminate** radio button.
- Step 5** Optionally, enter a message in the User Message field that will be displayed to users.
- Step 6** Click **OK**.
- Step 7** Click **Apply** to apply the configuration.

## Verifying DAP

### Client Side

The figure consists of three numbered screenshots illustrating DAP verification on a client side:

- Step 1:** A screenshot of the Cisco SSL VPN Service interface. A yellow exclamation mark icon is present in the top right corner. A callout box points to it with the text: "The DAP message appears when this icon is clicked." Below the icon, a message box is displayed with the title "ACTIVATED DAP POLICY FOR SALES TEAM" and a "Message Text" field. A "Close" button is visible at the bottom right of the message box.
- Step 2:** A screenshot showing the "Unauthorized Access" dialog box. The address bar shows "http://192.168.1.2002". A dropdown menu is open, showing "Web Applications", "Sales-Charts", and "Sales-Presentations". A callout box points to "Sales-Presentations" with the text: "Bookmarks in Sales-Bookmarks List".
- Step 3:** A screenshot showing a "Connection failed" dialog box. The message reads: "Access to this resource has been denied." There are "Back" and "Deny Message" buttons.

Small text at the bottom of the screenshots includes "© 2010 Cisco Systems, Inc. All rights reserved." and "VPN-10-6.12".

To verify DAP on the client side, log into a VPN session. The example in the figure shows verification of DAP using a clientless SSL VPN session. After you log in, a user message displays as a yellow exclamation mark (!). This exclamation mark blinks three times to attract attention, and then it is still. When you click this exclamation mark, the user message is shown.

You can verify other DAP-assigned attributes by trying to access the resource that is not allowed in DAP policy or by examining bookmarks that are added by DAP policy.

## Verifying DAP

### Server Side

```
ASA# show vpn-sessiondb detail webvpn
<<Output omitted.>
Clientless:
  Tunnel ID      : 18.1
  Public IP     : 192.168.227.127
  Encryption    : RC4
  Hashing       : SHA1
  Encapsulation : TLSv1.0
  TCP Dest Port : 443
  Auth Mode     : userPassword
  Idle Time Out: 20 Minutes
  Idle TO Left  : 19 Minutes
  Client Type   : Web Browser
  Client Ver    : Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
  Trident/4.0; SLCC2; .N
  Bytes Tx     : 276263
  Bytes Rx     : 333333
  Filter Name   : DAP-web-user-04DP5501
  Network filter is applied by DAP
  when the VPN is established.

ASA# show access-list | include DAP
access-list DAP-web-user-04DP5501: 3 elements
access-list DAP-web-user-04DP5501 line 2 webtype permit url
http://10.0.0.11:80/ log default (hitcnt=0) (dynamic)
access-list DAP-web-user-04DP5501 line 3 webtype permit url
http://10.0.0.11:81/ log default (hitcnt=0) (dynamic)
access-list DAP-web-user-04DP5501 line 4 webtype permit url
http://10.0.0.11:8080/ log default (hitcnt=0) (dynamic)
```

To verify DAP on the Cisco ASA adaptive security appliance server side, use the **show vpn-session detail** command. In the example, details for clientless sessions (specified with the **webvpn** keyword) are displayed. In the Filter Name area of the output you can see, that a specific webtype ACL has been applied to the session.

You can also use the **show access-list** command to see the webtype ACL applied to the session.

### show vpn-sessiondb

To display information about VPN sessions, use the **show vpn-sessiondb** command in privileged EXEC mode. The command includes options for displaying information in full or in detail, lets you specify type of sessions to display, and provides options to filter and sort the information. The syntax table and usage notes organize the choices accordingly.

```
show vpn-sessiondb [detail] [full] {remote | l2l | index indexnumber | webvpn | email-proxy | svc} [filter {name username | ipaddress IPAddr | a-ipaddress IPAddr | p-ipaddress IPAddr | tunnel-group groupname | protocol protocol-name | encryption encryption-algo | inactive}] [sort {name | ipaddress | a-ipaddress | p-ipaddress | tunnel-group | protocol | encryption | inactivity}]
```

### show vpn-sessiondb Parameters

Parameter	Description
<b>detail</b>	(Optional) Displays extended details about a session. For example, using the <b>detail</b> option for an IPsec session displays additional details such as the Internet Key Exchange IKE hashing algorithm, authentication mode, and rekey interval.  If you choose <b>detail</b> , and the <b>full</b> option, the adaptive security appliance displays the detailed output in a machine-readable format.
<b>filter</b> <i>filter_criteria</i>	(Optional) Filters the output to display only the information that you specify by using one or more of the filter options.

Parameter	Description
<code>full</code>	(Optional) Displays streamed, untruncated output. Output is delineated by   characters and a    string between records.
<code>session_type</code>	(Optional) To show data for a specific session type, enter one of the following keywords: <ul style="list-style-type: none"> <li>■ <b>email-proxy</b>: Displays email-proxy sessions</li> <li>■ <b>index <i>indexnumber</i></b>: Displays a single session by index number. Specify the index number for the session, 1 to 750</li> <li>■ <b>I2I</b>: Displays VPN LAN-to-LAN session information</li> <li>■ <b>ratio</b>: Displays VPN Session protocol or encryption ratios</li> <li>■ <b>remote</b>: Displays IPsec remote access sessions</li> <li>■ <b>summary</b>: Displays the VPN session summary</li> <li>■ <b>svc</b>: Displays SSL VPN Client sessions</li> <li>■ <b>vpn-lb</b>: Displays VPN Load Balancing management sessions</li> <li>■ <b>webvpn</b>: Displays information about clientless SSL VPN sessions</li> </ul>
<code>sort <i>sort_criteria</i></code>	(Optional) Sorts the output according to the sort option you specify.

## show access-list

To display the counters for an access list, use the **show access-list** command in privileged EXEC mode.

**show access-list** *acl\_name\_1* [...*acl\_name\_2*] [**brief**]

### show access-list Parameters

Parameter	Description
<code><i>acl_name_1</i></code>	A name or set of characters that identifies an existing access list
<code><i>acl_name_2</i></code>	A name or set of characters that identifies an existing access list
<code><b>brief</b></code>	Displays the access list identifiers and hit count in hexadecimal format



## Deploying DAP

### Implementation Guidelines

- Recommended DAP usage:
  - Use to apply parameters resulting from security posture
  - Use to apply parameters not available in external AAA authorization profiles
- Secondary DAP usage:
  - Use to define exceptions from general rules for individual users or rare cases
- Not recommended to deploy DAP in parallel to policy groups and external AAA authorization to achieve the same results for large user groups (duplication and complexity)

DAP records can be used in parallel to statically configured policies to enforce desired authorization profiles. A mixing of both configuration approaches (static and DAP) to achieve the same goals can result in a highly complex ruleset that will be difficult to maintain and troubleshoot. Therefore, a clear strategy should be followed to limit the usage of DAP to the required scenarios.

It is recommended to use DAP primarily in these scenarios:

- Apply parameters resulting from security posture.
- Apply parameters not available in external AAA authorization profiles.

It is accepted practice to deploy DAP in this secondary scenario:

- Define exceptions from the general ruleset. This solution is commonly the simplest solution for individual users or rare cases.

DAP usage is discouraged for this scenario:

- Deployment in parallel to policy groups and external AAA authorization to achieve the same results for large user groups. In such configurations, DAP records may lead to duplication of policy profiles and unnecessary complexity.

# Aggregating DAP Records

This topic describes how to configure multiple DAP records and how multiple DAP records are aggregated.

## Aggregating DAP Records

### Overview

- VPN user can match multiple DAP policies.
- When several records match:
  - Some actions are concatenated (network ACLs, webtype ACLs, port-forwarding lists, bookmarks).
    - DAP priority defines the order.
  - Other actions depend on nature of each feature:

Priority: 10 Action: Continue	+	Priority: 5 Action: Terminate	=	Resulting Action: Terminate
Priority: 10 Action: Continue	+	Priority: 5 Action: Continue	=	Resulting Action: Continue
Priority: 10 ACL: 1	+	Priority: 5 ACL: 2	=	Resulting Action: ACL: 1, 2

© 2010 Cisco Systems, Inc. All rights reserved. IPN12-4837

An establishing VPN session can match multiple DAP policies. When a VPN session matches more than one DAP policy, the following occurs:

- Actions, such as networks ACLs, webtype ACLs, port-forwarding lists, and bookmarks are concatenated and DAP priority defines the order.
- Other actions are selected based on the nature of each feature:
  - **Action:** The aggregated attribute value will be Terminate if the Terminate value is configured in any of the selected DAP records and Continue if the Continue value is configured in all of the selected DAP records.
  - **User Message:** The aggregated attribute value will be a line-feed (hex value 0x0A) separated string that is created by linking together the attribute values from the selected DAP records.
  - **Clientless feature enabling attributes (port-forward, file-browsing, file-entry, http-proxy, url-entry):** The aggregated attribute value will be Auto-start if the Auto-Start value is configured in any of the selected DAP records. The aggregated attribute value will be Enable if there is no Auto-start value configured in any of the selected DAP records, and the Enable value is configured in at least one of the selected DAP records. The aggregated attribute value will be Disable if there is no Auto-start or Enable value that is configured in any of the selected DAP records, and the Disable value is configured in at least one of the selected DAP records.

**Note** Refer to the *ASA 8.x Dynamic Access Policies (DAP) Deployment Guide* available at [Cisco.com](http://Cisco.com) for examples of aggregated attributes.

In the figure, two examples are provided. In the first example, the first DAP policy has a priority 10 and action is set to terminate. The second policy has a priority 5 and action continue. If a session matches both policies, the resulting action will be Terminate.

In the second example, the first DAP policy has a priority 10 and action is set to continue. The second DAP policy has a priority 5 and action continue. If a session matches both policies, the resulting action will be Continue.

In the third example, the first DAP policy has a priority 10 and assigns ACL 1 to a session. The second DAP policy has a priority 5 and assigns ACL 2 to a session. If a session matches both policies, ACLs will be concatenated and statements from ACL 1 will be positioned above statements from ACL 2.

## Aggregating DAP Records

### Configuration Tasks

1. Create additional DAP policy.
2. Specify AAA attributes matching criteria.
3. Configure authorization parameters.

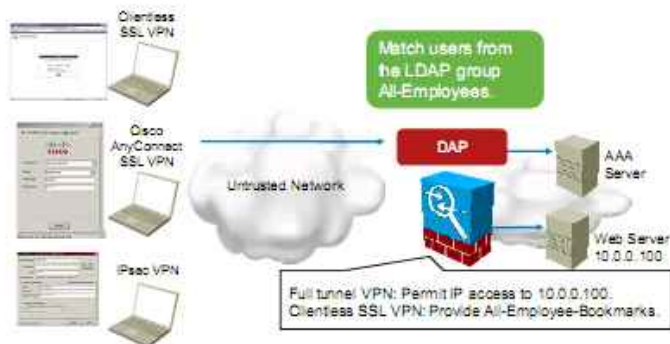
© 2010 Cisco Systems, Inc. All rights reserved. VPN-5-24-03

To configure aggregating DAP records, you have to create an additional DAP policy. Complete the following configuration tasks:

1. Create an additional DAP policy.
2. Specify AAA attributes matching criteria.
3. Configure authorization parameters.

## Aggregating DAP Records

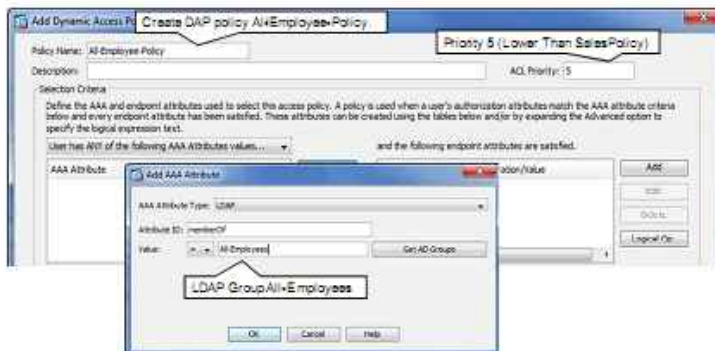
### Configuration Scenario



The figure shows an example, which will serve as the configuration scenario in ongoing configuration tasks. You will create another DAP policy that will match LDAP group All-Employees. You will permit access to the 10.0.0.100 web server for full tunnel VPN sessions and configure a bookmark list for a clientless SSL VPN session. When a VPN session matches a previously configured DAP policy and the one configured in this topic, attributes from both policies will be aggregated.

## Aggregating DAP Records

### Tasks 1-2: Create DAP Policy and Match Attributes



Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies  
Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

To create an additional DAP policy, complete the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** or **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies**.
- Step 2** Click **Add** button. The Add Dynamic Access Policy window appears.
- Step 3** Enter the policy name in the Policy Name field. In the example, All-Employee-Policy is entered.
- Step 4** Enter a priority in the ACL Priority field. In the example, the priority is set to 5.
- Step 5** Click the **Add** button to add the AAA attribute. The Add AAA Attribute window appears.
- Step 6** Select the LDAP AAA attribute type from the AAA Attribute Type drop-down menu.
- Step 7** Enter All-Employees in the Value field. Click **OK**.

## Aggregating DAP Records

### Task 3: Configure Authorization Parameters



Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

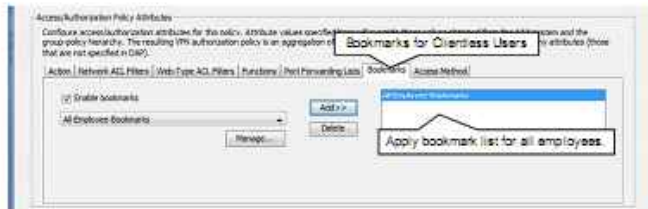
© 2010 Cisco Systems, Inc. All rights reserved. Cisco Confidential

To configure the network ACL authorization parameter, complete the following steps:

- Step 1** Click the **Network ACL Filters** tab.
- Step 2** Choose a network ACL from the drop-down menu. In the example, the **ALL-EMPLOYEE-ACL** is selected.
- Step 3** Click the **Add** button.

## Aggregating DAP Records

### Task 3: Configure Authorization Parameters (Cont.)



Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

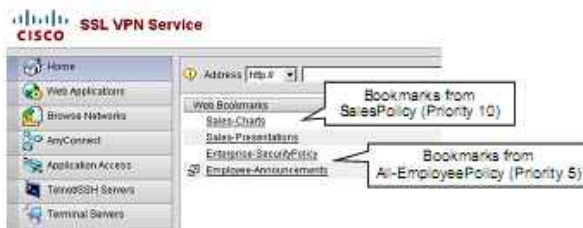
To configure bookmarks authorization parameter, complete the following steps:

- Step 4** Click the **Bookmarks** tab.
- Step 5** Check the **Enable bookmarks** check box to enable bookmarks.
- Step 6** Select a bookmark list from the drop-down menu. In the example, the **All-Employee-Bookmarks** is selected.
- Step 7** Click **Add** button.

## Verifying Aggregated DAP Policies

### Client Side

- Bookmark entries are aggregated according to DAP priorities.



You can verify aggregated DAP policies by logging into a VPN session. In the example, the user logged into a clientless SSL VPN session. If the session matches both configured DAP policies, you should see aggregated bookmarks in the SSL portal web page. Bookmarks are aggregated according to DAP policies priority.

## Verifying Aggregated DAP Policies

### Server Side

```
ASA# show vpn-sessiondb detail avc
c.output omitted.
DTLS-Tunnel:
  Tunnel ID      : 20.3
  Assigned IP    : 1.1.1.1                Public IP      : 192.168.227.137
  Encryption     : AES128                 Hashing        : SHA1
  Encapsulation  : DTLSv1.0              UDP Sec Port   : 51106
  UDP Dst Port   : 443                     Auth Mode     : userPassword
  Idle Time Out  : 30 Minutes              Idle TO Left  : 20 Minutes
  Client Type    : DTLS VPN Client
  Client Ver     : AnyConnect Windows 2.4.1012
  Bytes Tx      : 0                         Bytes Rx      : 2636
  Pkts Tx       : 0                         Pkts Rx      : 38
  Pkts Tx Drop  : 0                         Pkts Rx Drop : 0
  Filter Name   : DAP-ip-user-50F34708

ASA# show access-list | include DAP
access-list DAP-ip-user-50F34708 line 1 extended permit tcp any host 10.0.0.11 eq 8080 (hitcnt=0) 0x2da10fb7
access-list DAP-ip-user-50F34708 line 2 extended permit tcp any host 10.0.0.11 eq 81 (hitcnt=0) 0xcab361d7
access-list DAP-ip-user-50F34708 line 3 extended permit tcp any host 10.0.0.11 eq www (hitcnt=0) 0x1bb0f8b6
access-list DAP-ip-user-50F34708 line 4 extended permit ip any host 10.0.0.100 (hitcnt=0) 0xd0ea95b3
```

ACL entries are aggregated according to DAP policy priority.

Use the **show vpn-sessiondb detail** and **show access-list** commands to verify DAP policies on the Cisco ASA adaptive security appliance side. If a user logs in using a complete client VPN, you should see that access list entries are aggregated according to configured DAP policy priorities.



# Integrating Cisco Secure Desktop with DAP

This topic describes how to integrate DAP policies with Cisco Secure Desktop to determine remote endpoints posture.

## Integrating Cisco Secure Desktop with DAP

### Overview

- DAP supports two basic posture assessment methods to collect endpoint security attributes:
  - Cisco Secure Desktop Host Scan
  - Cisco NAC
- DAP evaluates Cisco Secure Desktop Host Scan and Endpoint Assessment results
- Cisco Secure Desktop is not available for IPsec VPNs

As previously described, DAP policies can be used to apply authorization attributes that are based on the remote endpoints posture. DAP supports two basic posture assessment methods to collect endpoint security attributes:

- Cisco Secure Desktop Host Scan and Endpoint Assessment
- Cisco Network Admission Control (NAC)

DAP evaluates Cisco Secure Desktop Host Scan and Endpoint Assessment results and applies authorization attributes to VPN sessions.

---

**Note** Cisco Secure Desktop is not available for IPsec VPNs.

---

## Integrating Cisco Secure Desktop with DAP

### Attribute Types

#### Endpoint Attribute Type

Anti-Spyware

Anti-Virus

Application

File

Device

NAC

Operating System

Personal Firewall

Policy

Process

Registry

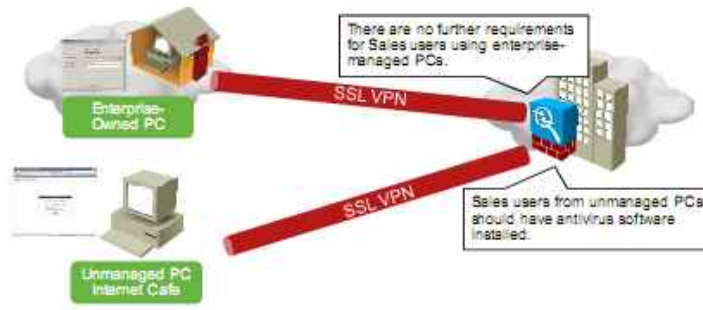


The figure shows all endpoint attributes that can be matched inside DAP policy.

## Integrating Cisco Secure Desktop with DAP

### Configuration Tasks

1. Add DAP policy.
2. Specify endpoint assessment matching criteria.
3. Configure authorization parameters.



To integrate Cisco Secure Desktop with DAP, create a DAP policy by completing the following configuration tasks:

1. Create an additional DAP policy.
2. Specify AAA attributes matching criteria.
3. Configure authorization parameters.

---

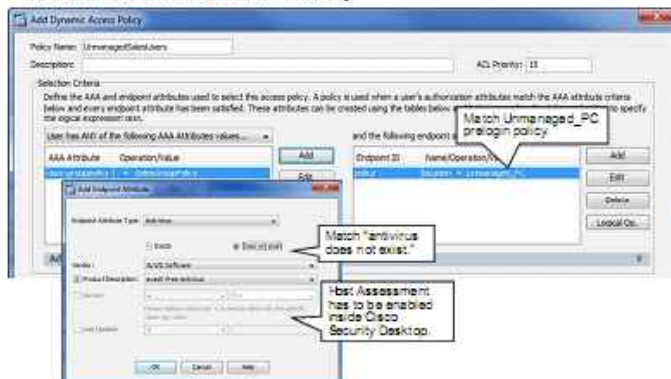
**Note** Cisco Secure Desktop and Host Scan with Endpoint Assessment has to be enabled to integrate DAP policy with Cisco Secure Desktop.

---

The figure shows an example, which will serve as the configuration scenario in ongoing configuration tasks. You will create another DAP policy that will allow access through SSL VPN connections only from enterprise-owned PCs or from unmanaged PCs with antivirus software installed. In the example, you will create an additional DAP policy that will match Sales users with the Unmanaged\_PC policy (configured in the Cisco Secure Desktop lesson) and without antivirus software installed. Action for such users will be to terminate connection.

# Integrating Cisco Secure Desktop with DAP

## Task 1-2: Create DAP Policy



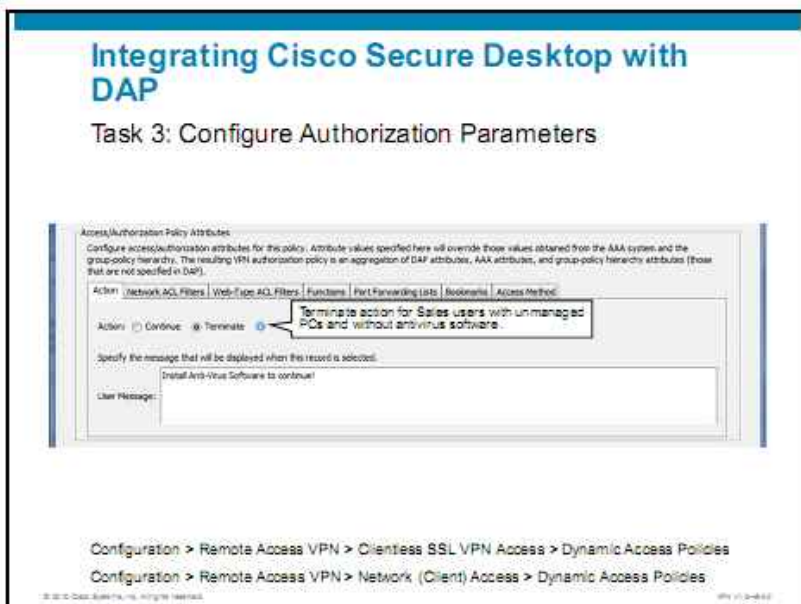
Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

To create an additional DAP policy, complete the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** or **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies**.
- Step 2** Click the **Add** button. The Add Dynamic Access Policy window appears.
- Step 3** Enter a policy name in the Policy Name field. In the example, UnmanagedSalesUsers is entered.
- Step 4** Enter the priority in the ACL Priority field. In the example, priority is set to 15.
- Step 5** Click the **Add** button to add an AAA attribute. The Add AAA Attribute window appears.
- Step 6** Choose the Cisco AAA attribute type from the AAA Attribute Type drop-down menu (not shown).
- Step 7** Check the Group Policy check box (not shown).
- Step 8** Enter SalesGroupPolicy in the input field (not shown).
- Step 9** Click **OK** in the Add AAA Attribute window.
- Step 10** Click the **Add** button to add an endpoint attribute. The Add Endpoint Attribute window appears.
- Step 11** Choose **Policy** from the Endpoint Attribute Type drop-down menu (not shown).
- Step 12** Choose **Unmanaged\_PC** policy from the drop-down menu. This policy has been configured in the Cisco Secure Desktop lesson.
- Step 13** Click **OK**.
- Step 14** Click **Add** again to add another endpoint attribute.
- Step 15** Choose **Anti-Virus** from the Endpoint Attribute Type drop-down menu.
- Step 16** Click the **Does Not exist** radio button.

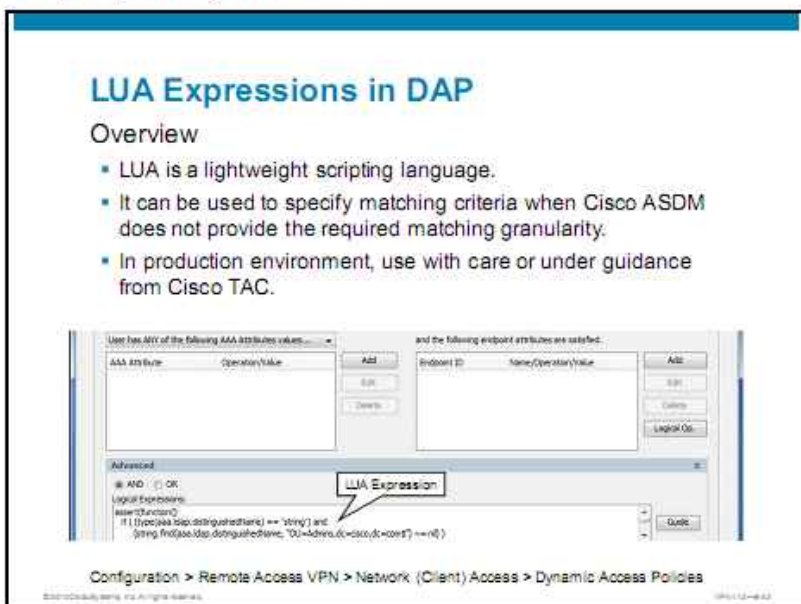
- Step 17** Choose a vendor from the Vendor drop-down list. In the example, ALWIL Software is selected.
- Step 18** Optionally, check the **Product Description** check box and select a specific product from the drop-down menu. In the example, avast! Free Antivirus is selected.
- Step 19** Click **OK**.



- Step 20** To apply a Terminate action to this DAP policy, click the **Terminate** radio button and optionally enter a message that will be shown to the user in the User Message field.
- Step 21** Click **OK**.
- Step 22** Click **Apply** to apply the configuration.

# Using LUA Expressions in DAP

This topic describes how to use LUA expressions to provide additional flexibility when configuring matching criteria for DAP.



LUA is a powerful, fast, lightweight, embeddable scripting language. You can use LUA to create matching criteria for DAP, when Cisco ASDM does not provide enough flexibility to specify matching criteria. For example, you might want to apply a different DAP based on the following:

- Organizational unit (OU) or other level of the hierarchy for the user object
- Group name that follows a naming convention but has many possible matches—you might require the ability to use a wildcard on group names.

You can accomplish this flexibility by creating a LUA logical expression in the Advanced area of the DAP pane in Cisco ASDM.

---

**Note** LUA means "Moon" in Portuguese. As such, it is neither an acronym nor an abbreviation.

---

Complete the following steps to create custom LUA expressions to specify matching criteria:

- Step 1** Expand the **Advanced** option in the Add Dynamic Access Policy window.
- Step 2** In the Logical expression field, you enter free-form LUA text that represents AAA or endpoint selection logical operations or both. Cisco 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 that it cannot parse.

---

**Note** Specifying custom LUA expressions requires sophisticated knowledge of LUA scripting language, which is outside of the scope of this course.

---

## LUA Expressions in DAP

### Script Examples

- Cisco ASDM provides a guide and sample scripts for:
  - Organizational unit-based match
  - Group membership
  - Antivirus
  - Antispyware
  - Firewall
  - Hotfix

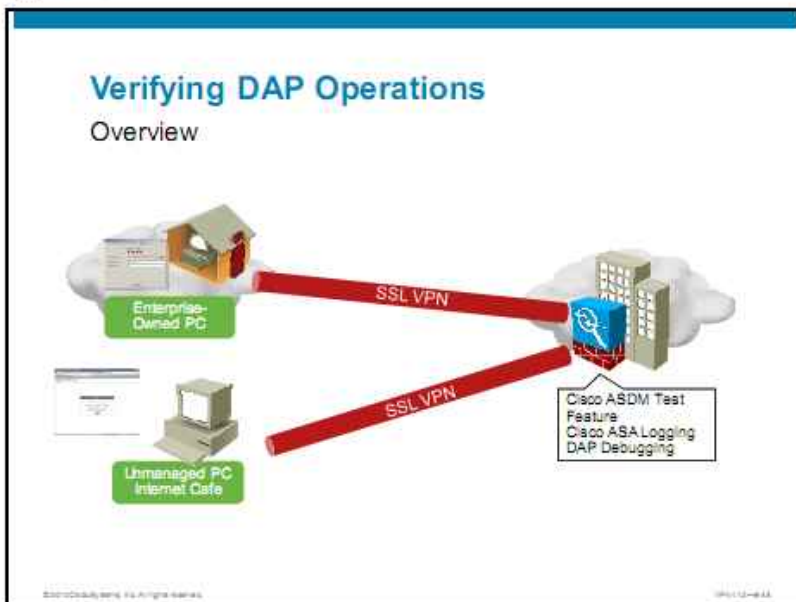


- [Links for Creating Lua EVAL Expressions](#)
  - [Constructing DAP EVAL Expressions](#)
- [The DAP Check/Setup Question](#)
  - [Checking for a Single Antivirus Program](#)
  - [Checking for Antivirus Definitions Within the Last 30 Days](#)
  - [Checking for a Hotfix on the User PC](#)
  - [Checking for Antivirus Programs](#)
  - [Checking for Antivirus Programs and Definitions Older than](#)
- [Additional Lua Functions](#)
  - [OU-based Match Example](#)
  - [Group Membership Example](#)
  - [Antivirus Example](#)
  - [Antispyware Example](#)
  - [Hotfix Example](#)
  - [Artificial Antispyware or Any Firewall Example](#)
- [Check/Setup with Custom Function Example](#)
- [Further Information on Lua](#)

Cisco ASDM provides a guide on how to construct logical expression for AAA and endpoint attributes. Click the **Guide** button in the Add Dynamic Access Policy window to open Cisco ASDM help. Cisco ASDM will provide detailed explanations on creating LUA expressions, as well as examples.

# Troubleshooting DAP

This topic describes how to troubleshoot DAP operations on the Cisco ASA adaptive security appliance.



To troubleshoot DAP on the Cisco ASA adaptive security appliance, you can use the following tools:

- Cisco ASDM Test feature
- Cisco ASA logging
- DAP debugging commands



## Verifying DAP Operations

### Test Feature

Configure Dynamic Access Policies

For IPsec, SSL, VPN Client, Clientless SSL VPN, and L2L through proxy servers, you can configure dynamic access policies (DAP) that define which network resources a user is authorized to access. All policies in the table below are evaluated for matching criteria during session establishment. After none of the DAP policies are matched, the ASA will enforce the DefaultAccessPolicy.

ACL Priority	Name	Network ACL List	Web-Type ACL List	Description	
0	DefaultAccessPolicy				+ Add
1	All Employee Policy	COMMON_WEB_PORTS	DEFAULT	Employee Access Policy	- Edit
2	InfoAccessPolicy	ALL_EMPLOYEE_ACL		Info Access Policy	Delete

Test Dynamic Access Policies

To test the dynamic access policies currently configured on the device click the button: Test Dynamic Access Policies...

Cisco ASDM Test Feature for Predeployment Testing

Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

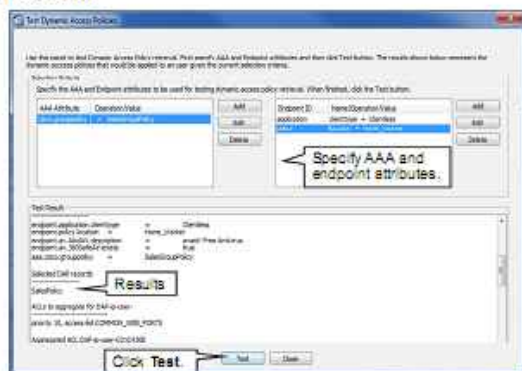
Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

The Dynamic Access Policies pane in Cisco ASDM allows for the testing of DAP records that are configured on the device by specifying authorization attribute-value pairs. To test a DAP record, complete the following steps:

- Step 3** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** or **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies**.
- Step 4** Click the **Test Dynamic Access Policies** button within the Dynamic Access Policies pane. The Test Dynamic Access Policies window appears.

## Verifying DAP Operations

### Test Results



Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Within the Test Dynamic Access Policies windows, continue with these steps:

- Step 5** Click the **Add** button within the AAA attributes area of the window. This selection allows for the selection of AAA attributes that were described previously in this topic. In this example, the Cisco AAA attribute for group policy equal to SalesGroupPolicy is selected.
- Step 6** Click the **Add** button within the Endpoint attribute area of the window. This allows for the selection of Endpoint attributes, which was already described previously in this topic. In this example, the Endpoint attribute for application that is equal to "Clientless" is selected and location that is equal to Home\_Worker is selected.
- Step 7** Click the **Test** button and the results are shown in the Test Results area of the window. In this example, the "SalesPolicy" DAP policy is applied to the session.
- Step 8** Click **Close** to return to the Dynamic Access Policies pane.

## Verifying DAP Operations

### DAP Debugging—Disabled Cisco Secure Desktop

```
ASA# debug dap trace
debug dap trace enabled at level 1
DAP_TRACE: Activating: flash:/dap.xml
DAP_TRACE: DAP_config_activate: Using XML translation script
DAP_TRACE: DAP_config_activate: memory usage = 36%

The DAP policy contains the following attributes for user: LocalSalesUser
.....
1: url-list = Sales-Bookmarks
2: port-forward list = Sales-PortForwardingList
3: port-forward = enable
4: action = continue
5: user-message = ACTIVATED DAP POLICY FOR SALES TEAM
6: network-acl = DAP-ip-user-9059370B
   rule 1: extended permit ip any 10.0.0.0 255.255.255.240
7: appl-acl = DAP-web-user-34202C09
   rule 1: permit url http://10.0.0.11:80/ log default
   rule 2: permit url http://10.0.0.11/ log default
   rule 3: permit url http://10.0.0.11/ log default
```

You can use the **debug dap trace** command to enable DAP debugging. The output shows debugging of DAP when Cisco Secure Desktop is disabled.

### debug dap

To enable logging of DAP events, use the **debug dap** command in privileged EXEC mode. To disable the logging of DAP debug messages, use the **no** form of this command.

**debug dap** {errors | trace}

#### debug dap Parameters

Parameter	Description
<b>errors</b>	Specifies DAP processing errors
<b>trace</b>	Specifies a DAP function trace

## Verifying DAP Operations

### DAP Debugging—Disabled Cisco Secure Desktop (Cont.)

```
DAP_TRACE: DAP_open: 7413EE30
DAP_TRACE: Username: LocalSalesUser, aaa.cisco.grouppolicy = SalesGroupPolicy
DAP_TRACE: Username: LocalSalesUser, aaa.cisco.class = SalesGroupPolicy
DAP_TRACE: Username: LocalSalesUser, aaa.cisco.username = LocalSalesUser
DAP_TRACE: Username: LocalSalesUser, aaa.cisco.tunnelgroup = Sales-Profile
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["grouppolicy"]="SalesGroupPolicy"
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["class"]="SalesGroupPolicy"
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"]="LocalSalesUser"
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"]="Sales-Profile"
DAP_TRACE:
dap_add_to_lua_tree:endpoint["application"]["clienttype"]="Clientless"
DAP_TRACE: Username: LocalSalesUser, Selected DAPs: ,SalesPolicy
DAP_TRACE: dap_request: memory usage = 36%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: LocalSalesUser, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: LocalSalesUser, dap_concat_fn: [ACTIVATED DAP POLICY FOR
SALES TEAM] 35 128
DAP_TRACE: Username: LocalSalesUser, dap_comma_str_fn: [Sales-Bookmarks] 15 128
DAP_TRACE: Username: LocalSalesUser, dap_comma_str_fn: [Sales-
PortForwardingList] 24 128
```

The figure shows continuation of output from the previous figure. You can see that only AAA attributes are examined.

## Verifying DAP Operations

### DAP Debugging—Enabled Cisco Secure Desktop

```
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.os.version = "Windows XP"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.os.servicepack = "2"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.policy.location = "Home Worker"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.device.protection = "secure desktop"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.device.hostname = "xp"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.device.protection_version = "3.3.0.118"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.device.protection_extension = "2.5.5.1"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.os.windows.hotfix["Q147522"] = "true"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.os.windows.hotfix["MS28366"] = "true"
< truncated list of all detected hotfixes >
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.device.port["135"] = "true"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.device.port["1905"] = "true"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.device.port["3389"] = "true"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.device.port["E2522"] = "true"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.device.MAC["00D0.295e.9ca5"] = "true"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.sw["MSWindowsFW"] = {}
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.sw["MSWindowsFW"].exists = "true"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.sw["MSWindowsFW"].description = "Microsoft
Windows Firewall"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.sw["MSWindowsFW"].version = "XP SP2-"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.sw["MSWindowsFW"].enabled = "ok"
DAP_TRACE: Username: LocalSalesUser, Selected DAPs: ,SalesPolicy
DAP_TRACE: Username: LocalSalesUser, dap_concat_fn: [ACTIVATED DAP POLICY FOR SALES TEAM]
DAP_TRACE: Username: LocalSalesUser, dap_comma_str_fn: [Sales-Bookmarks] 15 128
DAP_TRACE: Username: LocalSalesUser, dap_comma_str_fn: [Sales-PortForwardingList] 24 128
```

The figure shows output from DAP debugging when Cisco Secure Desktop is enabled. You can see that endpoint attributes are examined.

## Verifying DAP Operations

### Logging Output

```
ASA(config)# logging enable
ASA(config)# logging console 7
%ASA-6-737026: IPAA: Client assigned 10.100.0.1 from local pool
%ASA-6-737006: IPAA: Local pool request succeeded for tunnel-group 'Sales-
Profile'
%ASA-5-722033: Group <SalesGroupPolicy> User <LocalSalesUser> IP <10.0.1.11>
First TCP SVC connection established for SVC session.
%ASA-6-722022: Group <SalesGroupPolicy> User <LocalSalesUser> IP <10.0.1.11> TCP
SVC connection established without compression
%ASA-4-722051: Group <SalesGroupPolicy> User <LocalSalesUser> IP <10.0.1.11>
Address <10.100.0.1> assigned to session
%ASA-7-734003: DAP: User LocalSalesUser, Addr 10.0.1.11: Session Attribute
endpoint.os.version = "Windows XP"
%ASA-7-734003: DAP: User LocalSalesUser, Addr 10.0.1.11: Session Attribute
endpoint.os.servicepack = "2"
%ASA-7-734003: DAP: User LocalSalesUser, Addr 10.0.1.11: Session Attribute
endpoint.policy.location = "Home_Worker"
%ASA-7-734003: DAP: User LocalSalesUser, Addr 10.0.1.11: Session Attribute
endpoint.device.protection = "secure desktop"
%ASA-7-734003: DAP: User LocalSalesUser, Addr 10.0.1.11: Session Attribute
endpoint.device.hostname = "xp"
<...output omitted...>
```

You can verify DAP operations using Cisco ASA logging subsystem. In the example, you can see various logging messages 734003, which display AAA and endpoint attributes that are associated with a session.

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- DAP evaluates the AAA attributes and posture results.
- DAP applies actions to VPN connections matching the defined criteria.
- DAP records can be aggregated into policy sets.
- Cisco Secure Desktop host results can be evaluated by DAP policies.
- LUA functions provide a custom configuration interface for matching logic that is not available through the Cisco ASDM.
- You can troubleshoot DAP operations using Cisco ASA logging output or the **debug dap** command.

© 2010 Cisco Systems, Inc.

5-170-483

## References

For additional information, refer to this resource:

- *ASA 8.x Dynamic Access Policies (DAP) Deployment Guide* at [http://www.cisco.com/en/US/products/ps6120/products\\_white\\_paper09186a00809fcf38.shtml#t5](http://www.cisco.com/en/US/products/ps6120/products_white_paper09186a00809fcf38.shtml#t5)

# Deploying High Availability and High Performance in SSL and IPsec VPNs

---

## Overview

Two of the most challenging requirements of virtual private networks (VPNs) are high availability and high performance. High availability ensures continuous operation even if one or more VPN servers fail. High-performance enhancements are deployed to boost the system performance by alleviating the load that is placed on a single VPN server. This lesson discusses the methods of deploying high availability: cluster load balancing, server load balancing (SLB) load balancing, and active/standby failover. Quality of service (QoS) mechanisms are integrated with IP Security (IPsec) VPNs to ensure a timely forwarding of delay-susceptible traffic flows, police the transmission rates, and smooth the bursts by traffic shaping. The lesson explains the troubleshooting methods that can be employed to investigate high-availability problems.

## Objectives

Upon completing this lesson, you will be able to deploy and manage high-availability and high-performance features. This ability includes being able to meet these objectives:

- Choose VPN high-availability and high-performance features
- Configure and verify redundant peering with Cisco AnyConnect and IPsec client
- Deploy active/standby failover for SSL and IPsec VPNs
- Implement dynamic routing to achieve IPsec site-to-site VPN high availability
- Describe the deployment of VPN load-balancing clusters
- Provide high availability and high performance using an external SLB appliance
- Configure and verify QoS policies in IPsec VPNs
- Troubleshoot Cisco ASA adaptive security appliance failover and VPN clustering functions

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic describes the high availability options in SSL and IPsec VPNs.

## VPN High Availability and Performance

### Cisco ASA Platform Capacity

	5505	5510	5520	5540	5550	5580-20	5580-40
Firewall throughput	150 Mbps	300 Mbps	450 Mbps	500-650 Mb/s	1-1.2 Gb/s	5-10 Gb/s	10-20 Gb/s
Connections per second	4000	9000	12,000	25,000	36,000	90,000	150,000
Packets per second	85,000	190,000	320,000	500,000	600,000	250,000	4,000,000
Maximum connections	10,000/ 25,000	50,000/ 130,000	280,000	400,000	650,000	1,000,000	2,000,000
VPN throughput	100 Mb/s	170 Mb/s	225 Mb/s	325 Mb/s	425 Mb/s	1 Gb/s	1 Gb/s
Maximum VPN peers (IPsec/SSL)	10/25	250 / 250	750 / 750	5000/2500	5000/5000	10,000/ 10,000	10,000/ 10,000

© 2010 Cisco Systems, Inc. All rights reserved. 090012-01-00

The Cisco ASA adaptive security appliance platform portfolio gives customer-wide choice of different capacity and performance platforms while preserving availability of high performance and high availability across a whole range of devices.

The table provides the performance figures of each security appliance platform.

### The Performance Figures of Cisco ASA Adaptive Security Appliance Platforms

	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
Maximum simultaneous connections	25,000	130,000	280,000	400,000	650,000	1,000,000	2,000,000
Maximum number of IPsec and SSL VPN sessions	10/25	250/250	750/750	5000/ 2500	5000/ 5000	10,000/ 10,000	10,000/ 10,000
Cleartext throughput in Mb/s	150	300	450	650	1200	5000	10,000
AES and 3DES throughput in Mb/s	100	170	225	325	425	1000	1000



	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
CPU type	AMD Geode LX	Intel Celeron	Intel Pentium 4 Intel Celeron	Intel Pentium 4	Intel Pentium 4	AMD Opteron (2 CPU, 4 cores)	AMD Opteron (4 CPU, 8 cores)
CPU speed	500 MHz	1.6 GHz	2.0 GHz	2.0 GHz	3.0 GHz	2.6 GHz	2.6 GHz
Default RAM	256 MB	256 MB	512 MB	1 GB	4 GB	8 GB	12 GB
Default flash	64 MB	64 MB	64 MB	64 MB	64 MB	1 GB	1 GB

## VPN High Availability and Performance

### High Availability and Performance Options

Option	Features	VPN availability
Redundant peering	Multiple independent Cisco ASA security appliances nondeterministic load sharing (users given different gateway address).	No backup in clientless SSL VPN. Backup server configurable in all other VPNs.
Stateful active/standby failover	Tunnels not interrupted upon failure. Users do not have to reconnect or reauthenticate.	All VPN types. Not supported on ASA 5505. Additionally, routing-based failover in IPsec site-to-site VPNs.
Cluster load balancing	Load sharing. Cluster can include different Cisco ASA models and software versions.	Remote-access VPN technologies (SSL and Cisco Easy VPN).
Server load balancing	Based on ACE appliance or module installed in Cisco 7600/6500.	Acts as SSL VPN front end in clientless SSL VPN. Session stickiness in other VPNs.
QoS	Applies QoS policies to traffic classes traversing the VPN tunnel.	IPsec VPNs (Cisco Easy VPN and site-to-site).

The security appliance offers three native methods of high availability:

- Redundant peering using multiple independent Cisco ASA security appliances:** In this method, the users connect to their primary VPN server, which offers a simple but nondeterministic load-sharing method. You can define backup servers in the Cisco AnyConnect and IPsec client profile. The profile can be either provisioned locally on the client computer or downloaded from the Cisco ASA adaptive security appliance. There is no backup option in clientless SSL VPNs. IPsec site-to-site VPNs support redundant peering through the configuration of several peers that will take over when the primary gateway fails.
- Server load balancing (SLB):** This approach requires the deployment of a Cisco ACE Application Control Engine or a Cisco Catalyst 6500 Series Switch or a Cisco 7600 Series Router with an installed Cisco Application Control Engine Module (Cisco ACE Module) to dispatch the SSL VPN tunnels to multiple parallel VPN servers. The VPN servers do not have to run on identical platforms.

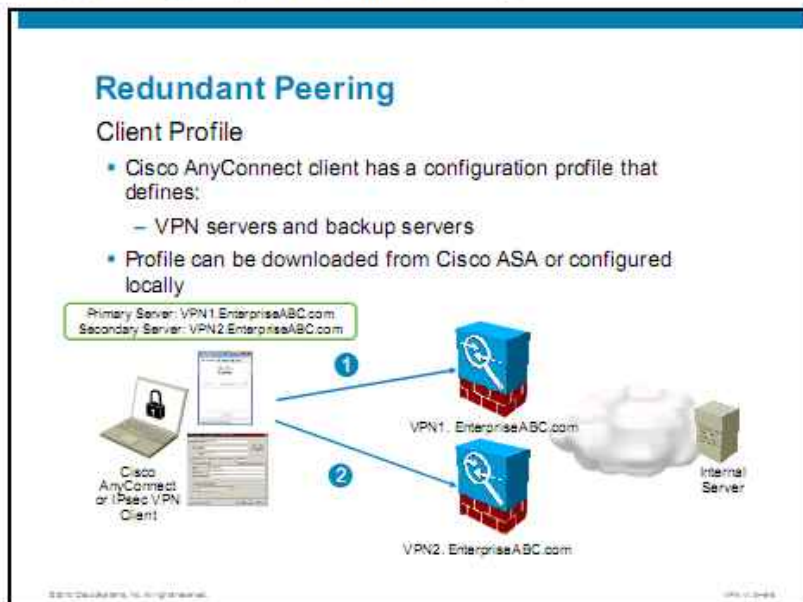
- **Active/standby failover:** Active/standby failover requires two identical adaptive security appliances that are connected to each other through a dedicated failover link. The health of the active interfaces and units is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs. This method does not provide load sharing, as active/active failover would. Active/active failover does not support VPNs. Active/standby failover can be stateless (regular) or stateful failover.

Stateful failover includes a VPN failover subsystem that enables VPN objects to be replicated to the standby unit. This method requires that the active and standby appliances are connected using a stateful failover link. The stateful failover link can be the same as the dedicated failover link.

- **Cluster load balancing:** This native mechanism shares the processing load across a cluster of SSL VPN servers without the need for any additional load balancers. The SSL VPN servers can be adaptive security appliances of any model and software version that supports Cisco AnyConnect SSL VPNs. Cluster members do not replicate the SSL VPN tunnels to other members. Therefore, when a cluster member fails, its tunnels are interrupted. The Cisco AnyConnect can leverage dead peer detection (DPD) to discover the failure and reconnect to virtual cluster address.

# Deploying Redundant Peering

This topic describes how to deploy redundant peering in full tunnel VPNs (Cisco AnyConnect VPN, Cisco Easy VPN, and site-to-site IPsec VPN).



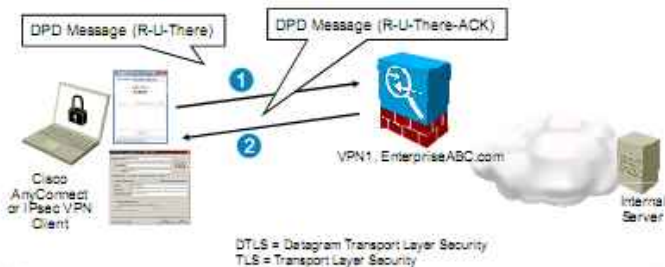
A Cisco AnyConnect or IPsec client user profile lets you identify a number of parameters, such as VPN servers and backup servers.

Usually, a user has a single profile file. This profile contains all the hosts that are needed by a user, and additional settings as needed. In some cases, you might want to provide more than one profile for a given user. The profile file is customized, and imported to the security appliance. The clients download it from the security appliance to the remote computers.

## Redundant Peering

### Dead Peer Detection

- Standards-based mechanism to check peer availability
- DPD messages exchanged when there is no tunnel traffic
- Prerequisite for DTLS-to-TLS fallback (Cisco AnyConnect)
- Configured separately for server-side and client-side (Cisco AnyConnect)



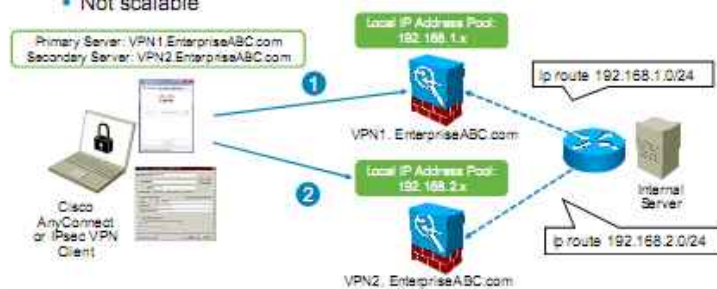
The Cisco AnyConnect and IPsec VPN clients and the security appliance use a keepalive mechanism that is called DPD to check the availability of the VPN device on the other tunnel. DPD is defined in RFC 3706 and is based on the challenge-response mechanism. If negotiated, the keepalives are exchanged only in inactivity periods, when no traffic is passing through the SSL or IPsec tunnel. Both tunnel endpoints (VPN client and Cisco ASA adaptive security appliance) can initiate DPD queries (R-U-There messages) and the other endpoint should respond with an R-U-There-ACK message. DPD is enabled by default.

If the network is unusually busy or unreliable, you might need to fine-tune the number of seconds to wait before the Cisco VPN Client decides that the peer is no longer active.

## Routing with Redundant Peers

### Local IP Address Pools

- Each Cisco ASA has its own IP address pool.
- VPN client receives address from local range.
- Static routing forwards return traffic to appropriate Cisco ASA.
- Not scalable



When multiple VPN servers are used to load balance VPN traffic or provide redundancy, you should make sure that routing delivers the traffic to the appropriate VPN client.

This figure illustrates the first option, in which the clients are assigned IP addresses taken from locally configured address pools. These ranges typically do not overlap. The internal routers are configured with static routes for the specific address ranges pointing to the appropriate security appliances.

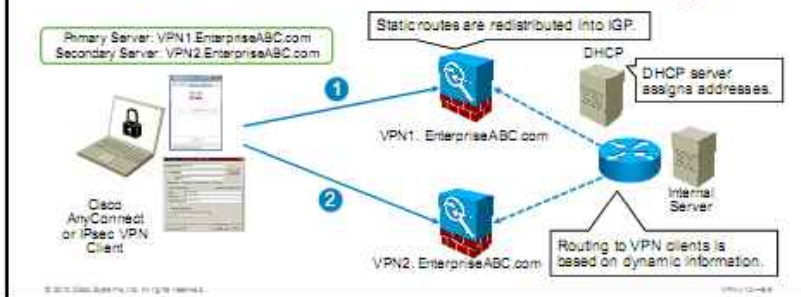
When the VPN client is connected to VPN1.EnterpriseABC.com, it receives an address from the range 192.168.1.x. It accesses resources on the Internal server. The internal router sends the return client traffic towards the primary appliance, because it has a static route for the range 192.168.1.x pointing to it.

When the primary appliance fails, the client uses the DPD mechanism to discover the failure and reconnects to VPN2.EnterpriseABC.com. It receives an IP address from the pool 192.168.2.x. It can again access internal resources. The return traffic will be sent to the secondary appliance because of the static route for the range 192.168.2.x.

## Routing with Redundant Peers

### External DHCP

- Static routes for connected clients are installed in Cisco ASA routing table automatically
- Static routes must be redistributed into internal IGP:
  - Cisco AnyConnect: redistribution has to be configured
  - IPsec VPN client: redistribution and RRI has to be configured



This figure illustrates a scenario, in which a DHCP server is used to assign IP addresses to the VPN clients. The DHCP server uses a large, flat pool of addresses, which are applied to the clients independently of the appliance, through which they connect.

With Cisco AnyConnect clients, the security appliance automatically installs static routes for the internal client addresses. These static routes are present in the security appliance routing table while the SSL VPN tunnel is up. In a Cisco Easy VPN environment, static routes for internal client addresses are also installed into the routing table.

To enable other routing devices to know these routes, the security appliance must redistribute these static routes into a running, dynamic routing protocol process. With Cisco Easy VPN, Reverse Route Injection (RRI) has to be enabled to redistribute these static routes. The Cisco ASA security appliance supports Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocols.

With such redistribution, each time a VPN client connects to the security appliance, the security appliance advertises its DHCP-obtained IP address to the distant end. When the tunnel is disconnected, the security appliance will remove the route and cease to advertise it. Therefore, a central-site device can connect to the distant end of the VPN tunnel, regardless of which security appliance is used.

## Configuring Redundant Peering

### Configuration Procedure

Cisco AnyConnect:	Cisco Easy VPN:	IPsec Site-to-Site:
1. Create profile.	1. Configure backup servers on Cisco ASA or client.	1. Configure backup servers.
2. Upload profile to Cisco ASA.	2. Tune DPD. (Optional)	2. Tune DPD. (Optional)
3. Assign profile to group or user policy.	3. Enable RRI (Optional).	3. Enable RRI. (Optional)
4. Tune DPD. (Optional)	4. Redistribute static routes into IGP. (Optional)	4. Redistribute static routes into IGP. (Optional)
5. Redistribute static routes into IGP. (Optional)		

The configuration procedure for redundant peering differs slightly depending on the VPN type.

### Cisco AnyConnect SSL VPN

In a Cisco AnyConnect SSL VPN, you will perform these tasks:

1. Create a configuration profile that is based on the profile template or use Cisco AnyConnect Client Profile Editor. The locations for the template and for the destination profile file are these:
  - **Default template (on Microsoft Windows):** \Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile\AnyConnectProfile.tmpl
  - **Final profile location:** \Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile\your-profile-name.xml
2. Upload the configuration profile to the security appliance.
3. Bind the configuration profile in a group or user policy.
4. Optionally, fine-tune DPD.
5. Optionally, redistribute static routes into interior gateway protocol (IGP).

### Cisco Easy VPN

In an IPsec remote access VPN, you will perform these tasks:

1. Configure backup servers on the Cisco ASA adaptive security appliance or client.
2. Optionally, fine-tune DPD.
3. Optionally, enable RRI.
4. Optionally, redistribute static routes into IGP.


## IPsec Site-to-Site VPN

In an IPsec site-to-site VPN, you will perform these tasks:

1. Configure backup servers.
2. Optionally, fine-tune DPD.
3. Optionally, enable RRI.
4. Optionally, redistribute static routes into IGP.

### Cisco AnyConnect Redundant Peering

#### Task 1: Create Configuration Profile



```
<ClientInitialization>
...
<BackupServerList>
  <HostAddress>VPN2.EnterpriseABC.com
</HostAddress>
</BackupServerList>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>VPN1</HostName>
    <HostAddress>VPN1.EnterpriseABC.com
    </HostAddress>
  </HostEntry>
</ServerList>
```

© 2010 Cisco Systems, Inc. All rights reserved. 999-0-0-000

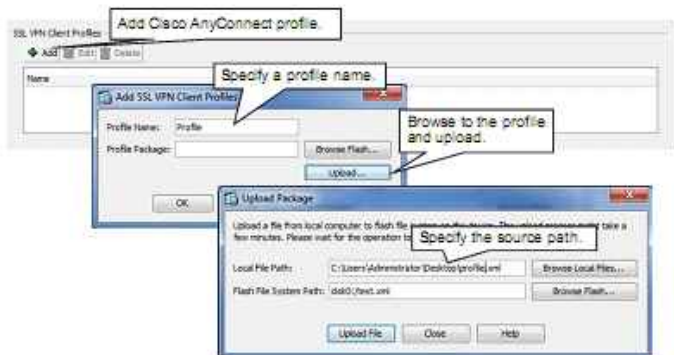
To specify backup security appliances using XML profile, complete the following steps:

- Step 1** Run the Cisco AnyConnect Client Profile Editor on a PC.
- Step 2** Select **File > New** (not shown in the figure).
- Step 3** Choose **Backup Servers** tab.
- Step 4** Specify address of the backup security appliance name in the Host Address field.
- Step 5** Click **Add**.
- Step 6** Save the profile locally by navigating to **File > Save**.



## Cisco AnyConnect Redundant Peering

### Task 2: Upload Profile to Cisco ASA

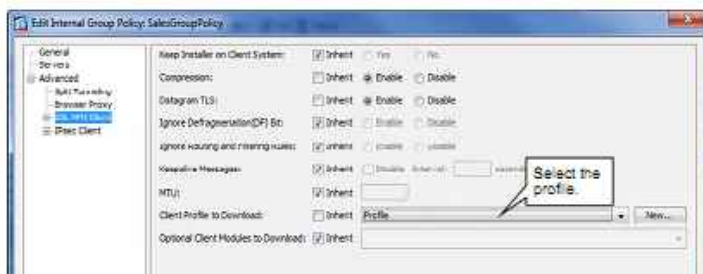


In the second Cisco AnyConnect task, you will import the configuration profile to the security appliance. Perform these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings**. This is the location where the AnyConnect image is specified. Locate the SSL VPN Client Profile area below the AnyConnect image area and choose **Add**.
- Step 2** Enter the profile name and choose one of two options:
  - **Browse Flash:** Choose this option if the profile has already been transferred to the flash memory.
  - **Upload:** Click this button to upload the profile from your local computer.
- Step 3** Enter the file path on the local computer or browse to that file using the **Browse Local Files** button. Enter the destination path in Cisco ASA security appliance flash memory, or browse to it using the **Browse Flash** button.
- Step 4** Click **Upload File**.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply the configuration.

## Cisco AnyConnect Redundant Peering

### Task 3: Assign Profile to a Group or User



Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Configuration > Device Management > Users/AAA > User Accounts

Next, you will assign the Cisco AnyConnect XML profile to a group policy or an individual user. Complete these steps if you want to assign the profile to a group policy:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
- Step 2** Select a group policy that you want to edit and click **Edit** button.
- Step 3** Choose **Advanced > SSL VPN Client > Client Profile to Download**.
- Step 4** Uncheck the **Inherit** check box and choose the required profile from the **Client Profile to Download** drop-down menu.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply configuration.

If you want to assign the XML profile to individual users, navigate to the user settings using one of these two menu paths:

- **Configuration > Remote Access VPN > AAA/Local Users > Local Users**
- **Configuration > Device Management > Users/AAA > User Accounts**

---

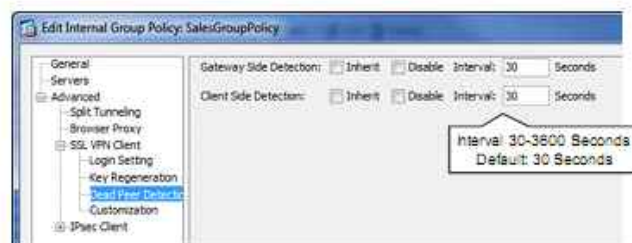
**Note** XML profiles should be applied to group policies to ensure a higher level of scalability and manageability.

---

## Cisco AnyConnect Redundant Peering

### Task 4: Tune DPD (Optional)

- Default: enabled, interval 30 seconds



Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Configuration > Device Management > Users/AAA > User Accounts

In the fourth Cisco AnyConnect task, you will configure DPD. DPD is separately enabled and configured for gateway- and client-side detection. Gateway-side detection enables the SSL server to send queries to the clients and monitor their responses. Client-side activates the equivalent process on the Cisco AnyConnect VPN Clients. The client obtains its configuration from the security appliance.

DPD can be configured at a group policy or an individual user. Complete these steps to configure DPD settings for a group policy:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
- Step 2** Select a group policy that you want to edit and click the **Edit** button.
- Step 3** Choose **Advanced > SSL VPN Client > Dead Peer Detection**.
- Step 4** Choose one of three DPD options:
  - Leave the default setting of Inherit to inherit the setting from the DfltGrpPolicy (where DPD is enabled with 30 seconds intervals for both sides).
  - Disable
  - Enter the DPD interval in the range 30 to 3600 seconds. This selection enables DPD. The default interval is 30 seconds.

You may configure DPD settings at the user level. Such a configuration overrides the setting that is applied to the policy group. This configuration is discouraged because of the complexity it may create. Navigate to the user settings using one of these two menu paths:

- **Configuration > Remote Access VPN > AAA/Local Users > Local Users**
- **Configuration > Device Management > Users/AAA > User Accounts**

## Cisco AnyConnect Redundant Peering

### CLI with Static Route Redistribution

```
router rip
network 10.0.0.0
redistribute static metric 5
version 2
no auto-summary
|
webvpn
svc profiles Profile disk0:/profile.xml
|
group-policy SalesGroupPolicy attributes
webvpn
svc dpd-interval client 30
svc dpd-interval gateway 30
svc profiles value Profile
```

Configure redistribution to IGP.

Specify Cisco AnyConnect profile location.

Configure DPD.

Assign the profile to a group policy.

This figure shows the command line interface (CLI) commands of static route redistribution into IGP). In this scenario, RIP version 2 (RIPv2) is used on the inside interface that belongs to a subnet of the 10.0.0.0/8 network. A metric is mandatory when redistributing to a distance vector IGP, such as RIP. In this example, it is set to 5. The **no auto-summary** command prevents the Cisco AnyConnect client routes from being summarized into classful networks. This IGP-related configuration can be provisioned using Cisco Adaptive Security Device Manager (Cisco ASDM), but the procedure is not presented in this course.

The remaining CLI commands have been provisioned by the Cisco ASDM in the presented configuration sequence. They describe the Cisco AnyConnect XML profile location, DPD settings of the SalesGroupPolicy, and assignment of the XML profile to the group policy.

### router rip

To start a RIP routing process and configure parameters for that process, use the **router rip** command in global configuration mode. To disable the RIP routing process, use the **no** form of this command.

### router rip

### redistribute (RIP)

To redistribute routes from another routing domain into the RIP routing process, use the **redistribute** command in router configuration mode. To remove the redistribution, use the **no** form of this command.

```
redistribute { {ospf pid [match {internal | external [1 | 2] | nssa-external [1 | 2]}} }
| static | connected | eigrp as-number } [metric {metric_value | transparent}] [route-
map map_name]
```

## redistribute (RIP) Parameters

Parameter	Description
<code>connected</code>	Specifies redistributing a network that is connected to an interface into the RIP routing process.
<code>igrp as-number</code>	Used to redistribute EIGRP routes into the RIP routing process. The <i>as-number</i> specifies the autonomous system number of the EIGRP routing process. Valid values are from 1 to 65,535.
<code>external type</code>	Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are 1 or 2.
<code>internal type</code>	Specifies OSPF metric routes that are internal to a specified autonomous system.
<code>match</code>	(Optional) Specifies the conditions for redistributing routes from OSPF to RIP.
<code>metric {metric_value   transparent}</code>	(Optional) Specifies the RIP metric value for the route being redistributed. Valid values for <i>metric_value</i> are from 0 to 16. Setting the metric to <b>transparent</b> causes the current route metric to be used.
<code>nssa-external type</code>	Specifies the OSPF metric type for routes that are external to a not-so-stubby area (NSSA); valid values are 1 or 2.
<code>ospf pid</code>	Used to redistribute an OSPF routing process into the RIP routing process. The <i>pid</i> specifies the internally used identification parameter for an OSPF routing process; valid values are from 1 to 65,535.
<code>route-map map_name</code>	(Optional) The name of the route map that is used to filter the imported routes from the source routing protocol to the RIP routing process. If not specified, all routes are redistributed.
<code>static</code>	Used to redistribute a static route into an OSPF process.

## network

To specify a list of networks for the RIP routing process, use the **network** command in router configuration mode. To remove a network definition, use the **no** form of this command.

**network** *ip\_addr*

### network Parameters

Parameter	Description
<code>ip_addr</code>	The IP address of a directly connected network. The interface that is connected to the specified network will participate in the RIP routing process.

## auto-summary

To enable the automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. To disable route summarization, use the **no** form of this command.

**auto-summary**

## webvpn

To enter webvpn mode, in global configuration mode, enter the **webvpn** command. To remove any commands that are entered with this command, use the **no webvpn** command. These **webvpn** commands apply to all WebVPN users.

These **webvpn** commands let you configure AAA servers, default group policies, default idle timeout, HTTP and HTTPS proxies, and NetBIOS Name Service (NBNS) servers for WebVPN. It also lets you configure the appearance of WebVPN screens that end users see.

## **webvpn**

### **svc profiles (webvpn)**

To specify a file as a profiles package, use the **svc profile** command from **webvpn** configuration mode. The adaptive security appliance loads the profile package in cache memory and makes it available to group policies and username attributes of Cisco AnyConnect VPN Client users.

To remove the command from the configuration and cause the adaptive security appliance to unload the package file from cache memory, use the **no** form of the command:

**svc profiles** *{profile path}*

#### **svc profiles (webvpn) Parameters**

Parameter	Description
<i>path</i>	The path and filename of the profile file in flash memory of the adaptive security appliance
<i>profile</i>	The name of the profile to create in cache

### **group-policy attributes**

To enter **group-policy** configuration mode, use the **group-policy attributes** command in **global** configuration mode. To remove all attributes from a group policy, use the **no** version of this command. In **group-policy** configuration mode, you can configure attribute-value pairs for a specified group policy or enter **group-policy webvpn** configuration mode to configure WebVPN attributes for the group.

**group-policy** *name* **attributes**

#### **group-policy attributes Parameters**

Parameter	Description
<i>name</i>	Specifies the name of the group policy.

### **webvpn (group-policy and username modes)**

To enter this **webvpn** mode, use the **webvpn** command in **group-policy** configuration mode or in **username** configuration mode. To remove all commands that are entered in **webvpn** mode, use the **no** form of this command. These **webvpn** commands apply to the username or group policy from which you configure them.

The **webvpn** commands for group policies and usernames define access to files, Messaging Application Programming Interface (MAPI) proxy, URLs, and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter.

## **webvpn**

### **svc dpd-interval**

To enable DPD on the adaptive security appliance and to set the frequency with which the remote client or the security appliance performs DPD over SSL VPN connections, use the **svc dpd-interval** command from **group policy** or **username webvpn** mode.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited.

```
svc dpd-interval {[gateway {seconds | none}] | [client {seconds | none}]}
```

#### **svc dpd-interval Parameters**

Parameter	Description
<b>gateway</b> <i>seconds</i>	Specifies the frequency, from 30 to 3600 sec, that the adaptive security appliance performs DPD.
<b>gateway</b> <b>none</b>	Disables DPD that the adaptive security appliance performs.
<b>client</b> <i>seconds</i>	Specifies the frequency, from 30 to 3600 sec, that the client performs DPD.
<b>client</b> <b>none</b>	Disables DPD that the client performs.

#### **svc profiles (group-policy or username attributes)**

To specify a Cisco AnyConnect VPN Client profiles package that is downloaded to users of the client, use the **svc profile** command from **group policy webvpn** or **username-attributes webvpn** configuration mode.

To remove the command from the configuration and cause the value it to be inherited, use the **no** form of the command.

```
svc profiles {value profile | none}
```

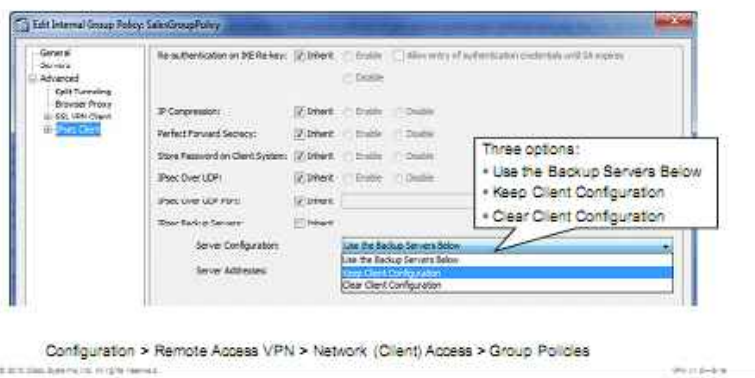
#### **svc profiles (group-policy or username attributes) Parameters**

Parameter	Description
<i>profile</i>	The name of the profile.

## Cisco Easy VPN Redundant Peering

### Task 1: Configure Backup Option on Cisco ASA

- Cisco ASA can push backup server list in mode configuration phase
- Default option: Keep Client Configuration



In the first task of Cisco Easy VPN configuration procedure, you define how the clients obtain the backup server information. Complete these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
- Step 2** Create a new or edit an existing group policy and choose **Advanced > IPsec Client** submenu.
- Step 3** Locate the IPsec Backup Servers area and choose one of these options in the Server Configuration field:
  - **Keep Client Configuration** (the default option)
  - **Use the Backup Servers Below**
  - **Clear Client Configuration**



## Cisco Easy VPN Redundant Peering

### Task 1: Configure Backup Option on Cisco ASA (Cont.)



Configuration > Remote Access VPN > Network (Client) Access > Group Policies

- Step 4** If you selected the option Use the Backup Servers Below, you will configure the backup server list in the Server Addresses field. Enter a space, colon, or semicolon delimited list of IP addresses or hostnames. The list is pushed to the VPN client in the mode configuration phase and it overwrites any setting that may have existed on the client.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply the configuration.

## Cisco Easy VPN Redundant Peering

### Task 1: Configure Backup Servers on Client

- Client shows list of locally configured backup servers
- List is cleared when Cisco ASA is set to Clear Client Configuration



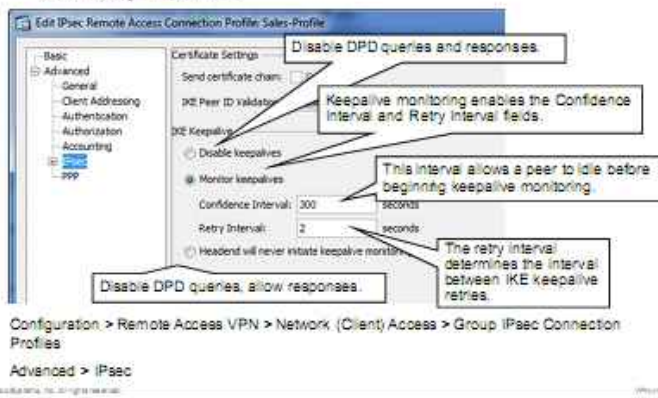
If the security appliance is configured for the default setting of Keep Client Configuration, you may enter the backup server list on the VPN client. Choose the Backup Servers tab and click **Add** to add a new backup server to the list. You have the option of removing or reordering server entries. The locally configured list is cleared when the Cisco ASA adaptive security appliance is configured using Clear Client Configuration.

The list is ordered according to the server priorities. When the primary server fails, the first server from the list is used, followed by the next entries, if the first server is unavailable.

## Cisco Easy VPN Redundant Peering

### Task 2: Tune DPD (Optional)

- Default: Enabled (Monitor Keepalives), Confidence Interval: 300, Retry Interval: 2



In the next task of the Cisco Easy VPN configuration sequence, you may optionally tune DPD parameters. Complete these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group IPsec Connection Profiles**.
- Step 2** Create a new or edit an existing connection profile and choose **Advanced > IPsec** submenu.
- Step 3** Locate the IKE Keepalive area and choose one of these options:
  - **Disable Keepalives.**
  - **Monitor keepalives:** This option enables or disables IKE keepalive monitoring. Selecting this option enables the Confidence Interval and Retry Interval fields:
    - **Confidence Interval:** specifies the number of seconds the adaptive security appliance should allow a peer to idle before beginning keepalive monitoring. The minimum is 10 seconds; the maximum is 300 seconds. The default for a remote access group is 300 seconds.
    - **Retry Interval:** specifies number of seconds to wait between IKE keepalive retries. The default is 2 seconds.
  - **Headend Will Never Initiate Keepalive Monitoring:** Choose this option to configure the central-site adaptive security appliance to never initiate keepalive monitoring.

---

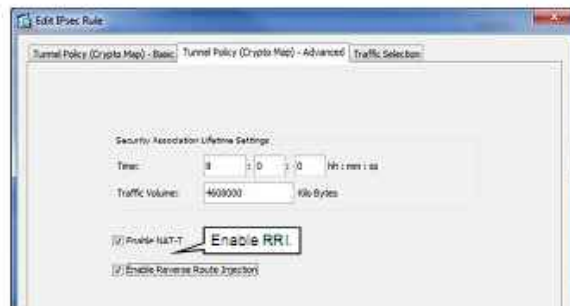
**Note** DPD configuration for Cisco Easy VPN differs from the approach that is used in full tunnel SSL VPNs.

---

- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration.

## Cisco Easy VPN Redundant Peering

### Task 3: Enable RRI (Optional)



Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps

© 2010 Cisco Systems, Inc. All rights reserved.

VPN 11-0-0-00

In the last Cisco Easy VPN configuration task, you can optionally enable RRI by completing these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps**.
- Step 2** Edit the existing IPsec rule. The default IPsec rule number 65535 is configured to match any IP traffic and matches a whole range of Cisco Easy VPN Internet Key Exchange (IKE) proposals. If you want to match using other criteria, you may add a new IPsec rule.
- Step 3** Select the **Tunnel Policy (Crypto Map) – Advanced** tab.
- Step 4** Check the **Enable Reverse Route Injection** check box.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply the configuration.

## Cisco Easy VPN Redundant Peering

### CLI Configuration

```
group-policy SalesGroupPolicy attributes
backup-servers vpn2.enterpriseABC.com vpn3.enterpriseABC.com
vpn4.enterpriseABC.com
!
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set reverse-route
!
tunnel-group Sales-Profile ipsec-attributes
isakmp keepalive threshold 300 retry 2
```

Configure backup servers.

Enable RRI.

Tune DPD.

The figure illustrates the CLI commands that are used to configure Cisco Easy VPN redundant peering. Use the **backup-servers** command in group-policy configuration mode to define a backup server list appliance.

Use the **set reverse-route** keyword to enable RRI for a crypto map.

Use the **isakmp keepalive** command in tunnel configuration mode to tune DPD.

### backup-servers

To configure backup servers, use the **backup-servers** command in group-policy configuration mode. To remove a backup server, use the **no** form of this command. To remove the backup-servers attribute from the running configuration, use the **no** form of this command without arguments. This enables inheritance of a value for backup servers from another group policy.

IPsec backup servers let a VPN client connect to the central site when the primary adaptive security appliance is unavailable. When you configure backup servers, the adaptive security appliance pushes the server list to the client as the IPsec tunnel is established.

**backup-servers** {*server1 server2 ... server10*} | **clear-client-config** | **keep-client-config**

#### backup-servers Parameters

Parameter	Description
<b>clear-client-config</b>	Specifies that the client uses <i>no</i> backup servers. The adaptive security appliance pushes a null server list.
<b>keep-client-config</b>	Specifies that the adaptive security appliance sends <i>no</i> backup server information to the client. The client uses its own backup server list, if configured.
<i>server1 server2 ... server10</i>	Provides a space that is delimited, priority-ordered list of servers for the VPN client to use when the primary adaptive security appliance is unavailable. Identifies servers by IP address or hostname. The list can be 500 characters long, but can contain only 10 entries.

## crypto dynamic-map set reverse route

See the **crypto map set reverse-route** command for additional information about this command.

**crypto dynamic-map** *dynamic-map-name* *dynamic-seq-num* **set reverse route**

### crypto dynamic-map set reverse route Parameters

Parameter	Description
<i>dynamic-map-name</i>	Specifies the name of the crypto map set
<i>dynamic-seq-num</i>	Specifies the number that you assign to the crypto map entry

## tunnel-group ipsec-attributes

To enter ipsec-attribute configuration mode, use the **tunnel-group ipsec-attributes** command in global configuration mode. This mode is used to configure settings that are specific to the IPsec tunneling protocol.

To remove all IPsec attributes, use the **no** form of this command.

**tunnel-group** *name* **ipsec-attributes**

### tunnel-group ipsec-attributes Parameters

Parameter	Description
<b>ipsec-attributes</b>	Specifies attributes for this tunnel-group
<i>name</i>	Specifies the name of the tunnel-group

## isakmp keepalive

To configure IKE DPD, use the **isakmp keepalive** command in tunnel-group ipsec-attributes configuration mode. In every tunnel group, IKE keepalives are enabled by default with default threshold and retry values. To return the keepalive parameters to enabled with default threshold and retry values, use the **no** form of this command.

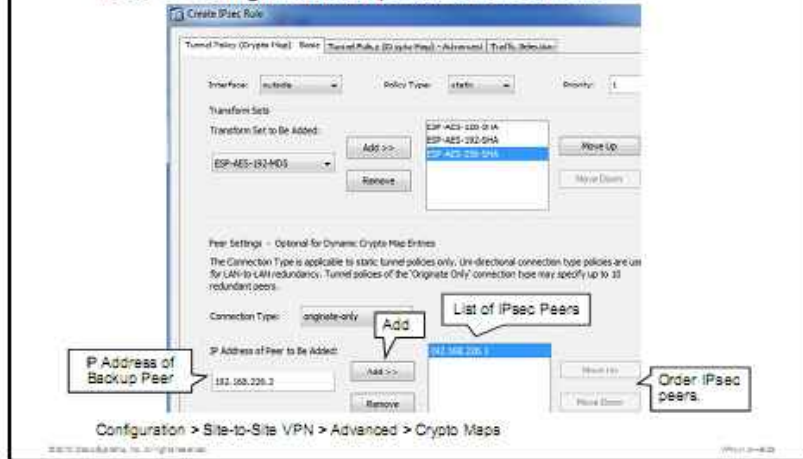
**isakmp keepalive** [**threshold** *seconds*] [**retry** *seconds*] [**disable**]

### isakmp keepalive Parameters

Parameter	Description
<b>disable</b>	Disables IKE keepalive processing, which is enabled by default.
<b>retry</b> <i>seconds</i>	Specifies the interval in seconds between retries after a keepalive response has not been received. The range is 2–10 sec. The default is 2 sec.
<b>threshold</b> <i>seconds</i>	Specifies the number of seconds the peer can idle before beginning keepalive monitoring. The range is 10–3600 sec. The default is 10 sec for a LAN-to-LAN group, and 300 sec for a remote access group.

## IPsec Site-to-Site Redundant Peering

### Task 1: Configure Backup Server or Servers



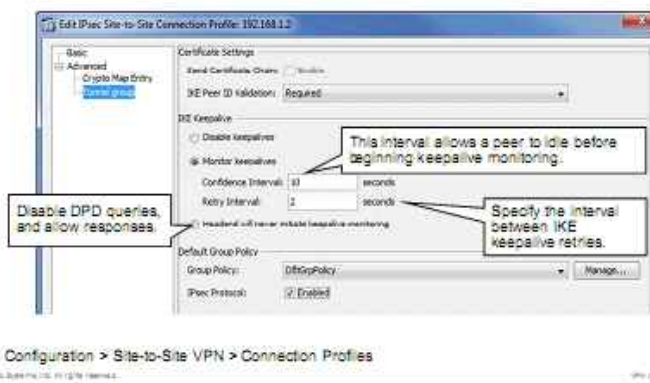
To configure redundant site-to-site IPsec peering using Cisco ASDM, complete the following configuration steps:

- Step 1** Choose **Configuration > Site-to-Site VPN > Advanced > Crypto Maps**.
- Step 2** Click **Add**. Create IPsec Rule dialog-box appears. Click the **Tunnel Policy (Crypto Map) – Basic** tab.
- Step 3** Enter the IP address of a backup peer into the IP Address of Peer to Be Added field.
- Step 4** Click **Add**.
- Step 5** Repeat the previous two steps to add other backup peers.
- Step 6** Click **OK**.
- Step 7** Click **Apply** to apply the configuration.

## IPsec Site-to-Site Redundant Peering

### Task 2: Tune DPD (Optional)

- Default: Enabled (Monitor Keepalives), Confidence Interval: 10, Retry Interval: 2



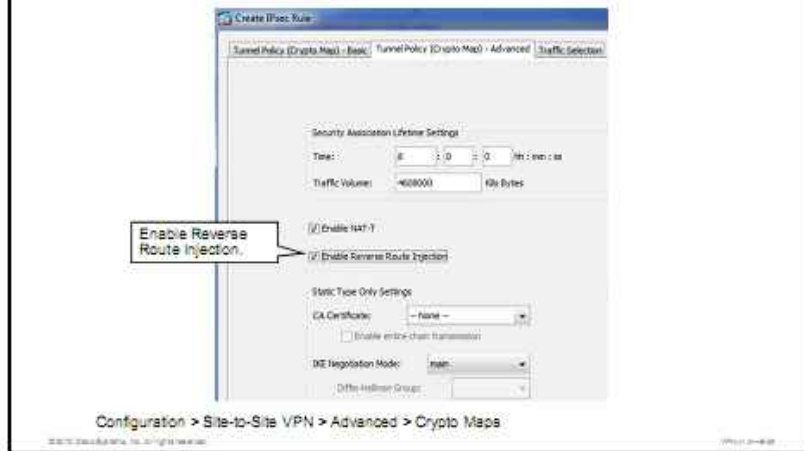
To tune the DPD settings in IPsec site-to-site VPNs, complete these steps:

- Step 1** Choose **Configuration > Site-to-Site VPN > Connection Profiles**.
- Step 2** Select the appropriate connection profile and click **Edit**.
- Step 3** Choose **Advanced > Tunnel group**.
- Step 4** Locate the IKE keepalives area and adjust the DPD parameters. They have been discussed in the Cisco Easy VPN configuration sequence.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply configuration.



## IPsec Site-to-Site Redundant Peering

### Task 3: Configure RRI (Optional)

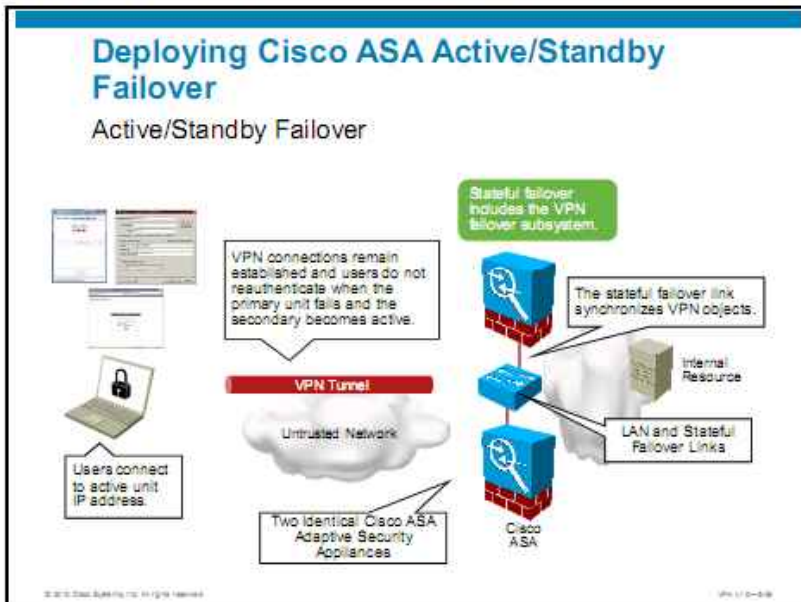


To enable Reverse Route Injection using Cisco ASDM, complete the following steps:

- Step 1** Choose **Configuration > Site-to-Site VPN > Advanced > Crypto Maps**.
- Step 2** Create a new or edit an appropriate IPsec rule.
- Step 3** Click the **Tunnel Policy (Crypto Map) – Advanced** tab.
- Step 4** Check the **Enable Reverse Route Injection** check box to enable RRI.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply the configuration.

# Deploying Cisco ASA Adaptive Security Appliance Active/Standby Failover

This topic describes how to deploy active/standby failover for SSL and IPsec VPNs.



This figure illustrates the active/standby failover pair that provides high-availability service to SSL and IPsec VPNs. Configuring high availability requires two identical adaptive security appliances that are connected to each other through a dedicated failover link and, optionally, a stateful failover link. The health of the active interfaces and units is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

The adaptive security appliance supports two failover configurations, active/active failover, and active/standby failover. Active/active failover does not support any VPN termination, neither IPsec nor SSL.

In stateless (regular) failover, all active connections and tunnels are dropped when the active unit fails. Clients need to re-establish the tunnels when the new active unit takes over.

When stateful failover is enabled, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same tunnel and connection information is available at the new active unit. The clients are not required to reconnect to keep the tunnel established. To use stateful failover, you must configure a stateful failover link to pass all state information, using one of three options:

- Use a dedicated Ethernet interface for the stateful failover link. If you are using a dedicated Ethernet interface for the stateful failover link, you can use either a switch or a crossover cable. If you use a switch, no other hosts or routers should be on this link.
- Share the failover link, if you are using LAN-based failover.
- Share a regular data interface, such as the inside interface. This option is not recommended.

## Deploying Cisco ASA Active/Standby Failover

### Considerations

Method	Considerations
Stateless failover	Does not support VPN failover. Stateful failover is mandatory to synchronize VPN elements. Stateless failover is not recommended.
Stateful failover	VPN connections remain established. Recommended method for all VPN types (VPN failover subsystem). Clientless features not supported with stateful failover: Smart tunnels Port forwarding Plug-ins Java applets IPv6 clientless or Cisco AnyConnect sessions Citrix authentication (Citrix users must reauthenticate after failover)
Both failover methods	Username, passwords and pre-shared keys (PSKs) used for establishing the tunnels exchanged over failover link. Encryption with failover key strongly recommended.

Stateless (regular) failover is discouraged because it does not support VPN failover.

Stateful failover offers these high-availability features:

- It includes VPN failover subsystem.
- VPN tunnels remain established.
- Users do not need to reauthenticate at failover.

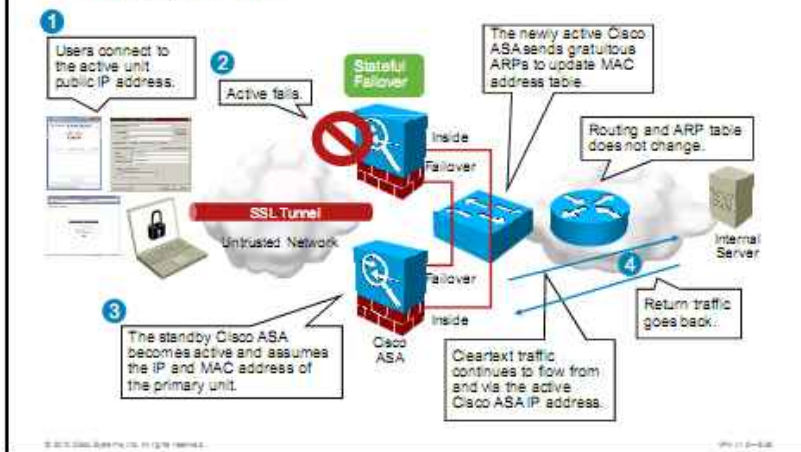
The following clientless SSL VPN features are not supported with stateful failover:

- Smart tunnels
- Port forwarding
- Plug-ins
- Java applets
- IP version 6 (IPv6) clientless or Cisco AnyConnect sessions
- Citrix authentication (Citrix users must reauthenticate after failover)

In both failover types (stateless and stateful), you should be aware of a potential security vulnerability of the communications between the failover units. Username, passwords, and other information that is used for establishing the sessions is exchanged over the failover link in cleartext. To prevent an attacker from eavesdropping on that exchange, encryption with a failover key is strongly recommended in VPN environments.

## Deploying Cisco ASA Active/Standby Failover

### Failover Routing



This figure illustrates the routing in an active/standby failover scenario. Both failover units are configured with an active and standby IP address and MAC address on each interface. When the primary unit fails, the secondary unit takes over the active IP address and MAC address. The routing and Address Resolution Protocol (ARP) tables on the adjacent routers do not change when the failover occurs. The adjacent switch needs to update its MAC address table that defines the binding of attached MAC addresses to its local ports. The newly active security appliance triggers the update by sending gratuitous ARP packets, from which the switch learns that the MAC address moved to another interface.

The path of the cleartext traffic that flows between the active unit and the internal server changes on the adjacent switch when the failover occurs. The routing information on the internal routers does not change.

The flow of traffic in a failover scenario is depicted in several steps:

1. The VPN user establishes a VPN connection with the primary address of the public Cisco ASA security appliance interface.
2. The active unit fails.
3. The standby security appliance becomes active and assumes the IP and MAC address of the primary unit.
4. VPN and cleartext traffic continue to flow via the active security appliance. Return traffic is delivered to the currently active Cisco ASA security appliance for one of two reasons:
  - **In full tunnel VPNs (Cisco AnyConnect or IPsec):** The cleartext return traffic is destined to the internal client IP address. This address is reachable via the active unit address.
  - **In clientless SSL VPNs:** The cleartext return traffic is destined to the active unit address, because the Cisco ASA adaptive security appliance acts as an SSL proxy for clientless SSL VPN sessions.

## Deploying Cisco ASA Active/Standby Failover

### Configuration Tasks

1. Configure failover link.
2. Configure active and standby addresses on interfaces used for traffic forwarding.
3. Define failover criteria.

To configure active/standby failover, you will perform the same tasks as in non-VPN scenarios:

1. Configure a failover link.
2. Configure active and standby addresses on interfaces that are used for traffic forwarding.
3. Define failover criteria.

Before you configure active/standby failover, you have to gather certain input parameters. They include the following:

- **LAN failover interface:** This interface is the interface that is used for exchanging failover information.
- **State failover interface:** This interface is used for exchanging state information.
- **Preferred role:** This role defines the active/standby role when both units are operational.
- **Interface list:** This list includes a list of interfaces on both failover units.
- **IP addressing:** This addressing information contains active/standby addresses on all interfaces, including the failover interface.
- **(Optional) Failover encryption key:** This key is the key that is used to encrypt failover messages that are exchanged between the units.
- **(Optional) MAC addresses:** Active and standby MAC addresses of the Cisco ASA security appliance interfaces can be configured manually or using the Cisco ASDM.

## Configuring Active/Standby Failover

### Task 1: Configure Failover Link

Configuration > Device Management > High Availability > Failover

Setup [ interfaces | criteria | MAC-Addresses ]

Specify a standby ASA to take over network connectivity in the event that the active unit fails.

Enable failover  Use 32 hexadecimal character key

Shared Key: [ ]

Parameters of the Failover Link

LAN Failover

Interface: [ GigabitEthernet0/0 ] Logical Name: [ Failover ]

Active IP: [ 192.168.2.1 ] Standby IP: [ 192.168.2.1 ]

Subnet Mask: [ 255.255.255.0 ] Preferred Role:  Primary  Secondary

State Failover

Interface: [ GigabitEthernet0/0 ]

Active IP: [ ] Standby IP: [ ]

Subnet Mask: [ ]

Role

Enable HTTP replication

These settings are needed if the state failover link is different from LAN failover.

HTTP state replication is disabled by default.

Configuration > Device Management > High Availability > Failover

© 2010 Cisco Systems, Inc. All rights reserved. IPN 11-0-000

In the first configuration task, you will enable failover, configure the failover link, and set generic failover parameters. Complete the following steps:

- Step 1** Choose **Configuration > Device Management > High Availability > Failover**.
- Step 2** Make sure that the Setup tab is selected.
- Step 3** Check the **Enable Failover** check box.
- Step 4** Locate the LAN Failover area, select the LAN failover interface, and configure its parameters: logical name, active and standby address, and subnet mask.
- Step 5** Choose the interface that is used for State Failover, and optionally (if it differs from the LAN failover interface) configure its parameters.
- Step 6** Select the preferred unit role: primary or secondary.
- Step 7** Optionally, check the check box, activating the encryption key and enter the key string.
- Step 8** Optionally, check the **Enable HTTP Replication** check box to activate the stateful synchronization of HTTP sessions. This setting is not required for Cisco AnyConnect VPNs but may be desired for other access types.
- Step 9** Click **Apply** to apply the configuration.

## Configuring Active/Standby Failover

### Task 2: Configure Active/Standby Interface Addresses

Configuration > Device Management > High Availability > Failover

Setup | Interfaces | Criteria | MAC Addresses |

Define interface standby IP addresses and monitoring status. Double-click on a standby address to edit. Press the Tab or Enter key after editing an address.

Interface Name	Active IP Address	Subnet Mask/ Pref. Length	Standby IP Ad.	Monitored
-dmz	192.168.1.1	255.255.255.0	192.168.1.3	<input checked="" type="checkbox"/>
-inside	10.0.0.1	255.255.255.0	10.0.0.3	<input checked="" type="checkbox"/>
outside	172.16.0.1	255.255.255.0	172.16.0.3	<input checked="" type="checkbox"/>

Address Used for Active Unit

Address Used on Standby Unit

This setting controls which interfaces affect failover:

- Disable monitoring of irrelevant interfaces.
- Enable monitoring of relevant interfaces (the default).

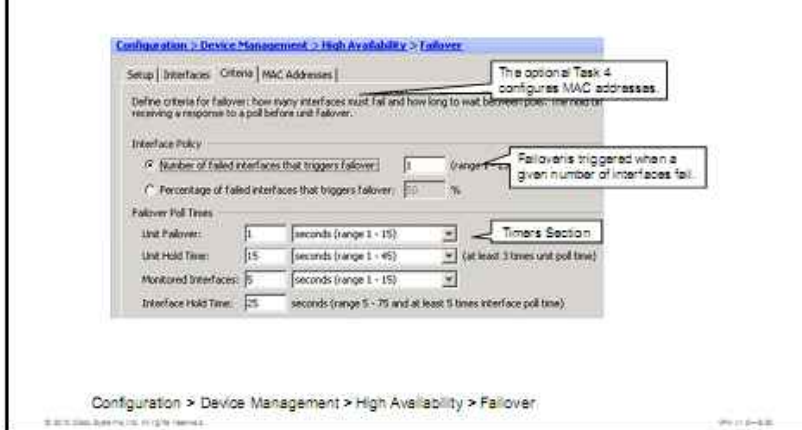
Configuration > Device Management > High Availability > Failover

In the second configuration task, you will configure the active and standby IP addresses for each interface participating in failover. Complete the following steps:

- Step 1** Choose the **Interfaces** tab in the **Configuration > Device Management > High Availability > Failover** submenu.
- Step 2** Configure the active and standby IP address for each interface. You can enter IP addresses by selecting the respective field in the configuration table.
- Step 3** Optionally, choose the interfaces that should be excluded from monitoring by unchecking their **Monitored** check boxes. By default, all interfaces are monitored and therefore affect the selection of the active unit.
- Step 4** Click **Apply** to apply the configuration.

## Configuring Active/Standby Failover

### Task 3: Configure Failover Criteria



In the third configuration task, you will configure the criteria that trigger the failover event. Complete the following steps:

- Step 1** Choose the **Criteria** tab in the **Configuration > Device Management > High Availability > Failover** submenu.
- Step 2** Optionally, locate the **Interface Policy** area and choose one of two thresholds that trigger failover:
  - **Number of failed interfaces that triggers failover.** The default number of failed interfaces that triggers failover is 1.
  - **Percentage of failed interfaces that triggers failover.**
- Step 3** Optionally, locate the **Failover Poll Times** area, and modify any of these timers:
  - **Unit Failover:** Default 1 second.
  - **Unit Hold Time:** Default 15 seconds.
  - **Monitored Interfaces:** Default 5 seconds.
  - **Interface Hold Time:** Default 25 seconds.

In the fourth configuration task, you may optionally set the active and standby MAC addresses for each of the failover interfaces (not shown in the figure). Complete the following steps:

- Step 1** Choose the **MAC Addresses** tab in the **Configuration > Device Management > High Availability > Failover > MAC Addresses** submenu.
- Step 2** Configure the desired MAC addresses.



## Configuring Active/Standby Failover

### CLI Configuration

```
interface GigabitEthernet0/0
ip address 172.16.0.1 255.255.255.0 standby 172.16.0.3
interface GigabitEthernet0/1
ip address 10.0.0.1 255.255.255.0 standby 10.0.0.3
interface GigabitEthernet0/2
ip address 192.168.1.1 255.255.255.0 standby 192.168.1.3
!
interface GigabitEthernet0/3
description LAN/STATE Failover Interface
!
failover lan unit primary
failover lan interface Failover GigabitEthernet0/3
failover polltime unit 2 holdtime 10
failover polltime interface 4 holdtime 20
failover interface-policy 10%
failover key *****
failover link Failover GigabitEthernet0/3
failover interface ip Failover 192.168.2.1 255.255.255.0 standby
192.168.2.3
failover
```

Configure active and standby IP addresses.

Configure failover.

This figure illustrates the CLI configuration that is applied to the security appliance as a result of the presented procedure. Each interface has two IP addresses that are associated with it: active and standby. GigabitEthernet0/3 is configured as a LAN and state failover interface. This device acts as the active unit when both units are operational. The failover messages are secured using a configuration key. The timers have been set to nondefault values to be presented in the configuration output.

### failover lan unit

To configure the adaptive security appliance as the primary or secondary unit in a LAN failover configuration, use the **failover lan unit** command in global configuration mode. To restore the default setting, use the **no** form of this command.

**failover lan unit** {primary | secondary}

#### failover lan unit Parameters

Parameter	Description
<b>primary</b>	Specifies the adaptive security appliance as a primary unit
<b>secondary</b>	Specifies the security appliance as a secondary unit

### failover lan interface

To specify the interface that is used for failover communication, use the **failover lan interface** command in global configuration mode. To remove the failover interface, use the **no** form of this command.

**failover lan interface** *if\_name* {*phy\_if* [*.sub\_if*] | *vlan\_if*}

## failover lan interface Parameters

Parameter	Description
<i>if_name</i>	Specifies the name of the adaptive security appliance interface dedicated to failover
<i>phy_if</i>	Specifies the physical interface
<i>sub_if</i>	(Optional) Specifies a subinterface number
<i>vlan_if</i>	Used on the Cisco ASA 5505 Adaptive Security Appliance to specify a VLAN interface as the failover link.

## failover interface ip

To specify the IP version 4 (IPv4) address and mask or IPv6 address and prefix for the failover interface and the stateful failover interface, use the **failover interface ip** command in global configuration mode. To remove the IP address, use the **no** form of this command.

**failover interface ip** *if\_name* [*ip\_address mask standby ip\_address* | *ipv6\_address/prefix standby ipv6\_address*]

## failover interface ip Parameters

Parameter	Description
<i>if_name</i>	Interface name for the failover or stateful failover interface
<i>ip_address mask</i>	Specifies the IP address and mask for the failover or stateful failover interface on the primary device
<i>ipv6_address</i>	Specifies the IPv6 address for the failover or stateful failover interface on the primary device
<i>prefix</i>	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address)
<i>standby ip_address</i>	Specifies the IP address that is used by the secondary device to communicate with the primary device
<i>standby ipv6_address</i>	Specifies the IPv6 address that is used by the secondary device to communicate with the primary device

## failover link

To specify the stateful failover interface, use the **failover link** command in global configuration mode. To remove the stateful failover interface, use the **no** form of this command.

**failover link** *if\_name* [*phy\_if*]

## failover link Parameters

Parameter	Description
<i>if_name</i>	Specifies the name of the adaptive security appliance interface that is dedicated to stateful failover.
<i>phy_if</i>	(Optional) Specifies the physical or logical interface port. If the stateful failover interface is sharing the interface that is assigned for failover communication or sharing a standard firewall interface, then this argument is not required.

## failover key

To specify the key for encrypted and authenticated communication between units in a failover pair, use the **failover key** command in global configuration mode. To remove the key, use the **no** form of this command.

**failover key** {*secret* | *hex key*}

### failover key Parameters

Parameter	Description
<i>hex key</i>	Specifies a hexadecimal value for the encryption key. The key must be 32 hexadecimal characters (0–9, a–f).
<i>secret</i>	Specifies an alphanumeric shared secret. The secret can be from 1 to 63 characters. Valid characters are any combination of numbers, letters, or punctuation. The shared secret is used to generate the encryption key.

## failover replication http

To enable HTTP (port 80) connection replication, use the **failover replication http** command in global configuration mode. To disable HTTP connection replication, use the **no** form of this command.

**failover replication http**

## failover

To enable failover, use the **failover** command in global configuration mode. To disable failover, use the **no** form of this command.

**failover**

## failover polltime

To specify the failover unit poll and hold times, use the **failover polltime** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

**failover polltime** [*unit*] [*msec*] *poll\_time* [*holdtime* [*msec*] *time*]

### failover polltime Parameters

Parameter	Description
<i>holdtime time</i>	(Optional) Sets the time during which a unit must receive a hello message on the failover link, after which the peer unit is declared failed. Valid values are from 3 to 45 sec or from 800 to 999 ms if the optional <b>msec</b> keyword is used.
<i>msec</i>	(Optional) Specifies that the given time is in milliseconds.
<i>poll_time</i>	Amount of time between hello messages. Valid values are from 1 to 15 sec or from 200 to 999 ms if the optional <b>msec</b> keyword is used.
<i>unit</i>	(Optional) Indicates that the command is used for unit poll and hold times. Adding this keyword to the command does not have any affect on the command. However, it can make it easier to differentiate this command from the <b>failover polltime interface</b> commands in the configuration.

## failover polltime interface

To specify the data interface poll and hold times in an active/standby failover configuration, use the **failover polltime interface** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

**failover polltime interface** [*msec*] *time* [*holdtime time*]

### failover polltime interface Parameters

Parameter	Description
<code>holdtime time</code>	(Optional) Sets the time during which a data interface must receive a hello message on the data interface, after which the peer is declared failed. Valid values are from 5 to 75 sec.
<code>interface time</code>	Specifies the poll time for interface monitoring. Valid values range from 1 to 15 sec. If the optional <code>msec</code> keyword is used, the valid values are from 500 to 999 ms.
<code>msec</code>	(Optional) Specifies that the given time is in milliseconds.

## Configuring Active/Standby Failover

### Implementation Guidelines

Consider the following implementation guidelines:

- Active/standby failover is the simplest high-availability method, but does not provide load sharing; this is the recommended method if only high availability is desired.
- All VPN configuration is automatically replicated between units; however, VPN-related files, such as images (Cisco AnyConnect, Cisco Secure Desktop), profiles and plug-ins must be manually provisioned to both devices.
- In Cisco ASA software version 8.2 (and earlier), you need both units to have the same licenses, or use shared licensing or both.

You should follow these implementation guidelines when planning the deployment of active/standby failover for Cisco AnyConnect SSL VPNs:

1. Active/standby failover is the simplest method for providing high availability, but it does not provide load sharing. Active/standby failover should be deployed if only high availability, but no load balancing, is desired.
2. All VPN configuration is automatically replicated between units; however, VPN-related files, such as images (Cisco AnyConnect, Cisco Secure Desktop), profiles, and plug-ins must be manually provisioned to both devices.
3. In Cisco ASA adaptive security appliance software version 8.2 (and earlier), you need both units to have the same licenses, use shared licensing, or both.

# Deploying Dynamic-Routing-Based VPN Failover

This topic describes how to implement dynamic routing to achieve IPsec site-to-site VPN high availability.

## Deploying Dynamic-Routing-Based Failover in IPsec Site-to-Site VPNs

### Overview

- Dynamic routing can be used across multiple IPsec site-to-site VPN tunnels to provide high availability.
- One tunnel is primary, another is secondary path.
- Cisco ASA supports OSPF over IPsec without GRE.
- OSPF traffic between two Cisco ASA security appliances is encrypted using IPsec.



Dynamic routing protocols are one of the most efficient and scalable tools that can be used to provide high availability in tunnel-based IPsec VPNs. In cases where multiple tunnels exist from one site to another (as in the example), one tunnel can be designated as the primary path and another as the secondary path. Routing protocol is used to select a primary tunnel based on a routing protocol metric. Cisco ASA adaptive security appliance supports Open Shortest Routing Protocol (OSPF) routing protocol over IPsec without Generic Routing Encapsulation (GRE). It supports OSPF as needed when running routing protocols over IPsec tunnels on Cisco IOS routers. OSPF traffic between two security appliances is encrypted using IPsec and is used to detect a failure on the primary path. In case of failure, the primary path is removed from the routing table and the secondary path is inserted.

## Deploying Dynamic-Routing-Based Failover in IPsec Site-to-Site VPNs

### Configuration Tasks

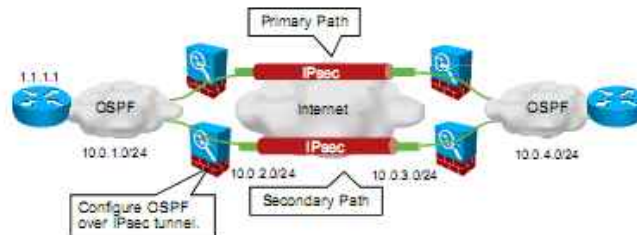
1. Add OSPF as interesting traffic to IPsec tunnel.
2. Enable OSPF process.
3. Specify advertised networks.
4. Set OSPF network type to nonbroadcast.
5. Change OSPF cost of one path.
6. Manually configure OSPF neighbor.

To implement OSPF dynamic routing through an IPsec site-to-site tunnel, you will perform these tasks:

1. Add OSPF as interesting traffic to IPsec tunnel.
2. Enable the OSPF process.
3. Specify advertised networks. When you specify advertised networks, you have to specify remote networks also.
4. Set the OSPF network type to nonbroadcast, because IPsec VPN does not support multicast traffic.
5. Change the OSPF cost of one path to prefer one path.
6. Manually configure an OSPF neighbor, because the Cisco ASA adaptive security appliance will not be able to detect a neighbor automatically.

## Deploying Dynamic-Routing-Based Failover in IPsec Site-to-Site VPNs

### Configuration Scenario

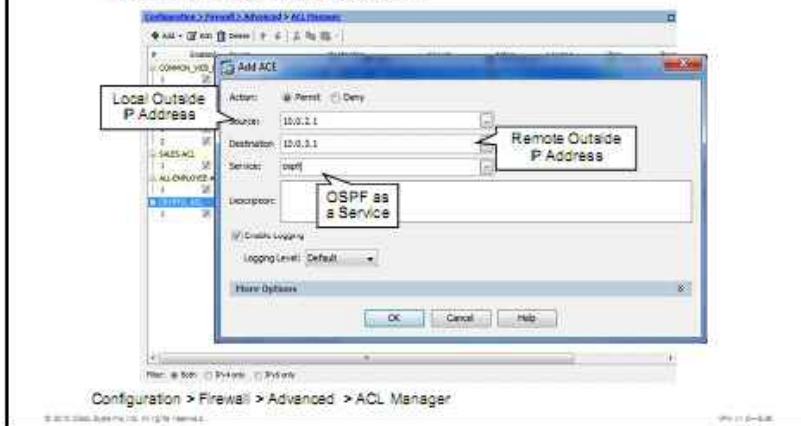


The figure shows an example that will be used as the configuration scenario in the ongoing configuration tasks. You will enable OSPF over IPsec VPN tunnel on the Cisco ASA adaptive security appliance. You will advertise all needed networks and specify the peer security appliance manually. The example will show configuration on the lowest left security appliance in the figure only. The configuration on other Cisco ASA security appliances is similar and it will not be shown in the example.

## Deploying Dynamic-Routing-Based Failover in IPsec Site-to-Site VPNs

### Task 1: Add OSPF as Interesting Traffic

- Add OSPF traffic to IPsec ACL.



The OSPF traffic that is exchanged between the outside interfaces must be included in access list defining IPsec VPN interesting traffic. Enable OSPF to be tunneled through the IPsec VPN tunnel by completing these steps:

- Step 1** Choose **Configuration > Firewall > Advanced > ACL Manager** (not shown in the figure).
- Step 2** Select the access list that is used for the existing VPN tunnel (not shown in the figure).
- Step 3** Right-click the access list and click **Insert** in order to insert a new row to the access list (not shown in the figure).
- Step 4** In the Source field, enter the IP address of the interface-terminating VPN tunnel on the local site. In the example, this is 10.0.2.1.
- Step 5** In the Destination field, enter the IP address of the remote site interface-terminating VPN tunnel. In the example, this is 10.0.3.1.
- Step 6** In the Service field, enter **ospf**.
- Step 7** Click **OK** and **Apply** to apply the configuration to the Cisco ASA security appliance.
- Step 8** Repeat the procedure on the remote side of the VPN tunnel.



## Deploying Dynamic-Routing-Based Failover in IPsec Site-to-Site VPNs

### Task 2: Enable OSPF Process

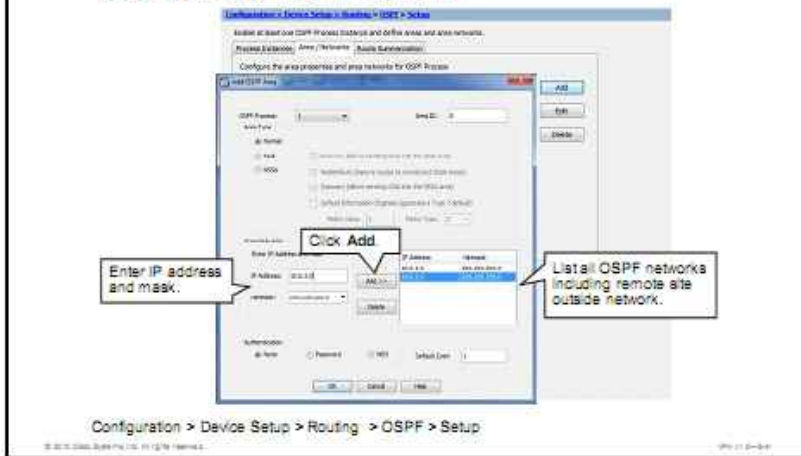


To configure the OSPF process on Cisco ASA adaptive security appliance, complete the following steps:

- Step 1** Choose **Configuration > Device Setup > OSPF > Setup** (not shown in the figure).
- Step 2** Make sure that the Process Instances tab is selected.
- Step 3** Check **Enable this OSPF Process** check box.
- Step 4** In the **OSPF Process ID** field, enter a number for the OSPF process ID. You can use any number. In the example, 1 is used as OSPF process number.
- Step 5** Click **Apply** to apply the configuration.

## Deploying Dynamic-Routing-Based Failover in IPsec Site-to-Site VPNs

### Task 3: Specify OSPF Networks

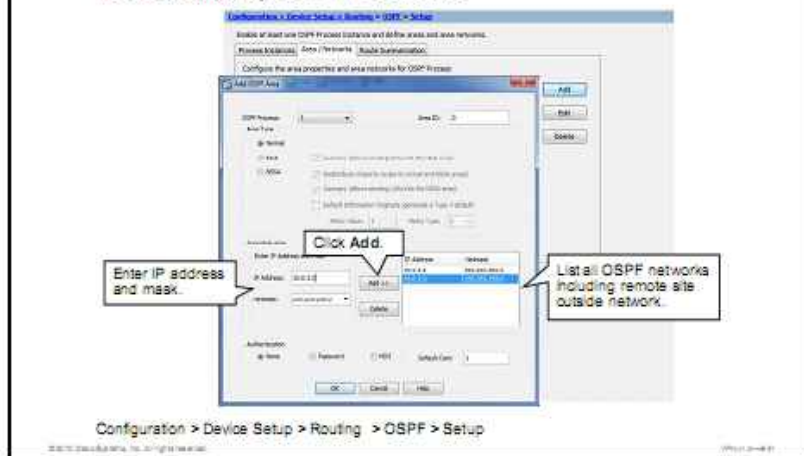


Complete these steps to configure OSPF networks using Cisco ASDM:

- Step 1** Choose **Configuration > Device Setup > OSPF > Setup** (not shown in the figure).
- Step 2** Choose the **Area/Networks** tab and click **Add** (not shown in the figure).
- Step 3** In the **Area ID** field, enter a number for the area ID.
- Step 4** In **Area Networks** area, enter all the networks that will be included in the OSPF routing process. Enter at least the networks of both VPN endpoints. Click the **Add** button for each network you want to add. In the example, 10.0.1.0/24, 10.0.2.0/24, and 10.0.3.0/24 networks have been added.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply the configuration.

## Deploying Dynamic-Routing-Based Failover in IPsec Site-to-Site VPNs

### Task 3: Specify OSPF Networks



To configure the OSPF nonbroadcast network type, complete these steps:

- Step 1** Choose **Configuration > Device Setup > OSPF > Interface** (not shown in the figure).
- Step 2** Click the **Properties** tab.
- Step 3** Select the interface that terminates the VPN and click **Edit**.
- Step 4** Disable OSPF broadcast by unchecking the **Broadcast** check box. In the example, broadcast is disabled for the outside interface.
- Step 5** Change the OSPF cost of an interface by entering a number into the **Cost** field. In the example, the tunnel over that Cisco ASA adaptive security appliance will be secondary, so you have to increase OSPF cost. In the example, OSPF cost of the outside interface is set to 20.
- Step 6** Click **OK**.
- Step 7** Click **Apply** to apply the configuration.

## Deploying Dynamic-Routing-Based Failover in IPsec Site-to-Site VPNs

### Task 5: Configure OSPF Neighbor



To configure an OSPF neighbor manually, complete these steps:

- Step 1** Choose **Configuration > Device Setup > OSPF > Static Neighbor** (not shown in the figure).
- Step 2** Click **Add**.
- Step 3** Select the OSPF process number from the OSPF Process drop-down menu. In the example, OSPF process 1 is selected.
- Step 4** Enter the IP address of the VPN remote peer into the Neighbor field. In the example, 10.0.3.1 is entered.
- Step 5** Select the interface toward the remote peer from the Interface drop-down menu. In the example, the outside interface is selected.
- Step 6** Click **OK**.
- Step 7** Click **Apply** to apply the configuration.

## Deploying Dynamic-Routing-Based Failover in IPsec Site-to-Site VPNs

### CLI Configuration

```
access-list CRYPTO_ACL line 1 extended permit ip 10.0.1.0
255.255.255.0 10.0.4.0 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255.0 area 0
 network 10.0.2.0 255.255.255.0 area 0
 network 10.0.1.0 255.255.255.0 area 0
 neighbor 10.0.3.1 interface outside
!
interface GigabitEthernet0/0
 ospf network point-to-point non-broadcast
 ospf cost 20
```

Annotations:

- Enable the OSPF process.
- Add OSPF to the crypto ACL.
- Specify advertised networks.
- Manually specify the neighbor.
- Change the OSPF cost.
- Enable unicast OSPF.

To configure dynamic routing-based failover, use the following CLI commands. First, use the **access-list** command to add OSPF traffic to the crypto access list. Then enable the OSPF process using the **router ospf** command. Then specify the advertised networks using the **network area** command. Then specify the neighbor on the other side of the IPsec VPN tunnel using the **neighbor interface** command.

Finally, enter interface configuration mode and disable OSPF broadcast on an interface using the **ospf network point-to-point non-broadcast** command. Change the OSPF cost using the **ospf cost** command.

### router ospf

To start an OSPF routing process and configure parameters for that process, use the **router ospf** command in global configuration mode. To disable OSPF routing, use the **no** form of this command.

**router ospf** *pid*

### router ospf Parameters

Parameter	Description
<i>pid</i>	Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65,535. The <i>pid</i> does not need to match the ID of OSPF processes on other routers.

## network area

To define the interfaces on which OSPF runs and to define the area ID for those interfaces, use the **network area** command in router configuration mode. To disable OSPF routing for interfaces that are defined with the address/netmask pair, use the **no** form of this command.

**network** *addr mask area area\_id*

### network area Parameters

Parameter	Description
<i>addr</i>	IP address.
<b>area</b> <i>area_id</i>	Specifies the area that is to be associated with the OSPF address range. The <i>area_id</i> can be specified in either IP address format or in decimal format. When it is specified in decimal format, valid values range from 0 to 4,294,967,295.
<i>mask</i>	The network mask.

## neighbor

To define a static neighbor on a point-to-point nonbroadcast network, use the **neighbor** command in router configuration mode. To remove the statically defined neighbor from the configuration, use the **no** form of this command. The **neighbor** command is used to advertise OSPF routes over VPN tunnels.

**neighbor** *ip\_address* [*interface name*]

### neighbor Parameters

Parameter	Description
<i>interface name</i>	(Optional) The interface name, as specified by the <b>nameif</b> command, through which the neighbor can be reached
<i>ip_address</i>	IP address of the neighbor router

## ospf network point-to-point non-broadcast

To configure the OSPF interface as a point-to-point nonbroadcast network, use the **ospf network point-to-point non-broadcast** command in interface configuration mode. To remove this command from the configuration, use the **no** form of this command. The **ospf network point-to-point non-broadcast** command lets you transmit OSPF routes over VPN tunnels.

**ospf network point-to-point non-broadcast**

## ospf cost

To specify the cost of sending a packet through the interface, use the **ospf cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

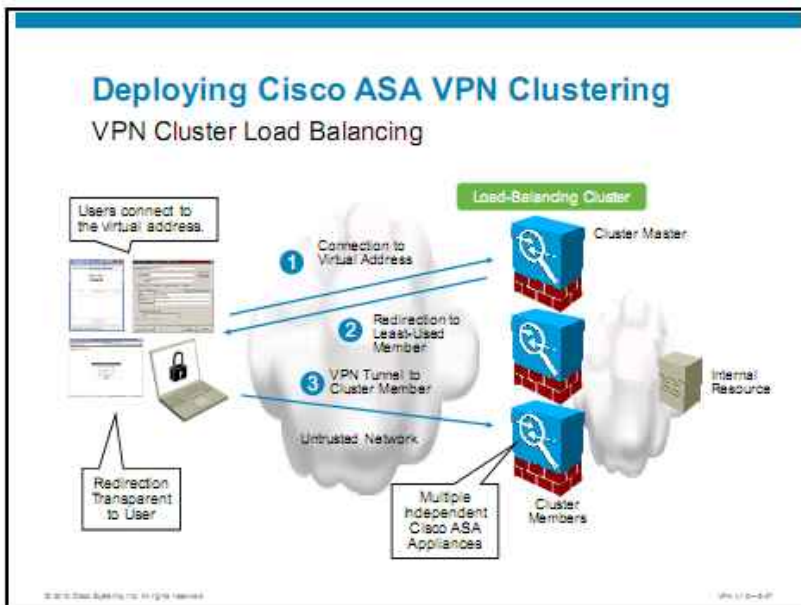
**ospf cost** *interface\_cost*

## ospf cost Parameters

Parameter	Description
<code>interface_cost</code>	<p>The cost (a link-state metric) of sending a packet through an interface. This is an unsigned integer value from 0 to 65,535. The 0 represents a network that is directly connected to the interface, and the higher the interface bandwidth, the lower the associated cost to send packets across that interface. In other words, a large cost value represents a low-bandwidth interface and a small cost value represents a high-bandwidth interface.</p> <p>The OSPF interface default cost on the adaptive security appliance is 10. This default differs from Cisco IOS Software, where the default cost is 1 for Fast Ethernet and Gigabit Ethernet and 10 for 10BASE-T. This information is important to take into account if you are using Equal-Cost Multipath (ECMP) in your network.</p>

# Deploying Cisco ASA Adaptive Security Appliance VPN Clustering

This topic describes the deployment of VPN load-balancing clusters.



In cluster load balancing, a group of security appliances work together as a single entity, a cluster. The cluster is known by one IP address, a virtual address, to the outside users. This virtual IP address is not tied to a specific physical device in the VPN cluster but will be serviced by the cluster virtual cluster master. The virtual IP address is a valid, routable address. When a user attempts to connect to the cluster address, the virtual cluster master redirects the request to the physical IP address of the least-loaded security appliance. The user then attempts to establish a tunnel with it.

Connections to the load-balancing cluster are based on the load. The designated virtual cluster master security appliance maintains load information from all secondary security appliances in the cluster. Each secondary security appliance periodically sends load information in a keepalive message exchange to the master security appliance. Load is calculated as a percentage of current active sessions that are divided by the configured maximum-allowed connections.

Cluster load balancing supports all types of remote access (SSL and IPsec) VPNs.

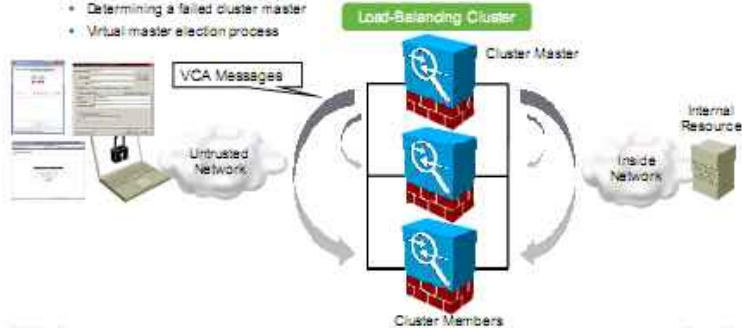


## Deploying Cisco ASA VPN Clustering

### Virtual Cluster Agent Messages

VCA messages used for:

- Cluster joins and leaves
- Establishing IPsec connections between peers in the cluster
- Calculating the load
- Sending periodic load and health check information to master
- Determining a failed cluster master
- Virtual master election process



For load balancing to operate, the Virtual Cluster Agent (VCA) is started on each security appliance when the security appliance begins participation in the virtual cluster. VCA is responsible for the following:

- Joining and exiting the virtual cluster
- Establishing IPsec connections between peers in the cluster
- Calculating the load
- Sending periodic load and health check information to the cluster master
- Determining a failed cluster master
- Participating in a virtual master election process

For VCA messages to flow between the cluster master and members, the public and private interfaces must be configured and added to the virtual cluster.

## Deploying Cisco ASA VPN Clustering

### Certificate Types in VPN LB

Certificate Format Version	Version 3
Certificate Serial Number	12457501
Signature Algorithm Identifier for CA	RSA with SHA-1
Issuer X.509 Name	CAUS O=C=us O=CA
Validity Period	Start=04/01/10 Expire=04/01/15
Subject X.509 Name	C=us OU=us domain.com
Subject Public Key Information	788CE0C84DC714C...
Subject Alternative Name	C=us OU=us domain.com
Subject Alternative Name	C=us OU=us domain.com
Subject Alternative Name	C=us OU=us domain.com
CA Signature	200807FE08E920D4394B...

Unified Communications Certificate (UCC)

Certificate Format Version	Version 3
Certificate Serial Number	12457501
Signature Algorithm Identifier for CA	RSA with SHA-1
Issuer X.509 Name	CAUS O=C=us O=CA
Validity Period	Start=04/01/10 Expire=04/01/15
Subject X.509 Name	*.domain.com
Subject Public Key Information	788CE0C84DC714C...
Extensions (v3)	
CA Signature	200807FE08E920D4394B...

Wildcard Certificate

Server-side certificate authentication requires special attention in cluster load balancing. It is used in both SSL VPN types (Cisco AnyConnect and clientless), and in IPsec VPN mutual authentication.

The VPN endpoint verifies the server certificate at the initial connection to the master, and then after the client is redirected to a participant. Certification verification should succeed independently of the elected cluster member, to which the user is redirected. Three types of certificates can be used in the cluster load-balancing scenario:

- **Standard X.509 identity certificate:** In this case, the common name attribute of the subject name field is set to the Domain Name System (DNS) name of the VPN server. Clients match the DNS name of the VPN server against the subject common name and then verify the certificate. This certificate type does not offer any load-balancing options.
- **Unified Communications Certificate (UCC):** Also called multiple-domain certificate, it uses an extension that is called Subject Alternative Name (SAN) to define an alternative trusted subject name. This feature is ideally suited for cluster load balancing.
- **Wildcard certificate:** This type uses a special notation of the subject name to indicate all hosts that belong to a specific domain. This option is considered less secure than UCC, but can be easily deployed in a cluster.

## Deploying Cisco ASA VPN Clustering

### Certificate Deployment

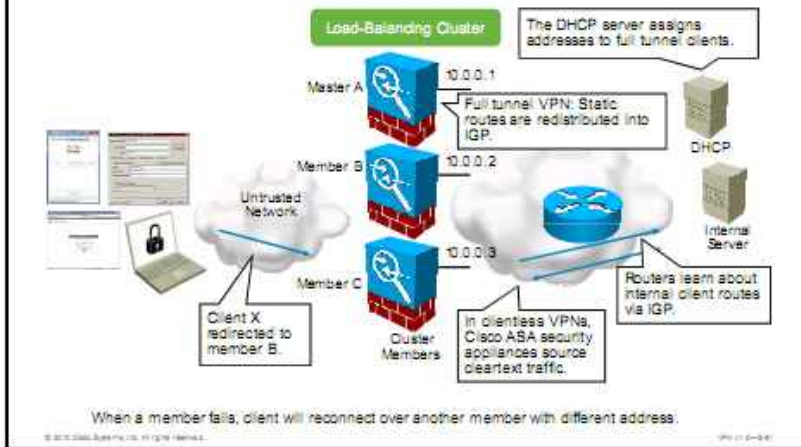
Feature	Unified Client Certificate (UCC)	Multiple or Wildcard Certificates
Number of certificates	Single certificate with multiple embedded Subject Alternative Name (SAN) extensions.	Multiple: N+1 certificates: one for virtual server, and one for each member Wildcard: 1.
Support and usage	Many certificate authority (CA) vendors, such as Entrust and VeriSign support UCC. Recommended option.	Wildcard certificates limited to single domain
Benefits	More trusted because UCC defines cluster members. Less expensive than purchasing multiple individual certificates. Tunnel redirection before AAA authentication.	Supported by all CAs Tunnel redirection to a host with trusted certificate Tunnel redirection before AAA authentication
Deployment procedure	UCC installed on each Cisco ASA.	Wildcard installed on each Cisco ASA or member certificates installed on each Cisco ASA Cluster certificate installed on each Cisco ASA

The three certificate options have pros and cons that are associated with them:

- **UCC:** The UCC is issued for the fully qualified domain name (FQDN) of the cluster master. The SANs, which are fields of the UCC, specify each cluster member. UCCs are supported by several public key infrastructure (PKI) vendors, such as Entrust or VeriSign. The UCC is installed on all devices in the cluster. When a client is redirected to a member, the certification verification succeeds and the user is not warned. The UCC is recommended as the best-practice deployment option.
- **Multiple individual certificates:** This option requires separate certificates for the IP address and FQDN of the virtual server and each cluster member. Therefore, for N devices in the cluster, you will need N+1 certificates. When a client is redirected to a member, the individual certificate of that member is verified. If the certificate is trusted by the user, the tunnel is established to the member. Multiple individual certificates are considered inferior to the UCC, because the cost of multiple certificates will typically exceed the cost of a single UCC.
- **Wildcard certificate:** This approach requires a single certificate that is issued for an FQDN that does not contain a common name and can therefore be used on multiple devices that share the remaining FQDN attributes. The wildcard certificate is installed on all devices in a cluster. When a client is redirected to a member, the certification verification succeeds and the user is not warned. Wildcard certificates are discouraged in favor of the UCC because of these limitations:
  - A UCC is more secure than wildcard certificates because a UCC specifies exactly which hosts and domains are to be protected.
  - A UCC is more flexible than wildcard certificates since a UCC is not limited to a single domain.

## Deploying Cisco ASA VPN Clustering

### Routing



This figure illustrates the routing in a load-balancing cluster.

After a client is redirected to a given cluster member, the user communicates with that member using its IP address or FQDN. The session remains attached to that member until it is terminated. If the member fails, the user will have to reconnect to the virtual server again.

The routing differs based on the VPN type:

- **Full tunnel VPN (Cisco AnyConnect or Cisco Easy VPN):** If the member assigns client addresses out of its local address pool, and the address pools do not overlap among the cluster members, the internal routers are typically configured with static routes to reach the internal client addresses over the appropriate appliance. If, however, an external DHCP server is deployed to assign client addresses, the appliances must redistribute client routes into the internal routing domain.
- **Clientless SSL VPN:** The cleartext traffic that traverses the internal network is sourced from the current cluster member, because the appliances act as SSL proxies in the clientless SSL VPNs.

## Deploying Cisco ASA VPN Clustering

### Considerations

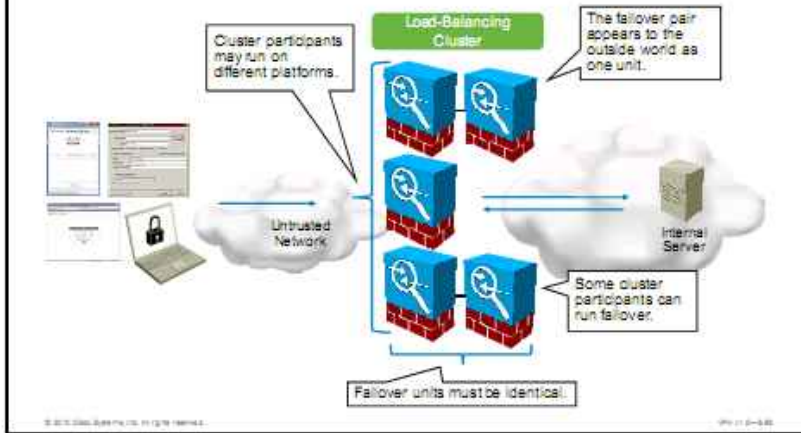
Feature or Scenario	Description
IP address or FQDN-based redirection	Default: Master redirects to IP address. Master can redirect the client at a FQDN rather than IP address. Relevant for certificate validation. FQDN option requires appropriate reverse DNS records (PTR). Resolution performed on Cisco ASA, not remote computer. Can be manual, such as: <code>name 10.10.1.1 asa-cluster.example.com</code> <code>name 10.10.1.2 asa1.example.com</code>
Failure of the current member	When the used cluster member goes down, client automatically reconnects to the virtual cluster address. Client-side DPD must be enabled.
Failure of the master	Another member takes over the master role. Virtual address served by the new master.
Licensing	Multiple devices active at the same time. The VPN licenses are added together to calculate the total number of VPN sessions per cluster.

You should consider these aspects when deploying Cisco ASA security appliance VPN clusters:

- **Redirection method:** The cluster master can be configured to redirect clients to cluster members using either their IP addresses or FQDNs. By default, the redirection is based on IP addresses. Both methods work with certificates, but the configured method must reflect the type of the certificate subject name. The FQDN-based redirection should be configured to avoid certificate hostname mismatch popup warnings when the certificates have been issued for hostnames rather than IP addresses. The FQDN-based redirection requires that appropriate reverse DNS records (pointer records, or PTRs) exist for the involved hostnames. The Cisco ASA security appliance, not the client, must be able to perform this resolution. If DNS is not available, you can configure the resolution manually, similarly to the `name 10.10.1.1 asa-cluster.example.com` and `name 10.10.1.2 asa1.example.com` commands.
- **Failure of the current member:** In this situation, the cluster does not offer an automated recovery. The user must reconnect to the virtual cluster address or FQDN.
- **Failure of the master:** An election procedure is triggered. Another member becomes the master and resumes its responsibilities.
- **Licensing:** In a VPN cluster, multiple devices are active at the same time. The licenses that are installed on each member may differ. The license units are added to calculate the total number of sessions per cluster.

## Deploying Cisco ASA VPN Clustering

### Combining VPN Clustering and Failover



This figure presents how cluster load balancing can be combined with active/standby stateful failover. Some or all of the cluster members can be implemented as a failover pair. The combination of cluster load balancing and active/standby stateful failover offers both load sharing and redundancy. If an active unit fails, the secondary unit takes over the active unit IP and MAC addresses and continues its operations as the cluster member. The VPN connections that are served by the member are maintained by the secondary unit. However, the files, such as images, profiles, or plug-ins, must be installed on each unit separately.

## Deploying Cisco ASA VPN Clustering

### Configuration Tasks

1. Install UCC or multiple server certificates.
2. Configure a cluster IP address.
3. (Optional) Configure encryption.
4. Configure an internal and external interface.
5. (Optional) Configure member priority.
6. (Optional) Configure FQDN-based redirection.

Perform the following tasks to configure Cisco ASA adaptive security appliance VPN clustering:

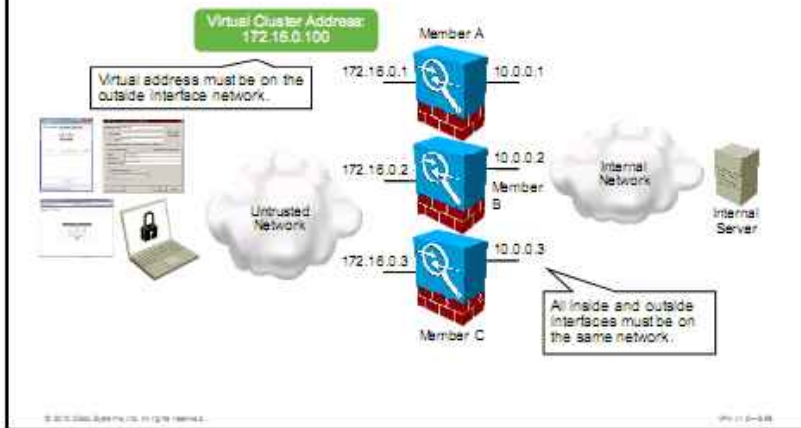
1. Install a UCC or multiple server certificates.
2. Configure the cluster IP address.
3. Optionally, configure encryption.
4. Optionally, configure the internal and external interface.
5. Optionally, configure member priority.
6. Optionally, configure FQDN-based redirection.

Before deploying cluster load balancing, you have to gather these input parameters:

- **Certificate parameters:** The required information includes the identity of the certificate authority (CA) and the supported enrollment method. The subject name depends on the certificate deployment option: UCC, multiple individual certificates, or a wildcard certificate. UCC will contain SAN extensions.
- **Cluster IP address:** This is the IP address that the clients use to access the VPN server.
- **UDP port:** This port is dedicated to communications between cluster master and cluster members.
- **IPsec encryption password:** This encryption key is used to protect communications between cluster participants.
- **Public and private interfaces:** Internal and external interfaces must belong to the same internal and external subnet.
- **Priority:** Number from 1 to 10, which indicates the likelihood of this device becoming the virtual cluster master, either at start-up or when an existing master fails. Device with higher priority is more likely to become the master.

## Deploying Cisco ASA VPN Clustering

### Configuration Scenario



This figure illustrates the network scenario that is used in the upcoming configuration tasks. The cluster consists of three adaptive security appliances, which are connected to the same internal subnet 10.0.0.0/24 and external subnet 172.16.0.0/24. The virtual cluster address is set to 172.16.0.100. The virtual cluster address must belong to the external subnet.



## Deploying Cisco ASA VPN Clustering

### Task 1A: Install UCC or Wildcard Certificate

1. On the master, configure a trustpoint.
  - **crypto ca import certificate**
2. On the master, import the UCC certificate.
  - **crypto ca export asa-cluster pkcs12 passphrase**
3. On the master, export the trustpoint certificate and keys as PKCS #12.
  - **crypto ca export asa-cluster pkcs12 passphrase**
4. On each member, import the PKCS #12.
  - **crypto ca import asa-cluster pkcs12 passphrase**

In the first task of the configuration scenario, you will install the certificates on the security appliances participating in the cluster. Follow these steps to install a UCC or wildcard certificate:

- Step 1** On the cluster master configure one trustpoint name pointing to the virtual cluster. The following configuration is an example configuration:
- ```
crypto ca trustpoint asa-cluster
subject-name CN=cluster.company.com, OU=Department, O=Company
enrollment terminal
```
- Step 2** On the cluster master, import the UCC certificate using the **crypto ca import certificate** command. The adaptive security appliance prompts you to paste the certificate to the terminal in base-64 format.
- Step 3** On the master, export the trustpoint as Public Key Cryptography Standard (PKCS) #12 using the **crypto ca export trustpoint-name pkcs12 passphrase** command. This operation exports both the certificate and private- and public-key pair. Copy the resulting output and save it to a text file.
- Step 4** On each member, import the PKCS #12 using the **crypto ca import trustpoint-name pkcs12 passphrase** command.

## Deploying Cisco ASA VPN Clustering

### Task 1B: Install Multiple Certificates

1. On each member, configure two trustpoints:
  - Cluster
  - Individual
2. On each member, import a certificate for the individual trustpoint.
3. On the master, import the cluster certificate.
4. On the master, export the cluster certificate and keys as PKCS #12.
  - **crypto ca export trustpoint-name pkcs12 passphrase**
5. On each member, import the PKCS #12.
  - **crypto ca import trustpoint-name pkcs12 passphrase**

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-11-0-007

Alternatively you may install separate individual certificates on each member by completing these steps:

- Step 1** On each member, configure two trustpoints: for the cluster and for the individual member. The following configuration is an example configuration:

```
crypto ca trustpoint asa-cluster
subject-name CN=cluster.company.com,OU=Department,O=Company
enrollment terminal
!
crypto ca trustpoint member1
subject-name CN=member1.company.com,OU=Department,O=Company
enrollment terminal
```

- Step 2** On each member, import the individual certificate using the **crypto ca import certificate** command. The adaptive security appliance prompts you to paste the certificate to the terminal in base-64 format.
- Step 3** On the master, import the cluster certificate using the **crypto ca import certificate** command. The adaptive security appliance prompts you to paste the certificate to the terminal in base-64 format.
- Step 4** On the master, export the cluster trustpoint as PKCS #12 using the **crypto ca export trustpoint-name pkcs12 passphrase** command. This operation exports both the cluster certificate and private- and public-key pair. Copy the resulting output and save it to a text file, as in this example:
- ```
crypto ca export asa-cluster pkcs12 cisco123
```
- Step 5** On each member, import the pkcs12 using the **crypto ca import trustpoint-name pkcs12 passphrase** command, as in this example:
- ```
crypto ca import asa-cluster pkcs12 cisco123
```

**Note** When you are using individual certificates, two certificates are needed for SSL VPN only. In IPsec VPN, which uses IKE for authentication, the certificate subject name is not verified. Therefore, one certificate, signed by a trusted CA, is adequate.

## Deploying Cisco ASA VPN Clustering

### Tasks 2-6: Configure Cluster Parameters

Configuration > Remote Access VPN > Load Balancing

Participate in Load Balancing Cluster

VPN Cluster Configuration

All servers in the cluster must get an identical cluster configuration.

Cluster IP address: 172.16.0.100 UDP port: 9023

Enable IPsec encryption

IPsec shared secret: \*\*\*\*\* Verify secret: \*\*\*\*\*

VPN Server Configuration

Public interface: outside Priority: 5

Private interface: inside NAT assigned IP address:

As a VPN cluster master, this device can send a fully qualified domain name (FQDN) using reverse DNS lookup of a cluster device, instead of its outside IP address, when redirecting VPN client connections to that cluster device.

Send FQDN to client instead of an IP address when redirecting

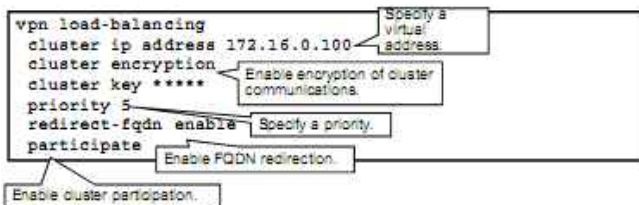
Configuration > Remote Access VPN > Load Balancing

In the remaining configuration tasks, you will configure the load-balancing parameters. Complete the following tasks:

- Step 1** Choose **Configuration > Remote Access VPN > Load Balancing**.
- Step 2** Check the **Participate in Load Balancing Cluster** check box.
- Step 3** In the VPN Cluster Configuration area, enter the cluster IP address and User Datagram Protocol (UDP) port for intracluster communications. In the example, cluster IP address is set to 172.16.0.100.
- Step 4** Optionally, enable IPsec encryption of intracluster signaling by checking the **Enable IPsec Encryption** check box, and enter the IPsec shared secret.
- Step 5** In the VPN Server Configuration area, choose the public and private interfaces from the respective drop-down menus.
- Step 6** Set the priority for this member by entering a number into the Priority field. The range is from 1 to 10. The priority indicates the likelihood of this device becoming the virtual cluster master, either at start-up or when an existing master fails. The higher you set the priority, the more likely it is that this device becomes the virtual cluster master. In the example, the priority is set to 5.
- Step 7** Optionally, enable FQDN-based redirection by checking the **Send FQDN to Client Instead of an IP Address when Redirecting** check box.
- Step 8** Click **Apply** to apply the configuration.

## Deploying Cisco ASA VPN Clustering

### CLI Configuration



To enable the Cisco ASA adaptive security appliance to participate in VPN clustering using command line interface (CLI), use the following commands. First enter **vpn load-balancing** mode using the **vpn load-balancing** command. Then specify IP address of a cluster using the **cluster ip address** command. Then enable encryption for message exchange between the cluster and the Cisco ASA adaptive security appliances using the **cluster encryption** command and specify the shared key using the **cluster key** command. Then use the **priority** command to specify the priority of a member in a cluster. Enable FQDN redirection when using certificate authentication using the **redirect-fqdn enable** command. Finally, enable cluster participation using the **participate** command.

### vpn load-balancing

To enter **vpn load-balancing** mode, in which you can configure VPN load balancing and related functions, use the **vpn load-balancing** command in global configuration mode.

#### vpn load-balancing

**Note** To use VPN load balancing, you must have a Cisco ASA 5510 Adaptive Security Appliance with a Plus license or a Cisco ASA 5520 Adaptive Security Appliance or higher. VPN load balancing also requires an active Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) license. The security appliance checks for the existence of this cryptographic license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing. It also prevents internal configuration of 3DES by the load-balancing system unless the license permits this usage.

### cluster ip address

To set the IP address of the virtual load-balancing cluster, use the **cluster ip address** command in **vpn load-balancing** configuration mode. To remove the IP address specification, use the **no** form of this command.

#### cluster ip address *ip-address*

## cluster ip address Parameters

| Parameter         | Description                                                                   |
|-------------------|-------------------------------------------------------------------------------|
| <i>ip-address</i> | The IP address that you want to assign to the virtual load-balancing cluster. |

## cluster encryption

To enable encryption for messages that are exchanged on the virtual load-balancing cluster, use the **cluster encryption** command in vpn load-balancing configuration mode. To disable encryption, use the **no** form of this command.

### cluster encryption

---

**Note** VPN load balancing requires an active 3DES or AES license. The security appliance checks for the existence of this cryptographic license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing. It also prevents internal configuration of 3DES by the load-balancing system unless the license permits this usage.

---

## cluster key

To set the shared secret for IPsec site-to-site tunnel exchanges on the virtual load-balancing cluster, use the **cluster key** command in vpn load-balancing configuration mode. To remove this specification, use the **no** form of this command.

**cluster key** *shared-secret*

### cluster key Parameters

| Parameter            | Description                                                                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>shared-secret</i> | A 3- through 17-character string defining the shared secret for the VPN load-balancing cluster. Special characters can appear in the string, but not spaces. |

## priority

To enable QoS priority queuing (PQ), use the **priority** command in class configuration mode. For critical traffic that cannot tolerate latency, such as VoIP, you can identify traffic for low latency queuing (LLQ) so that it is always transmitted at a minimum rate. To remove the priority requirement, use the **no** form of this command.

**priority**

## redirect-fqdn

To enable or disable redirection using a fully-qualified domain name in vpn load-balancing mode, use the **redirect-fqdn enable** command in global configuration mode.

**redirect-fqdn** {**enable** | **disable**}

---

**Note** To use VPN load balancing, you must have an ASA Model 5510 with a Plus license or an ASA Model 5520 or higher. VPN load balancing also requires an active 3DES or AES license. The security appliance checks for the existence of this cryptographic license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing. It also prevents internal configuration of 3DES by the load-balancing system unless the license permits this usage.

---

## redirect-fqdn Parameters

| Parameter            | Description                                                   |
|----------------------|---------------------------------------------------------------|
| <code>disable</code> | Disables redirection with fully-qualified domain names (FDQN) |
| <code>enable</code>  | Enables redirection with FDQN                                 |

## participate

To force the device to participate in the virtual load-balancing cluster, use the **participate** command in vpn load-balancing configuration mode. To remove a device from participation in the cluster, use the **no** form of this command.

### participate

### Deploying Cisco ASA VPN Clustering

#### Implementation Guidelines

Consider the following implementation guidelines:

- VPN clustering provides high availability and load sharing but requires that all members are individually configured.
- Instead of local policy configuration, consider using external AAA servers for consistent and scalable policy enforcement.
- Deploy the UCC option for maximum security and ease of use.

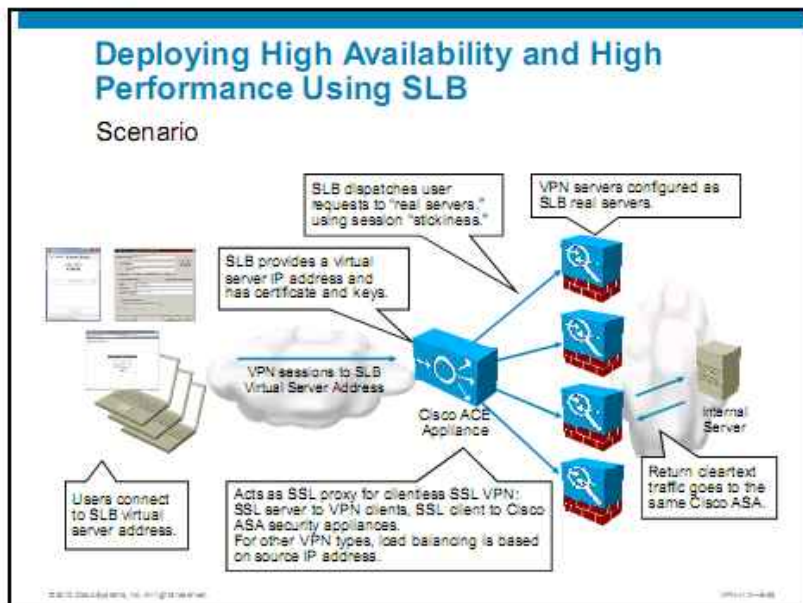
© 2010 Cisco Systems, Inc. All rights reserved. ASA 9.1(3)-9.0

Consider these implementation guidelines when deploying cluster load balancing:

- VPN clustering provides high availability and load sharing but requires that all members are individually configured. Active tunnels are not redirected to another member when the currently active cluster member fails.
- Instead of local policy configuration, consider using external authentication, authorization, and accounting (AAA) servers for consistent and scalable policy enforcement.
- Deploy the UCC option for maximum security and ease of use.

# Deploying High Availability and High Performance Using Network SLB

This topic describes how to provide high availability and high performance using an external SLB appliance.



This figure illustrates the deployment of an external Cisco ACE Application Control Engine appliance or Module that is installed in a Cisco Catalyst 6500 switch or Cisco 7600 series router that can evenly distribute VPN sessions to the VPN servers. You configure the Cisco ACE Module with a virtual server address. The users connect to it.

The ACE uses a special set of SSL commands to perform the SSL cryptographic functions between a client and a server. The SSL functions include server authentication, private and public key generation, certificate management, and data packet encryption and decryption that can be used for clientless SSL VPN load balancing.

In Cisco AnyConnect and Cisco Easy VPNs, the ACE does not terminate the VPN connections but distributes them to the Cisco ASA security appliances based on the source IP address and connection "stickiness."

In clientless SSL VPNs, the ACE can be configured to terminate the SSL sessions from the users. Based on the decrypted session description, the ACE deploys a load-balancing algorithm to dispatch the session to the appropriate security appliance. The algorithm guarantees that a given SSL session is sent to the same SSL VPN server, which is often referred to as "stickiness." The security appliances are defined on the ACE as real servers. The ACE secures the user session with SSL before forwarding it to the selected appliance.

For clientless SSL VPNs, you can partition the ACE into multiple contexts (virtual ACE devices) in which you configure each context with the certificate and key files the context needs to establish an SSL session with its peer. One context can terminate the SSL sessions from the SSL users while a separate context would initiate the connections to the appropriate security appliance. The ACE creates a secure storage area in flash memory for storing the certificates and keys that are associated with each context you create.



# Deploying VPN QoS

This topic describes how to integrate quality of service (QoS) mechanisms in IPsec VPNs on the Cisco ASA adaptive security appliance.

## IPsec VPN QoS

- Enterprises need to differentiate between delay-sensitive traffic and bulk data sent through the VPN.
- QoS is supported only in IPsec VPNs.
  - Remote access
  - Site-to-site



Enterprises need to differentiate between delay-sensitive traffic and bulk data that is sent through the VPN. The QoS mechanisms are supported only in IPsec VPNs, both in remote access (Cisco Easy VPN) and in site-to-site VPNs.

By default, the QoS is not enabled on the Cisco ASA security appliance, so traffic is placed in the default queue or best-effort queue. The best-effort queue works on a first-come first-served basis, and no traffic has priority over any other traffic. Best effort does not guarantee reliable delivery of packets because there is no sophisticated acknowledgment system in place for the best-effort queue. It does make a "best effort" to deliver packets to the destination. QoS is disabled by default because QoS can consume large amounts of resources and therefore degrade security appliance performance.

## Deploying IPsec VPN QoS

### Configuration Tasks

1. (Optional) Define a priority queue on the required interface or interfaces.
2. Create a service policy.
3. Define a traffic class.
4. Define match criteria.
5. Define an action.
6. (Optional) Repeat the process for other classes.

© 2010 Cisco Systems, Inc. All rights reserved.

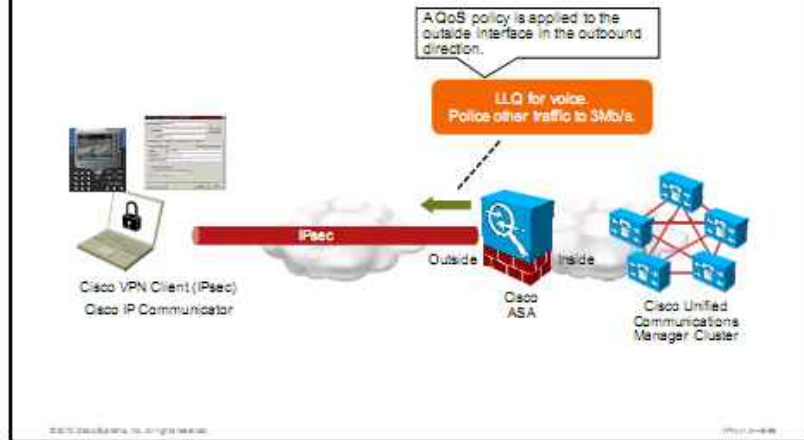
VPN-11-0-98

To deploy QoS on the security appliance, you will perform these configuration tasks:

1. Optionally, define the priority queue on the required interface or interfaces.
2. Create a service policy.
3. Define a traffic class.
4. Define match criteria.
5. Define an action.
6. Optionally, repeat the process for other classes.

## Deploying IPsec VPN QoS

### Configuration Scenario

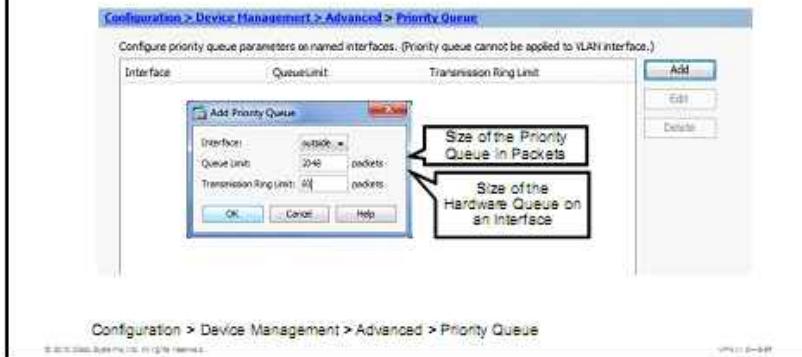


This figure illustrates the configuration scenario that is used in the upcoming deployment flow. In this example, Cisco VPN Clients are collocated with the Cisco IP Communicator, which provides telephony service to the remote users. Voice media traffic that the Cisco IP Communicator softphones exchange with other telephony endpoints is carried over Real-Time Transport Protocol (RTP) with the differentiated services code point (DSCP) value set to Expedited Forwarding (EF). In this scenario, you will match the voice media traffic flowing through the tunnels by checking its DSCP marking and assign it to the low-latency queue. All other traffic going out from the appliance through the outside interface should be policed to 3 Mb/s.

## Deploying IPsec VPN QoS

### Task 1: Configure Priority Queue

- Prerequisite for LLQ configuration
- Defined on interfaces that should manage congestion



In the first task, you will enable a priority queue on the physical interface. This task is mandatory for LLQ deployment. To configure a priority queue, complete these steps:

- Step 1** Choose **Configuration > Device Management > Advanced > Priority Queue**. The Priority Queue pane appears.
- Step 2** Click the **Add** button, and the Add Priority Queue window appears.
- Step 3** Choose the appropriate interface from the Interface drop-down menu. In the example, the outside interface is selected.
- Step 4** Enter the priority queue buffer size in the Queue Limit field. The default priority queue limit size is 2048 packets. The upper limit of the priority queue is determined dynamically at run time based primarily on available system memory. The only way to view the upper limit is from the CLI. Use the **help priority-queue** command. In this example, the default value of 2048 is left unchanged.
- Step 5** Enter the maximum number of packets to be placed in the transmit queue in the Transmission Ring Limit field. In this example, the transmission ring is left to the default value of 80 packets.
- Step 6** Click **OK**.
- Step 7** Click **Apply** to apply the configuration.

## Deploying IPsec VPN QoS

### Task 2: Create Service Policy

- One service policy per interface
- Does not specify direction (input or output)
  - Policing direction defined in actions page



In the second task, you will add a service policy by completing these steps:

- Step 1** Choose **Configuration > Firewall > Service Policy Rules**.
- Step 2** Click **Add** to create a new rule.
- Step 3** Choose the interface, to which the service policy will be applied, or the global policy option. At this point, you do not define the directionality of the action. In the example, the outside interface is chosen.
- Step 4** Enter the policy name and an optional description.
- Step 5** Click **Next**.

## Deploying IPsec VPN QoS

### Task 3: Define Traffic Class

- Maximum two traffic match criteria can be selected in a class.
- Match rules are defined in the next task.



In the third task, you will configure a traffic class by completing these steps:

**Step 1** When prompted, enter a name for the traffic class. In this example, the name is Tunneled-voice.

**Step 2** Choose the **Traffic Classification** tab and select the required matching criteria.

- **Default Inspection Traffic:** The class matches the default TCP and User Datagram Protocol (UDP) ports that are used by all applications that the security appliance can inspect. The security appliance includes a default global policy that matches the default inspection traffic and applies common inspections to the traffic on all interfaces. Not all applications whose ports are included in the Default Inspection Traffic class are enabled by default in the policy map.
- **Source and Destination IP Address (Uses ACL):** The class matches traffic that is specified by an extended access list. If the security appliance is operating in transparent firewall mode, you can use an ethertype access list.
- **Tunnel Group:** The class matches traffic for a tunnel group to which you want to apply QoS. You can also specify one other traffic match option to refine the traffic match, excluding Any traffic, Source and Destination IP Address (uses ACL), or Default Inspection Traffic. This option is used to identify VPN traffic, such as the tunneled traffic exchanged with Cisco AnyConnect SSL VPN clients.
- **TCP or UDP Destination Port:** The class matches a single port or a contiguous range of ports. For applications that use multiple, discontinuous ports, use the Source and Destination IP Address (Uses ACL) option to match each port.
- **RTP Range:** The class map matches Real-Time Transport Protocol (RTP) traffic.
- **IP DiffServ CodePoints (DSCP):** The class matches up to eight DSCP values in the IP header.
- **IP Precedence:** The class map matches up to four precedence values, represented by the type of service (ToS) byte in the IP header.
- **Any Traffic:** Matches all traffic.

In the example, Tunnel Group and IP DiffServ CodePoints (DSCP) criteria are selected.

- Step 3** Choose **Use class-default as the Traffic Class** if the traffic does not match an existing traffic class. This option uses the class-default class, which matches all traffic. The class-default class is created automatically by the security appliance and placed at the end of the policy. If you do not apply any actions to it, it is still created by the security appliance, but for internal purposes only. You can apply actions to this class, if desired, which might be more convenient than creating a new traffic class that matches all traffic. You can create only one rule using the class-default class, because each traffic class can be associated with only a single rule. In this example, the Tunnel Group and IP DiffServ CodePoints check boxes are checked.
- Step 4** Click the **Next** button to continue.

---

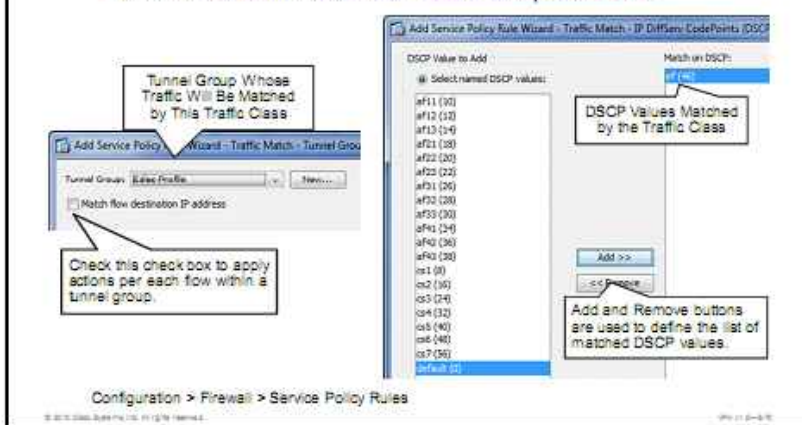
**Note** The wizard will adjust the match definition options based on the criteria that are selected on this screen. If different criteria are selected, the configuration options and the corresponding commands that are sent to the Cisco ASA adaptive security appliance will differ.

---

## Deploying IPsec VPN QoS

### Task 4: Define Match Criteria

- Selected traffic match criteria: Tunnel Group and DSCP



In the fourth task, you will define the match criteria.

On the previous Traffic Classification page, you selected the traffic match criteria, Tunnel Group, and IP DiffServ CodePoints. Now you must identify the specific Tunnel Group and the required DSCP values.

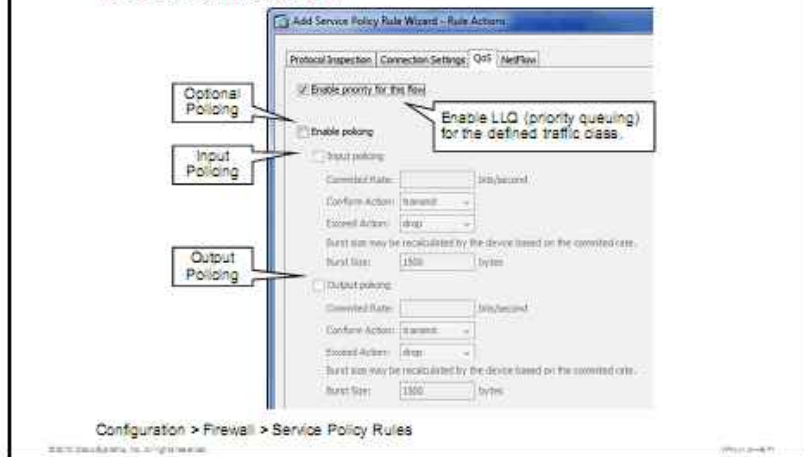
To define the specific class map Tunnel Group and DSCP match for the service policy map, continue with these steps:

- Step 1** Choose the tunnel group from the Tunnel Group drop-down list. If a new tunnel group needs to be defined, click the **New** button, and the Manage Connections Profile window appears. In this example, the tunnel group Sales-Profile is chosen.
- Step 2** Click the **Next** button to continue.
- Step 3** Select the appropriate DSCP values to add and click the **Add** button. In this example, the DSCP value for Expedited Forwarding (EF), ef (46), is selected because this DSCP bit of EF is set in the IP header for voice media packets.
- Step 4** Click the **Next** button to continue.



## Deploying IPsec VPN QoS

### Task 5: Define Action

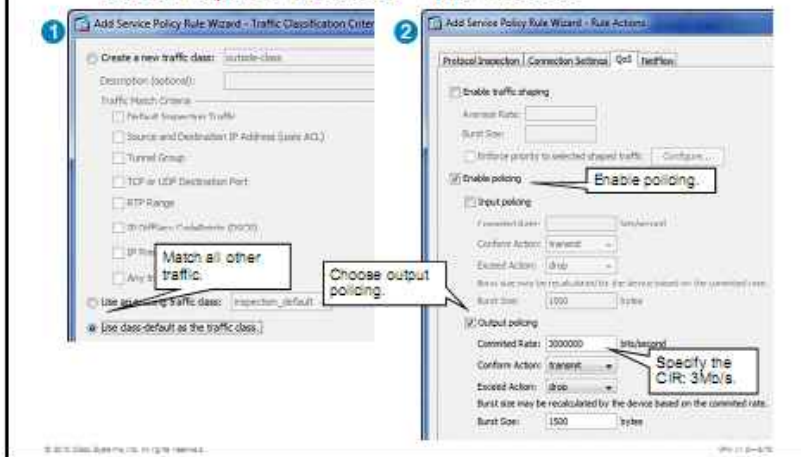


After the traffic criteria are defined, you configure the policy rule for the identified traffic. To define a QoS policy map rule for the selected class map, continue with these steps:

- Step 1** Choose the **QoS** tab. The **QoS** policy rules options appear.
- Step 2** Check the **Enable Priority for this Flow** check box. Based on this example, by checking this box, the traffic that matches the Tunneled-voice class map will be placed in the priority queue on the outside interface.
- Step 3** Click the **Finish** button.
- Step 4** Click **Apply** to apply the configuration.

## Deploying IPsec VPN QoS

### Task 6: Repeat Process for Other Classes



In the final configuration task, you repeat the process for other traffic classes. In this configuration scenario, you will apply output policing to the class-default traffic, which matches all other traffic that is sent through the interface.

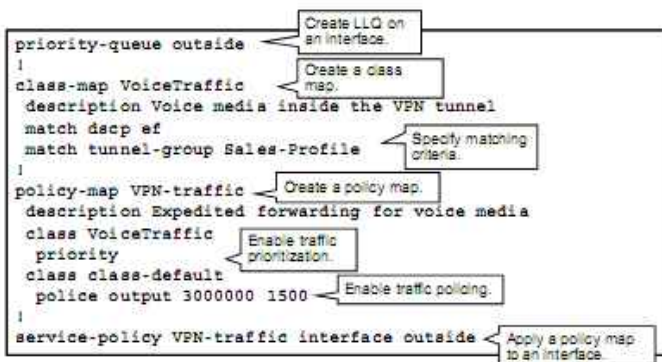
To continue configuring the service policy map and adding additional policy maps, complete these steps:

- Step 1** From the Service Policy Rules pane, click the **Add** button. (Not shown.)
- Step 2** In the Add Service Policy Rule Wizard window, click **Next**. (Not shown.)
- Step 3** For additional custom classes, choose the **Create a new traffic class** radio button. Then enter the new class map name in the field, and proceed with defining the matching criteria and actions, as described in the previous tasks.
- Step 4** To configure the policy actions for the class-default class, click the **Use Class-Default as the Traffic Class** radio button.
- Step 5** Click the **Next** button to continue.
- Step 6** In the Add/Edit Service Policy Rule pane, choose the QoS tab, select the required action, and configure its parameters. In this example, output policing is configured with these parameters:
  - Committed rate: 3,000,000 b/s (3 Mb/s)
  - Actions: conform – transmit, exceed – drop
  - Burst size: 1500 bytes (default)
- Step 7** Choose **Finish**.
- Step 8** Click **Apply** to apply the configuration.

**Note** The Traffic Shaping option can be provisioned for the class-default traffic. If you configure traffic shaping, you can select the Enforce Priority to Selected Shaped Traffic option to combine traffic shaping with PQ. This method of configuring PQ is mutually exclusive with the LLQ style that you configured in the previous tasks.

## Deploying IPsec VPN QoS

### CLI Configuration



To configure QoS for VPN using CLI, use the following commands. First, enable LLQ on an interface using the **priority-queue** command. Then create a class map to match VPN traffic using the **class-map** command. To specify matching criteria, use the **match dscp** and **match tunnel-group** commands.

Then create a policy map using the **policy-map** and refer to previously created class map and assign a priority action to it using the **priority** command. Then assign a policing action to class-default class using the **police output** command.

Finally, apply policy map to an interface using the **service-policy interface** command.

### priority-queue

To create a standard priority queue on an interface for use with the **priority** command, use the **priority-queue** command in global configuration mode. To remove the queue, use the **no** form of this command.

**priority-queue** *interface-name*

#### priority-queue Parameters

| Parameter             | Description                                                                                                                                      |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>interface-name</i> | Specifies the name of the physical interface on which you want to enable the priority queue, or for the ASA 5505, the name of the VLAN interface |

### class-map

When using the Cisco Modular Policy Framework, identify Layer 3 or 4 traffic to which you want to apply actions by using the **class-map** command (without the **type** keyword) in global configuration mode. To delete a class map, use the **no** form of this command.

**class-map** *class\_map\_name*

## class-map Parameters

| Parameter             | Description                                                                                                                                                                                                                                                                              |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>class_map_name</i> | Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot reuse a name that has been used by another type of class map. |

## match dscp

To identify the Internet Engineering Task Force (IETF)-defined DSCP value (in an IP header) in a class map, use the **match dscp** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

**match dscp** {*values*}

### match dscp Parameters

| Parameter     | Description                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------|
| <i>values</i> | Specifies up to eight different the IETF-defined DSCP values in the IP header. Range is 0 to 63. |

## match tunnel-group

To match traffic in a class map that belongs to a previously defined tunnel-group, use the **match tunnel-group** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

**match tunnel-group** *name*

### match tunnel-group Parameters

| Parameter   | Description                     |
|-------------|---------------------------------|
| <i>name</i> | Text for the tunnel group name. |

## policy-map

When using the Cisco Modular Policy Framework, assign actions to traffic that you identified with a Layer 3 and 4 class map (the **class-map** or **class-map type management** command) by using the **policy-map** command (without the **type** keyword) in global configuration mode. To remove a Layer 3 and 4 policy map, use the **no** form of this command.

**policy-map** *name*

### policy-map Parameters

| Parameter   | Description                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i> | Specifies the name for this policy map up to 40 characters in length. All types of policy maps use the same name space, so you cannot reuse a name that has been used by another type of policy map. |

## class (policy-map)

To assign a class map to a policy map where you can assign actions to the class map traffic, use the **class** command in policy-map configuration mode. To remove a class map from a policy map, use the **no** form of this command.

**class** *classmap\_name*

### class (policy-map) Parameters

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>classmap_name</i> | Specifies the name for the class map. For a Layer 3 and 4 policy map (the <b>policy-map</b> command), you must specify a Layer 3 and 4 class map name (the <b>class-map</b> or <b>class-map type management</b> command). For an inspection policy map (the <b>policy-map type inspect</b> command), you must specify an inspection class map name (the <b>class-map type inspect</b> command). |

## priority

To enable QoS PQ, use the **priority** command in class configuration mode. For critical traffic that cannot tolerate latency, such as VoIP, you can identify traffic for LLQ so that it is always transmitted at a minimum rate. To remove the priority requirement, use the **no** form of this command.

**priority**

## police

To apply QoS policing to a class map, use the **police** command in class configuration mode. To remove the rate-limiting requirement, use the **no** form of this command. Policing is a way of ensuring that no traffic exceeds the maximum rate (in bits or seconds) that you configure, thus ensuring that no one traffic flow can take over the entire resource. When traffic exceeds the maximum rate, the adaptive security appliance drops the excess traffic. Policing also sets the largest single burst of traffic allowed.

**police** {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**]] [**exceed-action** [**drop** | **transmit**]]

### police Parameters

| Parameter             | Description                                                                                                                                                                  |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>conform-burst</i>  | Specifies the maximum number of instantaneous bytes that are allowed in a sustained burst before throttling to the conforming rate value, between 1000 and 512,000,000 bytes |
| <b>conform-action</b> | Sets the action to take when the rate is less than the <i>conform_burst</i> value                                                                                            |
| <i>conform-rate</i>   | Sets the rate limit for this traffic flow; between 8000 and 2,000,000,000 b/s                                                                                                |
| <b>drop</b>           | Drops the packet                                                                                                                                                             |
| <b>exceed-action</b>  | Sets the action to take when the rate is between the <i>conform-rate</i> value and the <i>conform-burst</i> value                                                            |
| <b>input</b>          | Enables policing of traffic flowing in the input direction                                                                                                                   |
| <b>output</b>         | Enables policing of traffic flowing in the output direction                                                                                                                  |
| <b>transmit</b>       | Transmits the packet                                                                                                                                                         |

## service-policy (global)

To activate a policy map globally on all interfaces or on a targeted interface, use the **service-policy** command in global configuration mode. To disable the service policy, use the **no** form of this command. Use the **service-policy** command to enable a set of policies on an interface.

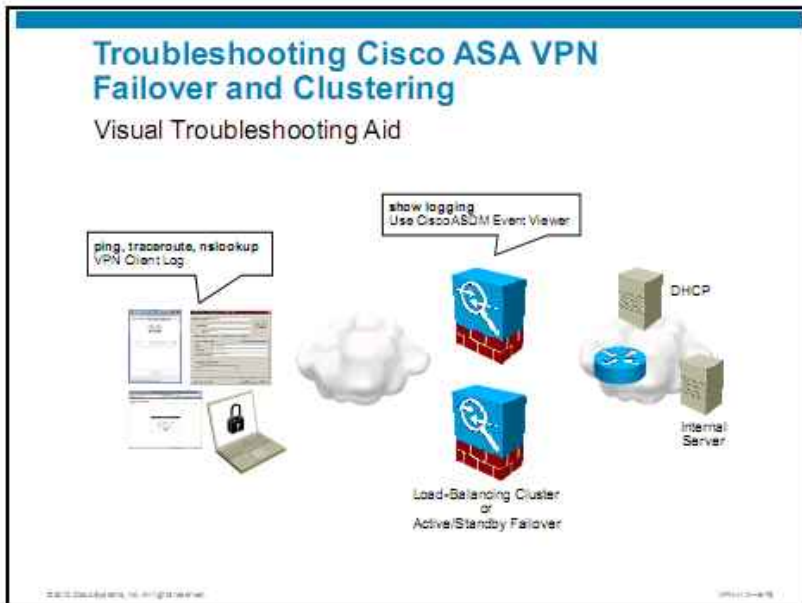
**service-policy** *policymap\_name* [**global** | **interface** *intf*]

### service-policy (global) Parameters

| Parameter                    | Description                                                                                                                                                                                               |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>policymap_name</i>        | Specifies the policy map name that you configured in the <b>policy-map</b> command. You can only specify a Layer 3 and 4 policy map, and not an inspection policy map ( <b>policy-map type inspect</b> ). |
| <b>global</b>                | Applies the policy map to all interfaces.                                                                                                                                                                 |
| <b>interface</b> <i>intf</i> | Applies the policy map to a specific interface.                                                                                                                                                           |

# Troubleshooting Cisco ASA Adaptive Security Appliance VPN Failover and Clustering

This topic describes how to troubleshoot Cisco ASA adaptive security appliance VPN failover and load balancing.

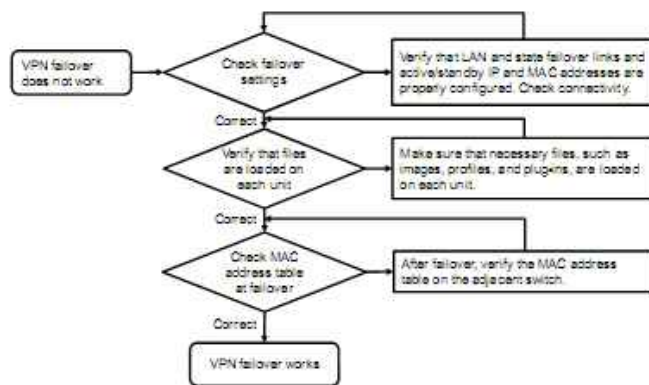


This figure illustrates the relevant network components in a VPN high-availability solution. Two high-availability methods will be discussed: active/standby failover, and cluster load balancing.

For the full tunnel VPNs, client IP addresses will be assigned by an external DHCP server. For load balancing, this approach requires that client routes are redistributed into the internal routing process to enable routing of return client traffic.

A variety of troubleshooting tools is available on the different components, such as general troubleshooting tools on the remote compute, and the logging output on the security appliance.

## Troubleshooting Cisco ASA VPN Failover and Clustering

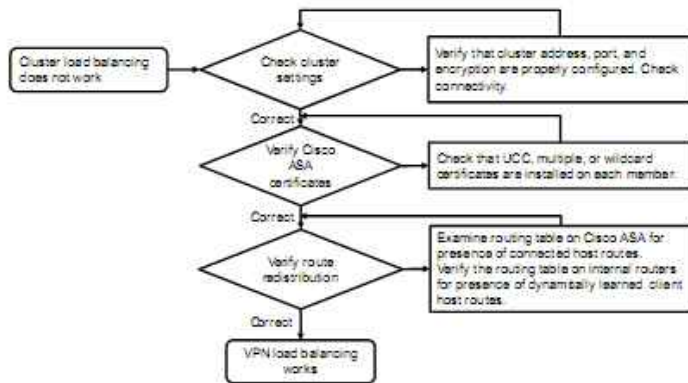


Perform these troubleshooting steps if the VPN active/standby failover is not working properly:

- Step 1** Check the failover configuration. Verify that all settings are correct. The relevant parameters include the LAN and state failover links and active/standby IP and MAC addresses. Verify the connectivity between the units over all links.
- Step 2** Ensure that any required files, such as images, profiles, and plug-ins, are installed on both units.
- Step 3** Ensure that the switch learns about the swap of MAC addresses at failover by viewing its CAM table. The active MAC addresses should after failover appear at the ports where the secondary unit is connected.



## Troubleshooting Cisco ASA VPN Failover and Clustering



Perform these troubleshooting steps if the cluster load balancing is not working properly:

- Step 1** Check the cluster settings on all members. Verify that all relevant parameters, such as virtual IP address, port, and encryption are consistent. Verify the connectivity among all members over the external and internal link.
- Step 2** Verify that the server certificates are installed on the members according to the selected deployment model: UCC, multiple individual certificates, or one wildcard certificate. You can verify each member certificate individually by connecting to its specific address.
- Step 3** For full tunnel VPNs, examine the redistribution of client routes into the IGP. Examine the routing table on the cluster member for presence of host routes for connected clients. The appliance installs such routes automatically when the Cisco AnyConnect client establishes the tunnel, and when RRI is configured for IPsec clients. Examine the routing tables of internal routers for presence of dynamically learned client routes.

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- Cisco ASA supports a range of VPN load-balancing and high-availability mechanisms.
- Redundant peering uses preconfigured backup servers to re-establish the VPN when the primary server fails.
- SLB is based on an external Catalyst 6500/7600 platform with Application Control Engine module that dispatches VPN connections to multiple Cisco ASA security appliances.
- Active/standby stateful failover includes VPN failover subsystem.
- IPsec site-to-site VPNs support OSPF-based failover.
- Cluster load balancing allows load sharing among multiple active Cisco ASA security appliances that can run on different platforms.
- LLQ ensures expedited forwarding while input/output policing prevents oversubscription of network bandwidth.
- Primary troubleshooting tool is the Cisco ASA logging output.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-17-34-4-10

# Module Summary

This topic summarizes the key points that were discussed in this module.

## Module Summary

- Scalable VPN deployments implement a centralized approach, where the access control policy is stored on an external database, from which it is downloaded to VPN servers on demand.
- Cisco Secure Desktop technology interoperates with the endpoint operating system and can ensure the total removal of all data, in particular, from an untrusted system with potentially malicious third-party software installed.
- DAP on the Cisco ASA adaptive security appliance allows for configuration of the authorization that addresses many variables that are found in various remote access VPNs.
- Two of the most challenging requirements of VPNs are high availability and high performance. High availability ensures continuous operation even if one or more VPN servers fail. High performance enhancements are deployed to boost system performance by alleviating the load that is placed on a single VPN server.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-11-541



# Deploying External Authentication in Cisco AnyConnect Full Tunnel SSL VPNs

---

## Overview

When deploying virtual private networks (VPNs) in general, it is very important for you to use strong authentication options. This lesson describes several external authentication options that you have when implementing Cisco AnyConnect full tunnel SSL VPNs on the Cisco ASA adaptive security appliance. These authentication options offer adequate security and scalability, as opposed to the basic local authentication. This lesson describes certificate-based authentication using external certificate authorities (CAs) and options that are available to verify user certificates for password management on external Lightweight Directory Access Protocol (LDAP) servers.

## Objectives

Upon completing this lesson, you will be able to deploy and manage external authentication in a Cisco AnyConnect full tunnel SSL VPN. This ability includes being able to meet these objectives:

- Configure and verify Cisco ASA adaptive security appliance and Cisco AnyConnect client to use an external CA and provision client certificates
- Implement password management using external LDAP servers

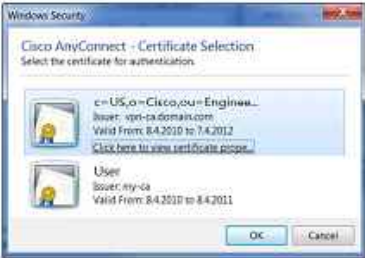
# Deploying Certificate-Based Client Authentication Using External CAs

This topic describes how to configure and verify Cisco ASA adaptive security appliance and Cisco AnyConnect client to use an external CA and provision client certificates.

## Configure Certificate-Based Client Authentication Using External CAs

### Preprovisioned Certificates

- Cisco AnyConnect can use existing client certificates:
  - System certificate store
  - Browser certificate store
  - Smartcards and smart tokens
  - Filesystem store (Linux)
- On Microsoft Windows, you can use user or computer certificates.
- You can influence certificate selection through XML profiles.



© 2010 Cisco Systems, Inc. All rights reserved. VPN-113-1020-0

When using certificate-based authentication for full client (Cisco AnyConnect) SSL connections, you can also use already existing certificates that are obtained from an external CA. Cisco AnyConnect can use existing client certificates that are stored in the system certificate store, web browser certificate store, or certificates on smart cards or smart tokens.

On Microsoft Windows computers, you can use computer or user certificates.

If there are multiple certificates that are available on a computer, Cisco AnyConnect will prompt you regarding which certificate you would like to use for authentication to the Cisco ASA adaptive security appliance. You can also preconfigure the Cisco AnyConnect client to select a certificate automatically. Configuration of certificate selection on the Cisco AnyConnect client is achieved using XML profiles.

---

**Note** XML profiles are XML files that are sent from the Cisco ASA adaptive security appliance to the Cisco AnyConnect. Inside the XML profile, specific parameters are set that influence Cisco AnyConnect behavior.

---

## Configure Certificate-Based Client Authentication Using External CAs

### Cisco AnyConnect SCEP Enrollment

Cisco AnyConnect can also enroll to a PKI using SCEP:

- Enrollment parameters controlled through XML profiles.
- Enrollment inside or outside a VPN tunnel.
- This topic only presents SCEP enrollment inside a VPN tunnel.



The Cisco AnyConnect client can enroll to an external public key infrastructure (PKI) using Simple Certificate Enrollment Protocol (SCEP) enrollment. However, for SCEP enrollment you have to modify the Cisco AnyConnect XML profile to include SCEP-related parameters. When a Cisco AnyConnect user connects to the security appliance, Cisco AnyConnect sends a certificate enrollment request to the CA server, and the CA server automatically accepts or denies the request.

Two different options are possible when you enroll the Cisco AnyConnect client to the external CA:

- **Enrollment inside an SSL VPN tunnel:** When using this deployment option, a user has to first establish an Secure Sockets Layer (SSL) tunnel to the Cisco ASA security appliance (using a special, dedicated connection profile that does not use certificates as the authentication means and that allows access to a CA server only). When the Cisco AnyConnect receives an XML profile with SCEP enrollment parameters, it will automatically send a certificate request to the CA inside the SSL tunnel. When the Cisco AnyConnect receives and installs a certificate, it will automatically disconnect the SSL connection. The user will then be able to reconnect to another connection profile that uses certificates as the authentication means.
- **Enrollment outside an SSL VPN tunnel:** When using this deployment option, a user has to try to connect to the connection profile that uses certificates as an authentication means. Because a certificate is not present yet on the computer of the user, the authentication will fail. However, before failed authentication, the Cisco AnyConnect received an XML profile that instructs the Cisco AnyConnect to enroll into the CA. A user will be presented with a Get Certificate button in the Cisco AnyConnect window. By clicking this button, Cisco AnyConnect will enroll into the CA using the parameters that are specified in the received XML profile. The Cisco AnyConnect client will enroll into the CA outside the SSL VPN tunnel.

In this topic, only the first option, deployment inside an SSL tunnel, is described.

## Configure Certificate-Based Client Authentication Using External CAs

### Configuration Tasks (Enrollment Inside a VPN Tunnel)

1. Configure XML profile enrollment parameters.
2. Configure a dedicated enrollment connection profile.
3. Enroll the client into a PKI.
4. (Optional) Configure client certificate selection.
5. Import CA certificate to the Cisco ASA adaptive security appliance.
6. Enable client certificate authentication and mapping for a connection profile.

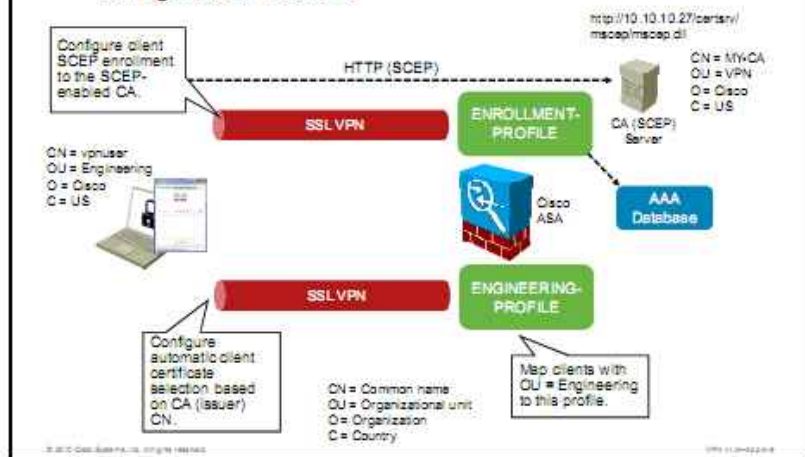
These are the configuration tasks that should be followed to configure certificate-based client authentication using external CAs:

1. Configure an XML profile with SCEP enrollment parameters.
2. Configure a dedicated enrollment connection profile that does not use certificates for authentication and allows access to a CA only.
3. Enroll the Cisco AnyConnect client into a PKI.
4. Optionally, configure client certificate selection.
5. Import the certificate of the CA to the Cisco ASA security appliance so that the security appliance will be able to verify certificates of the clients.
6. Enable certificate-based client authentication for a connection profile and mapping for a connection profile.



## Configure Certificate-Based Client Authentication Using External CAs

### Configuration Scenario



The figure shows an example that will serve as configuration scenario for the ongoing configuration tasks. You first configure a dedicated ENROLLMENT-PROFILE connection profile that will be used for the Cisco AnyConnect client to enroll into the CA server. You will configure an XML profile that will control SCEP enrollment parameters, such as enrollment URL and subject name that will be used in the certificate request. Users that connect to the ENROLLMENT-PROFILE connection profile will be authenticated using AAA database.

After users obtain a certificate, they connect to the ENGINEERING-PROFILE that you configure to use certificates as an authentication means. You will also configure a mapping between the organizational unit, or OU field, in authenticating certificates and ENGINEERING-PROFILE. This way, users with the Engineering string in the OU field of a certificate will be mapped to the ENGINEERING-PROFILE automatically.

# Configure Certificate-Based Client Authentication Using External CAs

## Task 1: Configure XML Profile Enrollment Parameters

The screenshot shows the Cisco AnyConnect Client Profile Editor interface. The 'Certificate Enrollment' tab is selected, and the 'Certificate Enrollment' checkbox is checked. The 'Automatic SCEP Host' field contains 'vpn.domain.com/Cert'. The 'CA URL' field contains 'http://10.10.10.27/certsrv/msoap/msoap.dll'. The 'Certificate Contacts' section is populated with the following information:

| Name (CN)       | Qualifer (OU) |
|-----------------|---------------|
| %USER%          | Engineering   |
| Department (OU) | Qualifer (OU) |
| Company (O)     | City (C)      |
| State (ST)      | Time (T)      |
| State (SP)      | CA Domain     |
| Country (C)     | Key Size 2048 |

On the right, the XML profile is displayed, showing the following structure:

```
<ClientInitialisations>
...
<CertificateEnrollment>
  <AutomaticSCEPHost>vpn.domain.com/
  <Certificate-enrollment
  </AutomaticSCEPHost>
  <CAURL PromptForChallengePW="False">
  http://10.10.10.27/certsrv/msoap/msoap.dll
  </CAURL>
  <CertificateSCEP>
  <Name_CN>%USER%</Name_CN>
  <Department_OU>Engineering
  </Department_OU>
  <Company_O>Cisco</Company_O>
  <Country_C>US</Country_C>
  <KeySize>2048</KeySize>
  <DisplayGetCertificateButton>
  </DisplayGetCertificateButton>
  </CertificateSCEP>
  </CertificateEnrollment>
...
</ClientInitialisations>
```

Below the XML is the label 'SCEP-ENROLL.XML'.

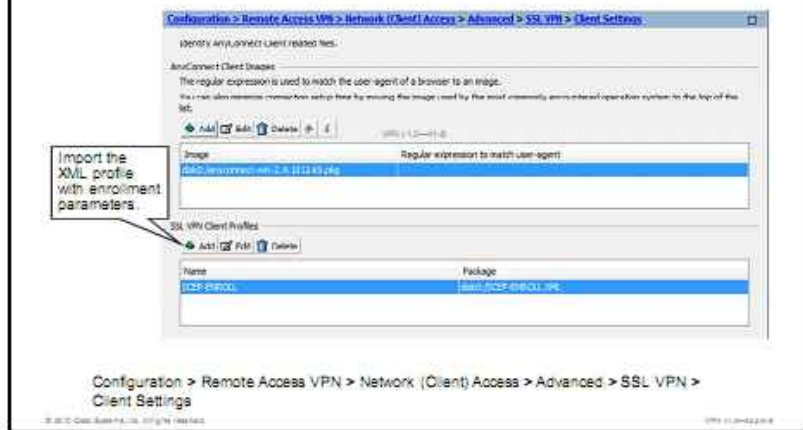
To configure XML Profile enrollment parameters, complete the following configuration steps:

- Step 1** Start the Cisco AnyConnect Client Profile Editor on a PC. Using the Cisco AnyConnect Client Profile Editor is also discussed in more details in another lesson within this course.
- Step 2** Click the **Certificate Enrollment** tab.
- Step 3** Check the **Certificate Enrollment** check box.
- Step 4** Enter the Cisco ASA security appliance fully qualified domain name (FQDN), followed by an alias of a connection profile that will be used as enrollment connection profile, into the Automatic SCEP Host field. If the Cisco ASA security appliance to which a user is connecting and the connection profile match the information that is specified in this field, a SCEP process will be triggered. In the example, `vpn.domain.com/Certificate-enrollment` is entered.
- Step 5** Enter a CA URL into the CA URL field to specify the CA enrollment location. In the example, `http://10.10.10.27/certsrv/msoap/msoap.dll` is entered.
- Step 6** Configure the following substeps to configure the subject name that will be used in the certificate request:
  - Enter `%USER%` into the Name (CN) field. This is a variable that will be replaced by a username that is used to authenticate a user into the enrollment connection profile.
  - Fill in the other fields as needed. In the example, the Department (OU), Company (O) and Country (C) fields are populated.
- Step 7** Click the **File** option from the menu and click **Save**. Save the profile locally on the PC (not shown in the figure).

The figure shows a part of the XML file that is generated by the Cisco AnyConnect Client Profile Editor.

## Configure Certificate-Based Client Authentication Using External CAs

### Task 1: Configure XML Profile Enrollment Parameters (Cont.)

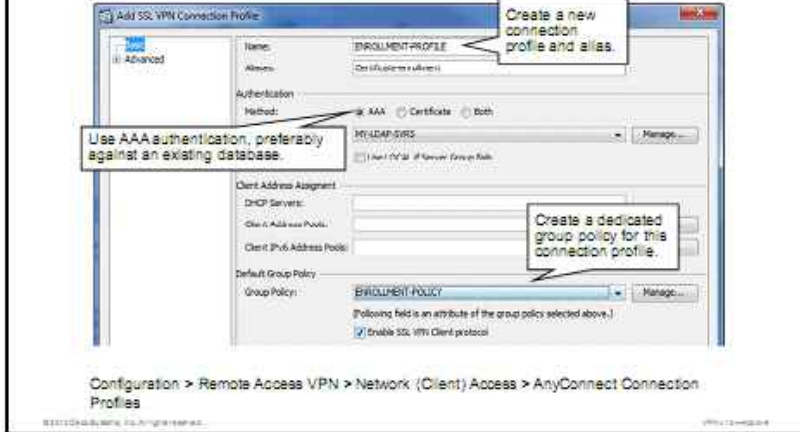


After you are done with configuring the XML profile, add the profile to the Cisco ASA security appliance by completing the following configuration steps.

- Step 8** Inside Cisco Adaptive Security Device Manager (Cisco ASDM), choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings**. The Client Settings pane appears.
- Step 9** Click the **Add** button in the SSL VPN Client Profiles area of the Client Settings pane. The Add SSL VPN Client Profiles window appears.
- Step 10** Enter a profile name into the Profile Name field. This name will be used later to refer to the XML profile. In the example, SCEP-ENROLL is entered.
- Step 11** The XML profile should be stored on the Cisco ASA security appliance Flash File System (FFS). If the XML profile file has not been copied to the security appliance yet, you can do it now by clicking the Upload button. After you are done with copying the file to the security appliance, click the **Browse Flash** button and select the file (not shown in the figure).
- Step 12** Click **OK** in the Add SSL VPN Client Profiles window.

## Configure Certificate-Based Client Authentication Using External CAs

### Task 2: Configure a Dedicated Enrollment Connection Profile



The second task when configuring certificate-based authentication using external CA is configuration of a dedicated enrollment connection profile. Complete the following steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** (not shown in the example). The AnyConnect Connection Profile window appears.
- Step 2** Click **Add** in the Connection Profiles area of the AnyConnect Connection Profiles window (not shown in the example). The Add SSL VPN Connection Profile window appears.
- Step 3** Enter a connection profile name into the Name field. In the example, the ENROLLMENT-PROFILE is entered.
- Step 4** Enter a connection profile alias into the Aliases field. In the example, the Certificate-enrollment alias is entered. Aliases are used when a user has an option to choose to which connection profile the user would like to connect, by selecting a connection profile alias from the Group drop-down menu in the Cisco AnyConnect client.
- Step 5** Click the **AAA** radio button in the Authentication area of the window to specify authentication method.
- Step 6** Specify an AAA server group that will be used to authenticate clients connecting to the ENROLLMENT-PROFILE. In the example, the MY-LDAP-SRVS group has been selected.
- Step 7** Click the **Manage** button in the Default Group Policy area of the window to create a new group policy. The Configure Group Policies window appears (not shown in the window).
- Step 8** Click the **Add** button in the Configure Group Policies window. The Add Internal Group Policy window appears (not shown in the example).

In the figure, a new group policy named ENROLLMENT-POLICY has been created and linked to the ENROLLMENT-PROFILE connection profile.

The next page shows the configuration of the ENROLLMENT-POLICY group policy.

**Note** In Cisco ASA security appliance software versions earlier than 8.1, the SCEP enrollment did not work unless you configured the **ssl certificate-authentication interface outside port 443** command on the security appliance. In Cisco ASA security appliance software version 8.2 and later, this issue no longer exists.

## Configure Certificate-Based Client Authentication Using External CAs

### Task 2: Configure a Dedicated Enrollment Connection Profile (Cont.)

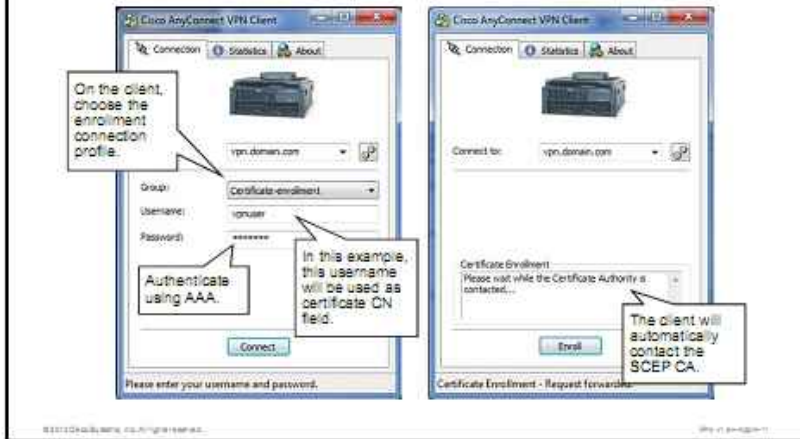
The screenshot shows the 'Add Internal Group Policy' configuration window. The 'Name' field contains 'ENROLLMENT-POLICY'. The 'Advanced' tab is active, showing various options for client system installation, compression, and TLS. The 'Client Profile to Download' is set to 'SCEP-ENROLL'. Two callouts provide additional context: one points to the 'Name' field stating 'In this policy, only allow access to the SCEP server using split tunneling and ACL rules.', and another points to the 'Client Profile to Download' dropdown stating 'In the group policy, reference the enrollment XML profile.'

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

- Step 9** Enter a name of the group policy into the Name field. In the example, the ENROLLMENT-POLICY is entered.
- Step 10** Specify split tunneling and ACL rules in the group policy as described in other lessons of the course to limit access to the CA server only (not shown in the example).
- Step 11** Expand the **Advanced** option from the menu on the left. Choose the **SSL VPN Client** option.
- Step 12** Uncheck the **Inherit** check box in the Client Profile to Download options and select the previously added XML profile from the drop-down menu. In the example, the SCEP-ENROLL profile is selected.
- Step 13** Click **OK** in the Add Internal Group Policy window.
- Step 14** Click **OK** in the Configure Group Policy window.
- Step 15** Click **OK** in the Add SSL VPN Connection Profile.
- Step 16** Click **Apply** to apply the configuration.

## Configure Certificate-Based Client Authentication Using External CAs

### Task 3: Enroll the Client into a PKI



After you are done with configuring the enrollment connection profile, users are already capable of enrolling into a PKI. A user has to start the Cisco AnyConnect client and select the enrollment connection profile from the Group drop-down menu. In the example, the Certificate-enrollment connection profile has been selected.

---

**Note** Recall that in the Cisco AnyConnect client, you see a configured alias for a connection profile, not the actual name of the connection profile. The alias name that was configured for the ENROLLMENT-PROFILE connection profile was called Certificate-enrollment.

---

The user has to provide credentials to authenticate to the enrollment connection profile and then click the **Connect** button. The Cisco AnyConnect establishes an SSL connection and automatically sends a certificate request to the SCEP CA.

## Configure Certificate-Based Client Authentication Using External CAs

### Task 3: Enroll the Client into a PKI (Cont.)



When the CA receives and processes a certificate request and issues a certificate to the Cisco AnyConnect client, the Cisco AnyConnect client will display a warning message asking you whether you are sure you want to install the received certificate. At this point, you should verify a thumbprint of the certificate using an out-of-band (OOB) communication with the CA. After you make sure that the thumbprint is correct, click the **Yes** button to install the certificate. After the certificate is installed, the Cisco AnyConnect client will notify you by displaying a “Certificate Enrollment—Certificate successfully imported” message. Click the **Accept** button. After that, the Cisco AnyConnect client will automatically disconnect from the SSL VPN connection.

## Configure Certificate-Based Client Authentication Using External CAs

### Task 4: (Optionally) Configure Client Certificate Selection

The screenshot displays the Cisco AnyConnect Client Profile Editor interface. The 'Certificate Match' tab is active, showing the 'Distinguished Name Entry' dialog box. The dialog box has 'Name' set to 'ISSUER-CN', 'Pattern' set to 'MY-CA', and 'Operator' set to 'Equal'. A callout box points to the dialog with the text: 'Specify that client certificates issued by MY-CA should be used.' To the right, a yellow box highlights the XML configuration for 'CERT-SELECTION.XML':

```
<ClientInitialisation>
...
<AutomaticCertificateSelection>true
</AutomaticCertificateSelection>
<CertificateMatch>
  <DistinguishedName>
    <DistinguishedNameDefinition
      Operator="Equal" Wildcards="Disabled">
      <Name>ISSUER-CN</Name>
      <Pattern>MY-CA</Pattern>
    </DistinguishedNameDefinition>
  </DistinguishedName>
</CertificateMatch>
...
</ClientInitialisation>
```

You can configure the Cisco AnyConnect to automatically select a certificate that will be used to authenticate to the Cisco ASA security appliance. Cisco AnyConnect can select a proper certificate based on defined matching rules. These matching rules have to be configured in an XML profile.

To configure XML Profile with certificate selection parameters that are based on a specific issuer common name, complete the following configuration steps:

- Step 1** Start the Cisco AnyConnect Client Profile Editor on a PC.
- Step 2** Click the **Certificate Match** tab.
- Step 3** Click the **Add** button in the Distinguished Name (MAX 10) area of the window. The Distinguished Name Entry window appears.
- Step 4** Choose the **ISSUER-CN** option from the Name drop-down menu, to specify that the issuer common name of a certificate should be verified.
- Step 5** In this example, enter **MY-CA** into the Pattern field to specify that the ISSUER CN field of a certificate should match the MY-CA string. (Recall from the last figure, in this example, the identity certificate that was received by the client was from MY-CA.)
- Step 6** Click **OK** in the Distinguished Name Entry window.
- Step 7** Click the **File** option from the menu and click **Save**. Save the profile locally.

The figure shows a part of the XML file that is generated by the Cisco AnyConnect Client Profile Editor.



## Configure Certificate-Based Client Authentication Using External CAs

### Task 4: (Optionally) Configure Client Certificate Selection (Cont.)

Alternatively, you can also disable automatic certificate selection to present users with a list of available client certificates.

```
<ClientInitialisation>
...
<AutomaticCertSelection>noSelSec/AutomaticCertSelection>
...
</ClientInitialisation>
```

CERT-SELECTION.XML

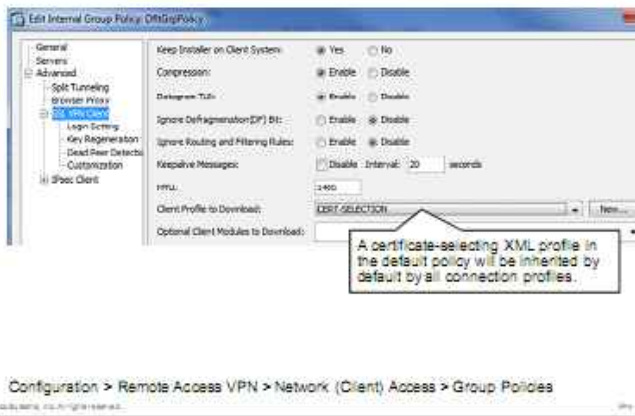
Alternatively, you can also disable automatic certificate selection and present users with a list of available client certificates. Complete the following steps to configure an XML profile that will instruct the Cisco AnyConnect client to present a list of available certificates.

- Step 1** Start the Cisco AnyConnect Client Profile Editor on a PC.
- Step 2** Click the **Preferences (Cont.)** tab.
- Step 3** Check the **Disable Cert Selection** check box.
- Step 4** Click the **File** option from the menu and select the **Save** option. Save the profile locally.

The figure shows a part of the XML file that is generated by the Cisco AnyConnect Client Profile Editor.

## Configure Certificate-Based Client Authentication Using External CAs

### Task 4: (Optionally) Configure Client Certificate Selection (Cont.)



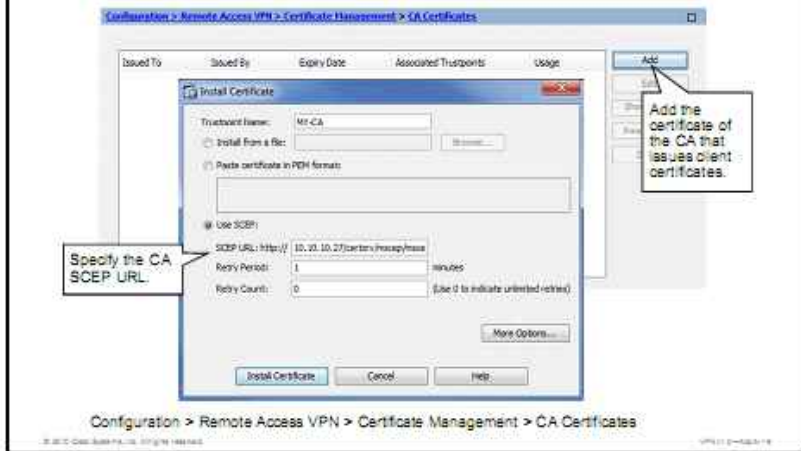
After you are done with configuring the XML profile, upload and add the XML profile to the Cisco ASA security appliance as described in Task 1. After you have uploaded and added the XML profile to the security appliance, edit the DfltGrpPolicy group policy to configure the security appliance to send the XML profile to Cisco AnyConnect clients.

**Note** The DfltGrpPolicy group policy has been selected because there might be several group policies that should use the same XML profile. Recall that all group policies inherit parameters from the DfltGrpPolicy group policy.

- Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** (not shown in the example). The Group Policies window appears.
- Step 2** Select the DfltGrpPolicy (System Default) from the table and click the **Edit** button. The Edit Internal Group Policy window appears.
- Step 3** Expand the **Advanced** option from the menu on the left and click the **SSL VPN Client** option.
- Step 4** Select the previously added XML profile from the Client Profile to Download drop-down menu. In the example, the CERT-SELECTION profile is selected.
- Step 5** Click **OK** in the Edit Internal Group Policy window.
- Step 6** Click **Apply** to apply the configuration.

## Configure Certificate-Based Client Authentication Using External CAs

### Task 5: Import CA Certificate to the ASA



The Cisco ASA security appliance needs a CA certificate to verify the identity certificates received from the client. Complete the following steps to import the CA certificate to the ASA:

- Step 1** Ensure that the device hostname and domain name are set correctly.
- Step 2** Optionally, if you have not already done so, create a Rivest, Shamir, and Adleman (RSA) key pair of appropriate strength. You can reuse existing keys, if they are of appropriate strength.
- Step 3** Using Cisco ASDM, choose **Configuration > Remote Access VPN > Certificate Management > CA Certificates**.
- Step 4** Click **Add** to create a new PKI trustpoint. Assign a local name to the new trustpoint. In the example, MY-CA is entered.
- Step 5** Click the **Use SCEP** radio button to specify that SCEP will be used to retrieve the CA certificate.
- Step 6** Enter SCEP CA URL into the SCEP URL field.
- Step 7** Click **Install Certificate** button to send a CA certificate request to the CA.

## Configure Certificate-Based Client Authentication Using External CAs

Task 6: Enable Client Certificate Authentication and Mapping for a Connection Profile



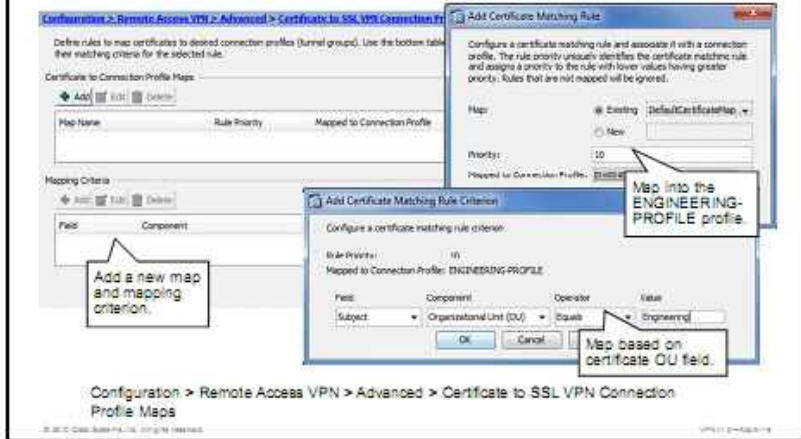
In the last task, you will enable certificate-based authentication for a connection profile. You will create a new connection profile, called **ENGINEERING-PROFILE** and select the authentication using certificates. You will also configure mapping of a certificate to this connection profile.

To configure a new connection profile using Cisco ASDM, complete the following configuration steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** (not shown in the example). The AnyConnect Connection Profiles window appears.
- Step 2** Click **Add** in the Connection Profiles area of the AnyConnect Connection Profiles window (not shown in the example). The Add SSL VPN Connection Profile window appears.
- Step 3** Enter a connection profile name into the Name field. In the example, the **ENGINEERING-PROFILE** is entered.
- Step 4** Click the **Certificate** radio button in the Authentication area of the window to specify the authentication method.
- Step 5** Optionally, create a new, dedicated group policy for the connection profile by clicking the **Manage** button in the Default Group Policy area of the window or select an existing group policy from the Group Policy drop-down menu. In the example, the **ENGINEERING-POLICY** group policy will be linked to the **ENGINEERING-PROFILE** connection profile.
- Step 6** Click **OK** in the Add SSL VPN Connection Profile window.
- Step 7** Click **Apply** to apply the configuration.

## Configure Certificate-Based Client Authentication Using External CAs

### Task 6: Client Certificate Authentication and Mapping for Enable a Connection Profile (Cont.)



To configure certificate to connection profile mapping using Cisco ASDM, complete the following steps:

- Step 1** Inside the Cisco ASDM, choose **Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps** and click **Add** under the Certificate to Connection Profile Maps area.
- Step 2** Select an existing map from the map drop-down menu. In the example, DefaultCertificateMap is chosen.
- Step 3** Alternatively, click the **New** radio button under Map and provide a name for the connection profile map.
- Step 4** Configure the rule priority by entering a value into the Priority field. A rule with a lower priority number will be consulted before a rule with a higher priority number.
- Step 5** Choose the desired connection profile from the Mapped to Connection Profile drop-down menu. In the example, ENGINEERING-PROFILE is chosen.
- Step 6** Click **OK** to accept the profile map.

After the profile map has been configured, configure the mapping criterion to identify to the Cisco ASA security appliance what will be used to map the connecting users to the desired connection profile.

- Step 1** Under the same submenu, click the **Add** button under the Mapping Criteria area.
- Step 2** Configure the **Field**, **Component**, **Operator**, and **Value** fields for the mapping criteria and click **OK** to accept the changes.

The following items can be selected under the Mapping Criteria:

- **Field:** Choose the part of the certificate to be evaluated from the drop-down list.
  - **Subject:** The person or system that uses the certificate. For a CA root certificate, the Subject and Issuer are the same.

- **Alternative Subject:** The subject alternative names extension allows additional identities to be bound to the subject of the certificate.
- **Issuer:** The CA or other entity (jurisdiction) that issued the certificate.
- **Component:** (Applies only if Subject or Issuer is selected.) Choose the distinguished name component that is used in the rule:
  - **Country (C):** The two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
  - **Common Name (CN):** The name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.
  - **DN Qualifier (DNQ):** A specific DN attribute.
  - **E-mail Address (EA):** The email address of the person, system or entity that owns the certificate.
  - **Generational Qualifier (GENQ):** A generational qualifier such as Jr., Sr., or III.
  - **Given Name (GN):** The first name of the certificate owner.
  - **Initials (I):** The first letters of each part of the name of the certificate owner.
  - **Locality (L):** The city or town where the organization is located.
  - **Name (N):** The name of the certificate owner.
  - **Organization (O):** The name of the company, institution, agency, association, or other entity.
  - **Organizational Unit (OU):** The subgroup within the organization.
  - **Serial Number (SER):** The serial number of the certificate.
  - **Surname (SN):** The family name or last name of the certificate owner.
  - **State/Province (S/P):** The state or province where the organization is located.
  - **Title (T):** The title of the certificate owner, such as Dr.
  - **User ID (UID):** The identification number of the certificate owner.
  - **Unstructured Name (UNAME):** The unstructured Name attribute type specifies the name or names of a subject as an unstructured ASCII string.
  - **IP Address (IP):** IP address field.
- **Operator:** Choose the operator that is used in the rule:
  - **Equals:** The distinguished name field must exactly match the value.
  - **Contains:** The distinguished name field must include the value within it.
  - **Does Not Equal:** The distinguished name field must not match the value.
  - **Does Not Contain:** The distinguished name field must not include the value within it.
  - **Value:** Enter up to 255 characters to specify the object of the operator.

In the example, if the subject OU field of a certificate contains the “Engineering” string, a user with that certificate will be mapped to the ENGINEERING-PROFILE connection profile.

Step 3 Click **Apply** to apply the configuration.

### Configure Certificate-Based Client Authentication Using External CAs

#### CLI Configuration

```
crypto ca certificate map DefaultCertificateMap 10
subject-name attr ou eq Engineering
}
webvpn
svc profiles SCEP-ENROLL disk0:/SCEP-ENROLL.XML
svc profiles CERT-SELECTION disk0:/CERT-SELECTION.XML
certificate-group-map DefaultCertificateMap 10 ENGINEERING-PROFILE
}
group-policy ENROLLMENT-POLICY internal
group-policy ENROLLMENT-POLICY attributes
webvpn
svc profiles value SCEP-ENROLL
}
tunnel-group ENROLLMENT-PROFILE type remote-access
tunnel-group ENROLLMENT-PROFILE general-attributes
default-group-policy ENROLLMENT-POLICY
tunnel-group ENROLLMENT-PROFILE webvpn-attributes
group-alias Certificate-enrollment enable
}
tunnel-group ENGINEERING-PROFILE type remote-access
tunnel-group ENGINEERING-PROFILE webvpn-attributes
authentication certificate
}
group-policy DfltGrpPolicy attributes
webvpn
svc profiles value CERT-SELECTION
```

Configure certificate map and criteria.

Specify XML profile files.

Apply certificate map to connection profile.

Create a dedicated group policy and specify XML profile.

Create a dedicated connection profile.

Enable authentication using certificates in a connection profile.

© 2010 Cisco Systems, Inc. All rights reserved. [www.cisco.com](http://www.cisco.com)

Use the following commands to configure certificate-based client authentication using external CAs. To create a certificate to connection profile map use the **crypto ca certificate map** command, followed by a name and rule priority number. Then use the **subject-name attr** command to specify which attribute in a subject name should contain which value. Finally, configure mapping between a connection profile and connection profile map using the **certificate-group-map** command in webvpn configuration mode.

To add XML profiles to the Cisco ASA security appliance, use the **svc profiles** command in webvpn configuration mode.

To create an internal group policy, use the **group-policy** command, followed by a group policy name and **internal** keyword. Then specify that the XML profile should be used inside that group policy by entering group-policy webvpn mode and using the **svc profiles values** command.

Then create a connection profile (tunnel group) using the **tunnel-group** command and specify the default group using the **default-group-policy** command. In addition, specify the alias of the tunnel group using the **group alias** command. In the example, the ENROLLMENT-PROFILE connection profile has been configured and uses the ENROLLMENT-POLICY as its default group policy. The ENROLLMENT-PROFILE connection profile will use the default AAA authentication.

Then configure another tunnel group that will use certificates-based authentication. In the example, the ENGINEERING-PROFILE tunnel group has been created and configured to use certificates for authentication.

Finally, enable an XML profile to enable the Cisco AnyConnect client to automatically select a certificate by assigning the CERT-SELECTION profile to the DfltGrpPolicy.

### svc profiles (webvpn)

To specify a file as a profiles package that the adaptive security appliance loads in cache memory and makes available to group policies and username attributes of Cisco AnyConnect VPN Client users, use the **svc profile** command from webvpn configuration mode.

To remove the command from the configuration and cause the adaptive security appliance to unload the package file from cache memory, use the **no** form of the command:

```
svc profiles {profile path}
```

### svc profiles (webvpn) Parameters

Parameter	Description
<i>path</i>	The path and filename of the profile file in flash memory of the adaptive security appliance
<i>profile</i>	The name of the profile to create in cache

### ssl certificate-authentication

To enable client certificate authentication for backwards compatibility for versions previous to 8.2(1), use the **ssl certificate-authentication** command in global configuration mode. To disable SSL certificate authentication, use the **no** version of this command.

```
ssl certificate-authentication interface interface-name port port-number
```

### ssl certificate-authentication Parameters

Parameter	Description
<i>interface-name</i>	The name of the selected interface, such as inside, management, and outside
<i>port-number</i>	The TCP port number, an integer in the range 1–65,535

### group-policy

To create or edit a group policy, use the **group-policy** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

```
group-policy name {internal [from group-policy_name] | external server-group server_group password server_password}
```

### group-policy Parameters

Parameter	Description
<b>external server-group</b> <i>server_group</i>	Specifies the group policy as external and identifies the authentication, authorization, and accounting (AAA) server group for the adaptive security appliance to query for attributes.
<b>from</b> <i>group-policy_name</i>	Initializes the attributes of this internal group policy to the values of a preexisting group policy.
<b>internal</b>	Identifies the group policy as internal.
<i>name</i>	Specifies the name of the group policy. The name can be up to 64 characters long and cannot contain spaces.
<b>password</b> <i>server_password</i>	Provides the password to use when retrieving attributes from the external AAA server group. The password can be up to 128 characters long and cannot contain spaces.



## group-policy attributes

To enter the group-policy configuration mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, use the **no** version of this command. In group-policy configuration mode, you can configure attribute-value pairs for a specified group policy or enter group-policy webvpn configuration mode to configure WebVPN attributes for the group.

### group-policy *name* attributes

#### group-policy attributes Parameters

Parameter	Description
<i>name</i>	Specifies the name of the group policy.

## webvpn (group-policy and username modes)

To enter this webvpn mode, use the **webvpn** command in group-policy configuration mode or in username configuration mode. To remove all commands that are entered in webvpn mode, use the **no** form of this command. These **webvpn** commands apply to the username or group policy from which you configure them.

The **webvpn** commands for group policies and usernames define access to files, Messaging Application Programming Interface (MAPI) proxy, URLs, and TCP applications over Cisco WebVPN. They also identify ACLs and types of traffic to filter.

### webvpn

## svc profiles (group-policy or username attributes)

To specify a Cisco AnyConnect VPN Client profiles package that is to be downloaded to AnyConnect VPN Client users, use the **svc profile** command from group policy webvpn or username attributes webvpn configuration mode.

To remove the command from the configuration and cause the value it to be inherited, use the **no** form of the command:

**svc profiles** {*value profile* | *none*}

#### svc profiles (group-policy or username attributes) Parameters

Parameter	Description
<i>profile</i>	The name of the profile

## tunnel-group

To create and manage the database of connection-specific records for IPsec and WebVPN tunnels, use the **tunnel-group** command in global configuration mode. To remove a tunnel group, use the **no** form of this command.

### tunnel-group *name type type*

#### tunnel-group Parameters

Parameter	Description
<i>name</i>	Specifies the name of the tunnel group. This can be any string that you choose. If the name is an IP address, it is usually the IP address of the peer.

Parameter	Description
<b>type</b> <i>type</i>	<p>Specifies the type of tunnel group:</p> <ul style="list-style-type: none"> <li>■ <b>remote-access</b>: Allows a user to connect using either IPsec remote access or WebVPN (portal or tunnel client).</li> <li>■ <b>ipsec-l2l</b>: Specifies IPsec LAN-to-LAN, which allows two sites or LANs to connect securely across a public network like the Internet.</li> </ul>
<b>Note</b>	<p>The following tunnel-group types are deprecated in Release 8.0(2):</p> <ul style="list-style-type: none"> <li>– <b>ipsec-ra</b>: IPsec remote access</li> <li>– <b>webvpn</b>: WebVPN</li> </ul> <p>The adaptive security appliance converts these to the remote-access type.</p>

## tunnel-group general-attributes

To enter the general-attributes configuration mode, use the **tunnel-group general-attributes** command in global configuration mode. This mode is used to configure settings that are common to all supported tunneling protocols.

To remove all general attributes, use the **no** form of this command.

**tunnel-group** *name* **general-attributes**

### tunnel-group general-attributes Parameters

Parameter	Description
<b>general-attributes</b>	Specifies attributes for this tunnel-group
<i>name</i>	Specifies the name of the tunnel-group

## default-group-policy

To specify the set of attributes that the user inherits by default, use the **default-group-policy** command in tunnel-group general-attributes configuration mode. To eliminate a default group policy name, use the **no** form of this command.

**default-group-policy** *group-name*

### default-group-policy Parameters

Parameter	Description
<i>group-name</i>	Specifies the name of the default group

## tunnel-group webvpn-attributes

To enter webvpn-attributes configuration mode, use the **tunnel-group webvpn-attributes** command in global configuration mode. This mode configures settings that are common to WebVPN tunneling.

To remove all WebVPN attributes, use the **no** form of this command.

**tunnel-group** *name* **webvpn-attributes**

## tunnel-group webvpn-attributes Parameters

Parameter	Description
<code>webvpn-attributes</code>	Specifies WebVPN attributes for this tunnel-group
<code>name</code>	Specifies the name of the tunnel-group

## group-alias

To create one or more alternate names by which the user can refer to a tunnel group, use the **group-alias** command in tunnel-group webvpn configuration mode. To remove an alias from the list, use the **no** form of this command.

**group-alias** *name* [**enable** | **disable**]

## group-alias Parameters

Parameter	Description
<code>disable</code>	Disables the group alias.
<code>enable</code>	Enables a previously disabled group alias.
<code>name</code>	Specifies the name of a tunnel group alias. This can be any string that you choose, except that the string cannot contain spaces.

## authentication

To configure the authentication method for WebVPN, use the **authentication** command in various modes. To restore the default method, use the **no** form of this command. The adaptive security appliance authenticates users to verify their identity.

**authentication** {[**aaa**] [**certificate**]}

## authentication Parameters

Parameter	Description
<code>aaa</code>	Provides a username and password that the adaptive security appliance checks against a previously configured AAA server.
<code>certificate</code>	Provides a certificate during SSL negotiation.

## Verify Certificate-Based Client Authentication Using External CAs

### Verify Manual Certificate Selection



You can configure the Cisco AnyConnect client to automatically select proper certificate-based on matching rules in the XML profile as described previously. However, you can also disable automatic selection of certificate. In the latter case (and also if automatic selection is configured, but more than one certificate matches a rule), the Cisco AnyConnect client presents to a user a list of available certificates. The user has to select one from the list, before the AnyConnect client continues with establishing the SSL VPN connection.

You may need to enable the certificate store override feature when nonadministrator users want to access a certificate in the machine store. This feature is configured in the XML-based local policy file.

## Verify Certificate-Based Client Authentication Using External CAs

### Implementation Guidelines

Consider the following implementation guidelines:

- Use manual certificate selection when it is too complex or infeasible to create automatic selection rules.
- With SCEP, the CA must be configured to automatically issue the certificate.
- It is strongly recommended to use split tunneling and ACLs only to provide SCEP connectivity inside the enrollment connection profile.

When you implement certificate-based client authentication using external CAs, consider the following implementation guidelines:

- Use manual certificate selection when it is too complex or infeasible to create automatic selection rules.
- With SCEP, the CA must be configured to automatically issue the certificate.
- It is strongly recommended to use split tunneling and ACLs only to provide SCEP connectivity inside the enrollment connection profile.


# LDAP Password Management

This topic describes how to implement Microsoft Active Directory password management for VPN users.

## LDAP Password Management

### Overview

- VPN users authenticating with external LDAP can change expiring passwords.
- Supported methods:
  - Native LDAP (Microsoft and Sun iPlanet only)
  - RADIUS-to-Active Directory (proxying to Active Directory)
- Supported VPN types:
  - Cisco AnyConnect SSL VPN
  - Clientless SSL VPN
  - Cisco Easy VPN



© 2010 Cisco Systems, Inc. All rights reserved. IPN 17-10-10-02

When the security appliance is configured to authenticate the VPN users against an external LDAP database, you can extend the password management capabilities of the external Active Directory systems to the VPN users. The VPN users can be notified when their passwords are about to expire, and can change the password according to the Active Directory policy.

The VPN system on the security appliance supports these two methods of Active Directory-based password management:

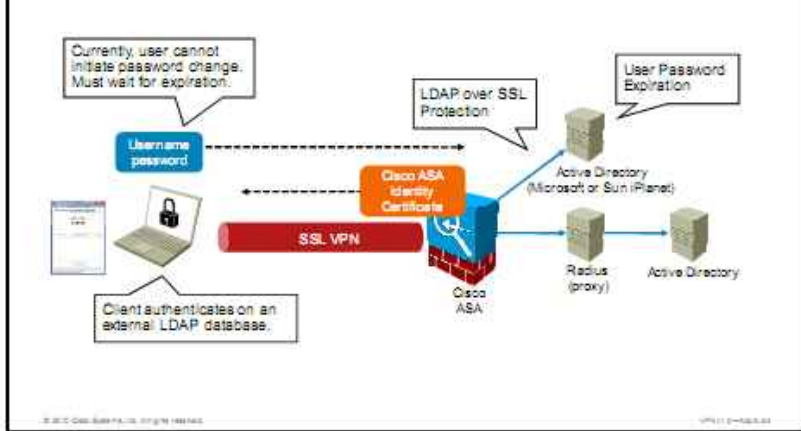
- **Native LDAP:** Only Microsoft and Sun iPlanet are supported for password management.
- **RADIUS-to-Active Directory:** In this option, the Radius server is configured as an authentication proxy to the external Active Directory.

Password management is supported for all remote access VPN types:

- Cisco AnyConnect SSL VPN
- Clientless SSL VPN
- Cisco Easy VPN

# LDAP Password Management

## Configuration Scenario



Password management and expiration can be configured in two network setups:

- The VPN server uses Secure LDAP to authenticate the VPN users against the Active Directory.
- The VPN server authenticates the VPN users against a RADIUS server, which acts as a proxy to the back-end Active Directory.

## LDAP Password Management

### Configuration Tasks

1. Enable the password management feature in connection profile settings.
2. On the Active Directory server, configure the user record to require a password change at next login.
  - Mandatory with RADIUS proxy
3. Set up secure LDAP communications (LDAPS).
4. Ensure that the login DN (used for the binding operation) has account operator privileges.
  - Superuser-level privileges not required

Complete these tasks to implement password management features on an external LDAP server:

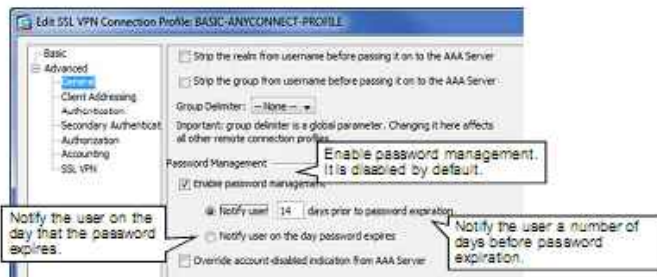
1. Enable the password management feature in connection profile settings.
2. On the Active Directory server, configure the user record to require a password change at next login. This setting is optional with native LDAP access and mandatory when using the RADIUS proxy.
3. Set up Secure LDAP communications. If you do not use native LDAP access, Secure LDAP must be configured between the RADIUS proxy and the LDAP server.
4. Ensure that the login DN (used for the binding operation) has account operator privileges. Superuser-level privileges are not required to enable the password management functionality.



## LDAP Password Management

### Task 1: Enable Password Management

- Other tasks covered earlier in the course or configured on LDAP server



Enable password management feature by completing these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** menu and edit the desired connection profile.

**Note** The password management feature is available in Cisco Easy VPNs and clientless SSL VPNs and can therefore be configured using the configuration paths **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles**, and **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

**Step 2** Choose the **General** submenu.

**Step 3** Check the **Enable Password Management** check box. Password management is disabled by default.

**Step 4** Optionally, configure how many days before password expiration the user should be notified. The default is 14 days.

**Step 5** Optionally, enable the notification on the day when the password expires.

**Note** The remaining configuration tasks are not covered here because they are either performed on the external LDAP server, or have been covered earlier in the lesson (setting up the LDAP server).

## LDAP Password Management

### CLI Configuration

```
tunnel-group BASIC-ANYCONNECT-PROFILE type remote-access
tunnel-group BASIC-ANYCONNECT-PROFILE general-attributes
 authentication-server-group MY-LDAP-SVR8
 password-management password-expire-in-days 14
```

Enable password management.

To enable LDAP password management using CLI, use the **password management** command in tunnel-group general-attributes configuration mode.

### password-management

To enable password management, use the **password-management** command in tunnel-group general-attributes configuration mode. To disable password management, use the **no** form of this command. To reset the number of days to the default value, use the **no** form of the command with the **password-expire-in-days** keyword specified.

**password-management** [**password-expire-in-days** *days*]

### password-management Parameters

Parameter	Description
<i>days</i>	Specifies the number of days (0 through 180) before the current password expires. This parameter is required if you specify the <b>password-expire-in-days</b> keyword.
<b>password-expire-in-days</b>	(Optional) Indicates that the immediately following parameter specifies the number of days before the current password expires that the adaptive security appliance starts warning the user about the pending expiration. This option is valid only for LDAP servers. See the Usage Notes section for more information.

## LDAP Password Management

### Implementation Guidelines

- Users must wait for password expiration and cannot initiate password change:
  - Workaround for Cisco AnyConnect users with Start Before Logon: Change password using the Start Before Logon Ctrl-Alt-Del mechanism.
- Password management not supported on the Active Directory Global Catalog Server (AD-GCS):
  - Password attributes not included in AD-GCS response.
- Password management works in Microsoft Windows 2008 domain only with secure LDAP (LDAPS).

Consider these guidelines when deploying LDAP-based password management:

- Client-initiated password change, without being triggered by the headend, is currently not supported. Users must wait for password expiration and then change the password.
  - There is a workaround for Cisco AnyConnect users with Start Before Logon. Change the password using the Start Before Logon Ctrl-Alt-Del mechanism.
- Password management that is not supported on the Active Directory Global Catalog Server (AD-GCS) because password attributes are not included in AD-GCS response.
- Password management works in Microsoft Windows 2008 domain only with Secure LDAP. Consult <http://support.microsoft.com/kb/321051> to find out how to enable LDAP over SSL with a third-party certification authority.



